JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

Subscriber-Aware and Application-Aware Traffic Treatment User Guide

Published
2021-04-18

JUNOS

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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

Junos® OS Subscriber-Aware and Application-Aware Traffic Treatment User Guide
Copyright © 2021 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide | xxiv

1 **Subscriber-Aware and Application-Aware Traffic Treatment Overview**

Subscriber-Aware and Application-Aware Traffic Treatment Overview | 2

Subscriber-Aware and Application-Aware Traffic Treatment Overview | **2**

Configuring Subscriber-Aware and Application-Aware Traffic Treatment Overview | **6**

2 **Applying Subscriber-Aware and Application-Aware Policies and Services**

Configuring the Service PIC, Session PIC, and TDF Gateway | 9

TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment | **9**

Configuring Service PICs and Session PICs Overview | **12**

Preconfigured Groups for Service PICs and for Session PICs Overview | **13**

Configuring a Services Interface for a Session PIC or Service PIC | **15**

Configuring a TDF Gateway | **16**

Making Predefined Groups Available for Session PIC and Service PIC Configuration | **17**

Configuring Service PICs | **18**

Configuring Session PICs | **19**

Configuring Tracing for TDF Gateway | **20**

Configuring Application Identification | 23

Application Identification Overview | **23**

Downloading and Installing Predefined Junos OS Application Signature Packages | **24**

Configuring Custom Application Signatures | **26**

Uninstalling a Predefined Junos OS Application Signature Package | **33**

Configuring HTTP Header Enrichment | 34

Junos Web Aware HTTP Header Enrichment Overview | **34**

HTTP Content Manager (HCM) | **35**

Configuring HTTP Header Enrichment Overview | **41**

Configuring Tag Rules | **42**

Configuring HCM Profiles and Assigning Tag Rules | **49**

Configuring Policy and Charging Enforcement | 51

Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | **52**

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | **56**

Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Dynamically by a PCRF | **58**

Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Statically | **63**

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | **64**

Understanding PCEF Profiles | **70**

Understanding Network Elements | **71**

Understanding AAA Profiles | **73**

Understanding Static Time-of-Day PCC Rule Activation and Deactivation | **74**

Understanding Usage Monitoring for TDF Subscribers | **74**

Configuring Dynamic Policy Control by PCRF | **76**

Configuring Static Policy Control | **77**

Configuring Policy Control by RADIUS Servers | **78**

Configuring Service Data Flow Filters | **79**

Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware | **83**

Configuring Policy and Charging Control Rules | **86**

Configuring a Policy and Charging Control Rulebase | **89**

Configuring RADIUS Servers | **91**

Configuring RADIUS Network Elements | **94**

Configuring an AAA Profile | **96**

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Dynamic Policies | **98**

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Static Policies | **100**

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Policies That a RADIUS Server Controls | **101**

Configuration of Static Time-of-Day PCC Rule Activation and Deactivation Overview | **102**

Configuring the NTP Server | **103**

Configuring Static Time-of-Day PCC Rule Activation and Deactivation in a Junos OS Subscriber Aware PCEF Profile | **103**

Configuring TDF Subscriber Usage Monitoring for Traffic That Matches Predefined PCC Rules | **105**

Configuring TDF Subscribers | 106

IP-Based and IFL-Based TDF Subscribers Overview | **107**

IP-Based Subscriber Setup Overview | **107**

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | **108**

Understanding Source IP Filtering with Address Pools in TDF Domains for IP-Based Subscribers | **110**

Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**

Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | **114**

Understanding IFL-Based Subscriber Setup | **115**

Understanding the Definition of a Set of IFL-Based Subscriber Properties with a TDF Domain | **116**

Configuring IP-Based TDF Subscriber Setup When MX Series Router Is a RADIUS Server | **117**

Configuring IP-Based TDF Subscriber Setup When Accounting Requests Are Snooped | **118**

Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers | **119**

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | **121**

- Configuring the TDF Domain Name and AAA Parameters | **121**
- Configuring Address Filtering | **124**
- Configuring Subscriber Services and Policies | **125**
- Configuring Access Interfaces | **125**

Configuring Session Controls | **126**

Configuring Default Policy | **126**

Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | **128**

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**

Configuring the Term Name | **130**

Configuring Match Conditions for the RADIUS Client | **131**

Configuring Match Conditions for Snoop Segments | **131**

Configuring Match Conditions for Predefined AVPs | **131**

Configuring Match Conditions for Custom AVP Attributes | **133**

Configuring the TDF Domain to Select | **135**

Configuring the PCEF Profile to Select | **135**

Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | **136**

Configuring IFL-Based TDF Subscriber Setup | **139**

Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | **140**

Configuring the TDF Domain Name and Type | **140**

Configuring IFL-Based Subscribers | **141**

Configuring Address Filtering | **142**

Configuring Subscriber Services and Policies | **142**

Configuring Session Controls | **142**

Configuring a TDF Logical Interface | **143**

Configuring TDF Interface to Access Interface Associations in VRFs | **144**

Configuring Services | 145

Overview of Applying Services to Subscribers | **145**

Applying Services to Subscriber-Aware Traffic with a Service Set | **146**

Configuring Diameter | 149

Diameter Profiles Overview | **149**

Juniper Networks Diameter AVPs for Subscriber Aware Policy Control | **150**

Configuring Diameter Overview | **152**

Configuring Diameter Profiles | **152**

Configuring Diameter Bindings | 154

Configuring Diameter Network Elements | 155

Configuring Diameter AVPs for Gx Applications | 156

Configuring Diameter Peers | 158

Configuring the Diameter Transport | 161

Configuring Advertisements in Diameter Messages | 162

Configuring Parameters for Diameter Applications | 162

Configuring the Origin Attributes of the Diameter Instance | 163

3 Configuring Reporting for Subscriber-Aware Data Sessions

Configuring Reporting | 166

Logging and Reporting Function for Subscribers | 166

Log Dictionary for Template Types | 174

Configuring Logging and Reporting for Junos OS Subscriber Aware | 186

Configuring an LRF Profile for Subscribers | 187

- Configuring the LRF Profile Name | 187
- Configuring Policy-Based Logging | 188
- (Optional) Configuring HTTP Transaction Logging | 188
- Configuring Collectors | 188
- Configuring Templates | 190
- Configuring Logging and Reporting Rules | 192

Assigning an LRF Profile to Subscribers | 194

Configuring the Activation of an LRF Rule by a PCC Rule | 196

4 Modifying Subscriber-Aware Configuration

Modifying Subscriber-Aware Configuration in Maintenance Mode | 200

Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200

Changing Address Attributes in the Address Pool | 202

Deleting an Address Pool | 203

Changing AMS Interface Parameters on a TDF Gateway | 205

Modifying a TDF Domain | **208**

Modifying the TDF Interface of a TDF Domain | **210**

Deleting a TDF Domain | **212**

Changing a TDF Interface | **214**

Deleting a TDF Interface | **216**

Changing TDF Gateway Parameters with Maintenance Mode | **218**

Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles | **220**

- Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles with the TDF Domain in Maintenance Mode | **221**
- Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles with the TDF Gateway in Maintenance Mode | **223**

Deleting a PCEF Profile | **225**

- Deleting a PCEF Profile with the TDF Domain in Maintenance Mode | **226**
- Deleting a PCEF Profile with the Gateway in Maintenance Mode | **228**

Changing Static Time-of-Day Settings for PCC Rules | **231**

Deleting a Services PIC | **232**

Deleting a Session PIC | **234**

5 **Monitoring and Troubleshooting**

Monitoring and Troubleshooting | 239

Configuring Tracing for PCEF Operations | **239**

Configuring Call-Rate Statistics Collection | **241**

Using the Enterprise-Specific Utility MIB | **242**

- Using the Enterprise-Specific Utility MIB | **242**
- Populating the Enterprise-Specific Utility MIB with Information | **243**
- Stopping the SLAX Script with the CLI | **251**
- Clearing the Utility MIB | **251**
- Recovering from an Abnormal SLAX Script Exit or a SLAX Script Exit with the CLI | **251**

6 **Configuration Statements and Operational Commands**

Configuration Statements | 253

3gpp-imsi | **262**

aaa clients (TDF) | **264**

aaa-policy-control (PCEF Profile) | **265**

aaa-profile (PCEF Profile) | **267**

access-interfaces (IFL Subscriber) | **268**

access-interfaces (IP Subscriber) | **270**

accounting (AAA Profile) | **271**

accounting (RADIUS Client) | **273**

accounting-port (RADIUS Server) | **274**

accounting-secret (RADIUS Server) | **275**

activation-attribute (AAA Profile) | **277**

address (Diameter Peer) | **278**

address (LRF Profile) | **279**

address (RADIUS Clients) | **281**

address (RADIUS Server) | **282**

address-mapping (Application Identification) | **283**

address-pools | **285**

allow-dynamic-requests (RADIUS Server) | **287**

alt-name (Application Identification) | **288**

application (Application Identification) | **289**

application-group | **292**

application-groups (PCC Rules) | **293**

application-identification (Application Identification) | **295**

application-identification-profile (Service Set) | **299**

applications (Services Application Identification) | **300**

applications (Diameter) | **301**

applications (PCC Rules) | **303**

attribute | **305**

attributes (Diameter Gx Profiles) | **308**

authentication (AAA Profile) | **309**

burst-size (Default Local Policy) | **311**

burst-size (TDF Domain) | **312**

cac (TDF Gateway) | **314**

cacheable (Application Identification) | **315**

call-rate-statistics | **316**

called-station-id | **318**

calling-station-id | **319**

chain-order (Application Identification) | **321**

check-bytes (Application Identification) | **322**

class | **323**

client | **325**

clients | **327**

coa-accounting (AAA Profile) | **328**

code | **330**

code (AAA Profile) | **331**

code (Application Identification) | **333**

collector (LRF Profile) | **334**

collector (LRF Rule) | **336**

compatibility (Application Identification) | **337**

connect-actively | **338**

constant | **341**

context (Application Identification) | **342**

count (HTTP Header Enrichment) | **344**

cpu (TDF Gateway) | **346**

deactivation-attribute (AAA Profile) | **347**

dead-criteria-retries (RADIUS Server) | **348**

default-local-policy | **350**

default-pool (Address Pools) | **351**

description (Application Identification) | **353**

destination (Application Identification) | **354**

destination (LRF Profile) | **355**

destination-address (HTTP Header Enrichment) | **357**

destination-address-range (HTTP Header Enrichment) | **359**

destination-ip-address (RADIUS Snoop Segment) | **360**

destination-port (RADIUS Snoop Segment) | **362**

destination-port-range (HTTP Header Enrichment) | **363**

destination-ports (HTTP Header Enrichment) | **365**

destination-prefix-list (HTTP Header Enrichment) | **366**

diameter (Subscriber Aware Policy Control) | **368**

diameter (TDF Gateway) | **370**

diameter-profile (PCEF Profile) | **372**

direction (Application Identification) | **373**

direction (Service Data Flow Filters) | **375**

disconnect-peer-timeout | **377**

domain (TDF Domain Selection) | **378**

domain-selection | **380**

domains | **384**

dynamic-policy-control | **387**

dynamic-requests-secret (RADIUS Server) | **389**

encrypt (HTTP Header Enrichment) | **390**

equals | **392**

exclude (Diameter Gx Profiles) | **394**

external-assigned (Address Pools) | **395**

family (Address Pools) | **397**

family (Exclude Prefix) | **398**

family (TDF Interface) | **400**

flow-action | **401**

flow-descriptions | **403**

flows (PCC Rules) | **405**

format (Unified Edge Gateways) | **407**

format (LRF Profile) | **409**

forwarding-class (PCC Action Profiles) | **410**

firmware-revision | **412**

framed-ip-address | **414**

framed-ipv6-prefix | **415**

from (HTTP Header Enrichment) | **417**

from (PCC Rules) | **418**

from (TDF Domain Selection) | **420**

function (Diameter Network Element) | **424**

gate-status | **425**

greater-than | **427**

gx-profile | **429**

has-prefix (Unified Edge Gateways) | **431**

has-suffix | **432**

hcm (HTTP Header Enrichment) | **434**

hcm-profile (HTTP Header Enrichment) | **436**

hcm-profile (PCC Action Profiles) | **438**

host (Diameter Origin) | **439**

http-log-multiple-transactions (LRF Profile) | **441**

icmp-mapping (Application Identification) | **442**

id-components | **443**

idle-timeout | **446**

ifl-subscriber | **447**

immediate-accounting-response | **449**

include (Diameter Gx Profiles) | **450**

incoming-queue | **452**

inet (TDF Subscriber Address) | **453**

inet (TDF Subscriber Exclude Prefix) | **455**

inet6 (TDF Subscriber Address) | **456**

inet6 (TDF Subscriber Exclude Prefix) | **457**

integer | **459**

interface (Services PIC) | **460**

interface (Session PICs) | **462**

interface-service (Services Interfaces) | **464**

ip-protocol-mapping (Application Identification) | **465**

ip-subscriber | **467**

ipv4-address (Steering Path) | **469**

ipv4-mask (HTTP Header Enrichment) | **471**

ipv4-or-value (HTTP Header Enrichment) | **472**

ipv6-address (Steering Path) | **474**

ipv6-mask (HTTP Header Enrichment) | **475**

ipv6-or-value (HTTP Header Enrichment) | **477**

keep-existing-steering | **478**

less-than | **480**

local-port-range | **481**

local-ports | **483**

logging-rule (PCC Action Profile) | **485**

lrf-profile (Service Set) | **487**

matches | **489**

maximum-bit-rate (Default Local Policy) | **492**

maximum-bit-rate (PCC Action Profiles) | **493**

maximum-bit-rate (TDF Domain) | **495**

maximum-pending-reqs-limit | **497**

maximum-pending-requests (Diameter) | **498**

maximum-sessions (TDF Gateway) | **500**

maximum-subscribers | **501**

maximum-sessions-trap-percentage (TDF Gateway) | **502**

member (Application Identification) | **504**

memory (TDF Gateway) | **505**

mif (TDF Interface) | **507**

monitoring-key (PCC Action Profile) | **508**

mtu (TDF Interface) | **509**

nas-ip-address | **511**

nat-rule-sets (Service Set) | **512**

nat-rules | **514**

network-element (AAA Profile) | **515**

network-element (Diameter Base Protocol) | **516**

network-element (Subscriber Aware Policy Control) | **518**

network-elements (RADIUS) | **520**

network (Address Pools) | **521**

network (TDF Domain) | **523**

no-application-system-cache | **525**

no-send-to-ue | **526**

order (Application Identification) | **527**

order-priority (Application Identification) | **529**

origin (Diameter Base Protocol) | **531**

outgoing-queue | **532**

over (Application Identification) | **534**

packet-capture (Next Gen Services) | **536**

path (Steering) | **539**

pattern (Application Identification) | **540**

pattern (Class Attribute) | **542**

pcc-action-profile (PCC Rules) | **543**

pcc-action-profiles | **545**

pcc-rule | **548**

pcc-rulebases (PCEF) | **550**

pcc-rulebases (PCEF Profile) | **551**

pcc-rules (PCEF) | **554**

pcc-rules (PCEF Profile) | **556**

pcc-time-of-day-profiles | **558**

pcef | **560**

pcef-profile (Service Set) | **563**

pcef-profile (TDF Domain) | **564**

pcef-profile (TDF Domain Selection) | **566**

peer (Diameter Base Protocol) | **568**

peer (Diameter Network Element) | **569**

pending-queue-watermark | **571**

pending-queue-watermark-abate | **572**

policy-based-logging (LRF Profile) | **574**

pool (TDF Domain) | **575**

port (LRF Profile) | **577**

port (RADIUS Server) | **578**

port-range (Application Identification) | **579**

prefer-framed-ip-address (RADIUS Clients) | **581**

prefer-framed-ipv6-prefix (RADIUS Clients) | **582**

priority (Diameter Network Element) | **583**

priority (RADIUS Network Elements) | **585**

product-name | **586**

profile | **587**

profile (HTTP Header Enrichment) | **589**

profile (LRF) | **590**

profile (Services Application Identification) | **593**

profile (Services PCEF) | **594**

profiles (AAA) | **595**

profiles (PCEF) | **597**

protocol (Application Identification) | **600**

protocol (Flow Descriptions) | **602**

realm (Diameter Origin) | **604**

redirect (PCC Action Profiles) | **605**

regex (Class Attribute) | **607**

remote-address | **608**

remote-port-range | **610**

remote-ports | **612**

report (LRF Rule) | **614**

request-cache-timeout (RADIUS Snoop Segment) | **616**

request-timeout | **617**

response-cache-timeout (RADIUS Client) | **618**

retry (RADIUS Server) | **620**

revert-interval (RADIUS Server) | **621**

routing-instance (PCC Action Profiles) | **623**

rule (HTTP Header Enrichment for Tag Rule Set) | **625**

rule (LRF) | **626**

rule-activation-time | **628**

rule-deactivation-time | **630**

secret (RADIUS Client) | **632**

secret (RADIUS Server) | **633**

server (RADIUS Network Elements) | **634**

servers (RADIUS) | **636**

service-mode | **638**

service-pics | **640**

service-set (Subscriber-Aware) | **641**

service-set (TDF Interface) | **643**

session-pics | **644**

session-pics (Diameter) | **645**

shared-secret (RADIUS Snoop Segment) | **647**

snoop-segment (TDF Domain Selection) | **649**

snoop-segments (RADIUS) | **650**

snoop-segments (TDF Gateway) | **652**

source (Application Identification) | **653**

source-address (LRF Profile) | **655**

source-interface | **656**

source-interface (RADIUS Server) | **657**

source-interface (RADIUS Snoop Segment) | **659**

source-ip-address (RADIUS Snoop Segment) | **660**

static-policy-control | **661**

steering | **663**

string | **665**

subscriber-address | **667**

subscriber-awareness (Service Set Options) | **668**

subscriber-aware-services | **669**

subscriber-exclude-prefix | **670**

subscriber-type (TDF Domain) | **672**

subscription-id | **674**

subscription-id-options | **675**

subscription-id-type (Class Attribute) | **677**

tag (HTTP Header Enrichment) | **679**

tag-attribute (HTTP Header Enrichment) | **680**

tag-attribute (HTTP Header Enrichment Tag Rule) | **682**

tag-header (HTTP Header Enrichment) | **683**

tag-operation (HTTP Header Enrichment) | **685**

tag-rule (Profiles for HTTP Header Enrichment) | **686**

tag-rule (HTTP Header Enrichment) | **688**

tag-rules (Service Set) | **690**

tag-rule-set (HTTP Header Enrichment) | **692**

tag-rule-sets (Service Set) | **693**

tag-separator (HTTP Header Enrichment) | **695**

tag-value (HTTP Header Enrichment) | **696**

tags (Application Identification) | **697**

targets | **699**

tdf (Unified Edge) | **701**

tdf-interface | **702**

template (LRF Profile) | **704**

template (LRF Rule) | **705**

template-tx-interval (LRF Profile) | **707**

template-type (LRF Profile) | **708**

term (HTTP Header Enrichment) | **711**

term (TDF Domain Selection) | **713**

then (HTTP Header Enrichment) | **717**

then (LRF rule) | **719**

then (PCC Rules) | **720**

then (TDF Domain Selection) | **722**

time | **724**

time-limit (LRF Rule) | **725**

timeout (Diameter Network Element) | **727**

timeout (RADIUS Server) | **728**

traceoptions (Diameter Base Protocol) | **730**

traceoptions (PCEF) | **732**

traceoptions (TDF Gateway) | **735**

trigger-type (LRF Profile) | **738**

type (Application Identification) | **740**

type (ICMP Mapping for Application Identification) | **741**

unit (TDF Interface) | **743**

url | **744**

use-class (Class Attribute) | **746**

user-name | **747**

user-password (PCEF Profile) | **749**

v4address | **750**

v6address | **752**

v6prefix | **753**

vendor-id | **755**

vendor-id (AAA Profile) | **756**

vendor-support | **758**

volume-limit (LRF Rule) | **759**

watchdog-timeout | **760**

Operational Commands | 763

clear services application-identification application-system-cache | **765**

clear services application-identification statistics | **767**

clear services lrf collector statistics | **769**

clear services lrf statistics | **771**

clear services sessions | **772**

clear unified-edge tdf aaa radius client statistics | **777**

clear unified-edge tdf aaa radius network-element statistics | **779**

clear unified-edge tdf aaa radius server statistics | **781**

clear unified-edge tdf aaa radius snoop-segment statistics | **782**

clear unified-edge tdf aaa statistics | **784**

clear unified-edge tdf address-assignment pool | **786**

clear unified-edge tdf address-assignment statistics | **788**

clear unified-edge tdf call-admission-control statistics | **790**

clear unified-edge tdf diameter network-element statistics | **791**

clear unified-edge tdf diameter pcc-gx statistics | **793**

clear unified-edge tdf diameter peer statistics | **795**

clear unified-edge tdf statistics | **797**

clear unified-edge tdf subscribers | **798**

clear unified-edge tdf subscribers peer | **800**

request interface load-balancing revert (Aggregated Multiservices) | **802**

request interface load-balancing switchover (Aggregated Multiservices) | **804**

request services application-identification application | **806**

request services application-identification download | **808**

request services application-identification download status | **809**

request services application-identification group | **811**

request services application-identification install | **813**

request services application-identification install status | **814**

request services application-identification proto-bundle-status | **816**

request services application-identification uninstall | **817**

request services application-identification uninstall status | **819**

request unified-edge tdf call-trace clear | **820**

request unified-edge tdf call-trace show | **822**

request unified-edge tdf call-trace start | **826**

request unified-edge tdf call-trace stop | 829

show interfaces anchor-group (Aggregated Packet Forwarding Engine) | 831

show interfaces load-balancing (Aggregated Multiservices) | 836

show services application-identification application | 841

show services application-identification application-system-cache | 850

show services application-identification counter | 856

show services application-identification group | 860

show services application-identification statistics application-groups | 865

show services application-identification statistics applications | 868

show services application-identification status | 870

show services application-identification version | 873

show services ha detail | 874

show services ha statistics | 877

show services hcm statistics | 885

show services hcm pic-statistics | 888

show services lrf collector statistics | 896

show services lrf rule statistics | 898

show services lrf statistics | 901

show services lrf template | 903

show services traffic-detection-function hcm statistics | 906

show services traffic-detection-function sessions | 911

show unified-edge tdf aaa radius client statistics | 915

show unified-edge tdf aaa radius client status | 923

show unified-edge tdf aaa radius network-element statistics | 925

show unified-edge tdf aaa radius server statistics | 930

show unified-edge tdf aaa radius server status | 936

show unified-edge tdf aaa radius snoop-segment statistics | **940**

show unified-edge tdf aaa statistics | **945**

show unified-edge tdf address-assignment pool | **958**

show unified-edge tdf address-assignment service-mode | **964**

show unified-edge tdf address-assignment statistics | **967**

show unified-edge tdf call-admission-control statistics | **970**

show unified-edge tdf call-rate statistics | **974**

show unified-edge tdf diameter network-element statistics | **978**

show unified-edge tdf diameter network-element status | **981**

show unified-edge tdf diameter pcc-gx statistics | **984**

show unified-edge tdf diameter peer statistics | **992**

show unified-edge tdf diameter peer status | **999**

show unified-edge tdf domain service-mode | **1004**

show unified-edge tdf domain statistics | **1007**

show unified-edge tdf resource-manager clients | **1014**

show unified-edge tdf service-mode | **1017**

show unified-edge tdf statistics | **1020**

show unified-edge tdf status | **1032**

show unified-edge tdf subscribers | **1038**

show unified-edge tdf system interfaces | **1059**

show unified-edge tdf system interfaces service-mode | **1061**

About This Guide

Use this guide to configure and monitor subscriber-aware and application-aware traffic policies. This lets you identify the mobile or fixed-line subscriber associated with a data session, and enforce traffic treatment for the subscriber based on Layer 7 or Layer 3/Layer 4 application information for the session.

1

PART

Subscriber-Aware and Application-Aware Traffic Treatment Overview

CHAPTER 1

Subscriber-Aware and Application-Aware Traffic Treatment Overview

IN THIS CHAPTER

- Subscriber-Aware and Application-Aware Traffic Treatment Overview | 2
- Configuring Subscriber-Aware and Application-Aware Traffic Treatment Overview | 6

Subscriber-Aware and Application-Aware Traffic Treatment Overview

IN THIS SECTION

- Introduction | 2
- Access-Independent Subscriber Traffic Treatment | 3
- Subscriber Identification Methods | 4
- Application Identification | 4
- Policy Control Methods | 5
- Subscriber-Aware Data Session Logging and Reporting | 5
- Usage Monitoring | 5

This topic contains an overview of subscriber-aware and application-aware traffic treatment.

Introduction

Junos Subscriber Aware identifies the mobile or fixed-line subscriber associated with a data session, and enforces traffic treatment based on policies assigned to the subscriber. This permits highly customizable differentiated services for subscribers. A subscriber policy can be based on Layer 7 application information for the IP flow (for example, YouTube) or can be based on Layer 3/Layer 4 information for

the IP flow (for example, the source and destination IP address). Junos Subscriber Aware resides on an MX Series router.

Subscriber-aware policies can specify the following actions:

- Redirecting HTTP traffic to another URL or IP address
- Forwarding packets to a routing instance so that packets are directed to external service chains (predefined sequence of services)
- Setting the forwarding class
- Setting the maximum bit rate
- Performing HTTP header enrichment (provided by Junos Web Aware, which resides on the same MX Series router as Junos Subscriber Aware)
- Setting the gating status to blocked or allowed

Subscriber-aware policies can also specify the time of day that the policies are in effect.

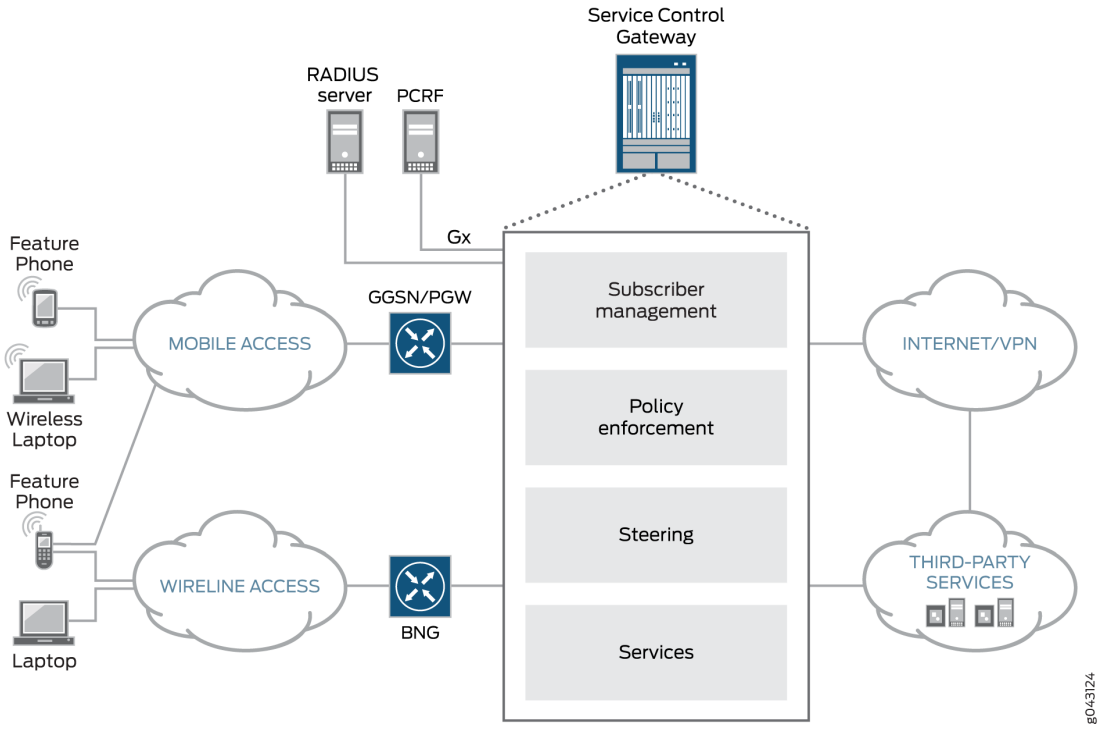
Access-Independent Subscriber Traffic Treatment

Subscriber identification for both mobile access and wireline access provides a unified experience for the subscriber, regardless of the connection method.

Junos Subscriber Aware resides on an MX Series router that is located between the gateway of the access network and the public network and network services, as shown in Figure 1 on page 4. Subscribers may be controlled by a broadband network gateway (BNG) in a wireline access network, by

a gateway GPRS support node (GGSN) in a 2G or 3G network architecture, or by a Packet Data Network Gateway (PGW) in a 4G/LTE network architecture.

Figure 1: Subscriber-Aware Policy Enforcement on the MX Series



Subscriber Identification Methods

You can use the following methods to identify subscribers:

- IP-based—Processes a RADIUS accounting start request to identify the subscriber. An IP-based subscriber session is for one unique user IP address.
- IFL-based—Requires you to configure a subscriber name and specify a set of MX Series router access interfaces for the subscriber. Junos Subscriber Aware assigns all data sessions received on those interfaces to the configured subscriber.

Application Identification

Layer 7 application identification is provided by Junos Application Aware, which performs deep packet inspection (DPI) to determine whether the subscriber's data packets match an application signature. When an application is identified, the appropriate subscriber policy is applied to the packets. Juniper

Networks provides a set of predefined application signatures that you can download and that are periodically updated. You can also configure your own custom application signatures.

Junos Subscriber Aware and Junos Application Aware reside on the same MX Series router, allowing policy control on a single platform.

Policy Control Methods

Subscriber-aware policies can be controlled dynamically by a policy and charging rules function (PCRF) server, can be activated by a RADIUS server, or can be under static control.

Under dynamic control, a PCRF either sends policies to the MX Series router or activates predefined policies that you configured on the MX Series router. Dynamic policy control is provided by Junos Policy Control, which resides on the same MX Series router as Junos Subscriber Aware.

Under RADIUS server control, the RADIUS server controls the activation of your predefined polices but does not send policies to the MX Series router.

Under static control, your predefined policies are not controlled by a PCRF or RADIUS server.

Subscriber-Aware Data Session Logging and Reporting

Junos Subscriber Aware can log data for subscriber-aware data sessions and send that data in an IPFIX format to an external log collector. These logs can include subscriber information, application information, HTTP metadata, data volume, time-of-day information, and source and destination details. You can then use the external collector, which is not a Juniper Networks product, to perform analytics that provide you with insights about subscriber and application usage, enabling you to create packages and policies that increase revenue.

Usage Monitoring

For subscriber data sessions that are under the dynamic policy control of a PCRF, Junos Subscriber Aware can monitor the volume of traffic or amount of time the subscriber uses during a session, and send reports to the PCRF. The PCRF can use this information to adjust the policies for a subscriber.

RELATED DOCUMENTATION

Configuring Subscriber-Aware and Application-Aware Traffic Treatment Overview | 6

Configuring Subscriber-Aware and Application-Aware Traffic Treatment Overview

To configure subscriber-aware and application-aware traffic treatment:

1. Configure service PICs and session PICs.

   See "Configuring Service PICs and Session PICs Overview " on page 12.

2. (Optional) Identify Layer 7 applications.

   a. Install application signature packages.

      See "Downloading and Installing Predefined Junos OS Application Signature Packages" on page 24.

   b. Configure custom application signatures.

      See "Configuring Custom Application Signatures" on page 26.

3. (Optional) Configure HTTP header enrichment.

   See "Configuring HTTP Header Enrichment Overview" on page 41.

4. Configure a policy enforcement method.

   - For dynamic policy control, see "Configuring Dynamic Policy Control by PCRF" on page 76.
   - For static policy control, see "Configuring Static Policy Control" on page 77.
   - For RADIUS server policy control, see "Configuring Policy Control by RADIUS Servers" on page 78.

5. Configure the policy enforcement for an IP-based subscriber. An IP-based subscriber session handles traffic for one unique user IP address.

   - If the MX Series router is identified as a RADIUS server for the access gateway, see "Configuring IP-Based TDF Subscriber Setup When MX Series Router Is a RADIUS Server" on page 117
   - If the MX Series router is not identifed as a RADIUS server for the access gateway, see "Configuring IP-Based TDF Subscriber Setup When Accounting Requests Are Snooped" on page 118

6. Configure the policy enforcement for an IFL-based subscriber. An IFL-based subscriber session handles all the traffic received on a specific set of interfaces.

   See "Configuring IFL-Based TDF Subscriber Setup" on page 139.

7. Apply services to a subscriber.

   See "Applying Services to Subscriber-Aware Traffic with a Service Set" on page 146.

8. (Optional) If you configured dynamic policy control, configure Diameter.

   See "Configuring Diameter Overview" on page 152.

RELATED DOCUMENTATION

Subscriber-Aware and Application-Aware Traffic Treatment Overview | 2

PART 2

Applying Subscriber-Aware and Application-Aware Policies and Services

Configuring the Service PIC, Session PIC, and TDF Gateway | 9

Configuring Application Identification | 23

Configuring HTTP Header Enrichment | 34

Configuring Policy and Charging Enforcement | 51

Configuring TDF Subscribers | 106

Configuring Services | 145

Configuring Diameter | 149

CHAPTER 2

Configuring the Service PIC, Session PIC, and TDF Gateway

IN THIS CHAPTER

- TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment | 9
- Configuring Service PICs and Session PICs Overview | 12
- Preconfigured Groups for Service PICs and for Session PICs Overview | 13
- Configuring a Services Interface for a Session PIC or Service PIC | 15
- Configuring a TDF Gateway | 16
- Making Predefined Groups Available for Session PIC and Service PIC Configuration | 17
- Configuring Service PICs | 18
- Configuring Session PICs | 19
- Configuring Tracing for TDF Gateway | 20

TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment

IN THIS SECTION

- TDF Gateway | 10
- Service and Session PICs | 10
- Redundancy for Service PICs and Session PICs | 11

You must configure at least one TDF gateway, one service PIC, and one session PIC to operate subscriber-aware traffic treatment. Each service PIC and session PIC is configured on an MS-MPC, and assigned to a TDF gateway.

TDF Gateway

The traffic detection function (TDF) gateway on the MX Series router establishes a context and framework for configuring subscriber-aware services. You assign service PICs and session PICs to the TDF gateway, and specify the call admission control (CAC) parameters for subscriber sessions.

Service and Session PICs

A service PIC provides subscriber-aware policy enforcement and traffic redirection (*steering*) that is application-aware. Traffic steering refers to the capability to direct or traverse traffic from a specified source to an endpoint or the adjacent network element in a routing path. The service PIC is configured with software plugins to perform the configured or requested services, which include the policy and charging enforcement function (PCEF), application detection and control, HTTP header enrichment, HTTP redirect, and network address translation.

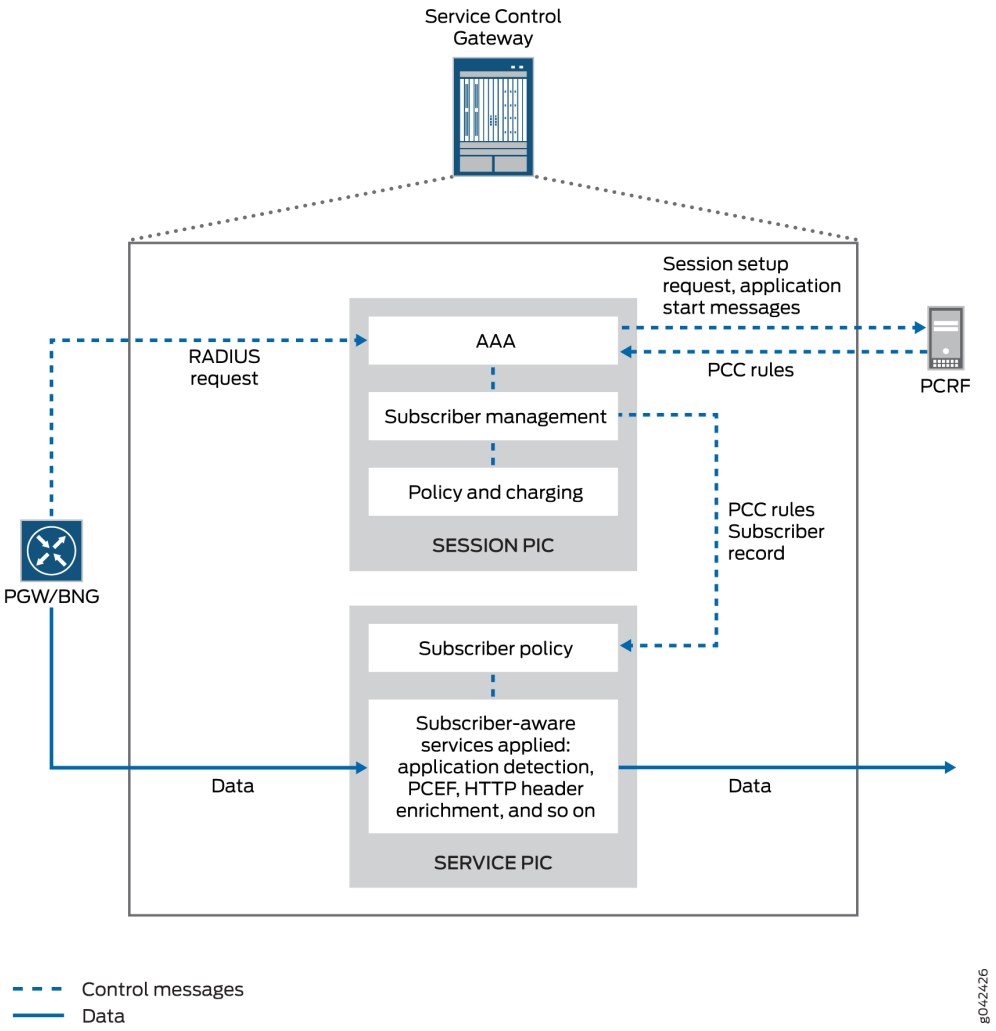
The service PIC also stores the policy and charging control (PCC) rules that it enforces, and holds the subscriber records and rules that are sent from the session PIC.

The subscriber's assigned TDF logical interface (mif) and the service set that is applied to the mif determine the service PIC to which a packet is sent. See "IP-Based Subscriber Setup Overview" on page 107.

A session PIC supports access subscriber session setup and management, enabling the steering of subscriber traffic to the correct services PIC. The session PIC also sets up a session with the policy and charging rules function (PCRF) so it can receive subscriber PCC rules from the PCRF and send application-start messages to the PCRF.

Figure 2 on page 11 shows an overview of a service PIC and a session PIC and their functions.

Figure 2: Service PIC and Session PIC Overview



Redundancy for Service PICs and Session PICs

You can configure a service PIC or a session PIC as an individual PIC or with a backup for redundancy. You can configure redundancy by including the interfaces for the primary and the backup PICs in an aggregated multiservices (AMS) interface .

You can configure a session PIC with 1:1 redundancy — a primary session PIC has one backup PIC that does not back up any other session PICs.

You can configure service PICs with N:1 redundancy — multiple service PICs can share the same backup MS-PIC.

In addition to the redundancy configuration, each PIC that is a primary or backup needs to be configured as a session PIC or service PIC at the **[edit unified-edge gateways tdf *gateway-name* system]** hierarchy level.

RELATED DOCUMENTATION

- Configuring a TDF Gateway | **16**
- Configuring Session PICs | **19**
- Configuring Service PICs | **18**
- *Configuring Aggregated Multiservices Interfaces*

Configuring Service PICs and Session PICs Overview

You must configure at least one service PIC and one session PIC under a TDF gateway. The service PIC provides subscriber-aware services, such as the policy and charging enforcement function (PCEF), application detection and control, and HTTP header enrichment. The session PIC supports access subscriber sessions, policy and charging rules function (PCRF) sessions, and PCEF library installation from the PCRF.

You can configure service PICs and session PICs on MS-MPCs, and you can configure them either as a member of a redundant group by using an aggregated multiservices (AMS) interface or as a standalone service PIC or session PIC.

To configure service and session PICs:

1. Configure the TDF gateway.

   See "Configuring a TDF Gateway" on page 16.
2. If you want any of the service or session PICs to be members of redundant groups, configure an aggregated multiservices (AMS) interface for each group.

   See *Configuring Aggregated Multiservices Interfaces*.
3. If you want any of the service or session PICs not to be members of redundant groups, configure a services interface.

   See "Configuring a Services Interface for a Session PIC or Service PIC" on page 15.
4. Install predefined groups that are needed for configuration of the service PICs and session PICs.

   See "Making Predefined Groups Available for Session PIC and Service PIC Configuration" on page 17.

5. Configure each service PIC.

   See "Configuring Service PICs" on page 18.

6. Configure each session PIC.

   See "Configuring Session PICs" on page 19.

RELATED DOCUMENTATION

TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment | 9

Preconfigured Groups for Service PICs and for Session PICs Overview | 13

Preconfigured Groups for Service PICs and for Session PICs Overview

To simplify configuration, Junos Subscriber Aware software includes predefined configuration groups that include the parameters for stable operation of session PICs and service PICs. These groups are included in the **/etc/config/tdf-defaults.conf** file, which you load and then merge with your configuration. Next, you apply the appropriate group to each session PIC and service PIC configuration as follows:

- For each session PIC, apply the **tdf-session-xlp** group.
- For each service PIC that requires application identification but not HTTP header enrichment, apply the **tdf-services-xlp-dpi** group.
- For each service PIC that requires both application identification and HTTP header enrichment, configure the **tdf-services-xlp-dpi-with-hcm** group.

The predefined **tdf-session-xlp** group contains the following statements:

```
[edit groups]
tdf-session-xlp {
    chassis {
        fpc <*> {
            pic <*> {
                adaptive-services {
                    service-package {
                        extension-provider {
                            boot-os embedded-junos64;
                            package jservices-mobile;
                        }
```

```
                    }
                }
            }
        }
    }
}
```

The predefined **tdf-services-xlp-dpi** group contains the following statements:

```
[edit groups]
tdf-services-xlp-dpi {
    chassis {
        fpc <*> {
            pic <*> {
                adaptive-services {
                    service-package {
                        extension-provider {
                            boot-os embedded-junos64;
                            package jservices-mss;
                            package jservices-jdpi;
                            package jservices-pcef;
                        }
                    }
                }
            }
        }
    }
}
```

The predefined **tdf-services-xlp-dpi-with-hcm** group contains the following statements:

```
[edit groups]
tdf-services-xlp-dpi-with-hcm {
    chassis {
        fpc <*> {
            pic <*> {
                adaptive-services {
                    service-package {
                        extension-provider {
                            boot-os embedded-junos64;
                            package jservices-mss;
```

```
                            package jservices-jdpi;
                            package jservices-pcef;
                            package jservices-hcm;
                            package jservices-crypto-base;
                        }
                    }
                }
            }
        }
    }
}
```

RELATED DOCUMENTATION

- Making Predefined Groups Available for Session PIC and Service PIC Configuration | 17
- Configuring Session PICs | 19
- Configuring Service PICs | 18

Configuring a Services Interface for a Session PIC or Service PIC

If a service PIC or a session PIC is not part of a redundant group (the service interface is not part of an aggregated multiservices interface), you must configure a services interface on the MS-MPC for the service PIC.

- Configure the services interface.

```
[edit]
user@host# set interfaces ms-fpc/pic/0 unit logical-unit-number family family address address
```

RELATED DOCUMENTATION

- *Configuring Aggregated Multiservices Interfaces*
- Configuring Service PICs | 18
- Configuring Session PICs | 19
- TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment | 9

Configuring a TDF Gateway

To run Junos Subscriber Aware, you must configure a traffic detection function (TDF) gateway on the MX Series router. The TDF gateway establishes a context and framework for configuring subscriber-aware services for subscriber data that is accessing the network through the MX Series router. You also specify the call admission control (CAC) parameters for the TDF gateway.

To configure the TDF gateway:

1. Configure a name for the TDF gateway.

```
[edit unified-edge gateways]
user@host# set tdf gateway-name
```

2. Configure the threshold for the maximum amount of CPU that the TDF gateway can use as a percentage from 1 through 90.

```
[edit unified-edge gateways tdf gateway-name]
user@host# set cac cpu cpu-pct
```

   If the amount of CPU that the TDF gateway uses reaches the threshold, the SNMP trap **jnxScgSMCPUThreshHigh** is generated.

3. Configure the maximum number of TDF subscriber sessions that can be running, expressed in thousands of sessions.

```
[edit unified-edge gateways tdf gateway-name]
user@host# set cac maximum-sessions max-sessions
```

   You can configure from 10 through 5000 sessions.

4. Configure the trap threshold for the number of TDF subscriber sessions as a percentage of the maximum number of sessions.

```
[edit unified-edge gateways tdf gateway-name]
user@host# set cac maximum-sessions-trap-percentage max-sessions-pct
```

   If the number of subscriber sessions reaches the threshold, the SNMP trap **jnxScgSMSessionThreshHigh** is generated.

5. Configure the threshold for the maximum amount of memory that the TDF gateway can use, as a percentage from 1 through 90.

```
[edit unified-edge gateways tdf gateway-name]
user@host# set cac memory memory-pct
```

If the amount of memory that the TDF gateway uses reaches the threshold, the SNMP trap **jnxScgSMMemoryThreshHigh** is generated.

RELATED DOCUMENTATION

Configuring Service PICs | 18

Configuring Session PICs | 19

Making Predefined Groups Available for Session PIC and Service PIC Configuration

You must make the predefined session PIC and service PIC groups available in your configuration. These groups are used when you configure the session PICs and the service PICs.

To make the predefined groups available in your configuration:

- Load and merge the **tdf-defaults.conf** file.

```
[edit]
user@host# load merge /etc/config/tdf-defaults.conf
```

RELATED DOCUMENTATION

Configuring Service PICs | 18

Configuring Session PICs | 19

TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment | 9

Configuring Service PICs

An MS-MPC must have a service interface configured as a service PIC in order to provide subscriber-aware services, such as the policy and charging enforcement function (PCEF), application detection and control, or HTTP header enrichment. Repeat this procedure for each service interface that you want to serve as a service PIC.

Before you begin to configure a service PIC:

- Make sure that you installed the predefined groups.
- If the service PIC is not part of a redundant group, make sure that you have configured the service interface on the MS-MPC.
- If the service PIC is to function as a member of a redundant group, make sure that you have configured an aggregated multiservices (AMS) interface with the service interface as a member interface.

To configure a service PIC:

1. Add the MS-MPC service interface to the list of service PICs.

```
[edit unified-edge gateways tdf gateway-name system]
user@host# set service-pics interface interface-name
```

   where *interface-name* is ams*n* if you have redundancy configured and is ms-*fpc*/*pic*/0 if you do not have redundancy configured.

2. Perform one of the following actions:
   - If application identification is required but not HTTP header enrichment, configure the **tdf-services-xlp-dpi** group to run on the PIC.

```
[edit chassis]
user@host# set fpc slot-number pic pic-number apply-groups tdf-services-xlp-dpi
```

   - If both application identification and HTTP header enrichment are required, configure the **tdf-services-xlp-dpi-with-hcm** group to run on the PIC.

```
[edit chassis]
user@host# set fpc slot-number pic pic-number apply-groups tdf-services-xlp-dpi-with-hcm
```

3. (Optional) For Next Gen Services, enable subscriber awareness. This steps loads MSS, PCEF, HCM (all subscriber related plugins) on the PIC.

```
[edit chassis]
user@host# set fpc slot-number pic pic-number subscriber-aware-services
```

RELATED DOCUMENTATION

Configuring a Services Interface for a Session PIC or Service PIC | 15

Configuring Aggregated Multiservices Interfaces

Making Predefined Groups Available for Session PIC and Service PIC Configuration | 17

TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment | 9

Configuring Session PICs

An MS-MPC must have a service interface configured as a session PIC in order to support access subscriber sessions, policy and charging rules function (PCRF) sessions, and PCEF library installation from the PCRF. Repeat this procedure for each service interface that you want to serve as a session PIC.

Before you begin to configure a session PIC:

- Make sure that you have installed the predefined groups.
- If the session PIC is not part of a redundant group, make sure that you have configured the service interface on the MS-MPC.
- If the session PIC is to function as a member of a redundant group, make sure that you have configured an aggregated multiservices (AMS) interface with the service interface as a member interface.

To configure a session PIC:

1. Add the MS-MPC service interface to the list of session PICs.

```
[edit unified-edge gateways tdf gateway-name system]
user@host# set session-pics interface interface-name
```

where *interface-name* is ams*n* if you have redundancy configured and is ms-*fpc*/*pic*/0 if you do not have redundancy configured.

2. Configure the **tdf-session-xlp** group to run on the PIC.

```
[edit chassis]
user@host# set fpc slot-number pic pic-number apply-groups tdf-session-xlp
```

RELATED DOCUMENTATION

Making Predefined Groups Available for Session PIC and Service PIC Configuration | 17

Configuring a Services Interface for a Session PIC or Service PIC | 15

Configuring Aggregated Multiservices Interfaces

TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment | 9

Configuring Tracing for TDF Gateway

To configure tracing operations for the TDF gateway:

1. Specify that you want to configure tracing options for the TDF gateway.

```
[edit unified-edge gateways tdf gateway-name]
user@host# edit traceoptions
```

2. Configure the name of the file used for the trace output.

```
[edit unified-edge gateways tdf gateway-name traceoptions]
user@host# set file file-name
```

3. (Optional) Configure the maximum size of each trace file.

```
[edit unified-edge gateways tdf gateway-name traceoptions]
user@host# set file file-name size size
```

4. (Optional) Configure the maximum number of trace files.

```
[edit unified-edge gateways tdf gateway-name traceoptions]
user@host# set file file-name files number
```

5. (Optional) Configure the read permissions for the log file.

```
[edit unified-edge gateways tdf gateway-name traceoptions]
user@host# set file file-name (no-world-readable | world-readable)
```

6. (Optional) Disable remote tracing capabilities.

```
[edit unified-edge gateways tdf gateway-name traceoptions]
user@host# set no-remote-trace
```

7. Configure flags to filter the operations to be logged.

```
[edit unified-edge gateways tdf gateway-name traceoptions]
user@host# set flag flag
```

Table 1 on page 21 describes the flags that you can include.

Table 1: Trace Flags

Flag	Description
all	Trace all operations.
bulkjob	Trace events that are handled by bulk jobs in order to prevent system overload.
config	Trace configuration events.
cos-cac	Trace class of service (CoS) and call admission control (CAC) events.
ctxt	Trace user equipment, Packet Data Network (PDN), or bearer context events.

Table 1: Trace Flags *(Continued)*

Flag	Description
fsm	Trace mobile subscriber finite state machine (FSM) events.
gtpu	Trace GPRS tunneling protocol, user plane (GTP-U) events.
ha	Trace high availability events.
init	Trace initialization events.
pfem	Trace Packet Forwarding Engine Manager events.
stats	Trace **stats** events. This flag is used internally by Juniper Networks engineers.
waitq	Trace **waitq** events. This flag is used internally by Juniper Networks engineers.

8. Configure the level of tracing.

```
[edit unified-edge gateways tdf gateway-name traceoptions]
user@host# set level (all | critical | error | info | notice | verbose | warning)
```

RELATED DOCUMENTATION

traceoptions (TDF Gateway) | 735

CHAPTER 3

Configuring Application Identification

IN THIS CHAPTER

- Application Identification Overview | 23
- Downloading and Installing Predefined Junos OS Application Signature Packages | 24
- Configuring Custom Application Signatures | 26
- Uninstalling a Predefined Junos OS Application Signature Package | 33

Application Identification Overview

Junos Application Aware is an infrastructure plug-in on MS-MPC service PICs and on the MX-SPC3 services card that provides information to clients about application protocol bundles based on deep packet inspection (DPI) of application signatures. These clients can be any of the plug-ins on the MX Series router service chain, such as traffic detection function (TDF), that request application classification data. Starting in Junos OS Release 16.1R4 and Junos OS Release 17.2R1, application identification is available in Junos OS Broadband Subscriber Management. Starting in Junos OS Release 19.3R2, application identification is also supported for Broadband Subscriber Management on the MX-SPC3 services card if you have enabled Next Gen Services on the MX240, MX480 or MX960 router.

In application identification, you can apply application signatures as follows:

- **Predefined signatures**—Junos Application Aware comes with a bundle of predefined, preinstalled application signatures, but we recommend that you download and install the latest version of predefined signatures. As new sets of signatures are supported, they are compiled and made available for you to download.

- **Custom application signatures**—For any application signatures that are not predefined, you can create custom signatures for HTTP, SSL, and stream signature contexts and install them for application identification. After you have configured and committed custom signatures, they are serialized and merged with the predefined application signatures. You can specify the following types of custom application signatures:

  - **Address based**—You can define an application identification based on a specific IP address, or port, or both where a source IP address, destination IP address, or both are used for a known

application in a customer's network. This is useful, for example, when a Session Initiation Protocol (SIP) server initiates a session from its well known port, 5060. The customer can put the SIP server IP address and port 5060 as source IP/port for the SIP application. This method provides efficiency and accuracy of application identification for customer's network.

- **Internet Control Message Protocol (ICMP) based**—Application identification based on types of ICMP messages.
- **IP protocol based**—Application identification based on IP protocol. TCP, UDP, and ICMP are not supported for this method of signature creation.
- **Pattern-matching signatures**—Application based on pattern matching combined with Layer 7 protocol identification.

Release History Table

Release	Description
19.3R1	Starting in Junos OS Release 19.3R2, application identification is also supported for Broadband Subscriber Management on the MX-SPC3 services card if you have enabled Next Gen Services on the MX240, MX480 or MX960 router.
16.1R4	Starting in Junos OS Release 16.1R4 and Junos OS Release 17.2R1, application identification is available in Junos OS Broadband Subscriber Management.

RELATED DOCUMENTATION

Configuring Custom Application Signatures

Downloading and Installing Predefined Junos OS Application Signature Packages

Downloading and Installing Predefined Junos OS Application Signature Packages

NOTE: Starting in Junos OS Release 19.3R2 and 19.4R1, application identification is also supported for Broadband Subscriber Management if you have enabled Next Gen Services on the MX240, MX480 or MX960 router with the MX-SPC3 card.

To download, install, and verify the installation of predefined Junos OS application signature packages:

1. Use **download ignore-server-validation** if you want to skip server certification validation during the download. Validation is enabled by default.

```
[edit services application-identification]
user@host# set download ignore-server-validation
```

2. Configure the URL for the application signature packages server.

```
[edit services application-identification]
user@host# set download url https://services.netscreen.com/cgi-bin/index.cgi
```

3. Download the application signature package.
   - To download the latest signature package, enter the following command:

```
user@host> request services application-identification download
```

   - To download a specific, known signature package, include the version number:

```
user@host> request services application-identification download version version-number
```

4. Confirm the successful download of the package.

```
user@host> request services application-identification download status
```

```
Downloading application package succeed.
```

5. Install the application signature package.

```
user@host> request services application-identification install
```

6. Confirm the successful installation of the application signature package.

```
user@host> request services application-identification install status
```

```
Compiling application signatures of package version.
```

or

```
Install application package succeed
```

7. View the protocol bundle status:

```
user@host> show services application-identification status
```

RELATED DOCUMENTATION

- *Uninstalling a Predefined Junos OS Application Signature Package*
- *Application Identification Overview*
- *Configuring Custom Application Signatures*

Configuring Custom Application Signatures

NOTE: Starting in Junos OS Release 19.3R2 and 19.4R1, application identification is also supported for Broadband Subscriber Management if you have enabled Next Gen Services on the MX240, MX480 or MX960 router with the MX-SPC3 card.

You can configure custom application definitions using custom signatures. These definitions enable identification of protocol bundles through deep packet inspection (DPI) for use by interested services in the service chain.

Before you configure custom application signatures, ensure that **jservices-jdpi** is configured on all required interfaces of your MS-MPC, or of your MX-SPC3 services card if you have enabled Next Gen Services on the MX240, MX480, or MX960. To review how to configure the package on your MS-MPC or MX-SPC3 services card:

- For Junos OS Subscriber Aware, see Preconfigured Groups for Service PICs and for Session PICs Overview.
- For Junos OS Broadband Subscriber Management, see *Installing Services Packages for Subscriber Management Application-Aware Policy Management*.

To configure one or more custom application signatures:

1. Specify a name for the application.

```
[edit services application-identification]
user@host# edit application application-name
```

For example:

```
[edit services application-identification]
user@host# edit application my:http
```

2. Specify a description for the application.

```
[edit services application-identification application application-name]
user@host# set description description
```

For example:

```
[edit services application-identification application my:http]
user@host# set description "Test application"
```

3. Specify an alternative name for the application.

```
[edit services application-identification application application-name]
user@host# set alt-name alt-name
```

For example:

```
[edit services application-identification application my:http]
user@host# set alt-name my:http-app
```

4. Enable saving of the application system cache (ASC).

```
[edit services application-identification application my:http]
user@host# set cacheable
```

5. Specify the name of the Junos OS release for compatibility.

```
[edit services application-identification application application-name]
user@host# set compatibility junos-compatibility-version
```

For example:

```
[edit services application-identification application my:http]
user@host# set compatibility 17.1
```

6. Specify any desired application tags, consisting of a user-defined name and value.

```
[edit services application-identification application application-name]
user@host# set tags tag-name tag-value
```

For example:

```
[edit services application-identification application my:http]
user@host# set tags traffic-type video-stream
```

7. Specify one or more address-based signatures.

- Specify a destination address and destination port-range.

```
[edit services application-identification application application-name]
user@host# set filter ip 200.0.0.2/24 port-range [80]
```

8. Specify an ICMP-based signature.

a. Specify ICMP type and code.

```
[edit services application-identification application application-name]
user@host# set icmp-mapping type icmp-type code icmp-code
```

For example:

```
[edit services application-identification application my:http]
user@host# set icmp-mapping type 33 code 34
```

9. Specify an IP protocol-based signature.

   a. Specify the IP protocol by protocol number.

```
[edit services application-identification application application-name]
user@host# set ip-protocol-mapping protocol protocol-number
```

   For example:

```
[edit services application-identification application my:http]
user@host# set ip-protocol-mapping protocol 103
```

   All ip-protocol-mappings are allowed except Protocol numbers 1,6,17 are not allowed to be configured under ip-protocol based signatures. If you try to configure protocols 1,6,17 under ip-protocol-mapping you will get commit errors.

10. Specify one or more Layer 4 and Layer 7 signatures using pattern matching in conjunction with a Layer 4 protocol.

    a. Specify a name for the Layer 4 and Layer 7 signature.

```
[edit services application-identification application application-name
over protocol-type]
user@host# set signature l4-l7-signature-name
```

   For example:

```
[edit services application-identification application my:http over http]
user@host# set signature myl3l7
```

b. Specify the order to be used if conflicts occur during the application classification. In such a case, the application with lowest order is classified.

```
[edit services application-identification application application-name
over protocol-type signature l4-l7-signature-name member member-name]
user@host# set order order
```

For example:

```
[edit services application-identification application my:http over http
signature myl3l7 member m01]
user@host# set order 1
```

c. Specify the priority for using this signature instead of using any matched predefined signatures.

```
[edit services application-identification application application-name
over protocol-type signature l4-l7-signature-name]
user@host# set order-priority (high | low)
```

For example:

```
[edit services application-identification application my:http over http
signature myl3l7]
user@host# set order-priority high
```

d. (Optional) Specify the protocol. If you are using Next Gen Services with the MX-SPC3 services card, do not perform this step.

```
[edit services application-identification application application-name
over protocol-type signature l4-l7-signature-name]
user@host# set protocol (http | ssl | tcp | udp)
```

For example:

```
[edit services application-identification application my:http over http
signature myl3l7]
user@host# set protocol http
```

e. (Optional) Specify that members are to be matched in order.

```
[edit services application-identification application application-name
over protocol-type signature l4-l7-signature-name]
user@host# set chain-order
```

f. Specify a member. You can repeat this step to define up to four members.

```
[edit services application-identification application application-name
over protocol-type signature l4-l7-signature-name]
user@host# edit member member-name
```

For example:

```
[edit services application-identification application my:http over http
signature myl3l7]
user@host# edit member m01
```

g. Specify the member's identifying pattern.

```
[edit services application-identification application application-name
over protocol-type signature l4-l7-signature-name member member-name]
user@host# set pattern pattern
```

For example:

```
[edit services application-identification application my:http over http
signature myl3l7 member m01]
user@host# set pattern "www\.facebook\.net"
```

h. Specify the direction of flows to which pattern matching is applied.

```
[edit services application-identification application application-name
over protocol-type signature l4-l7-signature-name member member-name]
user@host# set direction (any | client-to-server | server-to-client)
```

For example:

```
[edit services application-identification application my:http over http
signature myl3l7 member m01]
user@host# set direction any
```

i. Specify the number of check-bytes. This option applies to TCP and UDP only.

```
[edit services application-identification application application-name
over protocol-type signature l4-l7-signature-name member member-name]
user@host# set check-bytes max-bytes-to-check
```

For example:

```
[edit services application-identification application my:http over http
signature myl3l7 member m01]
user@host# set check-bytes 5000
```

11. (For Next Gen Services with the MX-SPC3 services card only) After you have committed your changes, you can check the status of the custom signature commitment.

```
[edit services application-identification application my:http over http
signature myl3l7 member m01]
user@host> show services application-identification commit-status
```

RELATED DOCUMENTATION

Application Identification Overview

Uninstalling a Predefined Junos OS Application Signature Package

NOTE: Starting in Junos OS Release 19.3R2 and 19.4R1, application identification is also supported for Broadband Subscriber Management if you have enabled Next Gen Services on the MX240, MX480 or MX960 router with the MX-SPC3 card.

To uninstall the current application signature package:

- Enter the uninstall command.

```
user@host> request service application-identification uninstall
```

RELATED DOCUMENTATION

Downloading and Installing Predefined Junos OS Application Signature Packages

CHAPTER 4

Configuring HTTP Header Enrichment

IN THIS CHAPTER

- Junos Web Aware HTTP Header Enrichment Overview | 34
- HTTP Content Manager (HCM) | 35
- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Configuring HCM Profiles and Assigning Tag Rules | 49

Junos Web Aware HTTP Header Enrichment Overview

Subscribers accessing Web-based services often need to have content added to the HTTP headers sent back and forth as part of the client-server exchange. You can use Junos Web Aware to configure HTTP header enrichment on the MX Series router. Junos Web Aware allows tag insertions. In addition to the International Mobile Subscriber Identity (IMSI) and mobile station ISDN (MSISDN) tags, you can specify tags for International Mobile Station Equipment Identity (IMEI), TDF gateway IP address, and Subscriber IP address.

Support added in Junos OS Release 20.2R1 for only the insertion of IPv4 or IPv6 tags user addresses in an HTTP headers. No other tags are supported in this release for Next Gen Services.

For example, this feature can add the last line to this sequence of HTTP headers:

```
GET /256k.html HTTP/1.1
Host: 10.45.45.2
Accept */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; NET CLR 1.1.4322
name: value
X-MSISDN: <MSISDN #>
```

You can also use HTTP header enrichment to replace a byte of the IPv4 or IPV6 user address in the HTTP header with a value you specify.

Release History Table

Release	Description
20.2R1	Support added in Junos OS Release 20.2R1 for only the insertion of IPv4 or IPv6 tags user addresses in an HTTP headers. No other tags are supported in this release for Next Gen Services.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm (HTTP Header Enrichment) | 434

HTTP Content Manager (HCM)

IN THIS SECTION

- Configuring the HTTP-Manager Package on the Router | 35

HTTP Content Management (HCM) is an application used for inspecting the HTTP traffic transmitted through port 80 (default) or any other port you use to transmit HTTP traffic. HCM can be installed on an MX Series router that is running the corresponding version of the Junos OS release. HCM inspects HTTP traffic even if the default port 80 is not used for HTTP traffic and is interoperable with ms, vms, and ams interface types. It supports fragmented HTTP request packets and GET, PUT, and POST requests.

Support added in Junos OS Release 20.2R1 for only the insertion of IPv4 or IPv6 tags user addresses in an HTTP headers. No other tags are supported in this release for Next Gen Services.

Configuring the HTTP-Manager Package on the Router

1. Before you install the HTTP-Manager package on the router, ensure that you have the appropriate version of the HTTP-Manager package for the Junos OS image you are using on the router. When

you have confirmed that you have the right package, use the **request system software add** command to install the HTTP-Manager package. You have to restart the CLI after the package is installed.

```
user@router> request system software add jservices-x86-32-19.4R1.1.tgz
NOTICE: Validating configuration against package-name.
NOTICE: Use the 'no-validate' option to skip this if desired.
Checking compatibility with configuration
```

```
Initializing...
```

```
WARNING: cli has been replaced by an updated version:
CLI release 19.4R1 built by builder on 2020-06-10 02:36:22 UTC
Restart cli using the new version ? [yes,no] (yes)
Restarting cli ...
```

2. When the CLI has restarted, use the **show version** command to see whether the HTTP-Manager packages are installed.

```
user@router> show version
...
HTTP-Manager Management Component [19.4R1-1-A1.2]
HTTP-Manager Dataplane Component [19.4R1-1-A1.2]
user@router>..
```

3. If you want to upgrade the Junos OS image on a router that has the HTTP-Manager package installed, you should first save and then delete the HTTP-Manager configuration from the router.

   - To view the HTTP-Manager configuration, use the **user@router>extension juniper-http-manager show <section>** command.
   - To delete the HTTP-Manager configuration from the router, use the **user@router>extension juniper-http-manager delete <section>** command.
   - Any remnant HTTP-Manager configuration left on the router will be deleted when the Junos OS image is upgraded. So, ensure that you have saved all necessary HTTP Content Management configurations.

- To delete the HTTP-Manager package from the router, use the **user@router> request system software delete <http-manager-package>** command.
- Reinstall the HTTP-Manager package on the router after you upgrade the Junos OS image on the router.

```
user@router> show version
Hostname: router
Model: mx480
JUNOS Base OS boot [19.4R1]
JUNOS Base OS Software Suite [19.4R1]
JUNOS Kernel Software Suite [19.4R1]
JUNOS Crypto Software Suite [19.4R1]
JUNOS Packet Forwarding Engine Support (M/T Common) [19.4R1]
JUNOS Packet Forwarding Engine Support (MX Common) [19.4R1]
JUNOS Online Documentation [19.4R1]
JUNOS Voice Services Container package [19.4R1]
JUNOS Border Gateway Function package [19.4R1]
JUNOS Services AACL Container package [19.4R1]
JUNOS Services LL-PDF Container package [19.4R1]
JUNOS Services PTSP Container package [19.4R1]
JUNOS Services Stateful Firewall [19.4R1]
JUNOS Services NAT [19.4R1]
JUNOS Services Application Level Gateways [19.4R1]
JUNOS Services Captive Portal and Content Delivery Container package [19.4R1]
JUNOS Services RPM [19.4R1]
JUNOS Services HTTP Content Management package [19.4R1]
JUNOS AppId Services [19.4R1]
JUNOS IDP Services [19.4R1]
JUNOS Services Crypto [19.4R1]
JUNOS Services SSL [19.4R1]
JUNOS Services IPSec [19.4R1]
JUNOS Runtime Software Suite [19.4R1]
 JUNOS Routing Software Suite [19.4R1]
```

```
HTTP-Manager Management Component [19.4R1-1-A1.2]
HTTP-Manager Dataplane Component [19.4R1-1-A1.2]
```

```
user@router> configure
Entering configuration mode
```

```
[edit]
user@router# extension juniper-http-manager show
## Last changed: 2020-06-07 13:21:36 PDT
services {
    http-manager {
        traceoptions {
            level all;
            flag all;
        }
```

```
    }
}
```

```
[edit]
user@router# extension juniper-http-manager delete
```

```
[edit]
user@router# extension juniper-http-manager show
```

```
[edit]
 user@router# commit
commit complete
```

```
[edit]
user@router# exit
Exiting configuration mode
```

```
user@router> request system software delete http-manager-services
Removing package 'http-manager-services' ...
Removing /opt/sdk/service-packages/http-manager-services ...
Removing http-manager-services-xlr-19.4R1-1-A1.2.tgz from /var/sw/pkg ...
Notifying mspd ...
```

```
user@router> request system software delete http-manager-mgmt
Removing package 'http-manager-mgmt' ...
Reloading /config/juniper.conf.gz ...
Activating /config/juniper.conf.gz ...
mgd: commit complete
```

```
Restarting mgd ...
Restarting http-manager ...
```

```
WARNING: cli has been replaced by an updated version:
CLI release 11.4R3.7 built by builder on 2020-05-14 19:51:45 UTC
Restart cli using the new version ? [yes,no] (yes)
```

```
Restarting cli ...
user@router>
```

```
user@router> show version
Hostname: router
Model: mx480
JUNOS Base OS boot [19.4R1]
JUNOS Base OS Software Suite [19.4R1]
JUNOS Kernel Software Suite [19.4R1]
JUNOS Crypto Software Suite [19.4R1]
JUNOS Packet Forwarding Engine Support (M/T Common) [19.4R1]
JUNOS Packet Forwarding Engine Support (MX Common) [19.4R1]
JUNOS Online Documentation [19.4R1]
JUNOS Voice Services Container package [19.4R1]
JUNOS Border Gateway Function package [19.4R1]
JUNOS Services AACL Container package [19.4R1]
JUNOS Services LL-PDF Container package [19.4R1]
JUNOS Services PTSP Container package [19.4R1]
JUNOS Services Stateful Firewall [19.4R1]
JUNOS Services NAT [19.4R1]
JUNOS Services Application Level Gateways [19.4R1]
JUNOS Services Captive Portal and Content Delivery Container package [19.4R1]
JUNOS Services RPM [19.4R1]
JUNOS Services HTTP Content Management package [19.4R1]
JUNOS AppId Services [19.4R1]
JUNOS IDP Services [19.4R1]
JUNOS Services Crypto [19.4R1]
JUNOS Services SSL [19.4R1]
JUNOS Services IPSec [19.4R1]
JUNOS Runtime Software Suite [19.4R1]
JUNOS Routing Software Suite [19.4R1]
```

Release History Table

Release	Description
20.2R1	Support added in Junos OS Release 20.2R1 for only the insertion of IPv4 or IPv6 tags user addresses in an HTTP headers. No other tags are supported in this release for Next Gen Services.

RELATED DOCUMENTATION

show services hcm statistics | 885

Configuring HTTP Header Enrichment Overview

You configure HTTP header enrichment by configuring tag rules and an HCM profile that points to specific tag rules. Tag rules identify the HTTP enrichment actions to take when the conditions in the tag rule are matched. For subscriber traffic under static policy control, a tag rule is used if it is included in the HCM profile specified in a PCC rule that the traffic matches. For subscribers under dynamic policy control, a message from the PCRF identifies the configured HCM profile to use for HTTP header enrichment.

Support added in Junos OS Release 20.2R1 for only the insertion of IPv4 or IPv6 tags user addresses in an HTTP headers. No other tags are supported in this release for Next Gen Services.

If you change the configuration of tag rules during an existing subscriber data session, the changes do not impact the existing session. The configuration changes are used by any new subscriber data sessions.

To configure HTTP header enrichment for a subscriber:

1. Configure one or more tag rules to specify the HTTP header enrichment actions.

   See "Configuring Tag Rules" on page 42.
2. Configure an HCM profile and assign tag rules to it.

   See "Configuring HCM Profiles and Assigning Tag Rules" on page 49.
3. (For subscribers under static policy control) Assign the HCM profile to a PCC action profile.

   See "Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware" on page 83.
4. (For subscribers under static policy control) Configure a PCC rule that includes the PCC action profile.

   See "Configuring Policy and Charging Control Rules" on page 86.
5. Enable HTTP enrichment for a subscriber's service set.

   See "Applying Services to Subscriber-Aware Traffic with a Service Set" on page 146.

Release History Table

Release	Description
20.2R1	Support added in Junos OS Release 20.2R1 for only the insertion of IPv4 or IPv6 tags user addresses in an HTTP headers. No other tags are supported in this release for Next Gen Services.

RELATED DOCUMENTATION

Junos Web Aware HTTP Header Enrichment Overview | 34

Configuring Tag Rules

Tag rules include one or more **term** statements that identify the HTTP enrichment actions to take when the conditions in the **term** are matched. You must configure at least one **tag** in the **then** clause of a **term**, and you can configure multiple tags.

Terms are evaluated in the order they are configured. If a data packet matches all the criteria in the **from** statement in a **term**, then the actions specified in the **then** statement of the **term** are applied. If the **from** statement does not identify any criteria, then all traffic matches. After a data packet matches a term, further terms are not evaluated. If no terms match, then the HTTP header is not enriched.

To configure a tag rule:

1. Configure the list of tag attributes that may be used in tag rules.

```
[edit services hcm]
user@host# set tag-attribute tag-attr-name
```

The tag attributes currently supported for Adaptive Services are **apn**, **ggsnipv4**, **ggsnipv6**, **imei**, **imsi**, **ipv4addr**, **ipv6addr**, and **msisdn**. To configure multiple tag attributes, include them in square brackets ([ ]). Starting in Junos 20.2R1 IPv4 and IPv6 tags for HTTP Header Enrichment are supported for Next Gen Services on MX240, MX480 and MX960. No other tags are supported for Next Gen Services in this release.

For example:

```
[edit services hcm]
user@host# set tag-attribute [msisdn apn]
```

2. Configure a name for the tag rule.

```
[edit services hcm]
user@host# set tag-rule rule-name
```

For example:

```
[edit services hcm]
user@host# set tag-rule rule1
```

3. Configure a term for the tag rule.

```
[edit services hcm set tag-rule rule-name]
user@host# set term term-number
```

NOTE: The **term** argument must have a numeric value.

For example:

```
[edit services hcm set tag-rule rule1]
user@host# set term 1
```

4. (Optional) Specify the prefix that the HTTP request destination IP address must match.

```
[edit services hcm tag-rule rule-name term term-number from]
user@host# set destination-address prefix
```

For example:

```
[edit services hcm tag-rule rule1 term 1 from]
user@host# set destination-address 192.0.2.0/24
```

You can also specify the type of address to match:

```
[edit services hcm tag-rule rule-name term term-number from]
user@host# set destination-address (any-ipv4 | any-ipv6 | any-unicast)
```

You can specify multiple prefixes or address types by including the **destination-address** statement multiple times.

5. (Optional) Specify an IP address range that the HTTP request destination IP address must match.

```
[edit services hcm tag-rule rule-name term term-number from]
user@host# set destination-address-range low address high address
```

For example:

```
[edit services hcm tag-rule rule1 term 1 from]
user@host# set destination-address-range  low 10.10.10.1 high 10.10.10.255
```

You can specify multiple address ranges by including the **destination-address-range** statement multiple times.

6. (Optional) Specify the destination prefix list that the HTTP request destination IP address must match. The prefix list must already be defined at the **[edit policy-options prefix-list]** hierarchy level.

```
[edit services hcm tag-rule rule-name term term-number from]
user@host# set destination-prefix-list prefix-name
```

For example:

```
[edit services hcm tag-rule rule1 term 1 from]
user@host# set destination-prefix-list customer1
```

You can specify multiple prefix lists by including the **destination-prefix-list** statement multiple times.

7. (Optional) Specify any addresses that you want to exclude from matching the HTTP request destination IP address with the **except** statement. To exclude addresses, you must also configure addresses that do match in a **destination-address**, **destination-address-range**, or **destination-prefix-list** statement at the **[edit services hcm tag-rule *rule-name* term *term-number* from]** hierarchy level.

For example:

```
[edit services hcm tag-rule rule1 term 1 from]
user@host# set destination-address-range  low 10.10.10.1 high 10.10.10.255
user@host# set destination-address 10.10.10.9/32 except
```

This matches all the addresses in the destination range except 10.10.10.9.

You can use **except** in the following statements at the **[edit services hcm tag-rule *rule-name* term *term-number* from]** hierarchy level:

```
destination-address {
    any-ipv4 except;
    any-ipv6 except;
    any-unicast except;
    prefix except;
}
destination-address-range {
    high address low address except;
}
destination-prefix-list {
    prefix-name except;
}
```

8. (Optional) Specify a port range that the HTTP request destination port number must match.

```
[edit services hcm tag-rule rule-name term term-number from]
user@host# set destination-port-range high port-number low port-number
```

You can specify multiple port ranges by including the **destination-port-range** statement multiple times.

NOTE: If you do not specify any ports or port ranges to match, then all ports are matched.

9. (Optional) Specify the HTTP request destination port number that must be matched.

```
[edit services hcm tag-rule rule-name term term-number from]
user@host# set destination-ports value
```

You can specify multiple ports by including the **destination-ports** statement multiple times.

10. (Optional) Specify that you want to apply all HTTP header enrichment actions specified in the **then** statement of the tag rule to all HTTP requests by not including any matching conditions in the **from** statement. You must include a **from** statement in each **term** of a tag rule.

```
[edit services hcm tag-rule rule-name term term-number ]
user@host# set from
```

For example:

```
[edit services hcm tag-rule rule2 term 1]
user@host# set from
[edit services hcm tag-rule rule2 term 1]
user@host# set then count
```

11. Configure a name for a tag.

```
[edit services hcm tag-rule rule-name term term-number then]
user@host# set tag tag-name
```

For example:

```
[edit services hcm tag-rule rule1 term 1 then]
user@host# set tag msisdn-tag
```

12. Configure the tag header that the tag applies to the HTTP header.

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name]
user@host# set tag-header header
```

For example:

```
[edit services hcm tag-rule rule1 term 1 then tag msisdn-tag]
user@host# set tag-header X_MSISDN
```

You can configure a maximum of 16 unique tag headers.

The *header* values cannot be **accept**, **accept-charset**, **accept-encoding**, **accept-language**, **authorization**, **expect**, **host**, **if-match**, **if-modified-since**, **if-none-match**, **if-range**, **if-unmodified-**

since, **max-forwards**, **proxy-authorization**, **referer**, **user-agent**, or **x-moz**. These header values are reserved; you cannot configure them.

13. Specify the tag attribute that the tag applies to the HTTP header. To specify multiple attributes at one time, include the attributes in square brackets ([]).

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name]
user@host# set tag-attribute [tag-attr-name]
```

> **NOTE**: The tag attribute must be listed in the tag attributes configured in Step "1" on page 42.

For example:

```
[edit services hcm tag-rule rule1 term 1 then tag msisdn-tag]
user@host# set tag-attribute msisdn
```

14. Specify the separator that the tag uses in the HTTP header.

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name]
user@host# set tag-separator separator
```

For example:

```
[edit services hcm tag-rule rule1 term 1 then tag msisdn-tag]
user@host# set tag-separator /
```

15. (Optional) Specify a hash method and prefix key for the insertion of the tag in the HTTP header.

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name
encrypt]
user@host# set hash algorithm prefix hash-prefix
```

Currently, only the **md5** hash method is supported.

For example:

```
[edit services hcm tag-rule rule1 term 1 then tag msisdn-tag encrypt]
user@host# set hash md5 prefix gatewaykey1
```

16. (Optional) Enable the collection of statistics for HTTP header enrichment for the tag rule.

```
[edit services hcm tag-rule rule-name term term-number then
user@host# set count
```

17. (Optional) Configure how the tag replaces a byte of the IPv4 or IPv6 user address with a different value in the HTTP header.

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name]
user@host# set (ipv4-mask ipv4-mask | ipv6-mask ipv6-mask) (ipv4-or-value ipv4-or-value | ipv6-or-value ipv6-or-value)
```

To identify the byte you want to replace, enter **255** for IPv4 or **ff** for IPv6 in the corresponding byte of the **ipv4-mask** or **ipv6-mask** and enter zero in the other bytes.

To specify the new value for that byte, enter the value in the corresponding byte of the **ipv4-or-value** or the **ipv6-or-value** and enter zero in the other bytes.

For example, the following replaces the first byte of the IPv4 user address with the value 168:

```
[edit services hcm tag-rule tag1 term term1 then tag subscip4]
user@host# set ipv4-mask 255.0.0.0 ipv4-or-value 168.0.0.0
```

18. If you want to configure more tags for the **then** statement in the term, repeat Step "11" on page 46 through Step "17" on page 48.
19. If you want to configure another **term** statement for the tag rule, repeat Step "3" on page 43 through Step "18" on page 48.

Release History Table

Release	Description
20.2R1	Starting in Junos 20.2R1 IPv4 and IPv6 tags for HTTP Header Enrichment are supported for Next Gen Services on MX240, MX480 and MX960. No other tags are supported for Next Gen Services in this release.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

Configuring HCM Profiles and Assigning Tag Rules | 49

Junos Web Aware HTTP Header Enrichment Overview | 34

Configuring HCM Profiles and Assigning Tag Rules

The HCM profile for a subscriber specifies the tag rules to apply to a subscriber's traffic. Tag rules identify the HTTP enrichment actions to take when the conditions in the tag rule are matched. You can have a maximum of 100 HCM profiles.

Support added in Junos OS Release 20.2R1 for only the insertion of IPv4 or IPv6 tags user addresses in an HTTP headers. No other tags are supported in this release for Next Gen Services.

For subscriber-aware traffic under static policy control, a tag rule is used if it is included in the HCM profile specified in a PCC rule that the traffic matches. For subscriber-aware traffic under dynamic policy control, a message from the PCRF identifies the configured HCM profile and tag rules to use for HTTP header enrichment.

To configure an HCM profile:

1. Configure the HCM profile name.

```
[edit services hcm]
user@host# set profile profile-name
```

For example:

```
[edit services hcm]
user@host# set profile hcm1
```

2. Assign a tag rule to the HCM profile.

```
[edit services hcm profile profile-name]
user@host# set tag-rule rule-name
```

For example:

```
[edit services hcm profile hcm1]
user@host# set tag-rule rule1
```

Release History Table

Release	Description
20.2R1	Support added in Junos OS Release 20.2R1 for only the insertion of IPv4 or IPv6 tags user addresses in an HTTP headers. No other tags are supported in this release for Next Gen Services.

RELATED DOCUMENTATION

- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Junos Web Aware HTTP Header Enrichment Overview | 34
- Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware | 83

CHAPTER 5

Configuring Policy and Charging Enforcement

IN THIS CHAPTER

- Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | **52**
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | **56**
- Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Dynamically by a PCRF | **58**
- Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Statically | **63**
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | **64**
- Understanding PCEF Profiles | **70**
- Understanding Network Elements | **71**
- Understanding AAA Profiles | **73**
- Understanding Static Time-of-Day PCC Rule Activation and Deactivation | **74**
- Understanding Usage Monitoring for TDF Subscribers | **74**
- Configuring Dynamic Policy Control by PCRF | **76**
- Configuring Static Policy Control | **77**
- Configuring Policy Control by RADIUS Servers | **78**
- Configuring Service Data Flow Filters | **79**
- Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware | **83**
- Configuring Policy and Charging Control Rules | **86**
- Configuring a Policy and Charging Control Rulebase | **89**
- Configuring RADIUS Servers | **91**
- Configuring RADIUS Network Elements | **94**
- Configuring an AAA Profile | **96**
- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Dynamic Policies | **98**
- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Static Policies | **100**
- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Policies That a RADIUS Server Controls | **101**

- Configuration of Static Time-of-Day PCC Rule Activation and Deactivation Overview | **102**
- Configuring the NTP Server | **103**
- Configuring Static Time-of-Day PCC Rule Activation and Deactivation in a Junos OS Subscriber Aware PCEF Profile | **103**
- Configuring TDF Subscriber Usage Monitoring for Traffic That Matches Predefined PCC Rules | **105**

Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF)

IN THIS SECTION

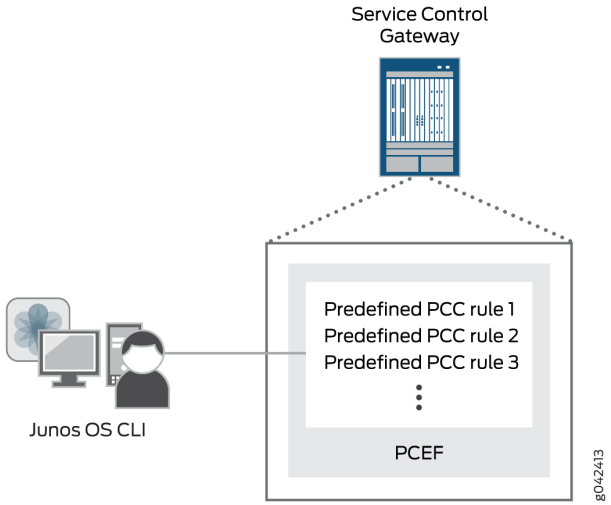
- Static Policy Control | **53**
- Dynamic Policy Control | **53**
- RADIUS Server Policy Control | **55**

The policy and charging enforcement function (PCEF) of Junos Subscriber Aware enforces policy and charging control (PCC) rules for the treatment of a subscriber's packets. A PCC rule is installed on, and enforced by, the PCEF. The PCC rules can be under static control, under dynamic control of the policy and charging rules function (PCRF), or under activation/deactivation control of a RADIUS server, depending on the PCEF profile that is assigned to a subscriber.

Static Policy Control

For static policies, the PCEF enforces PCC rules you predefined on the MX Series router with no interaction from the PCRF or a RADIUS server, as shown in Figure 3 on page 53.

Figure 3: Static Policy Control

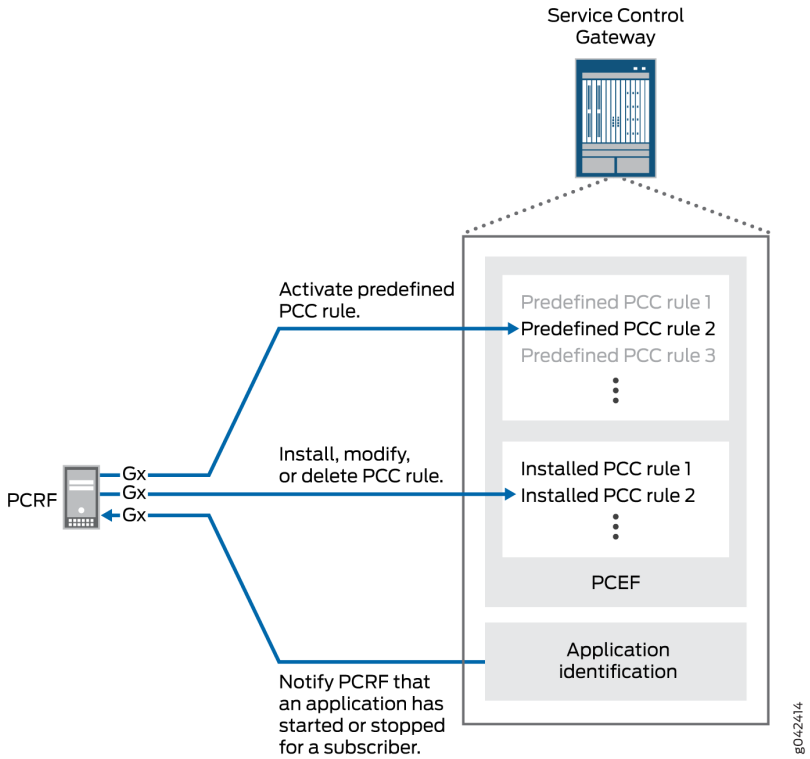


Dynamic Policy Control

For dynamic policies, the PCEF acts upon messages received from the PCRF. The PCRF is the central entity that makes policy and charging decisions based on input from different sources, such as mobile operator configuration, user subscription information, and services information. The PCC rules are either provisioned by the PCRF and sent to the PCEF over the Gx interface using Diameter AVPs, or predefined on the MX Series router and activated by a Diameter message from the PCRF. The PCEF also provides the PCRF with subscriber and access information. See Figure 4 on page 54.

When PCC rules are under dynamic control, the PCEF gives precedence to rules sent by the PCRF over rules that are predefined on the PCEF.

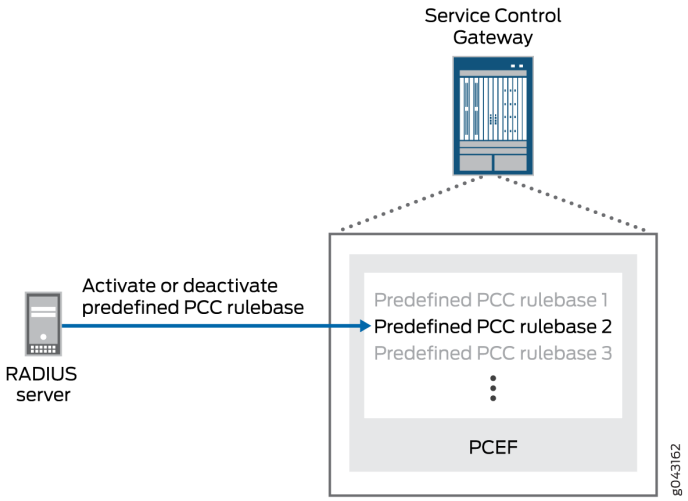
Figure 4: Dynamic Policy Control



RADIUS Server Policy Control

For polices under control of a RADIUS server, a RADIUS server activates and deactivates policy and PCC rules that you have predefined on the MX Series router, as shown in Figure 5 on page 55.

Figure 5: RADIUS Server Policy Control



RELATED DOCUMENTATION

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | 56

Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Dynamically by a PCRF | 58

Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Statically | 63

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment

IN THIS SECTION

- Understanding Service Data Flow Filters | 56
- Understanding Application Filters | 57
- Understanding PCC Action Profiles | 57

You can configure policy and charging control (PCC) rules to define the treatment to apply to specific service data flows or to packets associated with specific applications. A PCC rule is applicable to a subscriber's traffic if the rule is in the subscriber's PCEF profile.

These predefined PCC rules contain a **from** clause that identifies the service data flows or applications, and a **then** clause that specifies the PCC action profile that identifies the treatment to apply.

A predefined PCC rule can be used in three ways:

- When PCC rules are under static control, predefined rules are the only rules used. The provisioning of PCC rules involves no interaction from the policy and charging rules function (PCRF) or a RADIUS server.
- When PCC rules are under dynamic control, a predefined PCC rule must be activated by the PCRF. (With dynamic control, PCC rules can also be sent from the PCRF.)
- When PCC rules are under RADIUS server control, a predefined PCC rule must be activated by the RADIUS server.

This topic includes the following sections:

Understanding Service Data Flow Filters

Service data flow (SDF) filters (flow identifiers) are specified in the **from** clause of a PCC rule to identify IP packets belonging to a particular Layer 3 or Layer 4 service data flow. If the IP packet matches the SDF filter in a PCC rule, the treatment specified in the PCC action profile in the **then** clause of the rule is applied.

To configure Layer 3 or Layer 4 SDF filters, you specify one or more of the following parameters:

- Source IP address

- Destination IP address
- Source port
- Destination port
- Layer 4 protocol (UDP or TCP)

Understanding Application Filters

Applications or application groups are specified in the **from** clause of a PCC rule to identify IP packets belonging to a specific application. If the IP packet is for an application identified in a PCC rule, the treatment specified in the PCC action profile in the **then** clause of the rule is applied.

To configure application-aware PCC rules, you can specify one or more of the following parameters:

- application—Specifies the name of an application. This can be a Layer 7 protocol (for example, HTTP) or a particular application running on a Layer 7 protocol, such as Facebook and Yahoo Messenger.
- application-group—Specifies the name of an application group, which can be used to process a number of applications or subgroups at the same time.

NOTE: Application-aware PCC rules that reference specified applications can include wildcard or specific Layer-3 SDF filters, Layer-4 SDF filters, or both.

Understanding PCC Action Profiles

A PCC rule configuration includes an action profile in the **then** clause that defines the treatment to apply to a service data flow or to a packet belonging to an application identified in the **from** clause of the rule. You can configure a PCC action profile that is used in one or more PCC rules to provide the following functionality:

- HTTP redirection—Specifies HTTP redirection to a URL. You can use this action only for PCC rules that match only HTTP-based applications and all flows.
- HTTP Steering path—Specifies an IPv4 or IPv6 address for steering HTTP packets. You can use this action only for PCC rules that match only HTTP-based applications and all flows.

NOTE: A single PCC rule can support either HTTP redirection or HTTP steering path, but not both.

- Steering with a routing instance—Specifies a routing instance for steering of packets to a third-party server to apply services or to a local or external service chain. You can configure different routing instances for traffic from the subscriber (uplink) and traffic to the subscriber (downlink).
- Keep existing steering—Specifies that steering attributes configured in a PCC action profile that a PCC rule applies to a data flow session when it begins will continue to be applied to the data flow when the PCC rule match conditions are modified, deleted, or added to.
- Forwarding class—Specifies the forwarding class that you want assigned to the packet.
- Maximum bit rate—Specifies the maximum bit rate for uplink and for downlink traffic.
- HCM profile—Specifies the profile that identifies the HTTP header enrichment rules to apply. You can use this action only for PCC rules that match only HTTP-based applications and all flows.
- Gating status—Specifies whether to block or to forward IP packets.

RELATED DOCUMENTATION

Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | 52

Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Dynamically by a PCRF | 58

Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Statically | 63

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware | 83

Configuring Service Data Flow Filters | 79

Configuring Policy and Charging Control Rules | 86

Application Identification Overview | 23

Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Dynamically by a PCRF

IN THIS SECTION

- Policy Decisions | 59
- Supported Operations | 59

With dynamic policy control, the policy and charging rules function (PCRF) controls the provisioning of policy and charging control (PCC) rules on the Junos Subscriber Aware PCEF for a subscriber. Dynamic policy control is enabled when a dynamic-policy-control policy and charging enforcement function (PCEF) profile is assigned to a subscriber. Dynamic policy control requires Junos Policy Control.

This topic includes the following sections:

Policy Decisions

The PCRF is central in making policy and charging control decisions and can install, activate, modify, or deactivate a PCC rule on the PCEF at any time. The PCRF can make its policy and charging control decisions based on different sources, including:

- Subscription information for the user equipment that is received from the subscription profile repository (SPR)
- Operator configuration in the PCRF
- Information from the access network about the access technology
- Information from the PCEF, such as the name of the application that the subscriber is using

The Gx interface is used to send PCC rule provisioning information from the PCRF to the PCEF, and to provide notification of traffic-plane events from the PCEF to the PCRF.

Supported Operations

Junos Subscriber Aware and Junos Policy Control support the following operations with the PCRF:

- Install or modify rules—The PCRF sends the **Charging-Rule-Install** AVP to install a PCC rule that is not already installed or modify an existing rule on the PCEF.
- Remove rules—The PCRF sends the **Charging-Rule-Remove** AVP to remove a PCC rule that is already installed.
- Activate rules—The PCRF sends the **Rule-Activation-Time** AVP to indicate the time at which to activate the rule, and it is contained within the **Charging-Rule-Install** AVP. This operation results in a single activation of the rule, not a recurring activation schedule.

- Deactivate rules—The PCRF sends the **Rule-Deactivation-Time** AVP to indicate the time at which to deactivate the rule, and it is contained within the **Charging-Rule-Install** AVP. This operation results in a single deactivation of the rule, not a recurring deactivation schedule.

- PCEF session revalidation—The PCRF sends the **Revalidation-Time** AVP along with the **Event-Trigger** AVP with the value **REVALIDATION_TIMEOUT** to indicate the time at which the PCEF must request PCEF session revalidation from the PCRF. When the specified time is reached, the PCEF sends an event trigger with the value **REVALIDATION_TIMEOUT** to request PCEF session revalidation.

- Report application start or stop—The PCEF sends an event trigger when it detects the start or stop of an application.

The containers for the PCC rules are named **Charging-Rule-Definition**. Multiple **Charging-Rule-Definition** containers can be sent within a **Charging-Rule-Install** or **Charging-Rule-Remove**, each of which is applied per subscriber.

If a time zone is configured on the router, the activation and deactivation settings apply to the configured time zone and are adjusted for transitions to and from daylight saving time.

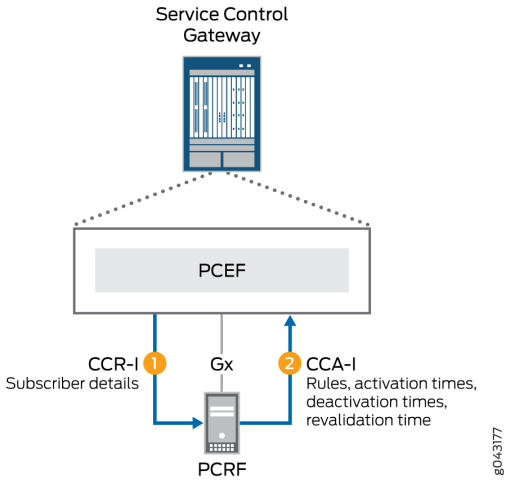
Methods for Provisioning PCC Rules

The PCRF uses one of the following procedures to specify the PCC rules that the PCEF applies:

- Pull mode during TDF subscriber creation—Applies when the MX Series gateway receives a request for a new TDF subscriber. The PCEF sends a credit control request initial (CCR-I) message to the PCRF with information about the subscriber. The PCRF downloads PCC rules to the PCEF in a credit control answer initial (CCA-I) message, which may also include any activation and deactivation times

that apply to the rules and the time at which the PCEF must re-request PCC rules from the PCRF. Figure 6 on page 61 shows the message flow for a pull procedure during TDF subscriber creation.

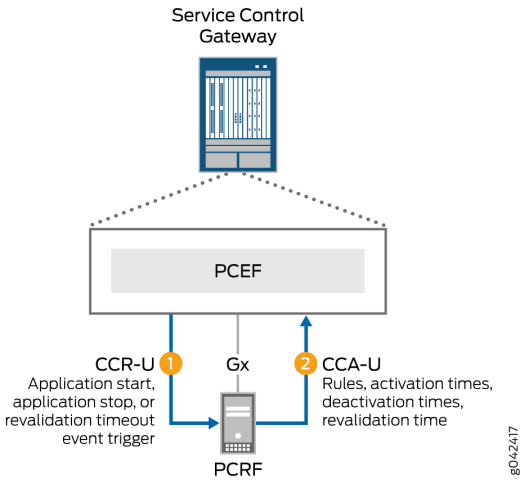
Figure 6: Message Flow for Pull Mode During TDF Subscriber Creation



- Pull mode after PCEF event trigger—Applies when the PCEF sends an event trigger to the PCRF. This can occur when the MX Series router detects a new application start or stop or when the revalidation time has occurred. The PCEF sends a credit control request update (CCR-U) message along with the appropriate event trigger to the PCRF. The PCRF might download new rules to the PCEF in a credit control answer update (CCA-U) message, which may also include any activation and deactivation times that apply to the rules and the time at which the PCEF must re-request PCC rules

from the PCRF. Figure 7 on page 62 shows the message flow for a pull procedure after a PCEF event trigger.

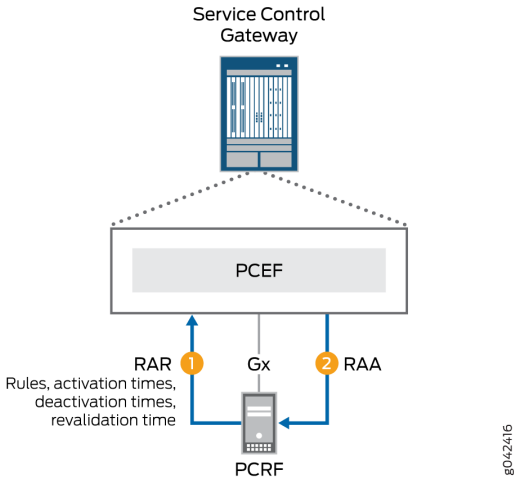
Figure 7: Message Flow for Pull Mode After PCEF Event Trigger



- Push mode—Applies when the PCRF provisions PCC rules without obtaining a request from the PCEF. The PCRF sends the PCC rules in a re-authorization request (RAR) to the PCEF based on information sent to the PCRF through the Rx interface or in response to a trigger within the PCRF. The RAR may also include any activation and deactivation times that apply to the rules and the time at which the PCEF must re-request PCC rules from the PCRF. The PCRF includes these PCC rules in an RAR message because the PCC rules were not requested by the PCEF, and no credit control request (CCR) or credit control answer (CCA) messages are triggered by the RAR. The PCEF responds

with a re-authorization answer (RAA) message. Figure 8 on page 63 shows the message flow for a push procedure.

Figure 8: Message Flow for Push Mode



RELATED DOCUMENTATION

- Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | 52
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | 56
- Configuring Dynamic Policy Control by PCRF | 76

Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Statically

Static policy control is enabled when a static-policy-control policy and charging enforcement function (PCEF) profile is assigned to a subscriber. The policy and charging control (PCC) rules that you configure on the MX Series router and assign to the PCEF profile are active, and are *not* controlled by the policy and charging rules function (PCRF) or RADIUS server.

RELATED DOCUMENTATION

- Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | 52

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | 56

Configuring Static Policy Control | 77

Understanding How a RADIUS Server Controls Policy and Charging Control Rules

IN THIS SECTION

- Rule Activation When TDF Session Begins | 64
- Rule Activation and Deactivation When RADIUS Server Sends Request | 65
- Supported Attributes in RADIUS Messages | 66

Policy control by a RADIUS server takes place when an aaa-policy-control policy and charging enforcement function (PCEF) profile is assigned to a subscriber. A RADIUS server activates and deactivates policy and charging control (PCC) rules that you have configured on the MX Series router and assigned to the PCEF profile. A network element, which is a load-balanced group of RADIUS servers, is assigned to the subscriber.

This topic includes the following sections:

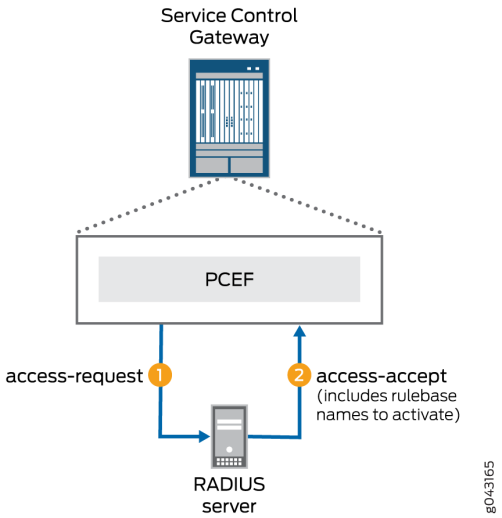
Rule Activation When TDF Session Begins

When the traffic detection function (TDF) subscriber session begins, the Junos Subscriber Aware PCEF sends an access request to the RADIUS server. This is shown in Figure 9 on page 65. This access request includes the subscriber username, IP address, and other relevant AVP information that Subscriber Aware received from the broadband network gateway or Packet Data Network Gateway during the subscriber session setup.

The RADIUS server responds to the PCEF with an access-accept message, which contains the names of the rulebases to activate. You can configure the AVP that carries the name of a rulebase to be activated;

by default the PCEF looks for a rulebase name in the ERX-Service-Activate Juniper vendor-specific attributes (VSA).

Figure 9: RADIUS Server Message Flow When TDF Session Begins

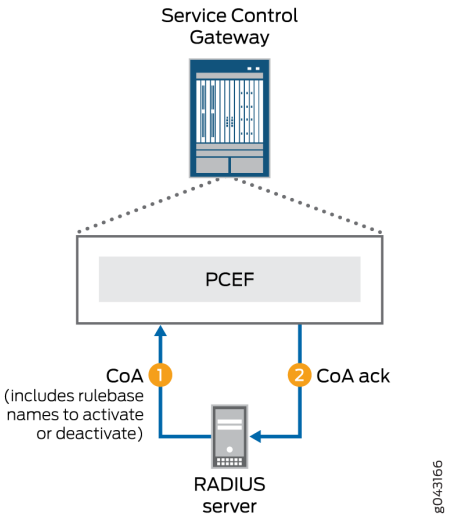


Rule Activation and Deactivation When RADIUS Server Sends Request

The RADIUS server can initiate the activation or deactivation of rulebases by sending a change of authorization (CoA) request to the PCEF, as shown in Figure 10 on page 66. You can configure the AVP that carries the name of a rulebase to be activated; by default the PCEF looks for a rulebase name in the ERX-Service-Activate Juniper VSA. You can also configure the AVP that carries the name of a rulebase to be deactivated; by default the PCEF looks for a rulebase name in the ERX-Service-Deactivate Juniper VSA.

The PCEF responds to the CoA request by sending a CoA Ack to the RADIUS server.

Figure 10: Message Flow When RADIUS Server Sends Request



Supported Attributes in RADIUS Messages

The following tables list the RADIUS attributes, 3GPP VSAs, and Juniper Networks VSAs that are supported in the RADIUS messages between the MX Series router and a RADIUS server.

Table 2 on page 67 lists the RADIUS attributes and 3GPP VSAs that are supported in the access-request messages sent to the RADIUS server.

Table 2: Attributes Supported in Access-Request Messages

Attribute Number	Attribute Name	Description	Content
1	User-Name	Username for the TDF subscriber if it is provided in the RADIUS accounting request received from the Packet Data Network Gateway (PGW) or broadband network gateway (BNG). This is a RADIUS IETF attribute.	String
2	User-Password	User password configured in the subscriber's PCEF profile. This is a RADIUS IETF attribute.	String
4	NAS-IP-Address	IPv4 address of the MX Series router for communication with the RADIUS server. This is a RADIUS IETF attribute.	IPv4 address
8	Framed-IP-Address	IPv4 address for the TDF subscriber if it is provided in the RADIUS accounting request received from the PGW or BNG. This is a RADIUS IETF attribute.	IPv4 address

Table 2: Attributes Supported in Access-Request Messages *(Continued)*

Attribute Number	Attribute Name	Description	Content
31	Calling-Station-ID	Identifier for the mobile station of the TDF subscriber if it is provided in the RADIUS accounting request received from the PGW or BNG. This is a RADIUS IETF attribute.	MSISDN in international format, UTF-8 encoded decimal characters
32	NAS-Identifier	Identifier of the NAS originating the request. This is a RADIUS IETF attribute.	String
44	Acct-Session-ID	User Session identifier generated by Subscriber Aware for the TDF subscriber. This is a RADIUS IETF attribute.	UTF-8 encoded string
97	Framed-IPv6-Prefix	IPv6 prefix for the TDF subscriber if it is provided in the RADIUS accounting request received from the PGW or BNG. This is a RADIUS IETF attribute.	Value indicating the prefix, as specified in RFC 3162
26/10415/1 (3GPP type 1)	3GPP-IMSI	IMSI for the TDF subscriber if it is provided in the RADIUS accounting request received from the PGW or BNG. This is a 3GPP VSA.	UTF-8 encoded string

Table 3 on page 69 lists the VSAs that are supported in the Access-Accept messages sent from the RADIUS server to the PCEF.

Table 3: Attributes Supported in Access-Accept Messages

Attribute Number	Attribute Name	Description	Content
26-65	ERX-Service-Activate	Specifies a PCC rulebase to activate for the subscriber. Tagged VSA, which supports 8 tags (1-8). This is a Juniper Networks VSA and is the default VSA for carrying rulebase activations; you can also specify a different AVP code and vendor ID.	string: *rulebase-name*

Table 4 on page 69 lists the VSAs that are supported in the CoA messages sent from the RADIUS server to the PCEF.

Table 4: Attributes Supported in CoA Messages

Attribute Number	Attribute Name	Description	Content
26-65	ERX-Service-Activate	Specifies a PCC rulebase to activate for the subscriber. Tagged VSA, which supports 8 tags (1-8). This is a Juniper Networks VSA and is the default VSA for carrying rulebase activations; you can also specify a different AVP code and vendor ID.	string: *rulebase-name*

Table 4: Attributes Supported in CoA Messages *(Continued)*

Attribute Number	Attribute Name	Description	Content
26-66	ERX-Service-Deactivate	Specifies a PCC rulebase to deactivate for the subscriber. This is a Juniper Networks VSA and is the default VSA for carrying rulebase deactivations; you can also specify a different AVP code and vendor ID.	string: *rulebase-name*

RELATED DOCUMENTATION

- Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | **52**
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | **56**
- Configuring Policy Control by RADIUS Servers | **78**

Understanding PCEF Profiles

A policy and charging enforcement function (PCEF) profile defines whether policy and charging control (PCC) rules for a subscriber are under static control, under dynamic control of the policy and charging rules function, or under activation/deactivation control of a RADIUS server by using the **static-policy-control**, **dynamic-policy-control**, or **aaa-policy-control** statement, respectively, in the PCEF profile configuration. The PCEF profile also identifies the predefined PCC rules and rulebases that the subscriber can use, and assigns a precedence value to each predefined rule. A subscriber is assigned a PCEF profile during the TDF subscriber session setup. See "Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber" on page 112.

A PCEF profile with dynamic policy control requires a Diameter Gx profile, which provides network access information for the Diameter application.

A PCEF profile with RADIUS server control requires an AAA profile, which provides the policy control attributes for RADIUS servers.

RELATED DOCUMENTATION

- Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | 52
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | 56
- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Dynamic Policies | 98
- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Static Policies | 100
- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Policies That a RADIUS Server Controls | 101
- Understanding Static Time-of-Day PCC Rule Activation and Deactivation | 74

Understanding Network Elements

IN THIS SECTION

- Load Balancing Within Network Elements | 71
- Server Priority | 72
- Dead Server Detection | 72
- Maximum Pending Requests for a Network Element | 72

A network element is a load-balanced group of RADIUS servers providing policy management for TDF subscribers.

Network elements are specified in the AAA profile that is applied to a policy and charging enforcement function (PCEF) profile. A subscriber is assigned to a PCEF profile.

Load Balancing Within Network Elements

The Junos Subscriber Aware PCEF distributes requests to RADIUS servers across the servers in the network element.

Server Priority

Within a network element, a RADIUS server can be assigned a priority of 1 through 16, with 1 being the highest priority. You can have multiple servers with the same priority in a network element. All access requests are load balanced among the highest priority servers. If all the servers with the highest priority in the network element fail, then requests are load balanced among servers with the next highest priority level.

Dead Server Detection

To determine whether a RADIUS server in a network element has failed, the PCEF keeps track of how often requests sent to a server time out and must be retransmitted. If the number of times that requests need to be retransmitted reaches a configured limit within a configured time interval, PCEF marks the server as **dead** and starts sending requests to the next available server in the network element with the same priority.

At the same time, the PCEF starts a timer for the RADIUS server. After this timer expires, the PCEF marks the dead server as alive again, and includes it in the rotation for sending RADIUS messages.

Maximum Pending Requests for a Network Element

You can configure the maximum number of requests that can be queued to the network element. When the pending request queue is full, any additional requests are dropped.

You can also configure a high and a low watermark that are percentages of the maximum number of requests that can be queued. If the number of pending requests reaches this high watermark, a **flow control on** message is generated. When the number of pending requests then falls below the low watermark, a **flow control off** message is generated.

RELATED DOCUMENTATION

Configuring RADIUS Network Elements | 94

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

Understanding AAA Profiles

IN THIS SECTION

- Network Elements | 73
- RADIUS Attributes That Carry Rulebase Names for Activation and Deactivation | 73

An AAA profile is a collection of attributes to specify how the Junos Subscriber Aware PCEF interacts with RADIUS servers that control the activation and deactivation of policy and charging control (PCC) rules. An AAA profile is assigned to a subscriber's policy and charging enforcement function (PCEF) profile, which specifies the PCC rulebases for the subscriber.

Network Elements

In the AAA profile, you specify a network element (load-balanced RADIUS server group) to be used for authorization of policy control. If the RADIUS servers in a Network Element cannot initiate a change of authorization (CoA) request without an accounting record, then the AAA profile must specify the network element for accounting as well as for authorization, and the AAA profile must enable CoA accounting.

RADIUS Attributes That Carry Rulebase Names for Activation and Deactivation

You can specify the RADIUS AVPs that carry the PCC rulebase names for activation or deactivation. By default, the PCC rulebase name for activations is carried in the ERX-Service-Activate Juniper vendor-specific attributes (VSA). By default, the PCC rulebase name for deactivations is carried in the ERX-Service-Deactivate Juniper VSA.

RELATED DOCUMENTATION

- Configuring an AAA Profile | 96
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

Understanding Static Time-of-Day PCC Rule Activation and Deactivation

With static time-of-day policy and charging control (PCC) rules activation and deactivation, you can specify a schedule for activating and deactivating PCC rules or rulebases within a static PCEF profile. The rule or rulebase activation and deactivation settings take effect for subscribers assigned to that static PCEF profile.

The activation and deactivation settings can consist of the time of day, the day, and the month of the year. The day can be expressed as a day of the week, as a numbered day of the month, or as the last day of the current month. If a day is not specified, then the rule activation and deactivation occurs daily at the specified times. If you configure a day of the month, you can also configure a month of the year.

If a day is not specified and the deactivation time of day setting is earlier than the activation time of day setting, then a rule is deactivated the day after it is activated.

If a time zone is configured on the router, the time-of-day settings apply to the configured time zone and are adjusted for transitions to and from daylight saving time.

You cannot use static time-of-day settings for dynamic PCC rules.

RELATED DOCUMENTATION

- Configuration of Static Time-of-Day PCC Rule Activation and Deactivation Overview | **102**
- Configuring the NTP Server | **103**
- Configuring Static Time-of-Day PCC Rule Activation and Deactivation in a Junos OS Subscriber Aware PCEF Profile | **103**
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | **56**

Understanding Usage Monitoring for TDF Subscribers

IN THIS SECTION

- Tracked Resource Identification | **75**
- Threshold Configuration | **75**
- Messages and AVPs That Are Used | **75**

For TDF subscribers that are assigned to a dynamic policy and charging enforcement function (PCEF) profile, you can monitor the subscriber use during a session as a volume of traffic, an amount of time, or both, and send reports to the policy and charging rules function (PCRF) when a threshold is exceeded or when the PCRF requests a report. Data volume and the amount of time used can be tracked for individual or multiple data flows or applications that appear in specific policy and charging control (PCC) rules, or for the entire subscriber session.

This topic includes the following sections:

Tracked Resource Identification

Data usage for a subscriber session is tracked through an object called a monitoring key, which the PCRF configures. Traffic for a particular data flow, application, or combination of data flows and applications can be tracked as a data set by assigning a monitoring key to the PCC rules that identify those flows or applications. For predefined PCC rules, you specify the monitoring key with the PCC rule's action profile. For dynamic PCC rules, the PCRF specifies the monitoring key for a rule.

Data usage can also be tracked for the entire TDF subscriber session by configuring the monitoring key level as SESSION.

Threshold Configuration

The PCRF specifies a threshold for reporting data usage when it configures a monitoring key. The threshold can be a combination of uplink volume, downlink volume, total volume, and time used. The MX Series router reports the usage information to the PCRF when this limit is exceeded, and resets the volume to zero.

Messages and AVPs That Are Used

The PCRF must first request usage monitoring by sending the Event-Trigger AVP with the value USAGE_REPORT. This request can be sent to the MX Series router in a CCA-I, CCA-U, or RAR message.

The PCRF configures a monitoring key by sending a Usage Monitoring Information (UMI) AVP that includes the following in a CCA-I, CCA-U, or RAR message to the MX Series router:

- Monitoring-key AVP, which is the identifier.
- Granted-Service-Unit AVP, which specifies the volume threshold, time threshold, or both.
- Usage-Monitoring-Level AVP, which indicates whether the monitoring key applies to the entire subscriber session or to particular PCC/ePCC rules.

The PCRF requests usage monitoring for traffic that matches a PCC rule's data flows or applications by sending the following in a CCA-I, CCA-U, or RAR message to the MX Series router:

- Charging-Rule-Definition AVP, which identifies the rule.
- UMI AVP that includes the Monitoring-key AVP, which identifies the monitoring key to which the rule is associated.

The MX Series router reports usage to the PCRF by sending a UMI AVP that includes the following in a CCR-U message:

- Monitoring-key AVP, which is the identifier.
- Used-Service-Unit AVP, which gives a combination of uplink volume, downlink volume, total volume, and time used.

The PCRF can request a usage report, regardless of whether the threshold is reached, by sending a UMI AVP that includes the following in a CCA-U or RAR message:

- Monitoring-key AVP, which is the identifier.
- Usage-Monitoring-Report AVP, which is set to the value USAGE_MONITORING_REPORT_REQUIRED (0).

The PCRF requests that usage monitoring be disabled for a monitoring key by sending a UMI AVP that includes the following in a CCA-U or RAR message:

- Monitoring-key AVP, which is the identifier.
- Usage-Monitoring-Support, which is set to the value USAGE_MONITORING_DISABLED (0).

RELATED DOCUMENTATION

IP-Based Subscriber Setup Overview | 107

Configuring TDF Subscriber Usage Monitoring for Traffic That Matches Predefined PCC Rules | 105

Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Dynamically by a PCRF | 58

Configuring Dynamic Policy Control by PCRF

You can configure policy management that is dynamically controlled by the policy and charging rules function (PCRF), which can both provision policy and charging control (PCC) rules on the MX Series router and activate PCC rules that are predefined on the MX Series router.

To configure policy management that is dynamically controlled by a PCRF:

1. (Optional) Configure any flow identifiers to be used in PCC rules.

See "Configuring Service Data Flow Filters" on page 79.

2. (Optional) Configure any custom applications to be used in PCC rules.

   See "Configuring Custom Application Signatures" on page 26.

3. (Optional) Configure the PCC action profiles to be used in PCC rules.

   See "Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware" on page 83

4. (Optional) Configure PCC rules.

   See "Configuring Policy and Charging Control Rules" on page 86.

5. (Optional) Configure PCC rulebases.

   See "Configuring a Policy and Charging Control Rulebase" on page 89.

6. Configure a Diameter Gx profile.

   See "Configuring Diameter Profiles" on page 152.

7. Configure a dynamic PCEF profile.

   See "Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Dynamic Policies" on page 98

8. (Optional) Configure an NTP server if you want the PCRF to send activation, deactivation, or revalidation times.

   See "Configuring the NTP Server" on page 103.

RELATED DOCUMENTATION

Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | 52

Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Dynamically by a PCRF | 58

Configuring Static Policy Control

You can configure static policy management that is controlled entirely by predefined policy and charging control (PCC) rules that you have configured on the MX Series router.

To configure static policy control:

1. Configure any flow identifiers to be used in PCC rules.

   See "Configuring Service Data Flow Filters" on page 79.

2. Configure any custom applications to be used in PCC rules.

   See "Configuring Custom Application Signatures" on page 26.

3. Configure the PCC action profiles to be used in PCC rules.

See "Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware" on page 83

4. Configure PCC rules.

   See "Configuring Policy and Charging Control Rules" on page 86.

5. (Optional) Configure PCC rulebases.

   See "Configuring a Policy and Charging Control Rulebase" on page 89.

6. Configure a policy and charging enforcement function (PCEF) profile for static policy control.

   See "Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Static Policies" on page 100

RELATED DOCUMENTATION

- Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | 52
- Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Statically | 63

Configuring Policy Control by RADIUS Servers

You can configure policy management that is controlled by RADIUS servers. A RADIUS server activates and deactivates policy and charging control (PCC) rules that have been configured on the MX Series router.

To configure policy management that is controlled by RADIUS servers:

1. Configure any flow identifiers to be used in PCC rules.

   See "Configuring Service Data Flow Filters" on page 79.

2. Configure any custom applications to be used in PCC rules.

   See "Configuring Custom Application Signatures" on page 26.

3. Configure the PCC action profiles to be used in PCC rules.

   See "Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware" on page 83

4. Configure PCC rules.

   See "Configuring Policy and Charging Control Rules" on page 86.

5. Configure PCC rulebases.

   See "Configuring a Policy and Charging Control Rulebase" on page 89.

6. Configure RADIUS servers.

   See "Configuring RADIUS Servers" on page 91.

7. Configure RADIUS network elements.

   See "Configuring RADIUS Network Elements" on page 94.

8. Configure an AAA profile.

   See "Configuring an AAA Profile" on page 96.

9. Configure a policy and charging enforcement function (PCEF) profile for policy control by a RADIUS server.

   See "Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Policies That a RADIUS Server Controls" on page 101

RELATED DOCUMENTATION

Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | 52

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

Configuring Service Data Flow Filters

NOTE: Starting in Junos OS Release 19.3R2, PCC rules are also supported if you have enabled Next Gen Services on the MX240, MX480 or MX960 router with the MX-SPC3 card.

A service data flow (SDF) filter is specified as a matching condition in the **from** clause of a policy and charging control (PCC) rule. Each SDF filter can have one or more flows associated with it; each flow is a five-tuple match.

NOTE: If you configure an SDF filter without specifying a remote address, port, port range, or protocol , then the SDF filter matches IP packets that have any value configured for the corresponding attribute. If you configure an SDF filter, you must configure at least one of the following attributes: direction, local port or local port range, protocol, remote address, or remote port or remote port range.

You can configure SDF filters for Junos OS Subscriber Aware or for Junos OS Broadband Subscriber Management, but you use a different CLI hierarchy level for each product.

- If you are using Junos OS Subscriber Aware, configure SDF filters at the **[edit unified-edge pcef]** hierarchy level.

- If you are using Junos OS Broadband Subscriber Management, configure SDF filters at the **[edit services pcef]** hierarchy level.

To configure Layer 3 and Layer 4 SDF filters:

1. Specify a name for the SDF filter.

   For Junos OS Subscriber Aware:

   ```
   [edit unified-edge pcef]
   user@host# set flow-descriptions flow-identifier
   ```

   For Junos OS Broadband Subscriber Management:

   ```
   [edit services pcef]
   user@host# set flow-descriptions flow-identifier
   ```

2. Specify the flow direction for the SDF filter.

   NOTE: If you do not specify a flow direction, then the SDF filter is applied in both the uplink and downlink directions.

   For Junos OS Subscriber Aware:

   ```
   [edit unified-edge pcef flow-descriptions flow-identifier]
   user@host# set direction (uplink | downlink | both)
   ```

   For Junos OS Broadband Subscriber Management:

   ```
   [edit services pcef flow-descriptions flow-identifier]
   user@host# set direction (uplink | downlink | both)
   ```

3. Specify a remote address (IPv4 or IPv6) for the SDF filter:

   NOTE: You can specify an IPv4 subnet or an IPv6 subnet but not both.

   - Specify an IPv4 address for the SDF filter.

For Junos OS Subscriber Aware:

```
[edit unified-edge pcef flow-descriptions flow-identifier]
user@host# set remote-address ipv4-address ipv4-address
```

For Junos OS Broadband Subscriber Management:

```
[edit services pcef flow-descriptions flow-identifier]
user@host# set remote-address ipv4-address ipv4-address
```

- Specify an IPv6 address for the SDF filter.

  For Junos OS Subscriber Aware:

  ```
  [edit unified-edge pcef flow-descriptions flow-identifier]
  user@host# set remote-address ipv6-address ipv6-address
  ```

  For Junos OS Broadband Subscriber Management:

  ```
  [edit services pcef flow-descriptions flow-identifier]
  user@host# set remote-address ipv6-address ipv6-address
  ```

4. Specify a protocol (using the standard protocol number) for the SDF filter.

   For Junos OS Subscriber Aware:

   ```
   [edit unified-edge pcef flow-descriptions flow-identifier]
   user@host# set protocol number
   ```

   For Junos OS Broadband Subscriber Management:

   ```
   [edit services pcef flow-descriptions flow-identifier]
   user@host# set protocol number
   ```

5. Specify a local port or a list of port numbers for the SDF filter. To specify a list of port numbers (up to a maximum of three), enclose the port numbers in square brackets ([]).

NOTE: You can configure a local port or local port range but not both in the same SDF filter.

For Junos OS Subscriber Aware:

```
edit unified-edge pcef flow-descriptions flow-identifier]
user@host# set local-ports number
```

For Junos OS Broadband Subscriber Management:

```
edit services pcef flow-descriptions flow-identifier]
user@host# set local-ports number
```

6. Specify a local port range for the SDF filter.

   For Junos OS Subscriber Aware:

```
[edit unified-edge pcef flow-descriptions flow-identifier]
user@host# set local-port-range low low-value high high-value
```

   For Junos OS Broadband Subscriber Management:

```
[edit services pcef flow-descriptions flow-identifier]
user@host# set local-port-range low low-value high high-value
```

7. Specify a remote port or list of remote ports for the SDF filter. To specify a list of port numbers (up to a maximum of three), enclose the port numbers in square brackets ([]).

   NOTE: You can configure a remote port or remote port range but not both in the same SDF filter.

   For Junos OS Subscriber Aware:

```
[edit unified-edge pcef flow-descriptions flow-identifier]
user@host# set remote-ports number
```

For Junos OS Broadband Subscriber Management:

```
[edit services pcef flow-descriptions flow-identifier]
user@host# set remote-ports number
```

8. Specify a remote port range for the SDF filter.

   For Junos OS Subscriber Aware:

```
[edit unified-edge pcef flow-descriptions flow-identifier]
user@host# set remote-port-range low low-value high high-value
```

   For Junos OS Broadband Subscriber Management:

```
[edit services pcef flow-descriptions flow-identifier]
user@host# set remote-port-range low low-value high high-value
```

RELATED DOCUMENTATION

- *Configuring Application-Aware Policy Control for Subscriber Management*
- *Understanding Application-Aware Policy Control for Subscriber Management*
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment
- *Configuring Policy and Charging Control Rules*

Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware

A PCC action profile defines the treatment to be applied to specific service data flows or to packets associated with specific applications. A PCC action profile is specified in the **then** clause of a PCC rule.

NOTE: To make a change to a PCC action profile, you must be in maintenance mode. (See "Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles" on page 220).

To configure PCC action profiles:

1. Specify a name for the PCC action profile.

```
[edit unified-edge pcef]
user@host# edit pcc-action-profiles profile-name
```

2. Configure the maximum bit rate for uplink and downlink subscriber traffic.

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set maximum-bit-rate uplink mbr-uplink-value downlink mbr-downlink-value
```

   The range is 0 through 6144000 Kbps.

3. Configure HTTP redirection to a URL.

```
[edit unified-edge pcef pcc-action-profiles profile-name redirect]
user@host# set url url-name
```

   NOTE: A PCC action profile that includes HTTP redirection can only be used in PCC rules that match only HTTP-based applications and all flows.

4. Configure the steering of traffic to a third-party server for applying services or to a service chain with one of the following methods:

   - Specify the IP address of the third-party server for HTTP traffic.

```
[edit unified-edge pcef pcc-action-profiles profile-name steering path]
user@host# set (ipv4-address ipv4-address | set ipv6-address ipv6-address)
```

     NOTE: A PCC action profile that includes a steering path can only be used in PCC rules that match only HTTP-based applications and all flows.

   - Specify the routing instance to use to reach the third-party server or service chain.

```
[edit unified-edge pcef pcc-action-profiles profile-name steering]
user@host# set routing-instance downlink downlink-vrf-name uplink uplink-vrf-name
```

The downlink routing instance is applied to traffic going to the access side, and the uplink routing instance is applied to traffic being sent from the access side.

5. Specify that steering attributes configured in a PCC action profile that a PCC rule applies to a data flow session when it begins will continue to be applied to the data flow when the PCC rule match conditions are modified, deleted, or added to.

```
[edit unified-edge pcef pcc-action-profiles profile-name steering]
user@host# set keep-existing-steering
```

6. Specify the HCM profile that you want to use for determining which HTTP header enrichment rules are applied.

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set hcm-profile hcm-profile-name
```

NOTE: A PCC action profile that includes an HCM profile can only be used in PCC rules that match only HTTP-based applications and all flows.

7. Specify the forwarding class that you want packets to be assigned.

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set forwarding-class class-name
```

8. Configure the gating status by enabling or disabling the forwarding of packets.

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set gate-status (disable-both | downlink | uplink | uplink-downlink)
```

RELATED DOCUMENTATION

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | 56

Configuring Policy and Charging Control Rules | 86

Configuring TDF Subscriber Usage Monitoring for Traffic That Matches Predefined PCC Rules | 105

Configuring Policy and Charging Control Rules

A policy and charging control (PCC) rule defines the treatment to be applied to packets associated with specific applications or to specific service data flows.

You can configure PCC rules for Junos OS Subscriber Aware or for Junos OS Broadband Subscriber Management, but you use a different CLI hierarchy level for each product.

- If you are using Junos OS Subscriber Aware, configure PCC rules at the **[edit unified-edge pcef]** hierarchy level.
- If you are using Junos OS Broadband Subscriber Management, configure PCC rules at the **[edit services pcef]** hierarchy level.

NOTE: If you are using Junos OS Subscriber Aware, you must be in maintenance mode to make a change to a PCC rule. (See Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles).

NOTE: If you are using Junos OS Broadband Subscriber Management, you cannot change a PCC rule while it is being used by a subscriber. To modify the rule, you must log off the subscribers that are using the rule.

Before you configure PCC rules, you must do the following:

- Configure the service data flow (SDF) filters that the PCC rules reference.
- Configure the application groups and any custom applications that you want to reference in application-aware PCC rules.
- Configure the PCC action profiles that the PCC rules reference.

NOTE: When specifying application-aware PCC rules in a PCEF profile, you must also configure a default Layer 3 or Layer 4 wildcard PCC rule to ensure that the default charging characteristics are applied to unmatched subscriber traffic without dropping that traffic. For example, the default Layer 3 or Layer 4 wildcard PCC rule prevents traffic based on DNS queries from being dropped. In addition, the policy (PCEF profile) that includes application-aware PCC rules must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

To configure PCC rules:

1. Specify a name for the PCC rule.

   For Junos OS Subscriber Aware:

   ```
   [edit unified-edge pcef]
   user@host# edit pcc-rules rule-name
   ```

   For Junos OS Broadband Subscriber Management:

   ```
   [edit services pcef]
   user@host# edit pcc-rules rule-name
   ```

2. In a **from** statement, specify an SDF filter to use Layer 3 or Layer 4 match conditions for filtering subscriber traffic.

   For Junos OS Subscriber Aware:

   ```
   [edit unified-edge pcef pcc-rules  rule-name]
   user@host# set from flows flow-identifier
   ```

   For Junos OS Broadband Subscriber Management:

   ```
   [edit services pcef pcc-rules  rule-name]
   user@host# set from flows flow-identifier
   ```

   If you do not want to filter subscriber traffic based on SDF filters, use the **any** option.

   For Junos OS Subscriber Aware:

   ```
   [edit unified-edge pcef pcc-rules  rule-name]
   user@host# set from flows any
   ```

   For Junos OS Broadband Subscriber Management:

   ```
   [edit services pcef pcc-rules  rule-name]
   user@host# set from flows any
   ```

3. (Optional) Specify an application as a match condition for filtering subscriber traffic.

For Junos OS Subscriber Aware:

```
[edit unified-edge pcef pcc-rules  rule-name]
user@host# set from applications application-name
```

For Junos OS Broadband Subscriber Management:

```
[edit services pcef pcc-rules  rule-name]
user@host# set from applications application-name
```

4. (Optional) Specify multiple applications instead of specifying each application separately by specifying an application group as a match condition for filtering subscriber traffic.

   For Junos OS Subscriber Aware:

   ```
   [edit unified-edge pcef pcc-rules rule-name]
   user@host# set from application-groups application-group-name
   ```

   For Junos OS Broadband Subscriber Management:

   ```
   [edit services pcef pcc-rules rule-name]
   user@host# set from application-groups application-group-name
   ```

5. Specify the PCC rules action profile that defines the treatment to be applied to specific service data flows or to packets associated with specific applications.

   NOTE: You can use PCC action profiles with HTTP redirection or HCM profiles only in PCC rules that match only HTTP-based applications and any flows.

   For Junos OS Subscriber Aware:

   ```
   [edit unified-edge pcef pcc-rules rule-name]
   user@host# set then pcc-action-profile profile-name
   ```

For Junos OS Broadband Subscriber Management:

```
[edit services pcef pcc-rules rule-name]
user@host# set then pcc-action-profile profile-name
```

RELATED DOCUMENTATION

- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment
- *Understanding Application-Aware Policy Control for Subscriber Management*
- Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware
- *Configuring Policy and Charging Control Action Profiles for Subscriber Management*
- *Configuring Service Data Flow Filters*
- *Configuring Custom Application Signatures*

Configuring a Policy and Charging Control Rulebase

A policy and charging control (PCC) rulebase contains a set of PCC rules. Each rule specified in the PCC rulebase is assigned a precedence to designate the priority in which PCC rules are evaluated for selection in a policy and charging enforcement function (PCEF) profile.

NOTE: Starting in Junos OS Release 19.3R1, application-aware policy control is also supported for Broadband Subscriber Management if you have enabled Next Gen Services on the MX240, MX480 or MX960 router with the MX-SPC3 card.

You can configure PCC rulebases for Junos OS Subscriber Aware or for Junos OS Broadband Subscriber Management, but you use a different CLI hierarchy level for each product.

- If you are using Junos OS Subscriber Aware, configure PCC rulebases at the **[edit unified-edge pcef]** hierarchy level.
- If you are using Junos OS Broadband Subscriber Management, configure PCC rulebases at the **[edit services pcef]** hierarchy level.

NOTE: If you are using Junos OS Subscriber Aware, you must be in maintenance mode to make a change to a PCC rulebase. (See Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles).

NOTE: If you are using Junos OS Broadband Subscriber Management, you cannot change a PCC rulebase while it is being used by a subscriber. To modify the rulebase, you must log off the subscribers that are using the rule.

Before you configure a PCC rulebase, you must do the following:

- Configure service data flow filters.
- Configure PCC action profiles.
- Configure PCC rules.

To configure a PCC rulebase:

1. Specify a name for the rulebase.

   For Junos OS Subscriber Aware:

   ```
   [edit unified-edge pcef ]
   user@host#   edit pcc-rulebases rulebase-name
   ```

   For Junos OS Broadband Subscriber Management:

   ```
   [edit services pcef ]
   user@host#   edit pcc-rulebases rulebase-name
   ```

2. Specify the PCC rules that the rulebase references and a precedence value (1 through 65,535) for each rule.

   NOTE:

   - The same rule can be configured in different rulebases and can have a different precedence.

- The precedence assigned must be unique among the configured PCC rules.
- A lower precedence value indicates a higher precedence. For example, if a PCC rulebase has two PCC rules with precedence 5 and 10 respectively, the PCC rule with precedence 5 is evaluated first.

For Junos OS Subscriber Aware:

```
[edit unified-edge pcef pcc-rulebases rulebase-name]
user@host#   set pcc-rule rule-name precedence number
user@host#   set pcc-rule rule-name precedence number
user@host#   set pcc-rule rule-name precedence number
```

For Junos OS Broadband Subscriber Management:

```
[edit services pcef pcc-rulebases rulebase-name]
user@host#   set pcc-rule rule-name precedence number
user@host#   set pcc-rule rule-name precedence number
user@host#   set pcc-rule rule-name precedence number
```

RELATED DOCUMENTATION

Configuring Policy and Charging Control Rules

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment

Understanding Application-Aware Policy Control for Subscriber Management

Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF)

Configuring RADIUS Servers

You must configure RADIUS servers before you can configure a RADIUS network element. A network element is a load-balanced group of RADIUS servers providing policy management for TDF subscribers.

To configure a RADIUS server:

1. Configure a name for the RADIUS server.

```
[edit access radius]
user@host# set servers name
```

2. Specify the IP address of the RADIUS server.

```
[edit access radius servers name]
user@host# set address server-address
```

3. Configure an interface and IPv4 address to specify the source for RADIUS requests. The MX Series router sends RADIUS requests to the RADIUS server using this source address.

```
[edit access radius servers name]
user@host# set source-interface interface [ipv4-address address]
```

4. Configure a shared secret (password) to be used by the MX Series router and the RADIUS server.

```
[edit access radius servers name]
user@host# set secret password
```

5. Configure the port number to which the RADIUS requests are sent.

```
[edit access radius servers name]
user@host# set port port-number
```

6. Specify the RADIUS server port number to which the MX Series router sends RADIUS accounting-start and accounting-stop requests. RADIUS accounting-start and accounting-stop requests are used when the RADIUS server is not able to initiate a change of authorization (CoA) request without an accounting record.

```
[edit access radius servers name]
user@host# set accounting-port port-number
```

7. Configure the secret password to be used when sending accounting-start requests to the RADIUS server if the accounting secret password is different from the authentication secret password.

RADIUS accounting-start requests are used when the RADIUS server is not able to initiate a CoA request without an accounting record.

```
[edit access radius servers name]
user@host# set accounting-secret password
```

8. Configure the number of attempts to contact the RADIUS server that the MX Series router is allowed to make when it does not receive a response to its initial request. You can specify from 1 through 10 retries. The default is 3.

```
[edit access radius servers name]
user@host# set retry attempts
```

9. Configure the amount of time that the MX Series router waits to receive a response from a RADIUS server before retrying a request. By default, the MX Series router waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

```
[edit access radius servers name]
user@host# set timeout seconds
```

10. Allow dynamic requests from the RADIUS server so that CoA requests can be received.

```
[edit access radius servers name]
user@host# set allow-dynamic-requests
```

11. Configure the secret password to be used for CoA requests from the RADIUS server.

```
[edit access radius servers name]
user@host# set dynamic-requests-secret password
```

12. Configure a limit to the number of request retries within a specified time interval that the MX Series router can send to the RADIUS server. If the number of retries reaches this limit, the RADIUS server is marked as dead, and the MX Series router begins to send requests to other RADIUS servers in the network element.

```
[edit access radius servers name]
user@host# set dead-criteria-retries retry-number interval seconds
```

13. Configure the amount of time that must pass after a RADIUS server is first marked dead until it is marked as alive by the MX Series router. When the MX Series router marks the RADIUS server as alive, it can again send requests to the RADIUS server.

```
[edit access radius servers name]
user@host# set revert-interval seconds
```

RELATED DOCUMENTATION

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

Configuring RADIUS Network Elements

A network element is a load-balanced group of RADIUS servers providing policy management for TDF subscribers.

Before you configure a network element, you must do the following:

- Configure the RADIUS servers that are to be part of the network element.

To configure a network element:

1. Specify a name for the network element.

```
[edit access radius]
user@host# set network-elements name
```

2. Specify the RADIUS servers that make up the network element.

```
[edit access radius network-elements name]
user@host# set server name
```

3. Assign each server in the network element a priority from 1 through 16 (1 is the highest priority). You can have multiple servers with the same priority in a network element. All access requests are load

balanced among the highest priority servers. If all the servers with the highest priority in the network element fail, then requests are load balanced among servers with the next highest priority level.

```
[edit access radius network-elements name server name]
user@host# set priority priority
```

4. Configure the maximum number of requests that can be queued to the network element. When the pending-request queue is full, any additional requests are dropped.

```
[edit access radius network-elements name]
user@host# set maximum-pending-reqs-limit number
```

5. Configure the pending-request queue high watermark for the network element. This is a percentage of the maximum number of requests that can be queued to the network element, which is configured in the **maximum-pending-reqs-limit *number*** statement. When the queue size reaches the high watermark, a **flow control on** message is generated.

```
[edit access radius network-elements name]
user@host# set pending-queue-watermark watermark
```

6. Configure the pending-request queue low watermark for the network element. This is a percentage of the maximum size of the pending-request queue, which is configured in the **maximum-pending-reqs-limit *watermark*** statement. When the number of pending requests drops below this low watermark value after having exceeded the high watermark, a **flow control off** message is generated.

```
[edit access radius network-elements name]
user@host# set pending-queue-watermark-abate abate-watermark
```

RELATED DOCUMENTATION

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

Understanding Network Elements | 71

Configuring RADIUS Servers | 91

Configuring an AAA Profile

An AAA profile is a collection of attributes to specify how the MX Series router interacts with RADIUS servers that control the activation and deactivation of policy and charging control (PCC) rules.

Before you configure an AAA profile, you must do the following:

- Configure the network elements that are to be included in the AAA profile.

To configure an AAA profile:

1. Configure a name for the AAA profile.

```
[edit unified-edge aaa]
user@host# set profiles aaa-profile-name
```

2. Specify the network element providing policy management for TDF subscribers.

```
[edit unified-edge aaa profiles aaa-profile-name radius authentication]
user@host# set network-element network-element-name
```

3. If the RADIUS servers in the network element providing policy management for TDF subscribers cannot initiate a change of authorization (CoA) request without an accounting record, specify that the network element is used for accounting.

```
[edit unified-edge aaa profiles aaa-profile-name radius accounting]
user@host# set network-element network-element-name
```

4. If the RADIUS servers in the network element providing policy management for TDF subscribers cannot initiate a CoA request without an accounting record, enable the initiation of a RADIUS accounting start from the MX Series router to the RADIUS servers.

```
[edit unified-edge aaa profiles aaa-profile-name radius policy]
user@host# set coa-accounting enable
```

5. Configure the RADIUS attribute that you want to carry the PCC rulebase name for rulebase activations from the RADIUS policy server to the MX Series router. By default, the rulebase name is carried in the ERX-Service-Activate Juniper vendor-specific attribute (VSA).

a. Specify the numeric value for the RADIUS AVP.

```
[edit unified-edge aaa profiles aaa-profile-name radius policy activation-
attribute]
user@host# set code numeric-code
```

b. If the RADIUS AVP is vendor-specific, specify the vendor identification.

```
[edit unified-edge aaa profiles aaa-profile-name radius policy activation-
attribute]
user@host# set vendor-id vendor-id
```

6. Configure the RADIUS attribute that you want to carry the PCC rulebase name for rulebase deactivations from the RADIUS policy server to the MX Series router. By default, the rulebase name is carried in the ERX-Service-Deactivate Juniper VSA.

a. Specify the numeric value for the RADIUS AVP.

```
[edit unified-edge aaa profiles aaa-profile-name radius policy
deactivation-attribute]
user@host# set code numeric-code
```

b. If the RADIUS AVP is vendor-specific, specify the vendor identification.

```
[edit unified-edge aaa profiles aaa-profile-name radius policy
deactivation-attribute]
user@host# set vendor-id vendor-id
```

RELATED DOCUMENTATION

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

Understanding AAA Profiles | 73

Configuring RADIUS Network Elements | 94

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Dynamic Policies

When a policy and charging enforcement function (PCEF) profile is configured with dynamic policy control, the policy and charging rules function (PCRF) can both provision policy and charging control (PCC) rules and activate PCC rules that are predefined on the Junos Subscriber Aware PCEF.

Before you configure a PCEF profile for dynamic policies, you must do the following:

- Configure a Diameter Gx profile.
- (Optional) Configure service data flow (SDF) filters.
- (Optional) Configure a PCC action profile.
- (Optional) Configure PCC rules, PCC rulebases, or both.

NOTE: You can add PCC rules or PCC rulebases to a dynamic PCEF profile without being in maintenance mode. To make other changes to a dynamic PCEF profile, you must be in maintenance mode.

NOTE: When a PCEF profile includes application-aware PCC rules, you must also include a default Layer 3 or Layer 4 wildcard PCC rule to ensure that the default charging characteristics are applied to unmatched subscriber traffic without dropping that traffic. For example, the default Layer 3 or Layer 4 wildcard PCC rule prevents traffic based on DNS queries from being dropped. In addition, the PCEF profile that includes application-aware PCC rules must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

To configure a PCEF profile for dynamic policies:

1. Specify a name for the PCEF profile.

```
[edit unified-edge pcef]
user@host#   edit profiles profile-name
```

2. Specify one or more PCC rules and a precedence for each rule for dynamic policy control. A lower precedence value indicates a higher precedence.

```
[edit unified-edge  pcef profiles profile-name]
user@host#  set dynamic-policy-control pcc-rules rule-name precedence number
```

NOTE: If the profile includes application-aware PCC rules, you must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

3. Specify one or more PCC rulebases for dynamic policy control.

```
[edit unified-edge  pcef profiles profile-name]
user@host#  set dynamic-policy-control pcc-rulebases rulebase-name
```

NOTE: Make sure that the PCC rules and PCC rulebases configured in a PCEF profile do not overlap.

4. Specify a Diameter Gx profile.

```
[edit unified-edge  pcef profiles profile-name dynamic-policy-control]
user@host#  set diameter-profile gx-profile-name
```

RELATED DOCUMENTATION

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | 56

Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | 52

Configuring Policy and Charging Control Rules | 86

Configuring a Policy and Charging Control Rulebase | 89

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Static Policies

A policy and charging enforcement function (PCEF) profile configured for static policy control specifies that policy and charging control (PCC) rules are provisioned by the Junos Subscriber Aware PCEF with no interaction from the policy and charging rules function (PCRF).

NOTE: To make a change to a static PCEF profile, you must be in maintenance mode. (See "Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles" on page 220).

Before you configure a PCEF profile for static policies, you must do the following:

- Configure service data flow filters for PCC rules.
- Configure PCC action profiles for PCC rules.
- Configure PCC rules.
- (Optional) Configure PCC rulebases.

To configure a PCEF profile for static policies:

1. Specify a name for the PCEF profile.

```
[edit unified-edge  pcef]
user@host#  edit profiles profile-name
```

2. Specify one or more PCC rules and a precedence for each rule for static policy control. A lower precedence value indicates a higher precedence.

```
[edit unified-edge  pcef profiles profile-name]
user@host#  set static-policy-control pcc-rules rule-name precedence number
```

3. Specify one or more PCC rule bases for static policy control.

```
[edit unified-edge  pcef profiles profile-name]
user@host#  set static-policy-control pcc-rulebases rulebase-name
```

RELATED DOCUMENTATION

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | 56

Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | 52

Configuring Policy and Charging Control Rules | 86

Configuring a Policy and Charging Control Rulebase | 89

Understanding Static Time-of-Day PCC Rule Activation and Deactivation | 74

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Policies That a RADIUS Server Controls

A policy and charging enforcement function (PCEF) profile configured for policy control by a RADIUS server specifies that the RADIUS server activates and deactivates policy and charging control (PCC) rulebases that you have predefined on the MX Series router.

Before you configure a PCEF profile for policies controlled by a RADIUS server, you must do the following:

- Configure PCC rulebases.
- Configure an AAA profile.

To configure a PCEF profile for policies controlled by a RADIUS server:

1. Specify a name for the PCEF profile.

```
[edit unified-edge  pcef]
user@host#  edit profiles profile-name
```

2. Specify one or more PCC rule bases for policy control by a RADIUS server.

```
[edit unified-edge  pcef profiles profile-name]
user@host#  set aaa-policy-control pcc-rulebases rulebase-name
```

3. Specify the AAA profile that identifies the RADIUS server policy control parameters.

```
[edit unified-edge  pcef profiles profile-name]
user@host#  set aaa-policy-control aaa-profile aaa-profile-name
```

4. Configure the user password for subscribers assigned to this PCEF profile.

```
[edit unified-edge  pcef profiles profile-name]
user@host#  set aaa-policy-control user-password password
```

RELATED DOCUMENTATION

- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | 56
- Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | 52
- Configuring Policy and Charging Control Rules | 86
- Configuring a Policy and Charging Control Rulebase | 89
- Configuring an AAA Profile | 96

Configuration of Static Time-of-Day PCC Rule Activation and Deactivation Overview

You configure static time-of-day PCC rule activation and deactivation to specify when a rule or rulebase within a static PCEF profile is active.

To configure static time-of-day PCC rules activation and deactivation:

1. Configure an NTP server.

   See "Configuring the NTP Server" on page 103.
2. Configure the activation and deactivation settings and apply them to a rule or rulebase.

   See "Configuring Static Time-of-Day PCC Rule Activation and Deactivation in a Junos OS Subscriber Aware PCEF Profile" on page 103

RELATED DOCUMENTATION

- Understanding Static Time-of-Day PCC Rule Activation and Deactivation | 74

Configuring the NTP Server

Before you use the static or dynamic time-of-day functionality for PCC rules, you must configure an NTP server.

To configure the NTP server:

1. Specify the IP address of the NTP server.

```
[edit system]
user@host# set ntp server ip-address
```

2. Enable the NTP process on the router.

```
[edit system]
user@host# set processes ntp enable
```

RELATED DOCUMENTATION

Configuring Static Time-of-Day PCC Rule Activation and Deactivation in a Junos OS Subscriber Aware PCEF Profile | 103

Understanding Static Time-of-Day PCC Rule Activation and Deactivation | 74

Configuring Static Time-of-Day PCC Rule Activation and Deactivation in a Junos OS Subscriber Aware PCEF Profile

You configure static time-of-day PCC rule activation and deactivation to specify when to activate or deactivate a rule or rulebase within a static PCEF profile.

Before you configure static time-of-day PCC rule activation and deactivation, configure the NTP server.

To configure static time-of-day PCC rule or rulebase activation and deactivation within a PCEF profile:

1. Specify a name for a time-of-day profile.

```
[edit unified-edge pcef]
user@host# set pcc-time-of-day-profiles profile-name
```

2. Specify the activation time in the time-of-day profile.

```
[edit unified-edge pcef pcc-time-of-day-profiles profile-name]
user@host# set rule-activation-time <day-of-week | day-of-month month> <hour:min>
```

You can specify the time of day, the day, and the month of the year. The day can be expressed as the day of the month (**DAY1** through **DAY31** or **Last-day-of-month**) or the day of the week (for example, **MONDAY**). If you specify the day of the month, you can also specify the month of the year. If a time zone is configured on the router, the time-of-day settings apply to the configured time zone.

3. Specify the deactivation time in the time-of-day profile. Use the same combination of options that you used in Step "2" on page 104.

```
[edit unified-edge pcef pcc-time-of-day-profiles profile-name]
user@host# set rule-deactivation-time <day-of-week | day-of-month month> <hour:min>
```

If a day is not specified and the deactivation time of day setting is earlier than the activation time of day setting, then a rule is deactivated the day after it is activated.

4. Within a static PCEF profile, apply the time-of-day profile to individual rules or rulebases.

```
[edit unified-edge pcef profiles profile-name static-policy-control]
user@host# set pcc-rules rule-name precedence number time-of-day-profile profile-name
user@host# set pcc-rulebases rulebase-name time-of-day-profile profile-name
```

Those rules or rulebases use the activation and deactivation settings for subscribers assigned to the PCEF profile.

RELATED DOCUMENTATION

- Understanding Static Time-of-Day PCC Rule Activation and Deactivation | 74
- Configuring the NTP Server | 103
- Understanding PCEF Profiles | 70

Configuring TDF Subscriber Usage Monitoring for Traffic That Matches Predefined PCC Rules

You can configure usage monitoring of TDF subscriber traffic that matches particular data flows or applications that are identified in a predefined PCC rule by identifying the appropriate monitoring key in the **pcc-action-profile** of the PCC rule. This monitoring key controls usage reporting for all the predefined PCC rules that use this **pcc-action-profile**.

To configure usage monitoring for a predefined PCC rule:

- For the **pcc-action-profile** that is used in the predefined PCC rule, specify the monitoring key that controls reporting:

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set monitoring-key key_string
```

RELATED DOCUMENTATION

Understanding Usage Monitoring for TDF Subscribers | 74

Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware | 83

CHAPTER 6

Configuring TDF Subscribers

IN THIS CHAPTER

- IP-Based and IFL-Based TDF Subscribers Overview | **107**
- IP-Based Subscriber Setup Overview | **107**
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | **108**
- Understanding Source IP Filtering with Address Pools in TDF Domains for IP-Based Subscribers | **110**
- Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**
- Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | **114**
- Understanding IFL-Based Subscriber Setup | **115**
- Understanding the Definition of a Set of IFL-Based Subscriber Properties with a TDF Domain | **116**
- Configuring IP-Based TDF Subscriber Setup When MX Series Router Is a RADIUS Server | **117**
- Configuring IP-Based TDF Subscriber Setup When Accounting Requests Are Snooped | **118**
- Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers | **119**
- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | **121**
- Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | **128**
- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**
- Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | **136**
- Configuring IFL-Based TDF Subscriber Setup | **139**
- Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | **140**
- Configuring a TDF Logical Interface | **143**
- Configuring TDF Interface to Access Interface Associations in VRFs | **144**

IP-Based and IFL-Based TDF Subscribers Overview

IN THIS SECTION

- IP-Based Subscribers | 107
- IFL-Based Subscribers | 107

Junos Subscriber Aware implements the Third-Generation Partnership Project (3GPP) traffic detection function (TDF), enabling subscriber-aware policy enforcement and traffic steering that is application-aware. Before a user's data traffic can undergo TDF processing, a TDF subscriber session must be set up.

You can configure two types of TDF subscribers:

IP-Based Subscribers

IP-based subscriber sessions are initiated when Junos Subscriber Aware processes a RADIUS accounting start request for a potential subscriber from a gateway GPRS support node (GGSN), Packet Data Network Gateway (PGW), or broadband network gateway (BNG). An IP-based subscriber session is for one unique user IP address.

IFL-Based Subscribers

IFL-based subscriber sessions are initiated when you configure the TDF subscriber and assign it a set of interfaces. All traffic that the MX Series router receives on those interfaces shares the same IFL-based subscriber session.

RELATED DOCUMENTATION

IP-Based Subscriber Setup Overview | 107

Understanding IFL-Based Subscriber Setup | 115

IP-Based Subscriber Setup Overview

Junos Subscriber Aware initiates an IP-based subscriber session when it receives a RADIUS accounting request from a gateway GPRS support node (GGSN), Packet Data Network Gateway (PGW), or

broadband network gateway (BNG). An individual subscriber session is created for each unique source IP address.

The MX Series router can receive a RADIUS accounting request in two ways:

- When the MX Series router is identified as a RADIUS server for the GGSN, PGW, or BNG, you configure the GGSN, PGW, or BNG as a RADIUS client of the MX Series router. The RADIUS client sends the accounting request to a designated interface and IP address on the MX Series router, which sends it to the subscriber processing module.
- When the GGSN, PGW, or BNG does not treat the MX Series router as a RADIUS server, you configure a filter called a *snoop segment*. Junos OS examines RADIUS accounting requests that pass through the MX Series router to determine whether they match the filter, which is known as *snooping*. When an accounting request matches the filter, Junos OS copies the request and sends it to the subscriber processing module.

You specify how an IP-based subscriber session is created and how a subscriber's traffic is processed by configuring TDF domains and PCEF profiles, and configuring a selection process for applying them to subscribers. The selection process identifies the attribute-value pair (AVP) values in the RADIUS accounting start request that must be matched to select a particular TDF domain or PCEF profile.

RELATED DOCUMENTATION

IP-Based and IFL-Based TDF Subscribers Overview | **107**

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | **108**

Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**

Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | **114**

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain

A traffic detection function (TDF) domain identifies a set of properties for creating a TDF IP-based subscriber session and specifying how TDF subscriber traffic is processed. You can create several TDF domains if you have multiple categories of subscribers. You configure a selection process to assign IP-based subscribers to a TDF domain. Multiple subscribers can be assigned to the same TDF domain.

IP-based TDF domains include the following information:

- An IP-based type of subscriber.

- The TDF logical interface (mif) that handles the subscriber traffic. A TDF interface is distinct from other types of interfaces and is used to associate a TDF domain's subscribers with an access interface in a virtual routing and forwarding table (VRF). The TDF logical interface also identifies the TDF service set that is applied to the traffic.
- (Optional) The PCEF profile that must be applied to the TDF subscriber. The PCEF profile specifies how to apply policy and charging rules to the TDF subscriber traffic. If the TDF domain does not specify a PCEF profile, you must configure a PCEF profile selection process in addtion to the TDF domain selection process.
- Source IP addresses for uplink traffic and destination IP addresses for downlink traffic that you do *not* want to undergo TDF processing.
- Idle timeout and maximum number of subscribers for the TDF domain.
- Source IP addresses for users who can become TDF subscribers, using address pools.
- (Not applicable to snooped messages) The enabling or disabling of an immediate RADIUS response message from the MX Series router to the accounting start message received from a gateway GPRS support node (GGSN), Packet Data Network Gateway (PGW), or broadband network gateway (BNG) RADIUS client.
- The method for constructing the Subscription-Id for the Diameter credit control request (CCR) message that is sent from the TDF to the PCRF for a TDF subscriber.
- The local policy (drop/forward packets, maximum bit rate, burst size) to apply to the subscriber packets entering the access interface of the TDF domain if a TDF subscriber session does not exist.
- One or more interfaces that face the access network and can carry traffic for the TDF subscriber.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | **121**

IP-Based Subscriber Setup Overview | **107**

Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**

Understanding Source IP Filtering with Address Pools in TDF Domains for IP-Based Subscribers

The TDF domain that is assigned to an IP-based subscriber can identify a set of source IP addresses of packets that need to undergo TDF processing. These sets of IP addresses are configured using address pools. Address pools can then be added to a TDF domain.

Address pools contain a set of IP addresses specified by network prefixes. You can configure more than one set of addresses in an address pool. You can configure address pools to contain IPv4 addresses or IPv6 addresses, but not both.

You can configure an address pool as a default pool, and a TDF domain uses the default address pool when an address pool is not explicitly specified for the TDF domain.

RELATED DOCUMENTATION

Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers | **119**

Understanding Selection of Properties for an IP-Based TDF Subscriber

When the MX Series router receives a RADIUS accounting start request from the access network's gateway GPRS support node (GGSN), Packet Data Network Gateway (PGW), or broadband network gateway (BNG) for an IP-based subscriber, it needs to select the properties to apply to a subscriber by selecting a traffic detection function (TDF) domain before setting up a TDF subscriber session. The domain-selection configuration identifies the values that various AVPs (such as the 3GPP IMSI or the IPv4 address) in the RADIUS request must match to select a particular TDF domain. For RADIUS requests that were snooped, the domain-selection configuration can identify the snoop segment that matched the request.

The domain-selection configuration includes one or more **term** statements, each of which includes **from** statements that must all be matched, and a **then** statement that identifies the name of the TDF domain. When a term matches, further terms are not evaluated if a PCEF profile is specified in either the selected TDF domain or in the **then** statement. If a PCEF profile is not specified in either the selected TDF domain or in the **then** statement, further terms are evaluated to find a PCEF profile for the subscriber.

If no TDF domain is selected, then the TDF subscriber session is not set up.

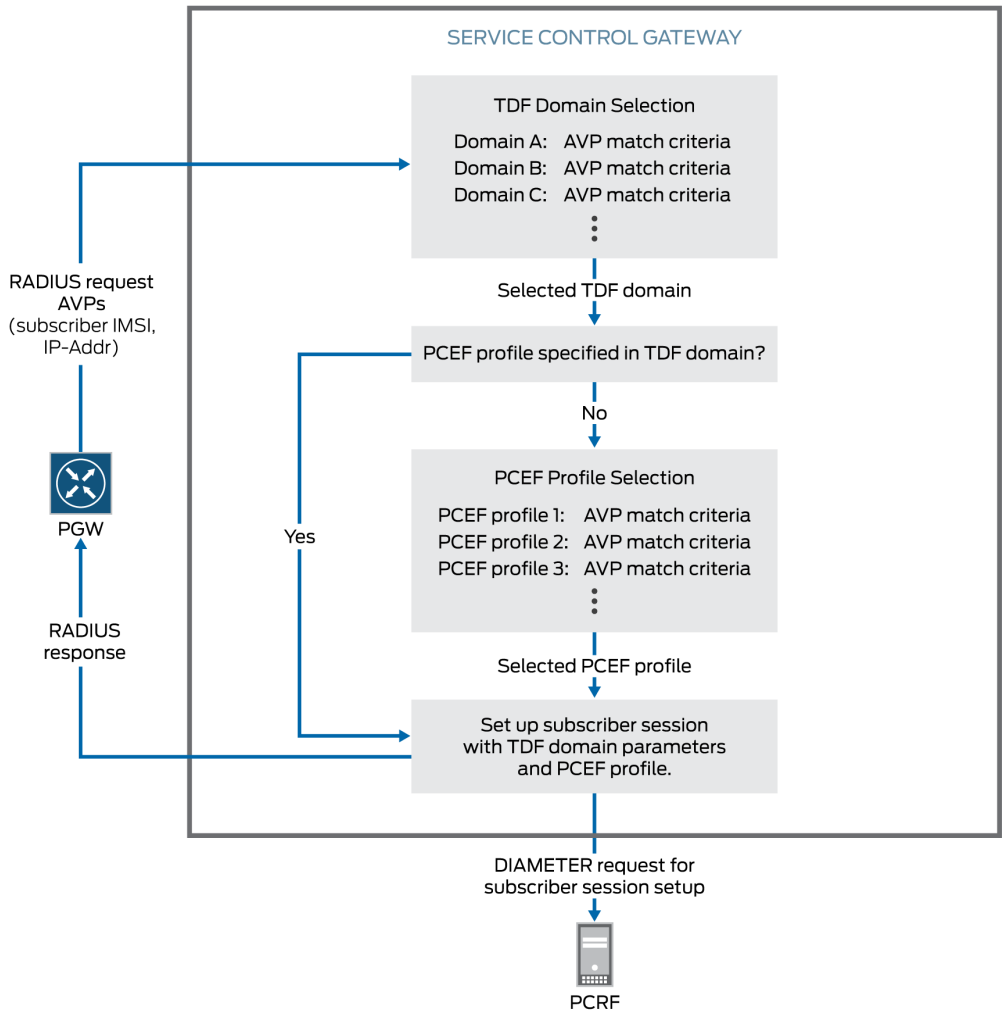
Before you can configure the TDF domain selection, you must configure a TDF gateway, the TDF domains, and the RADIUS client.

The match conditions for TDF domain selection include:

- (Not applicable to snooped messages) The RADIUS client (GGSN, PGW, or BNG) that is sending the accounting start request
- Values for called-station-id, calling-station-id, class, framed-ip-address, framed-ipv6-prefix, 3gpp-imsi, nas-ip-address, or user-name AVPs
- Values for other AVPs you identify

Figure 11 on page 111 shows an overview of the IP-based subscriber setup process.

Figure 11: IP-Based Subscriber Setup Process



RELATED DOCUMENTATION

- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based and IFL-Based TDF Subscribers Overview | 107
- IP-Based Subscriber Setup Overview | 107
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber

As part of the traffic detection function (TDF) subscriber session creation, the subscriber is assigned a policy and charging enforcement function (PCEF) profile, which specifies how policy and charging control (PCC) rules are defined on the TDF.

If every IP-based subscriber assigned to a TDF domain can share the same PCEF profile, then the PCEF profile can be specified within the TDF domain, under the **[edit unified-edge gateways tdf *gateway-name* domains]** hierarchy level. (For IFL-based subscribers, the PCEF profile *must* be specified within the TDF domain.)

If all of the IP-based subscribers assigned to the same TDF domain cannot share the same PCEF profile, the TDF domain does not specify a PCEF profile, and the PCEF profile selection must be configured under the **[edit unified-edge gateways tdf *gateway-name* domain-selection term]** hierarchy level. The **domain-selection term** consists of a **from** and a **then** statement.

The **from** statement identifies the match conditions for the subscriber. This includes the RADIUS client (GGSN, PGW, or BNG) that is sending the accounting start request for the subscriber and the values for particular AVPs in the message.

The **then** statement identifies the PCEF profile to assign to the subscriber. The **then** statement can also include the name of the TDF domain to assign to the subscriber. If the **then** statement only includes the PCEF profile, then another **domain-selection term** must assign a TDF domain to the subscriber.

When both a PCEF profile and a TDF domain are assigned to a subscriber in a **domain-selection term** statement, that PCEF profile is used even if the TDF domain specifies another PCEF profile.

Example: The TDF domain **domain1** specifies a PCEF profile. The **domain-selection term** does not need to specify a PCEF profile.

```
[edit unified-edge gateways tdf tdf1]
domain-selection {
```

```
    term 1 {
        from {
            client {
                client1;
            }
            user-name matches carrierA
        }
        then {
            domain domain1;
        }
    }
}
```

Example: The TDF domain **domain2** does not specify a PCEF profile. A **domain-selection term** must specify a PCEF profile. In this example, the PCEF profile is specified in the same term as the TDF domain.

```
[edit unified-edge gateways tdf tdf1]
domain-selection {
    term 1 {
        from {
            framed-ip-address equals 192.0.2.1/32
        }
        then {
            domain domain2;
            pcef-profile pcef3;
        }
    }
}
```

Example: The TDF domain **domain2** does not specify a PCEF profile. A **domain-selection term** must specify a PCEF profile. In this example, only the first term selects the TDF domain, so other terms must be added to select the PCEF profile.

```
[edit unified-edge gateways tdf tdf1]
domain-selection {
    term 1 {
        from {
            client {
                client2;
            }
```

```
            user-name matches carrierB
        }
        then {
            domain domain2;
        }
    }
    term 2 {
        from {
            framed-ip-address equals 192.0.2.1/32
        }
        then {
            pcef-profile pcef3;
        }
    }
    term 3{
        from {
            framed-ip-address equals 198.51.100.2/32
        }
        then {
            pcef-profile pcef4;
        }
    }
}
```

RELATED DOCUMENTATION

- IP-Based and IFL-Based TDF Subscribers Overview | 107
- IP-Based Subscriber Setup Overview | 107
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- Understanding Selection of Properties for an IP-Based TDF Subscriber | 110
- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130

Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview

When the gateway GPRS support node (GGSN), Packet Data Network Gateway (PGW), or broadband network gateway (BNG) does not identify the MX Series router as a RADIUS server, RADIUS accounting

requests are not sent to a particular MX Series router IP address and interface configured for RADIUS messages. In this situation, you can configure the MX Series router to actively examine RADIUS accounting requests that pass through the MX Series router. This process is known as *snooping*. Junos OS identifies accounting requests that match a filter you configure, copies those requests, and sends them to the subscriber processing module.

To configure snooping, you configure filters called *snoop segments*. You can include the following conditions in a snoop segment:

- Destination IP address of the accounting request
- Shared secret between the accounting request sender and the MX Series router
- (Optional) Destination port of the accounting request
- (Optional) MX Series router interface that receives the accounting request
- (Optional) Source IP address of accounting requests from a GGSN, PGW, or BNG

You can also configure the length of time to cache the accounting request that was snooped. Any duplicate request that is received by the MX Series router within this time is dropped.

You can configure multiple snoop segments.

RELATED DOCUMENTATION

IP-Based Subscriber Setup Overview | **107**

Configuring IP-Based TDF Subscriber Setup When Accounting Requests Are Snooped | **118**

Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | **136**

Understanding IFL-Based Subscriber Setup

You use the CLI to configure an IFL-based subscriber for a particular interface or set of access interfaces. All user traffic that uses these interfaces belongs to the same subscriber session. The IFL-based subscriber session becomes active when at least one of its access interfaces is up.

You can specify the following types of interfaces:

- Physical Layer 3 Ethernet interface
- Layer 3 Aggregated Ethernet interface
- Integrated routing and bridging (IRB) interface

- IRB that contains Ether-channel and physical interface members
- Logical Tunnel interface

You specify how an IFL-based subscriber's traffic is processed by configuring the properties of the TDF domain in which the IFL-based subscriber is configured, which includes a pointer to the PCEF profile to assign to the subscriber.

When an IFL-based subscriber session is created, it is anchored on a session PIC based on a round-robin selection process. If a stand-alone session PIC goes down and any IFL-based subscribers are anchored on that PIC, Junos OS re-anchors a subscriber onto another session PIC.

An IFL-based subscriber session is deleted in the following situations:

- All of the subscriber's access interfaces are down. When at least one interface comes back up, the subscriber session is restored.
- Subscriber is removed from the configuration with the CLI.
- Subscriber is set to deactivate with the CLI.
- Subscriber is cleared with the CLI. You can later restore the subscriber by using the revert option with the clear command. (See "clear unified-edge tdf subscribers" on page 798.)

RELATED DOCUMENTATION

IP-Based and IFL-Based TDF Subscribers Overview | 107

Understanding the Definition of a Set of IFL-Based Subscriber Properties with a TDF Domain | 116

Understanding the Definition of a Set of IFL-Based Subscriber Properties with a TDF Domain

A traffic detection function (TDF) domain identifies a set of properties for the IFL-based subscribers configured in the TDF domain. You can create several TDF domains if you have multiple categories of subscribers. Multiple subscribers can be assigned to the same TDF domain.

TDF domains include the following information:

- Logical interface-based type of subscriber.
- Name of each subscriber.
- Interfaces that belong to a subscriber. An interface can belong to only one subscriber.

- The TDF logical interface (mif) that handles the subscriber traffic. A TDF interface is distinct from other types of interfaces and is used to associate a TDF domain's subscribers with an access interface in a virtual routing and forwarding table (VRF). The TDF logical interface also identifies the TDF service set that is applied to the traffic.
- The PCEF profile that must be applied to the TDF subscriber. The PCEF profile specifies how to apply policy and charging rules to the TDF subscriber traffic.
- Source IP addresses for uplink traffic and destination IP addresses for downlink traffic you do not want to undergo TDF processing.

RELATED DOCUMENTATION

Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | **140**

Understanding IFL-Based Subscriber Setup | **115**

Configuring IP-Based TDF Subscriber Setup When MX Series Router Is a RADIUS Server

This task describes how to configure IP-based TDF subscriber setup when the gateway GPRS support node (GGSN), Packet Data Network Gateway (PGW), or broadband network gateway (BNG) identifies the MX Series router as a RADIUS server. An IP-based TDF subscriber is defined by the AVP values in the RADIUS accounting request received.

Before you configure the subscriber setup, you must do the following:

- Configure the access interfaces on the MX Series router chassis.
- Configure the PCEF profile.
- Configure the interface and IP address that you want to receive RADIUS requests on the MX Series router.
- Configure a TDF gateway.

To configure IP-based subscriber setup when the MX Series router acts as a RADIUS server:

1. Configure the TDF interfaces that can be used by TDF subscribers.

   See "Configuring a TDF Logical Interface" on page 143.
2. Associate the TDF interface to an access interface in a VRF routing instance.

   See "Configuring TDF Interface to Access Interface Associations in VRFs" on page 144.

3. Configure sets of source IP addresses that TDF domains can use to accept traffic.

   See "Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers" on page 119.

4. Configure TDF domains that can be assigned to subscribers.

   See "Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain" on page 121.

5. Configure RADIUS clients that can send the subscriber accounting requests.

   See "Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers" on page 128.

6. Configure how Junos OS selects TDF domains and PCEF profiles for subscribers.

   See "Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers" on page 130.

RELATED DOCUMENTATION

IP-Based Subscriber Setup Overview | 107

Configuring IP-Based TDF Subscriber Setup When Accounting Requests Are Snooped

This task describes how to configure IP-based TDF subscriber setup when the gateway GPRS support node (GGSN), Packet Data Network Gateway (PGW), or broadband network gateway (BNG) does not identify the MX Series router as a RADIUS server.

Before you configure the subscriber setup, you must do the following:

- Configure the PCEF profile.
- Configure a TDF gateway.

To configure IP-based subscriber setup when the MX Series router *does not* act as a RADIUS server:

1. Configure the TDF interfaces that can be used by TDF subscribers.

   See "Configuring a TDF Logical Interface" on page 143.

2. Associate the TDF interface to an access interface.

   See "Configuring TDF Interface to Access Interface Associations in VRFs" on page 144.

3. Configure sets of source IP addresses that TDF domains can use to accept traffic.

   See "Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers" on page 119.

4. Configure TDF domains that can be assigned to subscribers.

   See "Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain" on page 121.

5. Configure the snooping filters that examine RADIUS accounting requests.

   See "Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers" on page 136.

6. Configure how Junos OS selects TDF domains and PCEF profiles for subscribers.

   See "Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers" on page 130.

RELATED DOCUMENTATION

IP-Based Subscriber Setup Overview | 107

Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | 114

Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers

Address pools identify a set of IP addresses that a TDF domain for IP-based subscribers uses to determine which packets undergo TDF processing.

To configure address pools:

1. Specify a name for the address pool.

```
[edit access address-assignment]
user@host# set address-pools name
```

   The pool name can contain letters, numbers, and hyphens (-) and can be up to 63 characters long.

2. Specify the protocol family (**inet** for IPv4 addresses and **inet6** for IPv6 addresses) for the address pool.

```
[edit access address-assignment]
user@host# set address-pools name family (inet | inet6)
```

   For example, to configure an address pool named *mbg-pool1* with IPv4 addresses:

```
[edit access address-assignment]
user@host# set address-pools mbg-pool1 family inet
```

3. Specify the network prefix for the address pool for the configured protocol family.

```
[edit access address-assignment]
user@host# set address-pools name family (inet | inet6) network [network-prefix] external-assigned
```

> **NOTE**: A address pool must have at least one network prefix configured. You can configure more than one network prefix by including the **network** statement multiple times.
>
> The **external-assigned** statement is required.

For example, to configure an address pool with network prefixes 10.100.0.0/16 and 192.168.0.0/16:

```
[edit access address-assignment]
user@host# set address-pools mbg-pool1 family inet network 10.100.0.0/16 external-assigned
user@host# set address-pools mbg-pool1 family inet network 192.168.0.0/16 external-assigned
```

4. (Optional) Specify that the address pool is the default pool.

   A TDF domain uses the default address pool to specify the source addresses of packets that undergo TDF processing when an address pool is not specified for the TDF domain.

```
[edit access address-assignment]
user@host# set address-pools name default-pool
```

RELATED DOCUMENTATION

Understanding Source IP Filtering with Address Pools in TDF Domains for IP-Based Subscribers | 110

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

IP-Based Subscriber Setup Overview | 107

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain

IN THIS SECTION

- Configuring the TDF Domain Name and AAA Parameters | 121
- Configuring Address Filtering | 124
- Configuring Subscriber Services and Policies | 125
- Configuring Access Interfaces | 125
- Configuring Session Controls | 126
- Configuring Default Policy | 126

You define a set of properties for processing IP-based subscriber traffic and for setting up the subscriber session by configuring a TDF domain. You can create multiple TDF domains.

A potential IP-based subscriber is assigned to a TDF domain through a TDF domain-selection process that you configure in another topic.

Before you begin to create a TDF domain for IP-based subscribers, make sure that you have done the following:

- Configured the TDF interface (mif-) that the TDF domain uses.
- Configured the access-facing interfaces that the TDF domain uses.
- Configured a VRF routing instance that includes the TDF interface and the access-facing interfaces.
- Configured the PCEF profile if the TDF domain specifies one.
- Configured the address pool that contains source IP addresses of packets that are excluded from TDF processing for the TDF domain.

To configure a TDF domain for IP-based subscribers:

Configuring the TDF Domain Name and AAA Parameters

To configure the TDF domain name and the AAA parameters that are used by the TDF domain to create TDF IP-based subscriber sessions:

1. Specify a name for the TDF domain. The name can be from 1 through 50 characters long.

```
[edit unified-edge gateways tdf gateway-name]
user@host# set domains domain-name
```

2. (Optional) Configure the TDF domain for IP-based subscribers.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set subscriber-type ip
```

   You may omit this step because the default **subscriber-type** for TDF domains is **ip**.

3. Specify one or more methods for constructing the Subscription-Id for the Diameter credit control request (CCR) message that is sent from the TDF to the PCRF for subscribers belonging to the TDF domain.

   a. Specify the type of information to use for the Subscription-Id.

      You can specify multiple types, and the order of preference matches the order in which you enter the types. Table 5 on page 123 describes the types.

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-
subscriber]
user@host# set subscription-id subscription-id-options entry-name id-components [use-class | use-
imsi | use-msisdn | use-nai | use-nas-port | use-nas-port-id | use-realm | use-username]
```

      You can specify multiple methods by including the *entry-name* variable multiple times.

   b. If you selected **use-class** in Step a, you can also configure a regular expression to parse the Class attribute contents, specify characters to insert between the resulting regular expression groups, and specify the subscription ID type.

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-
subscriber subscription-id]
user@host# set use-class regex "value"
user@host# set use-class pattern "pattern"
user@host# set use-class subscription-id-type (imsi | msisdn | nai | private | sip-uri)
```

      where *value* is a regular expression and *pattern* indicates the characters to insert between regular expression groups, which are identified with **\n** for a group number.

For example, the following configuration generates **" 000118191129|ALICE:DRAV3:"** out of **" 000118191129#000118191129#ALICE:DRAV3:#7168#nflat#ADSL##"** and sets the type to IMSI:

```
[edit unified-edge gateways tdf TDF1 domains domain1 ip-subscriber
subscription-id ]
user@host# set use-class regex "[^#]*#\([^#]*\)\#\([^#]*\)"
user@host# set use-class pattern "\1|\2"
user@host# set use-class subscription-id-type imsi
```

c. Specify a constant string for the Subscription-Id-Data value.

This constant value is used if none of the **subscription-id-options** methods can be used. In such a case, the Subscription-Id-Type is END_USER_PRIVATE.

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-
subscriber]
user@host# set subscription-id constant value
```

Table 5: Options for id-components of Subscription-Id

Option	Subscription-Id Type	Subscription-Id Data
use-class	Configurable	Entire Class attribute by default. Class attribute value can be parsed with **regex** option under the **[edit unified-edge gateways tdf *gateway-name* domains *domain-name* subscription-id use-class]** hierarchy.
use-imsi	END_USER_IMSI	3GPP-IMSI
use-msisdn	END_USER_E164	Calling-Station-Id
use-nai	END_USER_NAI	User-Name
use-nas-port	END_USER_PRIVATE	NAS-Port

Table 5: Options for id-components of Subscription-Id *(Continued)*

Option	Subscription-Id Type	Subscription-Id Data
use-nas-port-id	END_USER_PRIVATE	NAS-Port-Id
use-realm	END_USER_PRIVATE	Realm portion of the User-Name in NAI format
use-username	END_USER_PRIVATE	Username portion of the User-Name in NAI format

4. (Not applicable to snooped messages) Enable or disable the sending of an immediate RADIUS response message to the accounting start message received from a gateway GPRS support node (GGSN), Packet Data Network Gateway (PGW), or broadband network gateway (BNG) RADIUS client (disabled is the default).

   If the option is disabled, the response is sent after the TDF subscriber session creation is complete.

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-
subscriber]
user@host# set immediate-accounting-response (enabled | disabled)
```

Configuring Address Filtering

To restrict the traffic that undergoes TDF processing for the TDF domain by identifying source IP addresses for uplink traffic and destination IP addresses for downlink traffic:

1. Identify the network prefix of source and destination IP addresses for packets that *do not* undergo TDF processing. Specify **inet** for IPv4 prefixes and **inet6** for IPv6 prefixes.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set subscriber-exclude-prefix family (inet | inet6) network address net-mask
```

2. Identify the address pool that contains source and destination IP addresses of packets that undergo TDF processing. Specify **inet** for IPv4 prefixes and **inet6** for IPv6 prefixes.

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-
subscriber ]
user@host# set subscriber-address (inet | inet6) pool pool-name
```

NOTE: The address pool must be configured at the **[edit access address-assignment]** hierarchy level.

Configuring Subscriber Services and Policies

To configure the services and policies for IP-based subscribers that belong to the TDF domain:

1. Identify the TDF interface for the TDF domain.

   The TDF domain uses the service set that is applied to this TDF interface.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set tdf-interface mif.number
```

   NOTE: The TDF interface (mif) must have been previously configured at the **[edit interfaces]** hierarchy level.

2. (Optional) Identify the PCEF profile that the TDF domain uses to apply policies.

   If you do not identify a PCEF profile, then the PCEF profile must be assigned under the **[edit unified-edge gateways tdf *gateway-name* domain-selection term]** hierarchy.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set pcef-profile name
```

   NOTE: The PCEF profile must have been previously configured at the **[unified-edge pcef]** hierarchy level.

Configuring Access Interfaces

To configure the interfaces that face the access network and carry traffic to and from the IP-based subscribers that belong to the TDF domain:

Specify at least one interface. You can specify multiple interfaces.

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber]
user@host# set access-interfaces interface-name
```

Configuring Session Controls

To configure the TDF session controls for subscribers that belong to the TDF domain:

1. Configure the idle timeout (in minutes) for the TDF subscriber session. The range is 0 through 300.

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-
subscriber]
user@host# set idle-timeout idle-timeout
```

2. Configure the default TDF subscriber maximum bit rate (MBR) for uplink and downlink traffic.

   Uplink traffic originates from the subscriber towards the public data network (PDN), and downlink traffic comes from the PDN and is destined for the subscriber. The range is 0 through 6,144,000 Kbps.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set maximum-bit-rate uplink mbr-uplink-value downlink mbr-downlink-value
```

3. Configure the default TDF subscriber allowed burst size for uplink and downlink traffic.

   Uplink traffic originates from the subscriber towards the public data network (PDN), and downlink traffic comes from the PDN and is destined for the subscriber. The range is 1500 through 1,500,000,000 bytes.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set burst-size uplink uplink-burst-size downlink downlink-burst-size
```

4. Configure the maximum number of subscriber sessions allowed (in thousands) for the TDF domain. The range is 100 thousands through 5000 thousands.

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-
subscriber]
user@host# set maximum-subscribers number
```

Configuring Default Policy

To configure the default local policy for handling subscriber traffic entering the access interface of the TDF domain if a TDF subscriber session does not exist:

1. Configure the flow action to take on the subscriber's traffic.

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-
subscriber]
user@host# set default-local-policy flow-action (drop | forward)
```

2. Configure the maximum bit rate for the subscriber's traffic.

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-
subscriber]
user@host# set default-local-policy maximum-bit-rate uplink mbr-uplink-value downlink mbr-downlink-
value
```

   Uplink traffic originates from the subscriber towards the public data network (PDN); downlink traffic comes from the PDN and is destined for the subscriber. The range is 0 through 6144000 Kbps.

3. Configure the allowed burst size for the subscriber's traffic.

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-
subscriber]
user@host# set default-local-policy burst-size uplink uplink-burst-size downlink downlink-burst-size
```

   Uplink traffic originates from the subscriber towards the public data network (PDN); downlink traffic comes from the PDN and is destined for the subscriber. The range is 1500 through 1,500,000,000 bytes.

RELATED DOCUMENTATION

- IP-Based and IFL-Based TDF Subscribers Overview | 107
- IP-Based Subscriber Setup Overview | 107
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers | 119
- Understanding PCEF Profiles | 70
- Configuring a Services Interface for a Session PIC or Service PIC | 15

Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers

You specify an MX Series router RADIUS client for each gateway GPRS support node (GGSN), Packet Data Network Gateway (PGW), or broadband network gateway (BNG) that sends IP-based subscriber session requests and identifies the MX Series router as a RADIUS server. This task is not used for snooped accounting requests.

Before you begin to configure a RADIUS client, make sure that you have configured the interface and IP address that you want to receive RADIUS requests on the MX Series router.

To configure the RADIUS clients:

1. Configure the name of the RADIUS client.

```
[edit access radius]
user@host# set clients client-name
```

2. Specify the IP address from which the RADIUS client sends the RADIUS requests.

```
[edit access radius]
user@host# set clients client-name address client-address
```

3. Specify the MX Series router interface and IPv4 address that receive RADIUS requests from the GGSN, PGW, or BNG.

```
[edit access radius]
user@host# set clients client-name source-interface interface ipv4-address address
```

4. Configure a shared secret to be used by the MX Series router and the RADIUS client for accounting.

```
[edit access radius]
user@host# set clients client-name accounting secret password
```

5. (Optional) Specify that the framed-ip-address is used for subscriber creation when both the framed-route and framed-ip-address attributes are in the RADIUS accounting request from the RADIUS client. The framed-ip-netmask is also used for subscriber creation if it is in the request.

```
[edit access radius]
user@host# set clients client-name prefer-framed-ip-address
```

   By default, the framed-route attribute is used for subscriber creation when both the framed-route and framed-ip-address attributes are in the RADIUS accounting request.

6. (Optional) Specify that the framed-ipv6-prefix is used for subscriber creation when both the delegated-ipv6-prefix and framed-ipv6-prefix attributes are in the RADIUS accounting request from the RADIUS client.

```
[edit access radius]
user@host# set clients client-name prefer-framed-ipv6-prefix
```

   By default, the delegated-ipv6-prefix attribute is used for subscriber creation when both the delegated-ipv6-prefix and framed-ipv6-prefix attributes are in the RADIUS accounting request.

7. Configure the duration, in seconds, that the RADIUS response messages (sent for request messages) are stored in the MX Series router response cache before they time out.

```
[edit access radius]
user@host# set clients client-name accounting response-cache-timeout seconds
```

8. Enable the RADIUS client for a specific TDF gateway.

```
[edit unified-edge gateways tdf gateway-name]
user@host# set aaa clients client-name
```

   Use the *client-name* that you configured in Step "1" on page 128.

RELATED DOCUMENTATION

IP-Based Subscriber Setup Overview | 107

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers

IN THIS SECTION

- Configuring the Term Name | 130
- Configuring Match Conditions for the RADIUS Client | 131
- Configuring Match Conditions for Snoop Segments | 131
- Configuring Match Conditions for Predefined AVPs | 131
- Configuring Match Conditions for Custom AVP Attributes | 133
- Configuring the TDF Domain to Select | 135
- Configuring the PCEF Profile to Select | 135

You must configure the criteria that Junos OS uses to select a TDF domain for an IP-based subscriber, which determines how the subscriber session is set up and how the subscriber traffic is treated. (The domain-selection process does not apply to IFL-based subscribers, who are automatically assigned to the TDF domain in which they are configured.) You configure a **term** to identify conditions that must be matched in the incoming RADIUS request in order to select a particular TDF domain.

You configure the selection of the policy-control properties by selecting a PCEF profile. The PCEF profile can be identified in the selected TDF domain, or you can independently configure the criteria for the selection of a PCEF profile.

Before you begin to configure TDF domain or PCEF profile selection, make sure that you have done the following:

- Configured a TDF gateway.
- Configured the TDF domains.
- Configured the PCEF profiles.
- Configured the RADIUS client.

To configure a term for TDF domain or PCEF profile selection, perform the following tasks and repeat this process for each term you want to configure:

Configuring the Term Name

To configure the name for the **term** that contains the **from** statements and the **then** statement:

- Configure a term name that is 1 through 50 characters in length.

```
[edit unified-edge gateways tdf gateway-name domain-selection]
user@host# set term term-name
```

Configuring Match Conditions for the RADIUS Client

Before you begin to configure a match condition for a RADIUS client, you must ensure that you have configured the RADIUS client at the **[edit access radius clients]** hierarchy level, and specified it as the **aaa-client** at the **[edit unified-edge gateways tdf *gateway-name*]** hierarchy level.

To configure a match condition for the RADIUS client that sent the incoming RADIUS request:

- Specify the client.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from client client-name
```

Configuring Match Conditions for Snoop Segments

For RADIUS requests that were snooped, the domain-selection configuration can identify the snoop segment that matched the request.

To configure a match condition for the snoop segment:

- Specify the snoop segment.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from snoop-segment snoop-segment-name
```

Configuring Match Conditions for Predefined AVPs

To configure match conditions for the called-station-id, calling-station-id, class, framed-ip-address, framed-ipv6-prefix, 3gpp-imsi, nas-ip-address, or user-name AVP in the incoming RADIUS request from the subscriber:

1. Configure any called-station-id match condition.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from called-station-id (equals | matches) value
```

Use **equals** to specify a value the called-station-id must equal or use **matches** to specify a regular expression the called-station-id must match.

2. Configure any calling-station-id match condition.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from calling-station-id equals value
```

or

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from calling-station-id matches value
```

Use **equals** to specify a value the calling-station-id must equal or use **matches** to specify a regular expression the calling-station-id must match.

3. Configure any class match condition.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from class (equals | has-prefix | has-suffix | matches) value
```

Use **equals** to specify a value the class must equal, use **has-prefix** to specify the prefix that the class must have, use **has-suffix** to specify the suffix that the class must have, or use **matches** to specify a regular expression the class must match.

4. Configure any framed-ip-address match condition.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from framed-ip-address equals value
```

5. Configure any framed-ipv6-prefix match condition.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from framed-ipv6-prefix equals value
```

6. Configure any 3gpp-imsi match condition.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from 3gpp-imsi (equals | has-prefix | has-suffix | matches) value
```

Use **equals** to specify a value the 3gpp-imsi must equal, use **has-prefix** to specify the prefix that the 3gpp-imsi must have, use **has-suffix** to specify the suffix that the 3gpp-imsi must have, or use **matches** to specify a regular expression the 3gpp-imsi must match.

7. Configure any nas-ip-address match condition.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from nas-ip-address equals value
```

8. Configure any user-name match condition.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from user-name (equals | has-prefix | has-suffix | matches) value
```

Use **equals** to specify a value the user-name must equal, use **has-prefix** to specify the prefix that the user-name must have, use **has-suffix** to specify the suffix that the user-name must have, or use **matches** to specify a regular expression the user-name must match.

Configuring Match Conditions for Custom AVP Attributes

To configure match conditions for up to five custom AVP attributes (other than the called-station-id, calling-station-id, class, framed-ip-address, framed-ipv6-prefix, 3gpp-imsi, nas-ip-address, or user-name) in the incoming RADIUS request from the subscriber:

1. Configure an attribute name that is 1 through 50 characters in length.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from attribute name
```

2. Configure any match condition for the custom attribute's AVP code.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name]
user@host# set code numeric-code
```

3. Configure any match condition for the custom attribute's vendor-id.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name]
user@host# set vendor-id vendor-id
```

4. Configure any match condition for custom attribute data in integer format.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name]
user@host# set format integer (equals | greater-than | less-than) value
```

5. Configure any match condition for custom attribute data in string format.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name]
user@host# set format string (equals | has-prefix | has-suffix | matches) value
```

   Use **equals** to specify a value the string must equal, use **has-prefix** to specify the prefix that the string must have, use **has-suffix** to specify the suffix that the string must have, or use **matches** to specify a regular expression the string must match.

6. Configure any match condition for custom attribute data in time format.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name]
user@host# set format time (equals | greater-than | less-than) value
```

7. Configure any match condition for custom attribute data in IPv4 address format.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name]
user@host# set format v4address equals value
```

8. Configure any match condition for custom attribute data in IPv6 address format.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name]
user@host# set format v6address equals value
```

9. Configure any match condition for custom attribute data in IPv6 address prefix format.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name]
user@host# set format v6prefix equals value
```

Configuring the TDF Domain to Select

To specify the TDF domain to select when the **from** conditions in the **term** have been matched:

- Specify the TDF domain name.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set then domain tdf-domain-name
```

Configuring the PCEF Profile to Select

If a particular TDF domain does not specify a PCEF profile or you want different members of the same TDF domain to have different PCEF profiles, you must specify the PCEF profile under the **[edit unified-edge gateways tdf *gateway-name* domain-selection]** hierarchy level.

To specify the PCEF profile to select when the **from** conditions in the **term** have been matched, use one of the following methods:

- Specify the PCEF profile name in the same **term** statement that specifies the TDF domain.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from {...}
user@host# set then domain tdf-domain-name
user@host# set then pcef-profile pcef-profile-name
```

- Specify the PCEF profile name in a different **term** statement.

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
user@host# set from {...}
user@host# set then pcef-profile pcef-profile-name
```

RELATED DOCUMENTATION

IP-Based and IFL-Based TDF Subscribers Overview | **107**

IP-Based Subscriber Setup Overview | **107**

Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | **121**

Configuring a TDF Gateway | 16

Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | 128

Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers

If a gateway GPRS support node (GGSN), Packet Data Network Gateway (PGW), or broadband network gateway (BNG) does not treat the MX Series router as a RADIUS server, Junos OS must actively snoop RADIUS accounting requests from that gateway to set up TDF subscriber sessions. Snooping uses a filter called a *snoop segment* to identify the requests to send to the subscriber management module.

To configure snooping of RADIUS accounting requests:

1. Configure a name for the snoop segment.

```
[edit access radius]
user@host# set snoop-segments snoop-segment-name
```

For example:

```
[edit access radius]
user@host# set snoop-segments 123
```

2. Specify the destination IP address of accounting requests to snoop.

```
[edit access radius snoop-segments snoop-segment-name]
user@host# set destination-ip-address destination-address
```

For example:

```
[edit access radius snoop-segments 123]
user@host# set destination-ip-address 10.102.30.102
```

3. (Optional) Specify the destination port of accounting requests to snoop.

```
[edit access radius snoop-segments snoop-segment-name]
user@host# set destination-port destination-port
```

For example:

```
[edit access radius snoop-segments 123]
user@host# set destination-port 52000
```

If this statement is not included, the destination port is set to 1813.

4. (Optional) Specify the source IP address of accounting requests from a GGSN, PGW, or BNG to snoop.

```
[edit access radius snoop-segments snoop-segment-name]
user@host# set source-ip-address source-address
```

For example:

```
[edit access radius snoop-segments 123]
user@host# set source-ip-address 10.11.11.11
```

If the source IP address is not included, snooping of accounting requests is not restricted by their source.

5. Specify the MX Series router interface on which the accounting requests to be snooped are received.

```
[edit access radius snoop-segments snoop-segment-name]
user@host# set source-interface source-interface
```

For example:

```
[edit access radius snoop-segments 123]
user@host# set source-interface ge-0/0/0.0
```

If the source interface is not included, snooping of accounting requests is not restricted by the interface that receives the request.

6. Specify the shared secret for the MX Series router and the accounting request sender.

```
[edit access radius snoop-segments snoop-segment-name]
user@host# set shared-secret secret
```

For example:

```
[edit access radius snoop-segments 123]
user@host# set shared-secret juniper
```

If the shared secrets do not match, the subscriber session is not set up.

7. (Optional) Configure the number of seconds to cache the accounting request that was snooped. If the same request is received by the MX Series router within this time, it is considered a duplicate request and is dropped.

```
[edit access radius snoop-segments snoop-segment-name]
user@host# set request-cache-timeout timeout
```

For example:

```
[edit access radius snoop-segments 123]
user@host# set request-cache-timeout 4
```

8. Repeat Steps "1" on page 136 through "7" on page 138 to configure additional snoop segments.

9. Assign one or more snoop segments to the TDF gateway.

```
[edit unified-edge gateways tdf gateway-name aaa]
user@host# set snoop-segments [snoop-segment-name]
```

For example, the following configures **gateway1** to snoop accounting requests destined for the RADIUS server 10.102.30.102 on port 52000 that originate from IP address 10.11.11.11 and are received on interface ge-0/0/0.0:

```
[edit unified-edge gateways tdf gateway1 aaa]
user@host# set snoop-segments 123
```

RELATED DOCUMENTATION

Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | 114

Configuring IP-Based TDF Subscriber Setup When Accounting Requests Are Snooped | 118

IP-Based Subscriber Setup Overview | 107

Configuring IFL-Based TDF Subscriber Setup

This task describes how to configure IFL-based TDF subscriber setup.

Before you configure the subscriber setup, you must do the following:

- Configure the interfaces on the MX Series router chassis.
- Configure the PCEF profile.
- Configure a TDF gateway.

To configure IFL-based subscriber setup:

1. Configure the TDF interfaces that TDF subscribers can use.
   See "Configuring a TDF Logical Interface" on page 143.
2. Associate the TDF interface to an access interface in a VRF routing instance.
   See "Configuring TDF Interface to Access Interface Associations in VRFs" on page 144.
3. Configure the IFL-based subscribers.
   See "Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain" on page 140.

RELATED DOCUMENTATION

Understanding IFL-Based Subscriber Setup | 115

Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain

IN THIS SECTION

- Configuring the TDF Domain Name and Type | 140
- Configuring IFL-Based Subscribers | 141
- Configuring Address Filtering | 142
- Configuring Subscriber Services and Policies | 142
- Configuring Session Controls | 142

You configure one or more IFL-based TDF subscribers and a set of properties for processing the traffic for those subscribers by configuring a TDF domain. You can create multiple TDF domains.

Before you begin to create a TDF domain for IFL-based subscribers, make sure that you have done the following tasks:

- Configured the TDF interface (mif-) that the TDF domain uses.
- Configured the interfaces that the TDF domain uses.
- Configured a VRF routing instance that includes the TDF interface and the interfaces that the TDF domain uses.
- Configured the PCEF profile that the TDF domain uses.

To configure a TDF domain for IFL-based subscribers, perform the following:

Configuring the TDF Domain Name and Type

To configure the TDF domain name and type:

1. Specify a name for the TDF domain. The name can be from 1 through 50 characters long.

```
[edit unified-edge gateways tdf gateway-name]
user@host# set domains domain-name
```

For example:

```
[edit unified-edge gateways tdf TDF1]
user@host# set domains ifl-1
```

2. Configure the subscriber type for IFL-based subscribers.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set subscriber-type ifl
```

Configuring IFL-Based Subscribers

To configure IFL-based subscribers:

1. Configure the name for a subscriber.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set ifl-subscriber subscriber-name
```

For example:

```
[edit unified-edge gateways tdf TDF1 domains ifl-1]
user@host# set ifl-subscriber ifl-sub1
```

2. Configure one or more interfaces for the subscriber.

```
[edit unified-edge gateways tdf gateway-name domains domain-name  ifl-
subscriber subscriber-name]
user@host# set access-interfaces [interface-name]
```

For example:

```
[edit unified-edge gateways tdf TDF1 domains ifl-1 ifl-subscriber ifl-sub1]
user@host# set access-interfaces ae0.736
```

You can assign only one IFL-based subscriber to an interface.

3. Repeat Step "1" on page 141 and Step "2" on page 141 for each IFL-based subscriber you want to configure in the TDF domain.

Configuring Address Filtering

To restrict the traffic that undergoes TDF processing for the TDF domain by identifying source IP addresses for uplink traffic and destination IP addresses for downlink traffic:

- Identify the network prefix of source and destination IP addresses for packets that *do not* undergo TDF processing. Specify **inet** for IPv4 prefixes and **inet6** for IPv6 prefixes.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set subscriber-exclude-prefix family (inet | inet6) network address net-mask
```

Configuring Subscriber Services and Policies

To configure the services and policies for IFL-based subscribers that belong to the TDF domain:

1. Identify the TDF interface for the TDF domain.

   The TDF domain uses the service set that is applied to this TDF interface.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set tdf-interface mif.number
```

> **NOTE**: The TDF interface (mif) must have been previously configured at the **[edit interfaces]** hierarchy level.

2. Identify the PCEF profile that the TDF domain uses to apply policies.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set pcef-profile name
```

> **NOTE**: The PCEF profile must have been previously configured at the **[unified-edge pcef]** hierarchy level.

Configuring Session Controls

To configure the TDF session controls for subscribers that belong to the TDF domain:

1. Configure the default TDF subscriber maximum bit rate (MBR) for uplink and downlink traffic.

Uplink traffic originates from the subscriber towards the public data network (PDN), and downlink traffic comes from the PDN and is destined for the subscriber. The range is 0 through 6,144,000 Kbps.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set maximum-bit-rate uplink mbr-uplink-value downlink mbr-downlink-value
```

2. Configure the default TDF subscriber allowed burst size for uplink and downlink traffic.

   Uplink traffic originates from the subscriber towards the public data network (PDN), and downlink traffic comes from the PDN and is destined for the subscriber. The range is 1500 through 1,500,000,000 bytes.

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set burst-size uplink uplink-burst-size downlink downlink-burst-size
```

RELATED DOCUMENTATION

- Understanding IFL-Based Subscriber Setup | 115
- Understanding the Definition of a Set of IFL-Based Subscriber Properties with a TDF Domain | 116
- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Dynamic Policies | 98
- Configuring a Services Interface for a Session PIC or Service PIC | 15

Configuring a TDF Logical Interface

A TDF logical interface is distinct from other types of interfaces and is used to associate a TDF domain's subscribers with an access interface in a virtual routing and forwarding (VRF) table and with a TDF service set. You need to configure one TDF interface logical interface (unit) for every TDF domain.

To configure a TDF interface, you configure one or more logical interfaces (units) for the interface:

1. Configure a TDF logical interface. Repeat this step for each TDF domain.

```
[edit interfaces]
user@host# set mif unit interface-unit-number family family-name
```

2. (Optional) Configure the maximum transmission unit (MTU) size for the TDF logical interface.

```
[edit interfaces]
user@host# set mtu mtu-size
```

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | 140

Configuring TDF Interface to Access Interface Associations in VRFs | 144

Applying Services to Subscriber-Aware Traffic with a Service Set | 146

Configuring TDF Interface to Access Interface Associations in VRFs

Junos associates TDF interfaces (mif) with access interfaces. You must configure a virtual routing and forwarding (VRF) table for each TDF domain. The VRF must include the TDF interface and one or more access interfaces for the TDF domain.

Before you begin, make sure that you have done the following:

- Configured the access interfaces on the MX Series router chassis.
- Configured the TDF interfaces.

To configure a TDF interface-to-access port mapping in a VRF, specify the VRF and place both the TDF interface (unit) and the physical access interface unit in the same VRF.

- Configure the VRF routing instance.

```
[edit routing-instances]
user@host# set routing-instance interface mif.n
user@host# set routing-instance interface interface-name
```

RELATED DOCUMENTATION

Configuring a TDF Logical Interface | 143

Applying Services to Subscriber-Aware Traffic with a Service Set | 146

CHAPTER 7

Configuring Services

IN THIS CHAPTER

- Overview of Applying Services to Subscribers | 145
- Applying Services to Subscriber-Aware Traffic with a Service Set | 146

Overview of Applying Services to Subscribers

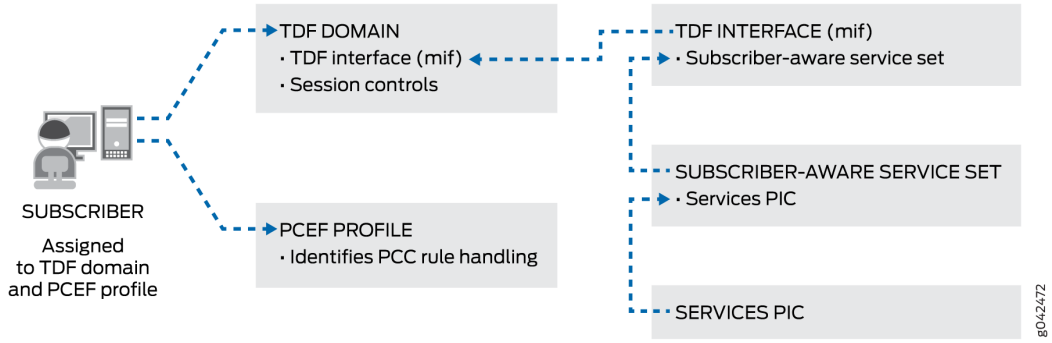
Subscriber-aware services are enabled for the subscribers belonging to a specific TDF domain by creating a subscriber-aware service set. This service set is applied to the TDF domain's TDF interface (mif). These services are carried out on the service PIC that is identified by the service interface in the service set.

Subscriber-aware services are applied to a subscriber's traffic based on policy and control (PCC) rules. The PCC rules are either under local control, under PCRF dynamic control, or under activation and deactivation control by a RADIUS server, depending on the PCEF profile for the TDF domain.

You may also apply network address translation (NAT) services independently of the PCC rules by specifying NAT rules in the service set.

Figure 12 on page 146 shows the relationships among subscriber-aware service sets and other configured objects.

Figure 12: Subscriber-Aware Service Set Relationships



RELATED DOCUMENTATION

Applying Services to Subscriber-Aware Traffic with a Service Set | 146

Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | 52

Applying Services to Subscriber-Aware Traffic with a Service Set

Junos OS supports subscriber-aware services for the subscribers belonging to a particular TDF domain through the configuration of a subscriber-aware service set. The service set is assigned to the TDF domain's TDF interface (mif).

Before you configure the service set, complete the following tasks:

- Configure the service PIC for the service set.
- Configure the TDF interface (mif).
- Configure the PCEF profile at the **[edit unified-edge pcef]** hierarchy level.
- Configure any NAT rules or rule sets that you want to apply.

To configure the subscriber-aware services for a TDF domain's subscribers:

1. Configure a PCEF profile at the [**services**] hierarchy level by specifying a name for the PCEF profile. This profile is a placeholder profile with no configuration options, but it must be created.

```
[edit services]
user@host# set pcef profile pcef-profile-name
```

2. Configure an application identification profile by specifying a name for the profile. This profile is a placeholder profile with no configuration options, but it must be created.

```
[edit services application-identification]
user@host# set profile app-id-profile-name
```

3. Configure an HTTP header enrichment profile by specifying a name for the profile. This profile is a placeholder profile with no configuration options, but it must be created.

```
[edit services hcm]
user@host# set profile hcm-profile-name
```

4. Define a subscriber-aware service set.

```
[edit services]
user@host# set service-set service-set-name service-set-options subscriber-awareness
```

5. Enable PCEF services for the service set. Use the profile name that you configured in Step "1" on page 147.

```
[edit services service-set service-set-name]
user@host# set pcef-profile pcef-profile-name
```

6. Enable application identification for the service set. Use the profile name that you configured in Step "2" on page 147.

```
[edit services service-set service-set-name]
user@host# set application-identification-profile app-id-profile-name
```

7. Enable HTTP header enrichment for the service set. Use the profile name that you configured in Step "3" on page 147.

```
[edit services service-set service-set-name]
user@host# set hcm-profile hcm-profile-name
```

8. Specify NAT rules or rule-sets for the service set.

```
[edit services service-set service-set-name]
user@host# set ([nat-rules rule-name] | nat-rule-sets rule-set-name)
```

9. Specify the services PIC interface on which the services are performed.

```
[edit services service-set service-set-name]
user@host# set interface-service service-interface interface-name
```

The *interface-name* is ams*n* if you have redundancy configured and is ms-*fpc*/*pci*/0 if you do not have redundancy configured.

10. Apply the service set to the TDF interface (mif) that is part of the TDF domain.

```
[edit interfaces mif unit number family family service]
user@host# set input service-set service-set-name
user@host# set output service-set service-set-name
```

NOTE: The output service set for the mif is not used by the MX Series router, but it must be configured so that the configuration commit does not fail.

RELATED DOCUMENTATION

Configuring Service PICs | 18

Configuring a TDF Logical Interface | 143

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Dynamic Policies | 98

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Static Policies | 100

CHAPTER 8

Configuring Diameter

IN THIS CHAPTER

- Diameter Profiles Overview | 149
- Juniper Networks Diameter AVPs for Subscriber Aware Policy Control | 150
- Configuring Diameter Overview | 152
- Configuring Diameter Profiles | 152
- Configuring Diameter Bindings | 154
- Configuring Diameter Network Elements | 155
- Configuring Diameter AVPs for Gx Applications | 156
- Configuring Diameter Peers | 158
- Configuring the Diameter Transport | 161
- Configuring Advertisements in Diameter Messages | 162
- Configuring Parameters for Diameter Applications | 162
- Configuring the Origin Attributes of the Diameter Instance | 163

Diameter Profiles Overview

The Diameter profile provides network access information for the Diameter application. The Diameter profile specifies prioritized targets, or endpoints, for particular applications. The target specifies the destination realm, network element, and priority associated with the target.

Target selection is based on priority. A lower number has a higher priority. For load balancing, targets have the same priority.

From the prioritized list of targets for a Diameter profile, the target is selected as follows:

- The target with the highest priority (lowest number) is selected.
- In the event of a tie, where the priority is the same, target selection alternates among the peers with the same priority.

NOTE: Failover handling depends on what enables the policy for the application. Switching between targets based on priority, such as failing over between primary and secondary online charging servers, only occurs if the failover handling policy enables it.

After you configure the Diameter profiles, the Diameter applications can reference them. For example, when configuring transport profiles for online charging, you can associate the configured Diameter profile with the transport profile to interact with the online charging server. Similarly, when configuring profiles for provisioning Policy Charging and Control application rules, you can associate the configured Diameter profile with the policy and charging enforcement function (PCEF) profile to interact with the policy and charging rules function (PCRF).

RELATED DOCUMENTATION

Configuring Diameter Profiles | 152

Juniper Networks Diameter AVPs for Subscriber Aware Policy Control

Diameter conveys information by including various attribute-value pairs (AVPs) in Diameter messages.

Table 6 on page 150 lists the AVPs for subscriber policy control.

Table 6: Juniper Networks Diameter AVPs for Subscriber Policy Control

Attribute Number	Diameter AVP	Description	Type
1100	TDF-Application-Instance-Identifier-Base	Identifies the application-group.	UTF8String
1101	Service-Chaining-Information	Provides service chaining information for dynamic steering of packets.	UTF8String
1102	LRF-Profile-Name	Provides the name of the logging and reporting framework (LRF) profile.	UTF8String

Table 6: Juniper Networks Diameter AVPs for Subscriber Policy Control *(Continued)*

Attribute Number	Diameter AVP	Description	Type
1103	HCM-Profile-Name	Provides the name of the HTTP content module.	UTF8String
1104	Forwarding-Class-Name	Provides the forwarding class name on the router.	UTF8String
1105	Redirect-VRF	Specifies whether redirection is supported. If the application flows support redirection, Redirect-VRF specifies the redirect address and address type.	UTF8String
1106	Requested-Burstsize-UL	Provides the uplink burst size specified in a QoS policy.	Integer32
1107	Requested-Burstsize-DL	Provides the downlink burst size specified in a QoS policy.	Integer32
1108	Steering-Information	Specifies an optional grouped AVP that contains Steering-Uplink-VRF, Steering-Downlink-VRF, and Steering-IP-Address.	Grouped
1109	Steering-Uplink-VRF	Provides the address of uplink destination for packets if dynamic steering is supported.	UTF8String
1110	Steering-Downlink-VRF	Provides the address of downlink destination for packets if dynamic steering is supported.	UTF8String
1111	Steering-IP-Address	Identifies the IP address for HTTP redirect.	Address

Configuring Diameter Overview

If you are using a PCRF to dynamically control subscriber-aware policies, you must configure Diameter.

To configure Diameter for PCRF-controlled subscriber-aware policies:

1. Configure the remote peer to which the MX Series router sends Diameter messages.
   See "Configuring Diameter Peers" on page 158.
2. Identify the session PIC and PIC interfaces for a Diameter network element.
   See "Configuring Diameter Bindings" on page 154.
3. Configure the peers in a Diameter network element.
   See "Configuring Diameter Network Elements" on page 155.
4. Configure network access information in a Diameter profile.
   See "Configuring Diameter Profiles" on page 152.
5. (Optional) Specify the Diameter attribute-value pairs (AVPs) to include and exclude in the credit control request (CCR) messages.
   See "Configuring Diameter AVPs for Gx Applications" on page 156.
6. Configure the Diameter transport.
   See "Configuring the Diameter Transport" on page 161.
7. Configure the information to be advertised in Diameter messages.
   See "Configuring Advertisements in Diameter Messages" on page 162.
8. Configure the maximum number of pending requests for a Diameter application.
   See "Configuring Parameters for Diameter Applications" on page 162.
9. Configure the endpoint node that originates Diameter messages.
   See "Configuring the Origin Attributes of the Diameter Instance" on page 163.

RELATED DOCUMENTATION

Diameter Profiles Overview | 149

Configuring Diameter Profiles

The Diameter profile provides network access information for the Diameter application.

NOTE: To make a change to a Diameter profile, you must be in maintenance mode. (See "Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles" on page 220).

To configure the Diameter profile:

1. Create the Diameter profile for the Gx application (**gx-profile**).

```
[edit]
user@host# set unified-edge diameter-profiles gx-profile profile-name
```

2. Set up the target for the profile.

```
[edit unified-edge diameter-profiles gx-profile profile-name]
user@host# set targets target-name
```

3. Specify the destination realm associated with the target.

```
[edit unified-edge diameter-profiles gx-profile profile-name targets target-
name]
user@host# set destination-realm realm-name
```

4. Specify the priority associated with the target.

   The prioritization determines failover or load-balancing behavior. For load balancing, configure the targets with the same priority.

```
[edit unified-edge diameter-profiles gx-profile profile-name targets target-
name]
user@host# set priority priority-value
```

5. Specify the network element associated with the target.

```
[edit unified-edge diameter-profiles gx-profile profile-name targets target-
name]
user@host# set network-element element-name
```

6. (Optional) Specify the destination host associated with the target.

```
[edit unified-edge diameter-profiles gx-profile profile-name targets target-name]
user@host# set destination-host hostname
```

RELATED DOCUMENTATION

- Diameter Profiles Overview | 149
- Configuring Diameter Bindings | 154
- Configuring Diameter Network Elements | 155
- Configuring Diameter AVPs for Gx Applications | 156
- Configuring Diameter Peers | 158
- Configuring the Diameter Transport | 161
- Configuring Advertisements in Diameter Messages | 162
- Configuring Parameters for Diameter Applications | 162
- Configuring the Origin Attributes of the Diameter Instance | 163
- gx-profile | 429
- diameter (TDF Gateway) | 370
- diameter (Subscriber Aware Policy Control) | 368

Configuring Diameter Bindings

You can configure a Diameter network element to run on a specific session PIC. You can organize other session PICs in a group around the selected session PIC on which the configured network element runs. When organized in a group, the selected session PIC can send and receive messages for other session PICs in the group. By default, every Diameter network element runs on every session PIC.

NOTE: If you want to set up Diameter bindings for session PICs on the broadband gateway, contact Juniper Networks Professional Services for assistance.

To configure the Diameter binding for network elements:

1. Configure the network element used for the Diameter binding on the broadband gateway.

```
[edit]
user@host# set unified-edge tdf gateway gateway-name diameter network-element element-name
```

2. Specify the session PICs group that serves the network element.

```
[edit unified-edge tdf gateway gateway-name diameter network-element element-name]
user@host# set session-pics group group-name
```

3. Specify the session PIC interfaces in this group that serve the network element. The interface must be a multiservices interface.

```
[edit unified-edge tdf gateway gateway-name diameter network-element element-name session-pics group group-name]
user@host# set session-pic ams number
user@host# set session-pic ms-fpc/pic/port
```

RELATED DOCUMENTATION

Configuring Diameter Profiles | 152

Configuring Diameter Network Elements

A Diameter network element consists of associated functions and a list of prioritized peers. The functions associate a Diameter application with the network element. The prioritization determines failover or load-balancing behavior for peer selection.

Before you configure Diameter network elements, perform the following task:

- Define the Diameter peers. See "Configuring Diameter Peers" on page 158.

To configure a Diameter network element:

1. Specify the name of the network element.

```
[edit access diameter]
user@host# set network-element element-name
```

2. Associate one or more functions with the network element.

   All functions are associated by default.

```
[edit access diameter network-element element-name]
user@host# set function function-name
```

3. Associate a Diameter peer with the network element and set the priority for the peer.

   Peers with the lower priority number have the higher priority for peer selection. Peers with the same priority are load-balancing peers so the peer selection alternates between the two peers.

```
[edit access diameter network-element element-name]
user@host# set peer peer-name priority priority-value
```

4. (Optional) Associate a Diameter peer with the network element and set the amount of time to wait for a response from this peer before retransmitting the request to another peer. The default is 4 seconds.

```
[edit access diameter network-element element-name]
user@host# set peer peer-name timeout seconds
```

RELATED DOCUMENTATION

Configuring Diameter Profiles | 152

Configuring Diameter AVPs for Gx Applications

You can exclude Diameter attribute-value pairs (AVPs) from or include in the credit control request (CCR) messages between the MX Series router and the policy and charging rules function (PCRF) server.

NOTE: The configuration of the Diameter AVPs for dynamic PCEF policies is optional.

To configure Diameter AVPs for Gx applications:

1. Specify the name of the Diameter Gx profile for which you are configuring the Diameter AVPs.

```
[edit]
user@host# edit unified-edge diameter-profiles gx-profile profile-name
```

   The Diameter Gx profile name can contain letters, numbers, and hyphens (-) and can be up to 128 characters long.

2. Specify the optional AVPs to be excluded from the CCR messages between the MX Series router and the PCRF. By default, all AVPs are included in the CCR messages.

```
[edit unified-edge diameter-profiles gx-profile profile-name]
user@host# set attributes exclude [attribute]
```

   You can specify more than one AVP in a single line.

   Table 7 on page 157 describes the AVPs that you can exclude from CCR messages.

Table 7: Diameter AVP Exclusions for Gx Applications

AVP	Information in AVP
an-gw-address	AN-GW-Address AVP, which contains the IP addresses of the access node gateway.
default-eps-bearer-qos	Default-EPS-Bearer-QoS AVP.
packet-filter-information	Packet-Filter-Information AVP.
packet-filter-operation	Packet-Filter-Operation AVP.
rat-type	RAT-Type AVP.

3. Specify the optional AVPs to be included in the CCR messages between the MX Series router and the PCRF. By default, all AVPs are included in the CCR messages.

```
[edit unified-edge diameter-profiles gx-profile profile-name]
user@host# set attributes include [attribute]
```

You can specify more than one AVP in a single line.

Table 8 on page 158 describes the AVPs that you can included in CCR messages.

Table 8: Diameter AVP Inclusions for Gx Applications

AVP	Information in AVP
gx-capability-list	Gx-capability-list AVP.
rule-suggestion	Rule-suggestion AVP.

RELATED DOCUMENTATION

Configuring Diameter Profiles | 152

Configuring Diameter Peers

You can configure the remote peers to which Diameter sends messages. Port 3868 is used for active connections to peers by default.

To configure a remote peer for a Diameter instance:

1. Specify the name of the Diameter peer.

```
[edit access diameter]
user@host# set peer peer-name
```

2. Specify the address of the Diameter peer.

```
[edit access diameter peer peer-name]
user@host# set address ip-address
```

3. Specify the transport that Diameter uses for active connections to the peer.

```
[edit access diameter peer peer-name]
user@host# set connect-actively transport transport-name
```

4. (Optional) Specify the port that Diameter uses for active connections to the peer. The default is port 3868.

```
[edit access diameter peer peer-name]
user@host# set connect-actively port port-number
```

5. (Optional) Specify the time to wait for connection acknowledgment from the peer. The default is 10 seconds.

```
[edit access diameter peer peer-name]
user@host# set connect-actively timeout seconds
```

6. (Optional) Specify the time to wait before trying to reconnect to a peer after receiving a Disconnect-Peer-Request message with the DO_NOT_WANT_TO_TALK_TO_YOU value for the Disconnect-Cause AVP. If you do not set a value, no reconnection attempt is made.

```
[edit access diameter peer peer-name]
user@host# set connect-actively repeat-timeout seconds
```

7. (Optional) Specify the time to wait for a Capabilities-Exchange-Answer message from the peer. The default is 10 seconds.

```
[edit access diameter peer peer-name]
user@host# set connect-actively capabilities-exchange-timeout seconds
```

8. (Optional) Specify the time to wait between connection attempts for this peer. The default is 30 seconds.

```
[edit access diameter peer peer-name]
user@host# set connect-actively retry-timeout seconds
```

9. (Optional) Specify the time to wait for a Device-Watchdog-Answer message from the peer. The default is 30 seconds.

```
[edit access diameter peer peer-name]
user@host# set watchdog-timeout seconds
```

10. (Optional) Specify the time to wait in the Closing state while disconnecting this peer. The default is 10 seconds.

```
[edit access diameter peer peer-name]
user@host# set disconnect-peer-timeout seconds
```

11. (Optional) Specify the size of the incoming queue for the peer. The default is 6000. You can specify a smaller value if you want to throttle the peer.

```
[edit access diameter peer peer-name]
user@host# set incoming-queue size size
```

12. (Optional) Specify the size of the outgoing queue for the peer. The default is 6000. You can specify a smaller value if you want to throttle the peer.

```
[edit access diameter peer peer-name]
user@host# set outgoing-queue size size
```

13. (Optional) Specify the high watermark of the outgoing queue for the peer.

    The default is 80 percent. If the queue size reaches the high watermark, the peer is marked unavailable, any new messages to the Diameter network element are not sent to this peer, and the SNMP trap **Diameter_PeerOutQHiWMarkNotif** is generated.

```
[edit access diameter peer peer-name]
user@host# set outgoing-queue high-watermark high-watermark
```

14. (Optional) Specify the low watermark of the outgoing queue for the peer.

The default is 60 percent. If the queue size descends to the low watermark after reaching the high watermark, the peer becomes available and the SNMP trap **Diameter_PeerLowQHiWMarkNotif** is generated.

```
[edit access diameter peer peer-name]
user@host# set outgoing-queue low-watermark low-watermark
```

RELATED DOCUMENTATION

Configuring Diameter Profiles | 152

Configuring the Diameter Transport

You can configure one or more transports for a Diameter instance to set the source IP address for the local connection, and optionally configure a routing instance context. The routing instance for the transport connection must match that for the peer, or a configuration error is reported. Multiple peers can share the same transport.

To configure a transport for a Diameter instance:

1. Configure the transport name.

```
[edit access diameter]
user@host# set transport transport-name
```

2. Configure the source IP address for the Diameter local transport connection.

```
[edit access diameter transport transport-name]
user@host# set address ip-address
```

3. (Optional) Configure a routing instance, to which the address is bound, for the transport.

```
[edit access diameter transport transport-name]
user@host# set routing-instance routing-instance
```

RELATED DOCUMENTATION

Configuring Diameter Profiles | 152

Configuring Advertisements in Diameter Messages

You can configure information advertised in the Capabilities-Exchange-Request or Capabilities-Exchange-Answer messages. This information includes firmware revision, product name, and vendor identification.

To configure the advertisements:

1. (Optional) Specify the value for the Firmware-Revision AVP that is advertised. 0 is the default.

```
[edit access diameter]
user@host# set firmware-revision firmware-revision
```

2. (Optional) Specify the value of the Product-Name AVP that is advertised. Juniper Diameter Client is the default.

```
[edit access diameter]
user@host# set product-name name
```

3. (Optional) Specify the value of the Vendor-Id AVP that is advertised. 2636 is the default.

```
[edit access diameter]
user@host# set vendor-id vendor-id
```

RELATED DOCUMENTATION

Configuring Diameter Profiles | 152

Configuring Parameters for Diameter Applications

You can configure parameters for Diameter applications, including the maximum number of pending requests.

To configure the parameters for the Diameter application:

1. Specify the Gx application (**pcc-gx**), for which you want to configure parameters.

```
[edit access diameter]
user@host# set applications pcc-gx
```

2. (Optional) Specify the maximum number of pending requests for the Diameter application. The default is 20,000.

```
[edit access diameter applications pcc-gx]
user@host# set maximum-pending-requests requests
```

RELATED DOCUMENTATION

Configuring Diameter Profiles | 152

Configuring the Origin Attributes of the Diameter Instance

You can configure the identifying characteristics of the endpoint node that originates Diameter messages for the Diameter instance. The hostname is supplied as the value for the Origin-Host prefix. The realm is supplied as the value for the Origin-Realm attribute-value pair (AVP).

To configure the origin attributes:

1. Specify the Origin-Host prefix that originates the Diameter message.

```
[edit access diameter origin]
user@host# set host hostname
```

2. Specify the realm of the host that originates the Diameter message.

```
[edit access diameter origin]
user@host# set realm realm-name
```

RELATED DOCUMENTATION

Configuring Diameter Profiles | 152

PART 3

Configuring Reporting for Subscriber-Aware Data Sessions

Configuring Reporting | 166

CHAPTER 9

Configuring Reporting

IN THIS CHAPTER

- Logging and Reporting Function for Subscribers | **166**
- Log Dictionary for Template Types | **174**
- Configuring Logging and Reporting for Junos OS Subscriber Aware | **186**
- Configuring an LRF Profile for Subscribers | **187**
- Assigning an LRF Profile to Subscribers | **194**
- Configuring the Activation of an LRF Rule by a PCC Rule | **196**

Logging and Reporting Function for Subscribers

IN THIS SECTION

- Log and Report Control | **167**
- Templates | **167**
- HTTP Transaction Logging | **172**

The logging and reporting function (LRF) enables you to log data for subscriber application-aware policy control sessions and send that data in an IPFIX format to an external log collector using UDP-based transport. These data session logs can include subscriber information, application information, HTTP metadata, data volume, time-of-day information, and source and destination details.

Starting in Junos OS Release 16.1R4 and in Junos OS Release 17.2R1, LRF is available in Junos OS Broadband Subscriber Management. Starting in Junos OS Release 19.3R2, LRF is available in Junos OS Broadband Subscriber Management if you have enabled Next Gen Services on the MX240, MX480 or MX960 router with the MX-SPC3 card..

The external collector, which is not a Juniper Networks product, can then use this data to perform analytics that provide you with insights about subscriber and application usage, allowing you to create packages and policies that increase revenue.

Log and Report Control

A subscriber's data sessions are logged and sent to collectors based on an LRF profile that you configure and associate with the subscriber.

The LRF profile includes:

- Templates—Specify the type of data that you want sent and the trigger that causes data to be sent. You can configure a maximum of 16 templates in an LRF profile.
- Collectors—Identify the destination to send data to. You can configure a maximum of eight collectors in an LRF profile.
- LRF rules—Specify the template and collector to use and, if applicable, a data volume limit that triggers the sending of data. An LRF rule's actions are performed when the matching conditions in a static PCC rule that references the LRF rule are met. You can configure a maximum of 32 LRF rules in an LRF profile.

To associate the LRF profile with a subscriber:

- For Junos OS Subscriber Aware, assign the LRF profile to the subscriber-aware TDF service set that belongs to the TDF interface (mif) in the subscriber's TDF domain.
- For Junos OS Broadband Subscriber Management, assign the LRF profile to the service set that is configured for application-aware policy control.

Templates

NOTE: If you have enabled Next Gen Services with the MX-SPC3 services card, then the DNS, IPv4 extended, IPv6 extended, mobile subscriber, video, and wireline subscriber templates are not supported.

You specify the data fields in a template by configuring one or more types for the template; for example, HTTP and IPv4. Each type represents a set of fields, and the template you configure includes fields from all the types you configure. The template is sent to the collector when you configure it, and is re-sent at a configurable interval. The template types that you can select and the fields that are included by each type are:

- Device Data—Contains data fields specific to the device collecting the logging feed:

  - DPI Engine Version
  - IP address of TDF gateway (in IPv4 format)
- DNS—(Not available if Next Gen Services is enabled with the MX-SPC3 services card) Contains the DNS response time data field.
- Flow ID—Contains the Flow ID data field.

  When HTTP multiple transaction logging is enabled, FlowID is an implicit type that gets included with the HTTP template. When the consolidated session log is generated at the time of SESSION_CLOSE, LRF includes the FlowID that can be used to correlate with the HTTP transaction log records.
- HTTP—Contains data fields for the HTTP metadata from header fields:
  - User Agent
  - Content Length - Request
  - HTTP Response Code
  - Language
  - Host
  - Location
  - Http Method
  - Referer (HTTP)
  - MIME type
  - Time to First Byte
- IFL subscriber— Contains data fields specific to IFL-based subscribers:
  - Subscriber Name—Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).
  - IFL Name—Filled with default IFL name (filled with values Next Gen Services IFL)
- IPFlow—Contains data fields for the uplink and downlink octets and bytes. When a data record for volume limit is exported, these IPFlow statistics in the record are the actual data received after the last volume limit was reported in that data session and *not* cumulative data.
  - Uplink Octets
  - Downlink Octets

    - Uplink Packets
    - Downlink Packets
    - Ip Protocol—Protocol ID from IP header; for example, 17 (UDP), 6 (TCP).
    - Record Reason—A value of **1** for the session close and a value of **2** for volume-limit.
- IPFlow Extended—Contains data fields for the service set name, routing instance, and payload timestamps. The initiator of the very first packet of a session is the client and the responder is the server.
    - Service-Set-Name—Filled with active **service-set-name** (16 byte value is filled active **service-set-name**. For example, if **service-set-name** is: bng-service-set-1, the template has a value of: bng-service-set-(16bytes)
    - Routing-Instance—Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).
- IPFlow TCP—Contains data fields for TCP-related timestamps:
    - Retransmitted TCP packets uplink
    - Retransmitted TCP packets downlink
    - TCP flow creation timestamp
- IPFlow TCP Timestamp—Contains IBM-specific data fields for TCP-related timestamps:
    - Smooth RTT uplink
    - Smooth RTT downlink
    - Client setup time
    - Server Setup time
    - First Client Payload timestamp
    - Upload time
    - First Server Payload timestamp
    - Download time
    - Acknowledged volumes uplink
    - Acknowledged volumes downlink

To use the IPFlow TCP Timestamp template when configuring an LRF profile, identify the template as vendor specific to avoid a commit warning. See *Configuring an LRF Profile for Subscribers*.

- IPFlow Timestamp—Contains data fields for the flow start and end timestamps:
  - Flow Start Time—For TCP, the flow start time is when the SYN packet is received. For UDP, it is when the first packet is sent.
  - Flow End Time
- IPv4—Contains data fields for the basic source and destination IPv4 information:
  - Source IPv4 Address
  - Destination IPv4 Address
- IPv4 Extended—(Not available if Next Gen Services with the MX-SPC3 services card are enabled) Contains data fields for the elements of IPv4 extended fields:
  - IPv4 TOS / Class of Service
  - IPv4 Source Mask
  - IPv4 Destination Mask
  - IPv4 Next Hop
- IPv6—Contains data fields for the basic source and destination IPv6 information:
  - Source IPv6 Address
  - Destination IPv6 Address
- IPv6 Extended—(Not available if Next Gen Services are enabled with the MX-SPC3 services card) Contains data fields for the elements of IPv6 extended fields:
  - IPv6 Source Mask
  - IPv6 Destination Mask
  - IPv6 Next Hop
  - Traffic Class
- L7 Application—Contains data fields for the Layer 7 application:
  - Application Protocol—Application data protocol below the classified application name; for example, **http** or **ssl**.
  - Application Name—Application name; for example, **junos:facebook** or **junos:Netflix**.

    - Host—HTTP header host when application protocol is **http**, SSL common name when application protocol is **ssl**, DNS name when application protocol is **dns**.

- Mobile Subscriber—(Not available if Next Gen Services with the MX-SPC3 services card are enabled) Contains data fields specific to mobile subscribers:
    - IMSI
    - MSISDN
    - IMEI
    - RAT-type
    - ULI
    - RADIUS Called Station ID
- PCC—Contains the PCC rule name data field.Not applicable if Next Gen Services are enabled.
- Status Code Distribution—Contains data fields for the HTTP or DNS status codes:
    - Status code 1
    - Status code 2
    - Status code 3
    - Status code 4
    - Status code 5
    - Num Instances 1
    - Num Instances 2
    - Num Instances 3
    - Num Instances 4
    - Num Instances 5
- Subscriber Data—Contains data fields for Generic Subscriber information that can be included with wireless (mobile) subscribers or wireline subscribers:
    - NAS_IP_ADDR—Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).
    - Subscriber Type—1 for IP-based subscriber, 2 for IFL-based subscriber.
    - Subscriber IP Address

  - Subscriber VRF—Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).
  - NAS Port ID—Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).
  - Accounting-Session-Id—Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).
  - Class—Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).
  - NAS Port Type—Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).
- Transport Layer—Contains data fields for the transport layer:
  - Source Transport Port
  - Destination Transport Port
- Video—(Not available if Next Gen Services with the MX-SPC3 services card are enabled) Contains data fields for video traffic:
  - Bitrate
  - Duration
- Wireline Subscriber—(Not available if Next Gen Services with the MX-SPC3 serices card are enabled) Contains the UserName data field for wireline subscribers. This is the same as RADIUS Called Station ID.

The template that is specified in an LRF rule determines the set of data fields that are included when data is sent to a collector. The data message includes a pointer to the template ID so that the collector can correlate the data contents with the data field lengths and types.

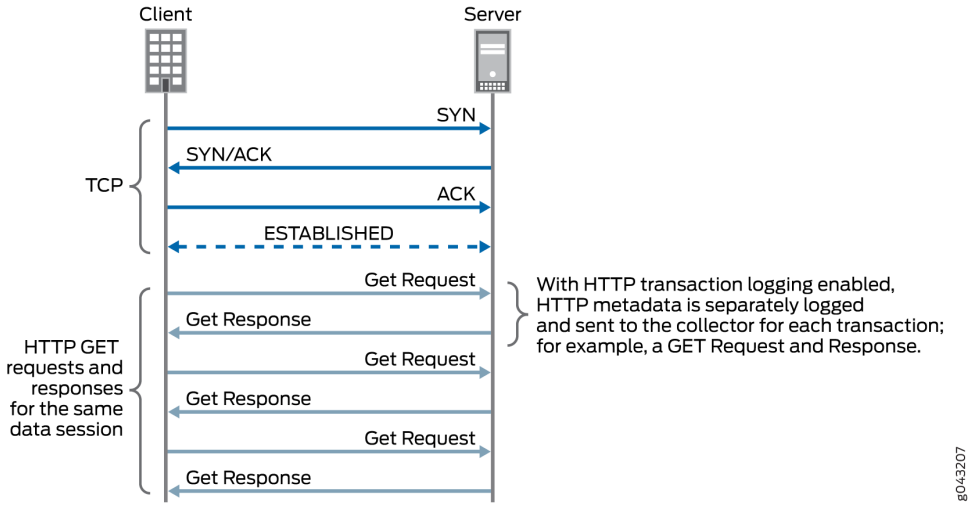
In a template, you also specify the type of trigger that determines when to send data to the collector. This trigger type can be a data volume limit, a time limit, or the closing of a data session (UDP sessions are considered closed after 60 seconds of inactivity; TCP sessions are considered closed when a FIN, FIN-ACK, or RST is received).

HTTP Transaction Logging

You may enable HTTP transaction logging in an LRF profile. This causes each HTTP transaction in a TCP session to be separately logged and sent to the collector, as shown in Figure 13 on page 173. This option is only relevant when the template being used includes HTTP in the template type.

By default, HTTP transaction logging is disabled, and the HTTP transaction records for a TCP session are sent together as one group of records.

Figure 13: HTTP Transaction Logging



Release History Table

Release	Description
19.3R1	Starting in Junos OS Release 19.3R2, LRF is available in Junos OS Broadband Subscriber Management if you have enabled Next Gen Services on the MX240, MX480 or MX960 router with the MX-SPC3 card..
16.1R4	Starting in Junos OS Release 16.1R4 and in Junos OS Release 17.2R1, LRF is available in Junos OS Broadband Subscriber Management.

RELATED DOCUMENTATION

Log Dictionary for Template Types

Configuring Logging and Reporting for Junos OS Subscriber Aware

Configuring Logging and Reporting for Subscriber Management

Log Dictionary for Template Types

Table 9 on page 174 shows the logging dictionary of the template types that LRF supports. The log fields are a mix of IETF standard fields and fields that Juniper Networks defined. The IPFIX convention for vendor-defined fields is an enterprise bit set to **1** and an enterprise ID set to the vendor-ID. (The Juniper Networks vendor-ID is 2636.) An IETF standard field has an enterprise bit set to **0** and no value for the enterprise ID.

NOTE: If you have enabled Next Gen Services with the MX-SPC3 services card, then the DNS, IPv4 extended, IPv6 extended, mobile subscriber, video, and wireline subscriber templates are not supported.

Table 9: Logging Dictionary for Template Types

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
Device Data	DPI Engine Version	1/2636	503	string	32
	IP address of TDF gateway.	1/2636	502	ipv4Address	4
DNS (Not available if Next Gen Services with the MX-SPC3 services card are enabled)	DNS response time	1/2636	876	dateTimeMilliseconds	8
Flow ID	Flow ID	1/2636	107	unsigned32	4
HTTP	User Agent	1/2636	152	string	32

Table 9: Logging Dictionary for Template Types *(Continued)*

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
	Content Length - Request	1/2636	154	unsigned32	4
	HTTP Response Code	1/2636	155	unsigned16	2
	Language	1/2636	156	string	16
	Host	1/2636	157	string	64
	Location	1/2636	158	string	64
	Http Method	1/2636	159	string	8
	Referer(HTTP)	1/2636	160	string	64
	MIME type	1/2636	161	string	32
	Http URI	1/2636	163	string	255
	Time to First Byte	1/2636	181	dateTimeMilliseconds	8

Table 9: Logging Dictionary for Template Types *(Continued)*

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
IFL Subscriber	Subscriber Name	1/2636	511	string Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).	16
	IFL Name	1/2636	512	string Filled with default IFL name (filled with values Next Gen Services IFL)	16
IPFlow	Uplink Octets	1/2636	103	unsigned32	4
	Downlink Octets	1/2636	104	unsigned32	4
	Uplink Packets	1/2636	105	unsigned32	4
	Downlink Packets	1/2636	106	unsigned32	4
	Ip Protocol	0	4	unsigned8	1

Table 9: Logging Dictionary for Template Types *(Continued)*

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
	Record Reason	1/2636	112	unsigned8	1
IPFlow Extended	Service-Set-Name	1/2636	520	string Contains data fields for the **service-set-name**, **routing-instance**, and payload timestamps. The initiator of the very first packet of a session is the client and the responder is the server. Filled with active **service-set-name** (16 byte value is filled active **service-set-name**. For example, if **service-set-name** is: bng-service-set-1, the template has a value of: bng-service-set-(16bytes)	16

Table 9: Logging Dictionary for Template Types *(Continued)*

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
	Routing-Instance	1/2636	521	string Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).	16
IPFlow TCP Timestamp	Retransmitted TCP packets uplink	1/2636	115	unsigned32	4
	Retransmitted TCP packets downlink	1/2636	116	unsigned32	4
	Smooth RTT uplink	1/2636	117	dateTimeMilliseconds	8
	Smooth RTT downlink	1/2636	118	dateTimeMilliseconds	8
	Client setup Time	1/2636	119	dateTimeMilliseconds	8
	Server Setup time	1/2636	120	dateTimeMilliseconds	8

Table 9: Logging Dictionary for Template Types *(Continued)*

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
	TCP flow creation timestamp	1/2636	121	dateTimeMilliseconds	8
	First Client Payload TS	1/2636	108	dateTimeMilliseconds	8
	Upload time	1/2636	113	dateTimeMilliseconds	8
	First Server Payload TS	1/2636	110	dateTimeMilliseconds	8
	Download time	1/2636	114	dateTimeMilliseconds	8
	Acknowledged volumes uplink	1/2636	122	unsigned64	8
	Acknowledged volumes downlink	1/2636	123	unsigned64	8
IPFlow Timestamp	Flow Start Time	1/2636	101	dateTimeMilliseconds	8
	Flow End Time	1/2636	102	dateTimeMilliseconds	8

Table 9: Logging Dictionary for Template Types *(Continued)*

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
IPv4	Source IPv4 Address	0	8	ipv4Address	4
	Destination IPv4 Address	0	12	ipv4Address	4
IPv4 Extended (Not available if Next Gen Services with the MX-SPC3 services card are enabled)	IPv4 TOS/ Class of Service	0	5	unsigned8	1
	IPv4 Source Mask	0	9	unsigned8	1
	IPv4 Destination Mask	0	13	unsigned8	1
	IPv4 Next Hop	0	15	ipv4Address	4
IPv6	Source IPv6 Address	0	27	ipv6Address	16
	Destination IPv6 Address	0	28	ipv6Address	16
IPv6 Extended (Not available if Next Gen Services are	IPv6 Source Mask	0	29	unsigned8	1

Table 9: Logging Dictionary for Template Types *(Continued)*

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
enabled on the MX-SPC3 services card)	IPv6 Destination Mask	0	30	unsigned8	1
	IPv6 Next hop	0	62	ipv6Address	16
	Traffic Class	1/2636	126	unsigned8	1
L7 Application	Application Protocol	1/2636	151	string	32
	Application Name	1/2636	170	string	32
	Host	1/2636	157	string	64
Mobile Subscriber (Not available if Next Gen Services are enabled on the MX-SPC3 services card)	IMSI	1/2636	504	string	16
	MSISDN	1/2636	505	string	16
	IMEI	1/2636	506	string	16
	RAT-type	1/2636	507	unsigned8	1
	ULI	1/2636	508	string	13

Table 9: Logging Dictionary for Template Types *(Continued)*

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
	RADIUS Called Station ID	1/2636	509	string	32
PCC	PCC rule name	1/2636	901	string Not applicable if Next Gen Services are enabled.	64
Status Code Distribution	Status code 1	1/2636	171	unsigned16	2
	Status code 2	1/2636	172	unsigned16	2
	Status code 3	1/2636	173	unsigned16	2
	Status code 4	1/2636	174	unsigned16	2
	Status code 5	1/2636	175	unsigned16	2
	Num Instances 1	1/2636	176	unsigned16	2
	Num Instances 2	1/2636	177	unsigned16	2
	Num Instances 3	1/2636	178	unsigned16	2

Table 9: Logging Dictionary for Template Types *(Continued)*

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
	Num Instances 4	1/2636	179	unsigned16	2
	Num Instances 5	1/2636	180	unsigned16	2
Subscriber Data	NAS_IP_ADDR	1/2636	519	ipv4Address Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).	4
	Subscriber Type	1/2636	515	unsigned8 1 for IP-based subscriber, 2 for IFL-based subscriber	1
	Subscriber IP address	1/2636	516	ipv4Address	4

Table 9: Logging Dictionary for Template Types *(Continued)*

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
	Subscriber VRF	1/2636	517	unsigned32 Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).	4
	NAS Port ID	1/2636	518	string Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).	32
	Accounting-Session-Id	1/2636	514	string Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).	32

Table 9: Logging Dictionary for Template Types *(Continued)*

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
	Class	1/2636	522	String Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).	32
	NAS Port Type	1/2636	523	unsigned32 Not applicable for BNG subscribers, hence this value is not be honored (is filled with zero).	4
Transport Layer	Source Transport Port	0	7	unsigned16	2
	Destination Transport Port	0	11	unsigned16	2
Video (Not available if Next Gen Services are enabled on the MX-SPC3 services card)	Bitrate	1/2636	851	unsigned32	2

Table 9: Logging Dictionary for Template Types *(Continued)*

Template Type	Field Name	Enterprise Bit/ID	Information Element Identifier	Data Type	Data Length (bytes)
	Duration	1/2636	852	unsigned32	4
Wireline Subscriber (Not available if Next Gen Services are enabled on the MX-SPC3 services card)	UserName	1/2636	513	string	32

Configuring Logging and Reporting for Junos OS Subscriber Aware

To configure logging and reporting for traffic belonging to a set of subscribers, you configure LRF rules, collectors, and templates in an LRF profile; assign that LRF profile to the TDF service set associated with the subscribers' TDF domain; and assign each LRF rule to a PCC rule to activate it.

Before you begin to configure logging and reporting, you must:

- Configure the TDF domain for the subscriber.
- Configure the subscriber-aware service set for those subscribers.

To configure logging and reporting:

1. Configure an LRF profile to specify a set of logging and reporting parameters, which includes data templates, collectors, and LRF rules.

   See "Configuring an LRF Profile for Subscribers" on page 187.
2. Assign the LRF profile to a set of subscribers.

   See "Assigning an LRF Profile to Subscribers" on page 194.
3. Configure activation of an LRF rule with a static PCC rule.

   See "Configuring the Activation of an LRF Rule by a PCC Rule" on page 196.

RELATED DOCUMENTATION

Logging and Reporting Function for Subscribers | 166

Configuring an LRF Profile for Subscribers

IN THIS SECTION

- Configuring the LRF Profile Name | 187
- Configuring Policy-Based Logging | 188
- (Optional) Configuring HTTP Transaction Logging | 188
- Configuring Collectors | 188
- Configuring Templates | 190
- Configuring Logging and Reporting Rules | 192

NOTE: Starting in Junos OS Release 19.3R1, LRF profiles are also supported for Broadband Subscriber Management if Next Gen Services are enabled on the MX-SPC3 services card.

Configure an LRF profile to specify a set of logging and reporting parameters, which includes data templates, collectors, and LRF rules.

To configure an LRF profile:

Configuring the LRF Profile Name

An LRF profile is identified by a name, which you later specify in the service set for the subscribers.

- Configure a name for the LRF profile.

```
[edit services lrf]
user@host# set profile profile-name
```

For example:

```
[edit services lrf]
user@host# set profile lrf_profile1
```

Configuring Policy-Based Logging

Policy-based logging causes the LRF rules to be activated by PCC rules in a static PCEF profile.

- Configure policy-based logging in the LRF profile.

```
[edit services lrf profile profile-name]
user@host# set policy-based-logging
```

For example:

```
[edit services lrf profile  lrf_profile1]
user@host# set policy-based-logging
```

(Optional) Configuring HTTP Transaction Logging

Configure HTTP transaction logging if you want the HTTP metadata generated and sent separately for each transaction of a data session. This option is only relevant if the template specified in an LRF rule includes **http** in the **template-type**.

- Configure HTTP transaction logging in the LRF profile.

```
[edit services lrf profile profile-name]
user@host# set  http-log-multiple-transactions
```

For example:

```
[edit services lrf profile  lrf_profile1]
user@host# set  http-log-multiple-transactions
```

Configuring Collectors

Configure one or more collectors that you want to receive logging and reporting data when an LRF rule is activated. You can configure up to eight collectors for an LRF profile. For each collector:

1. Configure a name for the collector.

```
[edit services lrf profile profile-name]
user@host# set collector collector-name
```

For example:

```
[edit services lrf profile lrf_profile1]
user@host# set collector collector1
```

2. Specify the destination IP address of the collector.

```
[edit services lrf profile profile-name collector collector-name destination]
user@host# set address collector-address
```

For example:

```
[edit services lrf profile  lrf_profile1 collector collector1 destination]
user@host# set address 192.0.2.5
```

3. Specify the destination port of the collector.

```
[edit services lrf profile profile-name collector collector-name destination]
user@host# set port collector-port-number
```

For example:

```
[edit services lrf profile  lrf_profile1 collector collector1 destination]
user@host# set port 4739
```

4. Configure the source address to be used when exporting data to the collector.

```
[edit services lrf profile profile-name collector collector-name]
user@host# set source-address source-address
```

For example:

```
[edit services lrf profile lrf_profile1 collector collector1]
user@host# set source-address 10.1.1.1
```

Configuring Templates

Configure one or more templates, each of which specifies a set of data to be transmitted when an LRF rule is activated. You can configure up to 16 templates for an LRF profile. For each template:

1. Configure a name for the template.

```
[edit services lrf profile profile-name]
user@host# set template template-name
```

For example:

```
[edit services lrf profile lrf_profile1]
user@host# set template template1
```

2. Configure a format for the template. Only the IPFIX format is supported for this release.

```
[edit services lrf profile profile-name template template-name]
user@host# set format ipfix
```

For example:

```
[edit services lrf profile lrf_profile1 template template1]
user@host# set format ipfix
```

3. Configure the template types, which specify the data fields to include. You must configure at least one type, and you can configure multiple types.

```
[edit services lrf profile profile-name template template-name]
user@host# set template-type template-type
```

For example:

```
[edit services lrf profile lrf_profile1 template template1]
user@host# set template-type http ipv4
```

This example results in a template that includes fields from both the HTTP and IPv4 templates.

NOTE: If you have enabled Next Gen Services on the MX-SPC3 services card, then the DNS, IFL subscriber, IPv4 extended, IPv6 extended, mobile subscriber, video, and wireline subscriber templates are not supported.

4. If you used the **ipflow-tcp-ts** template type, identify it as an IBM template to avoid a commit warning.

```
[edit services lrf profile profile-name]
user@host# set vendor-support ibm
```

5. Configure the interval, in seconds, at which you want the template to be retransmitted to the collector. The interval can be from 10 through 600, and the default is 60.

```
[edit services lrf profile profile-name template template-name]
user@host# set template-tx-interval tx-time
```

For example:

```
[edit services lrf profile lrf_profile1 template template1]
user@host# set template-tx-interval 100
```

6. Configure the type of trigger that causes the generation of data records and transmission to the collector. You can specify the trigger type as either the closing of the data session (default) or a data volume limit. The data volume limit value is specified within an LRF rule.

```
[edit services lrf profile profile-name template template-name]
user@host# set trigger-type (session-close | volume)
```

For example:

```
[edit services lrf profile lrf_profile1 template template1]
user@host# set trigger-type volume
```

Configuring Logging and Reporting Rules

Configure one or more LRF rules, which control how data sessions are logged and reported. You can configure up to 32 LRF rules for an LRF profile. For each LRF rule:

1. Configure a name for the LRF rule.

```
[edit services lrf profile profile-name]
user@host# set rule lrf-rule-name
```

For example:

```
[edit services lrf profile lrf_profile1]
user@host# set rule rule1
```

You cannot use the same LRF rule name in multiple LRF profiles.

2. Specify the collector that you want to receive the data if this rule is matched.

```
[edit services lrf profile profile-name rule lrf-rule-name ]
user@host# set then report collector collector-name
```

For example:

```
[edit services lrf profile lrf_profile1 rule rule1]
user@host# set then report collector collector1
```

3. Specify the template that identifies the type of data to report if this rule is matched.

```
[edit services lrf profile profile-name rule lrf-rule-name]
user@host# set then report template template-name
```

For example:

```
[edit services lrf profile lrf_profile1 rule rule1]
user@host# set then report template template1
```

4. If you specified **volume** for the template's trigger type in Step "6" on page 191 of "Configuring Templates" on page 190, configure the data volume limit to be used for reporting by this rule.

```
[edit services lrf profile profile-name rule lrf-rule-name]
user@host# set then report volume-limit volume
```

The data volume, in megabytes, can be from 1 through 1024.

For example:

```
[edit services lrf profile lrf_profile1 rule rule1]
user@host# set then report volume-limit 4
```

5. If you specified **time** for the template's trigger type in Step "6" on page 191 of "Configuring Templates" on page 190, configure the time limit to be used for reporting by this rule.

```
[edit services lrf profile profile-name rule lrf-rule-name]
user@host# set then report time-limit time-interval
```

The time limit, in seconds, can be from 60 through 1800. The default is 300.

For example:

```
[edit services lrf profile lrf_profile1 rule rule1]
user@host# set then report time-limit 360
```

RELATED DOCUMENTATION

Logging and Reporting Function for Subscribers

Applying Logging and Reporting Configuration to a Subscriber Management Service Set

Configuring the Activation of an LRF Rule by a PCC Rule

Configuring Custom Application Signatures

Assigning an LRF Profile to Subscribers

Before you can assign an LRF profile to a set of subscribers, you must:

- Configure the LRF profile.
- Configure the TDF interface (mif).
- Configure the TDF domain for the set of subscribers.
- Configure the service set for the TDF domain's TDF interface (mif).

Assign the LRF profile to a set of subscribers to apply the profile's logging and reporting configuration to the subscribers' traffic. You accomplish this by assigning the LRF profile to the subscriber-aware TDF service set associated with the TDF interface (mif) in the subscribers' TDF domain.

To assign an LRF profile to subscribers:

1. Identify the mif interface in the subscribers' TDF domain.

```
[edit unified-edge gateways tdf]
user@host# show domains domain-name
```

For example:

```
[edit unified-edge gateways tdf]
user@host# show domains domain1
```

```
pcef-profile pcef-prof-static;
tdf-interface mif.0;
access-interfaces {
    ge-1/0/1.0;
}
...
```

2. Identify the service set or sets assigned to the mif interface.

```
[edit interfaces]
user@host# show mif.number
```

For example:

```
[edit interfaces]
user@host# show mif.0
```

```
family inet {
    service {
        input {
            service-set sset1;
        }
        output {
            service-set sset1;
        }
    }
}
```

3. Assign the LRF profile to the service set or sets.

```
[edit services service-set service-set-name]
user@host# set lrf-profile profile-name
```

For example:

```
[edit services service-set sset1]
user@host# set lrf-profile lrf_profile1
```

RELATED DOCUMENTATION

- Logging and Reporting Function for Subscribers | 166
- Configuring an LRF Profile for Subscribers | 187
- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Applying Services to Subscriber-Aware Traffic with a Service Set | 146
- Configuring a TDF Logical Interface | 143

Configuring the Activation of an LRF Rule by a PCC Rule

NOTE: Starting in Junos OS Release 19.3R1, LRF rules are also supported for Broadband Subscriber Management if Next Gen Services are enabled on the MX-SPC3 services card.

NOTE: If you are using Junos OS Subscriber Aware, you must be in maintenance mode to make a change to a PCC action profile. (See Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles).

NOTE: If you are using Junos OS Broadband Subscriber Management, you cannot make a change to a PCC action profile that is being used by subscribers. To modify the PCC action profile, you must first log off the subscribers that are using the PCC action profile.

Before you configure activation of an LRF rule by a PCC rule, you must:

- Configure the LRF rule in an LRF profile.
- Configure policy-based logging in the LRF profile.
- Configure the PCC rule.

You use a PCC rule's matching conditions to activate an LRF rule, which controls how data sessions are logged and reported. You identify the LRF rule in the PCC rule's action profile.

You can configure a PCC rule to activate an LRF rule for Junos OS Subscriber Aware or for Junos OS Broadband Subscriber Management, but you use a different CLI hierarchy level for each product.

- If you are using Junos OS Subscriber Aware, configure PCC rules at the **[edit unified-edge pcef]** hierarchy level.
- If you are using Junos OS Broadband Subscriber Management, configure PCC rules at the **[edit services pcef]** hierarchy level.

To configure a PCC rule to activate an LRF rule:

1. Identify the PCC action profile that is used in the PCC rule.

For Junos OS Subscriber Aware:

```
[edit unified-edge pcef]
user@host# show pcc-rules rule-name
```

For Junos OS Broadband Subscriber Management:

```
[edit services pcef]
user@host# show pcc-rules rule-name
```

For example:

For Junos OS Subscriber Aware:

```
[edit unified-edge pcef]
user@host# show pcc-rules all-traffic
```

```
from {
    flows {
        all;
    }
}
then {
    pcc-action-profile all-traffic-action;
}
```

For Junos OS Broadband Subscriber Management:

NOTE: The **from** statement is not applicable for Next Gen Services MX-SPC3 services card.

```
[edit services pcef]
user@host# show pcc-rules all-traffic
```

```
from {
    flows {
        all;
```

```
    }
}
then {
    pcc-action-profile all-traffic-action;
}
```

2. Assign the LRF rule to the PCC action profile.

   For Junos OS Subscriber Aware:

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set logging-rule lrf-rule-name
```

   For Junos OS Broadband Subscriber Management:

```
[edit services pcef pcc-action-profiles profile-name]
user@host# set logging-rule lrf-rule-name
```

   For example:

   For Junos OS Subscriber Aware:

```
[edit unified-edge pcef pcc-action-profiles all-traffic-action]
user@host# set logging-rule rule1
```

   For Junos OS Broadband Subscriber Management:

```
[edit services pcef pcc-action-profiles all-traffic-action]
user@host# set logging-rule rule1
```

RELATED DOCUMENTATION

- *Logging and Reporting Function for Subscribers*
- *Configuring an LRF Profile for Subscribers*
- *Configuring Policy and Charging Control Rules*

4

PART

Modifying Subscriber-Aware Configuration

Modifying Subscriber-Aware Configuration in Maintenance Mode | 200

CHAPTER 10

Modifying Subscriber-Aware Configuration in Maintenance Mode

IN THIS CHAPTER

- Maintenance Mode Overview for Subscriber Aware Policy Enforcement | **200**
- Changing Address Attributes in the Address Pool | **202**
- Deleting an Address Pool | **203**
- Changing AMS Interface Parameters on a TDF Gateway | **205**
- Modifying a TDF Domain | **208**
- Modifying the TDF Interface of a TDF Domain | **210**
- Deleting a TDF Domain | **212**
- Changing a TDF Interface | **214**
- Deleting a TDF Interface | **216**
- Changing TDF Gateway Parameters with Maintenance Mode | **218**
- Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles | **220**
- Deleting a PCEF Profile | **225**
- Changing Static Time-of-Day Settings for PCC Rules | **231**
- Deleting a Services PIC | **232**
- Deleting a Session PIC | **234**

Maintenance Mode Overview for Subscriber Aware Policy Enforcement

With Junos OS maintenance mode, you can take certain network functionality offline to perform specific maintenance tasks without disrupting service. When the traffic detection function (TDF) domains, TDF gateways, TDF subscribers, TDF interfaces, subscriber polices, or service PICs need maintenance, entering maintenance mode prevents these subscriber services elements from accepting new requests. You have the option of allowing all existing services to complete, or clear them. When ready, you can proceed with critical maintenance functions with a minimum of service disruption.

Subscribers who attempt to access a gateway that is in maintenance mode receive a message that the service is not supported.

If you want to perform any of the following operations, you must do so in maintenance mode:

- Delete or modify the addresses of certain TDF (mif) interfaces
- Delete or change the type of a TDF domain
- Change TDF interface configuration parameters
- Change a TDF interface for a TDF domain
- Change a static time-of-day profile
- Delete or modify a policy and charging enforcement function (PCEF) profile (However, maintenance mode is not required to add PCC rules or rulebases to a dynamic PCEF profile.)
- Delete or modify a PCC rule
- Delete or modify a PCC rulebase
- Delete or modify a Diameter profile
- Delete or modify a flow description
- Delete an address pool or modify its parameters

You can perform all other maintenance tasks outside of maintenance mode.

The maintenance mode procedures listed do not include adding elements. New elements carry no traffic and thus do not need to be gracefully halted. However, you can create new network elements in maintenance mode as an environment in which to test configurations before deploying them.

RELATED DOCUMENTATION

Changing a TDF Interface | **214**

Deleting a TDF Interface | **216**

Changing Address Attributes in the Address Pool | **202**

Modifying a TDF Domain | **208**

Deleting a TDF Domain | **212**

Deleting a Session PIC | **234**

Deleting a Services PIC | **232**

Changing AMS Interface Parameters on a TDF Gateway | **205**

Changing TDF Gateway Parameters with Maintenance Mode | 218

Changing Address Attributes in the Address Pool

This procedure describes how to place an address pool of a virtual routing and forwarding (VRF) instance in maintenance mode, allow all existing sessions using this pool to gracefully terminate, and then delete or modify pool attributes (for example, change address ranges in a pool).

To change address attributes in the address pool:

1. From configuration mode, activate maintenance mode for an address pool.

```
[edit]
user@host# set routing-instance vrf-name access address-assignment address-pools juniper-pool
service-mode maintenance
user@host# commit
```

2. Verify that all subscriber sessions have ended.

```
user@host# run show unified-edge tdf address-assignment pool brief
```

   The service mode shows **Maintenance – Active Phase** if all the sessions are cleared. The service mode shows **Maintenance – In Phase** if some sessions are active. The service mode shows **Maintenance – Out Phase** if maintenance mode is not configured (that is, it is in operational mode).

3. (Optional) Terminate existing sessions using the **clear** command.

```
[edit]
user@host#   run clear unified-edge tdf subscribers routing-instance juniper-vrf
```

   When the subscriber count is zero and all sessions have terminated, the service mode status indicates **Maintenance – Active phase**. In this state, you can modify address pool attributes and commit changes.

4. Make changes to the pool.

5. Verify that changes were properly saved.

```
[edit]
user@host# run show configuration routing-instance access address-assignment address-pools pool-name detail
```

NOTE: These modifications, if made outside of active maintenance mode, fail.

6. Exit maintenance mode to return to normal operational mode.

```
[edit]
user@host# delete routing-instance juniper-vrf access address-assignment address-pools pool-name service-mode
```

7. Return the gateway to operational state.

```
[edit]
user@host# run show unified-edge tdf gateway service-mode
```

RELATED DOCUMENTATION

Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200

Deleting an Address Pool | 203

Deleting an Address Pool

This procedure describes how to delete an address pool. You must first halt new sessions from being started and verify that no active sessions remain. The steps are similar to those described in "Changing Address Attributes in the Address Pool" on page 202.

To delete an address from an address pool:

1. From configuration mode, activate maintenance mode for an address pool.

```
[edit]
user@host# set routing-instance juniper-vrf access address-assignment address-pools pool-name
service-mode maintenance
user@host# commit
```

2. Verify that all subscriber sessions have ended.

```
[edit]
user@host# run show unified-edge tdf address-assignment pool brief
```

   The service mode shows **Maintenance – Active Phase** if all the sessions are cleared. The service mode shows **Maintenance – In Phase** if some sessions are active. The service mode shows **Maintenance – Out Phase** if maintenance mode is not configured (that is, it is in operational mode).

3. (Optional) Terminate sessions that are using an address pool using the **clear** command.

```
[edit]
user@host#    run clear unified-edge tdf subscribers routing-instance juniper-vrf
```

   When the subscriber count is zero and all sessions have terminated, the service mode status indicates **Maintenance – Active phase**. In this state, you can modify pool attributes and commit changes.

4. When the subscriber count is zero and all sessions have ended, modify address pool attributes and commit changes.

   NOTE: These modifications, if made outside of active maintenance mode, fail.

5. Delete the address pool and commit the change.

```
[edit]
user@host# delete routing-instance juniper-vrf access address-assignment address-pools juniper-pool
user@host# commit
```

6. Verify that the address pool has been deleted (that is, it is not listed in the output).

```
[edit]
user@host# run show configuration routing-instance juniper-vrf access address-assignment address-
pools juniper-pool
```

RELATED DOCUMENTATION

Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200

Changing Address Attributes in the Address Pool | 202

Changing AMS Interface Parameters on a TDF Gateway

This procedure shows how to change the parameters for an aggregated multiservices (AMS) interface on a TDF gateway using maintenance mode at the **[edit interfaces]** hierarchy level. If an AMS interface is configured under a gateway's session PICs or services PICs, and you change any load-balancing options such as membership of AMS interfaces (mams), then the AMS interface must be in maintenance mode.

Before you change AMS parameters using maintenance mode:

- Make sure that this change has been coordinated with affected groups and users.

To configure maintenance mode and AMS parameter change:

1. Verify the current status of maintenance mode for the AMS.

```
[edit]
user@host> show unified-edge tdf gateway-name system interfaces service-mode
```

The **service-mode** option displays the information details about maintenance mode as well as status.

```
Maintenance Mode
   MM Active Phase - System is ready to accept configuration changes for all
                attributes of this object and its sub-hierarchies.
   MM In/Out Phase - System is ready to accept configuration changes only for
                non-maintenance mode attributes of this object and
                its sub-hierarchies.
```

```
Interface Name     Gateway Name        Service Mode
ms-1/0/0            SCG1                Operational
ms-1/1/0            SCG1                Operational
ms-2/0/0            SCG1                Operational
ms-2/1/0            SCG1                Operational
pfe-0/0/0            SCG1                Operational
pfe-0/1/0            SCG1                Operational
pfe-0/2/0            SCG1                Operational
pfe-0/3/0            SCG1                Operational
ams1                SCG1                Operational
```

2. From configuration mode, show the current configuration for the AMS interface.

```
user@host# show interfaces interface-name
load-balancing-options {
    member-interface mams-4/1/0;
    member-interface mams-5/1/0;
     member-failure-options {
        redistribute-all-traffic {
            enable-rejoin;
        }
    }
    high-availability-options {
        many-to-one {
            preferred-backup mams-5/1/0;
        }
    }
}
unit 1 {
    family inet;
}
unit 2 {
    family inet;
}
```

3. On the gateway, place the interface in maintenance mode.

```
[edit]
user@host# set unified-edge tdf gateway-name system interface interface-name service-mode
```

```
maintenance
user@host# commit
```

4. Verify that the AMS interface is in active maintenance mode where configuration changes are accepted for this object and all of its subhierarchies, after you commit the configuration.

```
user@host> show unified-edge tdf gateway-name system interfaces service-mode
```

```
Maintenance Mode
   MM Active Phase - System is ready to accept configuration changes for all
                attributes of this object and its sub-hierarchies.
   MM In/Out Phase - System is ready to accept configuration changes only for
                non-maintenance mode attributes of this object and
                its sub-hierarchies.

Interface Name     Gateway Name        Service Mode
ms-1/0/0            SCG1                Operational
ms-1/1/0            SCG1                Operational
ms-2/0/0            SCG1                Operational
ms-2/1/0            SCG1                Operational
pfe-0/0/0            SCG1                Operational
pfe-0/1/0            SCG1                Operational
pfe-0/2/0            SCG1                Operational
pfe-0/3/0            SCG1                Operational
ams1                SCG1                Maintenance - Active Phase
```

NOTE: All subscribers serviced by the AMS interface must go to zero. You can wait for these conditions to be met, or use the **clear** command for the interface (or gateway) to force these conditions.

5. Delete or change AMS member interfaces and parameters.

```
user@host> show unified-edge tdf gateway-name system interfaces service-mode
[edit unified-edge]
user@host# delete unified-edge tdf gateway-name system interface interface-name load-balancing-
options member-interface mams-interface-name
[edit interfaces]
```

```
user@host# set interfaces interface-name load-balancing-options member-interface mams-interface-name
user@host# delete interfaces interface-name load-balancing-options high-availability-options many-to-one preferred-backup mams-interface-name
user@host# set interfaces interface-name load-balancing-options high-availability-options many-to-one preferred-backup mams-interface-name
```

6. Exit maintenance mode and commit the changes.

```
user@host# delete unified-edge tdf gateway-name system interface interface-name service-mode maintenance
user@host# commit
```

RELATED DOCUMENTATION

- Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200
- Deleting a Session PIC | 234
- Deleting a Services PIC | 232
- Changing TDF Gateway Parameters with Maintenance Mode | 218

Modifying a TDF Domain

This procedure describes how to use maintenance mode to modify a TDF domain. Options include modifying such parameters as TDF domain, mobile-interface, address filtering, AAA parameters, session characteristics, and access interfaces. You must first halt new sessions from being started and verify that there are no active sessions remaining.

To change a TDF domain for a group of subscribers that belong to that domain:

1. From configuration mode, activate maintenance mode for an TDF domain.

```
[edit]
user@host# set unified-edge gateways tdf gateway-name domains domain-name service-mode maintenance
user@host# commit
```

2. Verify that the TDF domain is in maintenance mode.

```
[edit]
user@host# run show unified-edge tdf domains service-mode
```

This command displays the service-mode status for all the TDF domains. You can verify the status for the specific TDF domain and take action accordingly.

The service mode for the TDF domain shows **Maintenance – Active Phase** if all the sessions using this TDF domain are cleared. The service mode for the TDF domain shows **Maintenance - In Phase** if some sessions are actively using this TDF domain.

3. Verify that no subscribers are active on the TDF domain.

```
[edit]
user@host# run show unified-edge tdf subscribers | match domain-name
```

4. (Optional) Terminate sessions on a TDF domain using the **clear** command.

```
[edit]
user@host# run clear unified-edge tdf subscribers domain domain-name gateway gateway-name
```

5. When the subscriber count is zero and all sessions have ended, make and commit changes to the TDF domain in active maintenance mode.

NOTE: These modifications must be made in active maintenance mode or they fail.

6. Modify the TDF domain and commit the changes.
7. Exit maintenance mode and commit the changes.

```
[edit]
user@host# delete unified-edge gateways tdf gateway-name domains domain-name service-mode
user@host# commit
```

8. Verify that changes were properly committed.

```
[edit]
user@host# run show configuration unified-edge gateways tdf gateway-name tdf-services domains
domain-name
```

The command output displays the configuration changes you made to the TDF domain.

9. Return the gateway to operational state.

```
[edit]
user@host# run show unified-edge tdf gateway service-mode
```

NOTE: Although maintenance mode does not explicitly include AAA options, certain AAA changes require you to place affected TDF domains in maintenance mode first. These changes include changing an AAA profile name and changing authorization or accounting elements. If you attempt to make AAA changes that affect a TDF domain that is not in maintenance mode, you are prompted to place the appropriate TDF domain into maintenance mode before proceeding with AAA profile name or element changes.

RELATED DOCUMENTATION

- Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200
- Modifying the TDF Interface of a TDF Domain | 210
- Deleting a TDF Domain | 212
- Changing TDF Gateway Parameters with Maintenance Mode | 218

Modifying the TDF Interface of a TDF Domain

This procedure describes how to use maintenance mode to modify attributes of the TDF interface for a TDF domain. You must first halt new sessions from being started and verify that no active sessions remain.

To configure the mobile interface of a TDF domain:

1. From configuration mode, activate maintenance mode for the TDF domain using the mobile interface to be modified.

```
[edit]
user@host# set unified-edge gateways tdf gateway-name domains domain-name service-mode
maintenance
user@host# commit
```

2. Verify that the TDF domain of this mobile interface is in maintenance mode.

```
[edit]
user@host# run show unified-edge tdf domain service-mode
```

From the gateway hierarchy, the service mode for the gateway shows **Maintenance – Active Phase** if all the sessions using this TDF domain are cleared. The service mode for the gateway shows **Maintenance – In Phase** if some sessions are actively using this TDF domain. The service mode for the TDF domain shows **Maintenance – Out Phase** if maintenance mode is not configured (that is, it is in operational mode).

You cannot make and commit changes to a mobile interface unless the TDF domain to which it is attached is in maintenance mode.

3. Verify that no subscribers are active on the TDF domain.

```
[edit]
user@host# run show unified-edge tdf subscribers | match domain-name
```

4. (Optional) Terminate sessions that are using an address pool using the **clear** command.

```
[edit]
user@host# run clear unified-edge tdf subscribers domain domain-name gateway gateway-name
```

5. When the subscriber count is zero and all sessions have ended, make and commit changes to the TDF domain interface in active maintenance mode.

NOTE: These modifications must be made in active maintenance mode or they fail.

6. Modify the interface.
7. Exit maintenance mode and commit the changes.

```
[edit]
user@host# delete unified-edge gateways tdf gateway-name domain domain-name service-mode
user@host# commit
```

8. Verify that changes were properly committed.

```
[edit]
user@host# run show configuration unified-edge gateways tdf gateway-name domain domain-name
```

9. Return the gateway to operational state.

```
[edit]
user@host# run show unified-edge tdf service-mode
```

RELATED DOCUMENTATION

Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200

Deleting a TDF Domain | 212

Changing TDF Gateway Parameters with Maintenance Mode | 218

Deleting a TDF Domain

This procedure describes how to use maintenance mode to delete a TDF domain. You must first halt new sessions from being started and verify that there no active sessions remain.

To delete a TDF domain name:

1. From configuration mode, activate maintenance mode for a TDF domain.

```
[edit]
user@host# set unified-edge gateways tdf gateway-name domains domain-name service-mode
maintenance
user@host# commit
```

2. Verify that the TDF domain is in maintenance mode.

```
[edit]
user@host# run show unified-edge tdf domains service-mode
```

The service mode shows **Maintenance – Active Phase** if all the sessions are cleared. The service mode shows **Maintenance – In Phase** if some sessions are active. The service mode shows **Maintenance – Out Phase** if maintenance mode is not configured (that is, it is in operational mode).

3. Verify that no subscribers are active on the TDF domain.

```
user@host# run show unified-edge tdf domain domain-name gateway gateway-name
```

4. (Optional) Terminate sessions that are using a TDF domain using the **clear** command.

```
user@host#  run clear  unified-edge tdf subscribers domain domain-name gateway gateway-name
```

5. When the subscriber count is zero and all sessions have ended, delete the TDF domain in active maintenance mode.

> **NOTE**: These modifications must be made in active maintenance mode or they fail.

6. Delete the TDF domain and commit the changes.

```
user@host#  delete unified-edge gateways tdf  gateway-name tdf-services domains domain-name
user@host#  commit
```

7. Verify that changes were properly committed by showing the configuration for the entire unified edge to make sure the TDF domain is deleted.

```
[edit]
user@host#  run show configuration unified-edge gateways tdf gateway-name domain domain-name
```

8. Return the gateway to the operational state.

```
[edit]
user@host#  run show unified-edge tdf gateway service-mode
```

RELATED DOCUMENTATION

Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200

Modifying the TDF Interface of a TDF Domain | 210

Changing TDF Gateway Parameters with Maintenance Mode | 218

Changing a TDF Interface

This procedure describes how to use maintenance mode to halt new sessions from being started and to verify that no active sessions remain before making changes to a TDF interface address.

1. From configuration mode, activate maintenance mode for a gateway.

```
[edit]
user@host# set unified-edge gateways tdf gateway-name service-mode maintenance
user@host# commit
```

2. Verify that the TDF gateway is in maintenance mode.

```
[edit]
user@host# run show unified-edge tdf gateway service-mode
```

From the gateway hierarchy, the service mode for the TDF gateway shows **Maintenance – Active Phase** if all the sessions using this pool are cleared. The service mode for the gateway shows **Maintenance – In Phase** if some sessions are actively using this pool.

3. Verify that no subscribers are active on this gateway.

```
[edit]
user@host# run show unified-edge tdf subscribers gateway gateway-name
```

NOTE: If a large number of subscribers use this gateway, the preceding command can be process intensive, in which case you can use the following command to show the active contexts across all of the gateway instances:

```
[edit]
user@host# run show unified-edge tdf status
```

4. (Optional) Terminate sessions that are using the gateway using the following **clear** command:

```
[edit]
user@host# run clear  unified-edge tdf subscribers gateway  gateway-name
```

> **CAUTION**: This clear command deletes all of the existing subscribers on the gateway. Only issue these commands if you intend to disconnect service to all these subscribers.

5. When the subscriber count is zero, and all sessions have ended, modify the TDF interface in active maintenance mode.

```
[edit]
user@host# set unified-edge gateways tdf gateway-name domains domain-name
user@host# commit
```

> **NOTE**: These modifications must be made in active maintenance mode or they fail.

6. Verify that changes were properly committed.

```
[edit]
user@host# run show configuration unified-edge tdf gateway  gateway-name
```

7. Exit maintenance mode and commit the changes.

```
[edit]
user@host# delete unified-edge gateways tdf gateway-name gateway gateway-name service-mode
user@host# commit
```

8. Return the gateway to operational state.

```
[edit]
user@host# run show unified-edge tdf gateway service-mode
```

RELATED DOCUMENTATION

Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200

Changing TDF Gateway Parameters with Maintenance Mode | 218

Deleting a TDF Interface | 216

Deleting a TDF Interface

This procedure describes how to use maintenance mode to delete a TDF interface. You must first halt new sessions from being started and verify that no active sessions are remaining.

You can use maintenance mode to remove any of the TDF interfaces.

You can also enter maintenance mode to delete control and data portions of these interface configurations.

1. From configuration mode, activate maintenance mode for a gateway.

```
[edit]
user@host# set unified-edge gateways tdf gateway-name service-mode maintenance
user@host# commit
```

2. Verify that the TDF gateway is in maintenance mode.

```
[edit]
user@host# run show unified-edge tdf gateway service-mode
```

   From the gateway hierarchy, the service mode for the gateway shows **Maintenance – Active Phase** if all the sessions using this pool are cleared. The service mode for the gateway shows **Maintenance – In Phase** if some sessions are actively using this pool. The service mode for the gateway shows **Maintenance – Out Phase** if maintenance mode is not configured (that is, the gateway is in operational mode).

3. Verify that no subscribers are active on this gateway.

```
[edit]
user@host# run show unified-edge tdf subscriber gateway gateway-name
```

4. (Optional) Terminate sessions that are using the gateway and clear CDRs using the following **clear** command.

```
[edit]
user@host# run clear unified-edge tdf subscribers gateway gateway-name
```

5. When the subscriber count is zero, and all sessions have ended, delete the TDF interface in active maintenance mode.

> **NOTE**: These modifications must be made in active maintenance mode or they fail.

6. Delete the TDF interface.

```
[edit]
user@host# delete unified-edge gateways tdf gateway-name domains domain-name tdf-interface mif
interface-name
```

7. Exit maintenance mode and commit the changes.

```
user@host# delete unified-edge gateways tdf gateway-name gateway gateway-name service-mode
user@host# commit
```

8. Verify that changes were properly committed.

```
user@host# run show configuration unified-edge tdf gateway gateway-name
```

RELATED DOCUMENTATION

Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200

Changing TDF Gateway Parameters with Maintenance Mode | 218

Changing a TDF Interface | 214

Changing TDF Gateway Parameters with Maintenance Mode

This procedure shows how to change the parameters for a TDF gateway using maintenance mode at the **[edit unified-edge gateways tdf *gateway-name*]** hierarchy level.

The gateway must be in maintenance mode to change:

- Maximum number of sessions
- Maximum amount of memory and CPU utilization.

Before you change these gateway parameters using maintenance mode:

- Make sure that this change has been coordinated with affected groups and users.
- Make sure that this change is applied to the correct gateway type and name.

To configure maintenance mode for a gateway parameter change:

1. Verify the current status of maintenance mode for the gateway.

   Under normal operating conditions, the service mode is **Operational** (that is, not in maintenance mode).

   ```
   user@host> show unified-edge tdf gateway-name service-mode
   ```

   The **service-mode** option displays the information details about maintenance mode as well as status.

   ```
   Maintenance Mode
      MM Active Phase - System is ready to accept configuration changes for all
                    attributes of this object and its sub-hierarchies.
      MM In/Out Phase - System is ready to accept configuration changes only for
                    non-maintenance mode attributes of this object and
                    its sub-hierarchies.

   Gateway Name         Service Mode

   <gateway-name>    Operational
   ```

2. From configuration mode, place the gateway in maintenance mode.

```
[edit]
user@host# set unified-edge tdf gateway-name service-mode maintenance
user@host# commit
```

3. Verify that the gateway is in active maintenance mode where configuration changes are accepted for this object.

```
[edit]
user@host> show unified-edge tdf gateway-name service-mode
```

The **service-mode** option displays the information details about maintenance mode as well as status.

```
Maintenance Mode
   MM Active Phase - System is ready to accept configuration changes for all
                  attributes of this object and its sub-hierarchies.
   MM In/Out Phase - System is ready to accept configuration changes only for
                  non-maintenance mode attributes of this object and
                  its sub-hierarchies.

Gateway Name        Service Mode

<gateway-name>    Maintenance - Active Phase
```

NOTE: All subscribers serviced by the gateway must go to zero. You can wait for these conditions to be met, or use the **clear** command for the gateway to force these conditions.

4. Configure the threshold for the maximum amount of CPU that the TDF gateway can use as a percentage from 1 through 90.

```
[edit unified-edge gateways tdf gateway-name]
user@host# set cac cpu cpu-pct
```

5. Configure the maximum number of TDF subscriber sessions that may be running, expressed in thousands of sessions.

```
[edit unified-edge gateways tdf gateway-name]
user@host# set cac maximum-sessions max-sessions
```

6. Configure the threshold for the maximum amount of memory that the TDF gateway can use as a percentage from 1 through 90.

```
[edit unified-edge gateways tdf gateway-name]
user@host# set cac memory memory-pct
```

7. Exit maintenance mode and commit the changes.

```
[edit]
user@host# delete unified-edge tdf gateway-name service-mode maintenance
user@host# commit
```

RELATED DOCUMENTATION

- Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200
- Changing AMS Interface Parameters on a TDF Gateway | 205
- Deleting a Session PIC | 234
- Deleting a Services PIC | 232

Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles

IN THIS SECTION

- Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles with the TDF Domain in Maintenance Mode | 221

- Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles with the TDF Gateway in Maintenance Mode | 223

These procedures show how to enter maintenance mode to halt new sessions from being started and verify that no sessions remain on either the gateway or TDF domain before making changes to the following:

- PCEF profiles (However, maintenance mode is not required to add PCC rules or rulebases to a dynamic PCEF profile.)
- PCC rules
- PCC rulebases
- Diameter profiles
- Flow descriptions
- PCC action profiles

NOTE: Even when a PCEF profile is not associated with a TDF domain or a TDF domain-selection term, configuration changes or deletion of the PCEF profile and any referenced objects of the profile require you to activate maintenance mode for the TDF gateway.

Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles with the TDF Domain in Maintenance Mode

This procedure shows operators how to enter maintenance mode to halt new sessions from being started and to verify that no sessions remain on the TDF domain before making changes to PCEF profiles, PCC rules, PCC rulebases, Diameter profiles, flow descriptions, and PCC action profiles for a TDF domain.

To activate maintenance mode for the TDF domain and make changes:

1. From configuration mode, activate maintenance mode for the TDF domain.

```
[edit]
user@host# set unified-edge gateways tdf gateway-name domain domain-name service-mode
```

```
maintenance
user@host# commit
```

2. Verify that the TDF domain is in maintenance mode.

```
[edit]
user@host# run show unified-edge tdf domain service-mode
```

The service mode for the TDF domain shows **Maintenance–Active Phase** if all the sessions using this TDF domain are cleared. The service mode for the TDF domain shows **Maintenance - In Phase** if some sessions are actively using this TDF domain.

3. Verify that no subscribers are active on the TDF domain.

```
[edit]
user@host# run show unified-edge tdf subscribers | match domain-name
```

4. (Optional) Terminate any remaining sessions on the TDF domain by using the **clear** command.

```
[edit]
user@host# run clear unified-edge tdf subscribers | match domain-name
```

5. Verify that the TDF domain is in Active Phase.

```
[edit]
user@host# run show unified-edge tdf domain service-mode
```

6. Make the configuration changes and commit the changes.
7. Exit maintenance mode.

```
[edit]
user@host# delete unified-edge gateways tdf gateway-name domain domain-name service-mode
user@host# commit
```

8. Verify that changes were properly committed.

- To view a PCEF profile configuration:

```
[edit]
user@host# run show configuration unified-edge pcef profiles profile-name
```

- To view a PCC rulebase configuration:

```
[edit]
user@host# run show configuration unified-edge pcef pcc-rulebases rulebase-name
```

- To view a PCC rules configuration:

```
[edit]
user@host# run show configuration unified-edge pcef pcc-rules rule-name
```

- To view a flow description configuration:

```
[edit]
user@host# run show configuration unified-edge pcef flow-description flow-identifier
```

- To view a PCC action profile configuration:

```
[edit]
user@host# run show configuration unified-edge pcef pcc-action-profiles profile-name
```

9. Return the gateway to operational state.

```
[edit]
user@host# run show unified-edge tdf gateway service-mode
```

Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles with the TDF Gateway in Maintenance Mode

This procedure shows how to enter maintenance mode to halt new sessions from being started and to verify that no sessions remain on the TDF gateway before making changes to PCEF profiles, PCC rules, PCC rulebases, Diameter profiles, flow descriptions, and PCC action profiles across multiple TDF domains on the gateway.

To activate maintenance mode for the gateway and make changes:

1. From configuration mode, activate maintenance mode for the gateway.

```
[edit]
user@host# set unified-edge gateways tdf gateway-name service-mode maintenance
user@host# commit
```

2. Verify that the TDF gateway is in maintenance mode.

```
[edit]
user@host# run show unified-edge tdf service-mode
```

   From the gateway hierarchy, the service mode shows **Maintenance—Active Phase** if all the sessions are cleared. The service mode shows **Maintenance—In Phase** if some sessions are active. The service mode shows **Maintenance—Out Phase** if maintenance mode is not configured, and the gateway is in operational mode.

3. Make the configuration changes.

   You can modify a PCEF profile by making changes to the PCC rules, PCC rulebases, or flow identifiers that the PCEF profile references or by specifying a different PCC rule, rule precedence, PCC rulebase, or Diameter profile in the PCEF profile.

4. Exit maintenance mode and commit the changes.

```
[edit]
user@host# delete unified-edge gateways tdf gateway-name service-mode
user@host# commit
```

5. Verify that changes were properly committed.

   - To view a PCEF profile configuration:

```
[edit]
user@host# run show configuration unified-edge pcef profiles profile-name
```

   - To view a PCC rulebase configuration:

```
[edit]
user@host# run show configuration unified-edge pcef pcc-rulebases rulebase-name
```

- To view a PCC rules configuration:

```
[edit]
user@host# run show configuration unified-edge pcef pcc-rules rule-name
```

- To view a flow description configuration:

```
[edit]
user@host# run show configuration unified-edge pcef flow-description flow-identifier
```

- To view a PCC action profile configuration:

```
[edit]
user@host# run show configuration unified-edge pcef pcc-action-profiles profile-name
```

6. Return the gateway to operational state.

```
[edit]
user@host# run show unified-edge tdf gateway service-mode
```

SEE ALSO

Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200

Deleting a PCEF Profile | 225

Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles | 220

Deleting a PCEF Profile

IN THIS SECTION

- Deleting a PCEF Profile with the TDF Domain in Maintenance Mode | 226
- Deleting a PCEF Profile with the Gateway in Maintenance Mode | 228

These procedures show how to enter maintenance mode to halt new sessions from being started and verify that no sessions remain on the TDF domain or gateway before removing a policy and charging enforcement function (PCEF) profile from the TDF domain or service-selection profile configurations.

NOTE: Regardless of whether a PCEF profile is associated within a TDF domain or not, or whether a PCEF profile is associated with a TDF domain-selection term or not, configuration changes and deletion of a PCEF profile (and other referenced objects of the profile) require that the TDF gateway be placed in maintenance mode. However, you need not activate maintenance mode for the gateway if you are adding a new PCEF profile.

Deleting a PCEF Profile with the TDF Domain in Maintenance Mode

This procedure shows how to enter maintenance mode to halt new sessions from being started and to verify that there are no sessions remaining on the TDF domain before removing a PCEF profile configuration that a TDF domain or service-selection profile references.

To activate maintenance mode for the TDF domain and make changes to a PCEF profile:

1. From configuration mode, activate maintenance mode for the TDF domain that references the PCEF profile.

```
[edit]
user@host# set unified-edge gateways tdf gateway-name domains domain-name service-mode
maintenance
user@host# commit
```

2. Verify that the TDF domain is in maintenance mode.

```
[edit]
user@host# run show unified-edge tdf domain service-mode
```

   The service mode for the TDF domain shows **Maintenance—Active Phase** if all the sessions using this TDF domain are cleared. The service mode for the TDF domain shows **Maintenance—In Phase** if some sessions are actively using this TDF domain.

3. Verify that no subscribers are active on the TDF domain.

```
[edit]
user@host# run show unified-edge tdf subscribers | match domain-name
```

4. (Optional) Terminate any remaining sessions on the TDF domain.

```
[edit]
user@host# run clear unified-edge tdf subscribers domain domain-name
```

5. Verify that the TDF domain is in an active phase.

```
[edit]
user@host# run show unified-edge tdf domain service-mode
```

6. In the TDF domain or service-selection profile configuration, remove the referenced PCEF profile and commit the changes.

```
user@host# delete unified-edge gateways tdf gateway-name domains domain-name pcef-profile pcef-profile-name
```

```
user@host# delete unified-edge gateways tdf gateway-name domain-selection term term-name then pcef-profile pcef-profile-name
```

7. Verify that the changes were properly committed by showing the configuration for the entire TDF domain or service-selection profile to make sure the PCEF profile is deleted.
   - To view a PCEF profile configuration:

     ```
     [edit]
     user@host# run show configuration unified-edge pcef profiles profile-name
     ```

   - To view a PCC rulebase configuration:

     ```
     [edit]
     user@host# run show configuration unified-edge pcef pcc-rulebases rulebase-name
     ```

   - To view a PCC rules configuration:

     ```
     [edit]
     user@host# run show configuration unified-edge pcef pcc-rules rule-name
     ```

- To view a flow description configuration:

```
[edit]
user@host# run show configuration unified-edge pcef flow-description flow-identifier
```

- To view a PCC action profile configuration:

```
[edit]
user@host# run show configuration unified-edge pcef pcc-action-profiles profile-name
```

8. (Optional) If the PCEF profile is not used in other TDF domain or service-selection profile configurations, you can delete the PCEF profile configuration and commit the changes.

```
[edit]
user@host# delete unified-edge gateways tdf gateway-name domains domain-name service-mode
user@host# commit
```

9. Exit maintenance mode.

```
[edit]
user@host# delete unified-edge gateways tdf gateway-name service-mode
user@host# commit
```

10. Return the gateway to operational state.

```
user@host# run show unified-edge tdf gateway service-mode
```

Deleting a PCEF Profile with the Gateway in Maintenance Mode

This procedure shows how to enter maintenance mode to halt new sessions from being started and to verify that no sessions remain on the TDF gateway before deleting PCEF profiles that are referenced by one or more TDF domains on a gateway.

To activate maintenance mode for the gateway and make changes to a PCEF profile:

1. From configuration mode, activate maintenance mode for the gateway.

```
[edit]
user@host# set unified-edge gateways tdf gateway-name service-mode maintenance
user@host# commit
```

2. Verify that the TDF gateway is in maintenance mode.

```
[edit]
user@host# run show unified-edge tdf service-mode
```

   From the gateway hierarchy, the service mode shows **Maintenance—Active Phase** if all the sessions are cleared. The service mode shows **Maintenance—In Phase** if some sessions are active. The service mode shows **Maintenance—Out Phase** if maintenance mode is not configured, and the gateway is in operational mode.

3. Verify that no subscribers are active on the gateway.

```
[edit]
user@host# run show unified-edge tdf subscribers gateway gateway-name
```

4. (Optional) Terminate any remaining sessions on the gateway.

```
[edit]
user@host# run clear unified-edge tdf subscribers gateway gateway-name
```

5. Verify that the gateway is in an active phase.

```
[edit]
user@host# run show unified-edge tdf gateway service-mode
```

6. For each applicable TDF domain, delete the PCEF profile from the TDF domain configuration and commit the changes.

```
user@host# delete unified-edge gateways tdf gateway-name domains domain-name pcef-profile pcef-profile-name
user@host# commit
```

7. Verify that the changes were properly committed by showing the configuration for each TDF domain to make sure the PCEF profile is deleted.

- To view a PCEF profile configuration:

```
[edit]
user@host# run show configuration unified-edge pcef profiles profile-name
```

- To view a PCC rulebase configuration:

```
[edit]
user@host# run show configuration unified-edge pcef pcc-rulebases rulebase-name
```

- To view a PCC rules configuration:

```
[edit]
user@host# run show configuration unified-edge pcef pcc-rules rule-name
```

- To view a flow description configuration:

```
[edit]
user@host# run show configuration unified-edge pcef flow-description flow-identifier
```

- To view a PCC action profile configuration:

```
[edit]
user@host# run show configuration unified-edge pcef pcc-action-profiles profile-name
```

8. Exit maintenance mode.

```
[edit]
user@host# delete unified-edge gateways tdf gateway-name service-mode
user@host# commit
```

9. Return the gateway to operational state.

```
[edit]
user@host# run show unified-edge tdf gateway service-mode
```

SEE ALSO

Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200

Changing PCEF Profiles, PCC Rules, PCC Rulebases, Diameter Profiles, Flow Descriptions, and PCC Action Profiles | 220

Changing Static Time-of-Day Settings for PCC Rules

This procedure shows how to enter maintenance mode to make changes to static time-of-day activation and deactivation settings or to apply those settings to PCC rules and rulebases.

To make changes to the static time-of-day activation and deactivation configuration:

1. From configuration mode, activate maintenance mode for the gateway.

```
[edit unified-edge gateways]
user@host# set tdf gateway-name service-mode maintenance
user@host# commit
```

2. Verify that the gateway is in maintenance mode.

```
[edit unified-edge gateways]
user@host# run show unified-edge tdf service-mode
```

   The service mode shows **Maintenance—Active Phase** if all the sessions are cleared. The service mode shows **Maintenance—In Phase** if some sessions are active. The service mode shows **Maintenance—Out Phase** if maintenance mode is not configured, and the gateway is in operational mode.

3. Modify the time-of-day profile settings, the assignment of time-of-day profiles to rules and rulebases within a PCEF profile, or both, and commit the changes. See "Configuring Static Time-of-Day PCC Rule Activation and Deactivation in a Junos OS Subscriber Aware PCEF Profile" on page 103.

4. Exit maintenance mode.

```
[edit unified-edge gateways]
user@host# delete tdf gateway-name service-mode
user@host# commit
```

5. Verify that changes were properly committed.

- To view a PCEF profile configuration:

```
[edit]
user@host# run show configuration unified-edge pcef profiles profile-name
```

- To view a time-of-day profile configuration:

```
[edit]
user@host# run show configuration unified-edge pcef pcc-time-of-day-profiles profile-name
```

RELATED DOCUMENTATION

Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200

Deleting a Services PIC

This procedure shows how to delete a services PIC using maintenance mode at the **[edit unified-edge gateways tdf *gateway-name* system session-pics interface]** hierarchy level. The services PIC can be an aggregated multiservices (AMS) interface. Services PICs perform packet-related services on a broadband gateway.

Before you delete a services PIC using maintenance mode:

- Make sure that this change has been coordinated with affected groups and users.

To configure maintenance mode and services PIC deletion:

1. Verify the current status of maintenance mode for this services PIC.

```
user@host> show unified-edge tdf gateway-name system interfaces service-mode
```

The **service-mode** option displays the information details about maintenance mode as well as status.

```
Maintenance Mode
   MM Active Phase - System is ready to accept configuration changes for all
                     attributes of this object and its sub-hierarchies.
```

```
   MM In/Out Phase - System is ready to accept configuration changes only for
                  non-maintenance mode attributes of this object and
                  its sub-hierarchies.

Interface Name     Gateway Name        Service Mode
ms-1/0/0            SCG1                Operational
ms-1/1/0            SCG1                Operational
ms-2/0/0            SCG1                Operational
ms-2/1/0            SCG1                Operational
pfe-0/0/0            SCG1                Operational
pfe-0/1/0            SCG1                Operational
pfe-0/2/0            SCG1                Operational
pfe-0/3/0            SCG1                Operational
ams1                SCG1                Operational
```

2. From configuration mode, place the interface in maintenance mode.

```
[edit]
user@host# set unified-edge gateways tdf gateway-name system session-pics interface interface-name
service-mode maintenance
user@host# commit
```

3. Verify that the services PIC is in active maintenance mode where configuration changes are accepted for this object and all of its subhierarchies.

```
[edit]
user@host> show unified-edge tdf gateway-name system interfaces service-mode
```

```
Maintenance Mode
   MM Active Phase - System is ready to accept configuration changes for all
                  attributes of this object and its sub-hierarchies.
   MM In/Out Phase - System is ready to accept configuration changes only for
                  non-maintenance mode attributes of this object and
                  its sub-hierarchies.

Interface Name     Gateway Name        Service Mode
ms-1/0/0            SCG1                Operational
ms-1/1/0            SCG1                Operational
ms-2/0/0            SCG1                Maintenance - Active Phase
```

```
ms-2/1/0              SCG1                 Operational
pfe-0/0/0              SCG1                  Operational
pfe-0/1/0              SCG1                  Operational
pfe-0/2/0              SCG1                  Operational
pfe-0/3/0              SCG1                  Operational
ams1                  SCG1                 Operational
```

NOTE: All subscribers serviced by the services PIC must go to zero. You can wait for these conditions to be met, or use the **clear** command for the interface (or gateway) to force these conditions.

4. Delete the services PIC, exit maintenance mode, and commit the changes.

NOTE: Deletion of a services PIC automatically exits maintenance mode for the deleted PIC.

```
[edit]
user@host# delete unified-edge gateways tdf gateway-name system interface interface-name
user@host#  commit
```

RELATED DOCUMENTATION

Maintenance Mode Overview for Subscriber Aware Policy Enforcement | 200

Deleting a Session PIC | 234

Changing AMS Interface Parameters on a TDF Gateway | 205

Changing TDF Gateway Parameters with Maintenance Mode | 218

Deleting a Session PIC

This procedure shows how to delete a session PIC using maintenance mode at the **[edit unified-edge gateways tdf *gateway-name* system session-pics interface]** hierarchy level. The session PIC can be an aggregated multiservices (AMS) interface. Session PICs process control plane messages on a broadband gateway.

Before you delete a session PIC using maintenance mode:

- Make sure that this change has been coordinated with affected groups and users.

To configure maintenance mode and session PIC deletion:

1. Verify the current status of maintenance mode for this session PIC.

```
user@host> show unified-edge tdf gateway-name system interfaces service-mode
```

The **service-mode** option displays the information details about maintenance mode as well as status.

```
Maintenance Mode
   MM Active Phase - System is ready to accept configuration changes for all
                attributes of this object and its sub-hierarchies.
   MM In/Out Phase - System is ready to accept configuration changes only for
                non-maintenance mode attributes of this object and
                its sub-hierarchies.

Interface Name     Gateway Name        Service Mode
ms-1/0/0            SCG1                Operational
ms-1/1/0            SCG1                Operational
ms-2/0/0            SCG1                Operational
ms-2/1/0            SCG1                Operational
pfe-0/0/0            SCG1                Operational
pfe-0/1/0            SCG1                Operational
pfe-0/2/0            SCG1                Operational
pfe-0/3/0            SCG1                Operational
ams1                SCG1                Operational
```

2. From configuration mode on the TDF gateway, place the interface in maintenance mode.

```
[edit]
user@host# set unified-edge gateways tdf gateway-name system session-pics interface interface-name
service-mode maintenance
user@host# commit
```

3. Verify that the session PIC is in active maintenance mode where configuration changes are accepted for this object and all of its subhierarchies.

```
user@host> show unified-edge tdf gateway-name system interfaces service-mode
```

```
Maintenance Mode
   MM Active Phase - System is ready to accept configuration changes for all
                  attributes of this object and its sub-hierarchies.
   MM In/Out Phase - System is ready to accept configuration changes only for
                  non-maintenance mode attributes of this object and
                  its sub-hierarchies.

Interface Name     Gateway Name        Service Mode
ms-1/0/0            SCG1                Operational
ms-1/1/0            SCG1                Maintenance - Active Phase
ms-2/0/0            SCG1                Operational
ms-2/1/0            SCG1                Operational
pfe-0/0/0            SCG1                Operational
pfe-0/1/0            SCG1                Operational
pfe-0/2/0            SCG1                Operational
pfe-0/3/0            SCG1                Operational
ams1                SCG1                Operational
```

NOTE: All subscribers serviced by the session PIC must go to zero. You can wait for these conditions to be met, or use the **clear** command for the interface (or gateway) to force these conditions.

4. Delete the session PIC.

```
[edit]
user@host# delete unified-edge gateways tdf gateway-name system interface interface-name
```

5. Exit maintenance mode after committing the changes.

NOTE: Deletion of a session PIC automatically exits maintenance mode for the deleted PIC.

```
[edit]
user@host#  commit
```

RELATED DOCUMENTATION

- Maintenance Mode Overview for Subscriber Aware Policy Enforcement | **200**
- Deleting a Services PIC | **232**
- Changing AMS Interface Parameters on a TDF Gateway | **205**
- Changing TDF Gateway Parameters with Maintenance Mode | **218**

5

PART

Monitoring and Troubleshooting

CHAPTER 11

Monitoring and Troubleshooting

IN THIS CHAPTER

- Configuring Tracing for PCEF Operations | 239
- Configuring Call-Rate Statistics Collection | 241
- Using the Enterprise-Specific Utility MIB | 242

Configuring Tracing for PCEF Operations

To configure tracing operations for the policy and charging enforcement function (PCEF):

1. Specify that you want to configure tracing options for PCEF.

```
[edit unified-edge pcef]
user@host# edit traceoptions
```

2. (Optional) Configure the name of the file used for the trace output.

```
[edit unified-edge pcef traceoptions]
user@host# set file file-name
```

3. (Optional) Configure the maximum size of each trace file.

```
[edit unified-edge pcef traceoptions]
user@host# set file size size
```

4. (Optional) Configure the maximum number of trace files.

```
[edit unified-edge pcef traceoptions]
user@host# set file files number
```

5. (Optional) Configure the read permissions for the log file.

```
[edit unified-edge pcef traceoptions]
user@host# set file (no-world-readable | world-readable)
```

6. (Optional) Configure flags to filter the operations to be logged.

```
[edit unified-edge pcef traceoptions]
user@host# set flag flag
```

Table 10 on page 240 describes the flags that you can include.

Table 10: Trace Flags

Flag	Description
all	Trace all operations.
config	Trace configuration events.
debug	Trace the debug internal events.
fsm	Trace finite state machine events.
general	Trace general events that do not fit in any specific traces.
high-availability	Trace high availability events.
init	Trace initialization events.
tftmgr	Trace traffic flow manager events.

7. (Optional) Configure the level of tracing.

```
[edit unified-edge pcef traceoptions]
user@host# set level (all | critical | error | info | notice | verbose | warning)
```

RELATED DOCUMENTATION

traceoptions (PCEF) | 732

Configuring Call-Rate Statistics Collection

You can configure the collection of statistics for the rate of calls for a TDF gateway and for a TDF domain. You configure the length of the interval for statistics collection and the number of call-records to keep.

To configure call-rate statistics collection for the TDF gateway or TDF domain:

1. Configure the length of the interval for statistics collection:
   - For a TDF gateway:

     ```
     [edit unified-edge gateways tdf gateway-name]
     user@host# set call-rate-statistics interval minutes
     ```

   - For a TDF domain:

     ```
     [edit unified-edge gateways tdf gateway-name domains domain-name]
     user@host# set call-rate-statistics interval minutes
     ```

2. Configure the number of call-rate records to save.
   - For a TDF gateway:

     ```
     [edit unified-edge gateways tdf gateway-name]
     user@host# set call-rate-statistics history records
     ```

- For a TDF domain:

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
user@host# set call-rate-statistics history records
```

When the number of call-rate records equals the **history** value and a new record is received, the oldest record is replaced by the new record.

RELATED DOCUMENTATION

show unified-edge tdf call-rate statistics | 974

Using the Enterprise-Specific Utility MIB

IN THIS SECTION

- Using the Enterprise-Specific Utility MIB | 242
- Populating the Enterprise-Specific Utility MIB with Information | 243
- Stopping the SLAX Script with the CLI | 251
- Clearing the Utility MIB | 251
- Recovering from an Abnormal SLAX Script Exit or a SLAX Script Exit with the CLI | 251

Using the Enterprise-Specific Utility MIB

The enterprise-specific Utility MIB enables you to add SNMP-compliant applications information to the enterprise-specific Utility MIB. The application information includes:

- NAT mappings
- Carrier-grade NAT (CGNAT) pools
- Service set CPU utilization
- Service set memory usage
- Service set summary information

- Service set packet drop information
- Service set memory zone information
- Multiservices PIC CPU and memory utilization
- Stateful firewall flow counters
- Session application connection information
- Session analysis information
- Subscriber analysis information
- Traffic Load Balancer information

You use a delivered Stylesheet Language Alternative Syntax (SLAX) script to place applications information into the enterprise-specific Utility MIB. The script is invoked based on event policies (such as reboot of the router or switchover of Routing Engines) defined in an event script. The script can also be invoked from the command line as an op script. The script only runs on the primary Routing Engine. After the script is invoked, it polls data from the specified components at regular intervals using the XML-RPC API and writes the converted data to the Utility MIB as SNMP variables. The script automatically restarts after a configured polling cycle elapses.

Populating the Enterprise-Specific Utility MIB with Information

To use a SLAX script to populate the enterprise-specific Utility MIB with information:

1. Enable the **services-oids-slax** script.

```
user@host# set system scripts op file services-oids.slax
```

2. Configure the maximum amount of memory for the data segment during the execution of the script.

```
user@host# set event-options event-script max-database 512m
```

3. Enable the script.

```
user@host# set event-options event-script file services-oids-ev-policy.slax
```

4. (Optional) Enable the **log-stats** argument to allow sys logging of stateful firewall rate statistics when the event-script is run.

a. Display the event policies and the arguments that can be used.

```
user@host> show event-options event-scripts polices
```

```
event-options {
    policy services-oids-done {
        events system;
        attributes-match {
            system.message matches "Completed polling cycle normally.
Exiting";
        }
        then {
            event-script services-oids.slax {
                arguments {
                    max-polls 30;
                    interval 120;
                }
            }
        }
    }
    policy system-started {
        events system;
        attributes-match {
            system.message matches "Starting of initial processes
complete";
        }
        then {
            event-script services-oids.slax {
                arguments {
                    max-polls 30;
                    interval 120;
                }
            }
        }
    }
}
event-options {
    policy services-oids-done {
        events system;
        attributes-match {
            system.message matches "Completed polling cycle normally.
```

```
Exiting";
        }
        then {
            event-script services-oids.slax {
                arguments {
                    max-polls 30;
                    interval 120;
                }
            }
        }
    }
    policy system-started {
        events system;
        attributes-match {
            system.message matches "Starting of initial processes
complete";
        }
        then {
            event-script services-oids.slax {
                arguments {
                    max-polls 30;
                    interval 120;
                }
            }
        }
    }
}
```

The **log-stats** argument does not appear, so you must enable it.

b. Start the Linux shell.

```
user@host>  start shell
```

```
%
```

c. Open the **/var/db/scripts/event/services-oids-eve-policy.slax** file for editing.

```
<event-options> {
        /*
```

```
         * This policy detects when the services-oids.slax script ends,
then restarts it.
         */
        <policy> {
            <name> "services-oids-done";
            <events> "system";
            <attributes-match> {
                <from-event-attribute> "system.message";
                <condition> "matches";
                <to-event-attribute-value> "Completed polling cycle
normally. Exiting";
            }
            <then> {
                <event-script> {
                    <name> "services-oids.slax";
                    <arguments> {
                        <name>"max-polls";
                        <value>"30";
                    }
                    <arguments> {
                        <name>"interval";
                        <value>"120";
                    }
                    /*
                    <arguments> {
                        <name>"log-stats";
                        <value>"yes";
                    }
                    */
                }
            }
        }

        /*
         * This policy detects when the system has booted and kicks off
the services-oids.slax script.
         * This policy hooks the 'system started' event
         */
        <policy> {
            <name> "system-started";
            <events> "system";
            <attributes-match> {
                <from-event-attribute> "system.message";
```

```
                <condition> "matches";
                <to-event-attribute-value> "Starting of initial processes
complete";
            }
            <then> {
                <event-script> {
                    <name> "services-oids.slax";
                    <arguments> {
                        <name>"max-polls";
                        <value>"30";
                    }
                    <arguments> {
                        <name>"interval";
                        <value>"120";
                    }
                    /*
                    <arguments> {
                        <name>"log-stats";
                        <value>"yes";
                    }
                    */
                }
            }
        }

}
```

d. Remove the comment enclosures (**/*** and ***/**) surrounding the **<arguments>** tags containing **"log-stats"**.

e. Exit the Linux shell and return to the CLI.

```
% exit
```

f. Load the changes you made to the event script file.

```
user@host>request system scripts event-scripts reload
```

The **log-stats** argument is available the next time the event script restarts.

5. Set up the script logging file **services-oids.log**.

```
user@host# set system syslog file services-oids.log any info
user@host# set system syslog file services-oids.log match cscript
```

6. Synchronize scripts between Routing Engines so that when a switchover of Routing Engine occurs, the event policy starts on the new primary.

   - To synchronize on a per-commit basis:

     ```
     user@host# commit synchronize scripts
     ```

   - To synchronize scripts every time you execute a **commit synchronize**:

     ```
     [edit system scripts]
     user@host# set synchronize
     user@host# commit synchronize
     ```

7. The script starts automatically at system boot, but you can manually start it with the CLI.

```
user@host> op services-oids arguments
```

Table 11 on page 248 describes the arguments that you can use.

Table 11: Arguments for services-oids.slax Script

Argument	Description
clean	A value of **1** clears all Utility MIB OIDs. Use this only to clean OID tables.
clear-semaphore	A value of **1** resets the semaphore in the Utility MIB to recover from an abnormal script exit or from a manual script exit.
debug	Prints debug messages on console.

Table 11: Arguments for services-oids.slax Script *(Continued)*

Argument	Description
detail	Displays detailed output.
interval	Sets the number of seconds between poll cycles (default is 120).
invoke-debugger	Invokes script in debugger mode.
log-stats	**Yes** value enables sys logging of stateful firewall rate statistics (default is no).
max-polls	Sets the number of poll cycles before exiting the script (default is 30).
one-cycle-only	Value of **1** quits after one cycle of polling. Event policy does not restart the script. Use this option for testing only. The default is **0**.
signal-stop	A value of **1** stops the script and sets the semaphore, which causes the next iteration to exit.
silent	Prints trace messages on console if it is unset. Set it to zero-length string (“ ”) to unset it. Default is 1.
|	Pipes through a command.

8. Check the status of the script from the log file.

```
router> show /var/log/services-oids.log | no-more
```

```
Jun 27 19:51:47  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
Beginning polling cycle.
Jun 27 19:51:47  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing traffic load-balance statistics
Jun 27 19:51:48  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing cgnat pool detail
```

```
Jun 27 19:51:48  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing cgnat mappings summary
Jun 27 19:51:48  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing service-sets summary
Jun 27 19:51:48  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing service-sets cpu-usage
Jun 27 19:51:48  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing service-sets mem-usage
Jun 27 19:51:49  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing stateful firewall statistics
Jun 27 19:51:49  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing stateful firewall flow-analysis
Jun 27 19:51:49  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing stateful firewall flows counts
Jun 27 19:51:49  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing FW policy connections/second
Jun 27 19:51:49  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing FW/NAT app connections
Jun 27 19:51:51  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing service-set packet-drops
Jun 27 19:51:51  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing service-set memory-usage zone
Jun 27 19:51:51  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing service-set policy throughput stats
Jun 27 19:51:52  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing ms-pic CPU amd Memory utilization stats
Jun 27 19:51:52  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
1/30 Sleeping for 110 seconds.
```

9. Verify that you are getting Utility MIB OID updates.

```
router> show snmp mib walk jnxUtil ascii
```

```
. . .
jnxUtilCounter64Value."services10tcp-errors09CGN-SET-1" = 0
jnxUtilCounter64Value."services10tcp-errors09CGN-SET-2" = 0
jnxUtilCounter64Value."services10tcp-errors09CGN-SET-3" = 0
jnxUtilCounter64Value."services10udp-errors09CGN-SET-1" = 1119
jnxUtilCounter64Value."services10udp-errors09CGN-SET-2" = 0
. . .
```

To exclude the timestamp information, use

```
router> show snmp mib walk jnxUtil ascii | match Value
```

Stopping the SLAX Script with the CLI

To stop the SLAX script from the CLI:

- Issue the stop argument.

```
user@host> op services-oids signal-stop 1
```

Clearing the Utility MIB

To clear all the utility MIB OIDs:

- Issue the clean argument.

```
user@host> op services-oids clean 1
```

Recovering from an Abnormal SLAX Script Exit or a SLAX Script Exit with the CLI

To recover from an abnormal SLAX script exit or an SLAX script exit with the CLI:

- Issue the clear semaphore argument.

```
user@host> op services-oids clear-semaphore 1
```

RELATED DOCUMENTATION

SLAX Overview

PART 6

Configuration Statements and Operational Commands

Configuration Statements | 253

Operational Commands | 763

CHAPTER 12

Configuration Statements

IN THIS CHAPTER

- 3gpp-imsi | **262**
- aaa clients (TDF) | **264**
- aaa-policy-control (PCEF Profile) | **265**
- aaa-profile (PCEF Profile) | **267**
- access-interfaces (IFL Subscriber) | **268**
- access-interfaces (IP Subscriber) | **270**
- accounting (AAA Profile) | **271**
- accounting (RADIUS Client) | **273**
- accounting-port (RADIUS Server) | **274**
- accounting-secret (RADIUS Server) | **275**
- activation-attribute (AAA Profile) | **277**
- address (Diameter Peer) | **278**
- address (LRF Profile) | **279**
- address (RADIUS Clients) | **281**
- address (RADIUS Server) | **282**
- address-mapping (Application Identification) | **283**
- address-pools | **285**
- allow-dynamic-requests (RADIUS Server) | **287**
- alt-name (Application Identification) | **288**
- application (Application Identification) | **289**
- application-group | **292**
- application-groups (PCC Rules) | **293**
- application-identification (Application Identification) | **295**
- application-identification-profile (Service Set) | **299**
- applications (Services Application Identification) | **300**
- applications (Diameter) | **301**

- applications (PCC Rules) | **303**
- attribute | **305**
- attributes (Diameter Gx Profiles) | **308**
- authentication (AAA Profile) | **309**
- burst-size (Default Local Policy) | **311**
- burst-size (TDF Domain) | **312**
- cac (TDF Gateway) | **314**
- cacheable (Application Identification) | **315**
- call-rate-statistics | **316**
- called-station-id | **318**
- calling-station-id | **319**
- chain-order (Application Identification) | **321**
- check-bytes (Application Identification) | **322**
- class | **323**
- client | **325**
- clients | **327**
- coa-accounting (AAA Profile) | **328**
- code | **330**
- code (AAA Profile) | **331**
- code (Application Identification) | **333**
- collector (LRF Profile) | **334**
- collector (LRF Rule) | **336**
- compatibility (Application Identification) | **337**
- connect-actively | **338**
- constant | **341**
- context (Application Identification) | **342**
- count (HTTP Header Enrichment) | **344**
- cpu (TDF Gateway) | **346**
- deactivation-attribute (AAA Profile) | **347**
- dead-criteria-retries (RADIUS Server) | **348**
- default-local-policy | **350**
- default-pool (Address Pools) | **351**

- description (Application Identification) | **353**
- destination (Application Identification) | **354**
- destination (LRF Profile) | **355**
- destination-address (HTTP Header Enrichment) | **357**
- destination-address-range (HTTP Header Enrichment) | **359**
- destination-ip-address (RADIUS Snoop Segment) | **360**
- destination-port (RADIUS Snoop Segment) | **362**
- destination-port-range (HTTP Header Enrichment) | **363**
- destination-ports (HTTP Header Enrichment) | **365**
- destination-prefix-list (HTTP Header Enrichment) | **366**
- diameter (Subscriber Aware Policy Control) | **368**
- diameter (TDF Gateway) | **370**
- diameter-profile (PCEF Profile) | **372**
- direction (Application Identification) | **373**
- direction (Service Data Flow Filters) | **375**
- disconnect-peer-timeout | **377**
- domain (TDF Domain Selection) | **378**
- domain-selection | **380**
- domains | **384**
- dynamic-policy-control | **387**
- dynamic-requests-secret (RADIUS Server) | **389**
- encrypt (HTTP Header Enrichment) | **390**
- equals | **392**
- exclude (Diameter Gx Profiles) | **394**
- external-assigned (Address Pools) | **395**
- family (Address Pools) | **397**
- family (Exclude Prefix) | **398**
- family (TDF Interface) | **400**
- flow-action | **401**
- flow-descriptions | **403**
- flows (PCC Rules) | **405**
- format (Unified Edge Gateways) | **407**

- format (LRF Profile) | **409**
- forwarding-class (PCC Action Profiles) | **410**
- firmware-revision | **412**
- framed-ip-address | **414**
- framed-ipv6-prefix | **415**
- from (HTTP Header Enrichment) | **417**
- from (PCC Rules) | **418**
- from (TDF Domain Selection) | **420**
- function (Diameter Network Element) | **424**
- gate-status | **425**
- greater-than | **427**
- gx-profile | **429**
- has-prefix (Unified Edge Gateways) | **431**
- has-suffix | **432**
- hcm (HTTP Header Enrichment) | **434**
- hcm-profile (HTTP Header Enrichment) | **436**
- hcm-profile (PCC Action Profiles) | **438**
- host (Diameter Origin) | **439**
- http-log-multiple-transactions (LRF Profile) | **441**
- icmp-mapping (Application Identification) | **442**
- id-components | **443**
- idle-timeout | **446**
- ifl-subscriber | **447**
- immediate-accounting-response | **449**
- include (Diameter Gx Profiles) | **450**
- incoming-queue | **452**
- inet (TDF Subscriber Address) | **453**
- inet (TDF Subscriber Exclude Prefix) | **455**
- inet6 (TDF Subscriber Address) | **456**
- inet6 (TDF Subscriber Exclude Prefix) | **457**
- integer | **459**
- interface (Services PIC) | **460**

- interface (Session PICs) | **462**
- interface-service (Services Interfaces) | **464**
- ip-protocol-mapping (Application Identification) | **465**
- ip-subscriber | **467**
- ipv4-address (Steering Path) | **469**
- ipv4-mask (HTTP Header Enrichment) | **471**
- ipv4-or-value (HTTP Header Enrichment) | **472**
- ipv6-address (Steering Path) | **474**
- ipv6-mask (HTTP Header Enrichment) | **475**
- ipv6-or-value (HTTP Header Enrichment) | **477**
- keep-existing-steering | **478**
- less-than | **480**
- local-port-range | **481**
- local-ports | **483**
- logging-rule (PCC Action Profile) | **485**
- lrf-profile (Service Set) | **487**
- matches | **489**
- maximum-bit-rate (Default Local Policy) | **492**
- maximum-bit-rate (PCC Action Profiles) | **493**
- maximum-bit-rate (TDF Domain) | **495**
- maximum-pending-reqs-limit | **497**
- maximum-pending-requests (Diameter) | **498**
- maximum-sessions (TDF Gateway) | **500**
- maximum-subscribers | **501**
- maximum-sessions-trap-percentage (TDF Gateway) | **502**
- member (Application Identification) | **504**
- memory (TDF Gateway) | **505**
- mif (TDF Interface) | **507**
- monitoring-key (PCC Action Profile) | **508**
- mtu (TDF Interface) | **509**
- nas-ip-address | **511**
- nat-rule-sets (Service Set) | **512**

- nat-rules | **514**
- network-element (AAA Profile) | **515**
- network-element (Diameter Base Protocol) | **516**
- network-element (Subscriber Aware Policy Control) | **518**
- network-elements (RADIUS) | **520**
- network (Address Pools) | **521**
- network (TDF Domain) | **523**
- no-application-system-cache | **525**
- no-send-to-ue | **526**
- order (Application Identification) | **527**
- order-priority (Application Identification) | **529**
- origin (Diameter Base Protocol) | **531**
- outgoing-queue | **532**
- over (Application Identification) | **534**
- packet-capture (Next Gen Services) | **536**
- path (Steering) | **539**
- pattern (Application Identification) | **540**
- pattern (Class Attribute) | **542**
- pcc-action-profile (PCC Rules) | **543**
- pcc-action-profiles | **545**
- pcc-rule | **548**
- pcc-rulebases (PCEF) | **550**
- pcc-rulebases (PCEF Profile) | **551**
- pcc-rules (PCEF) | **554**
- pcc-rules (PCEF Profile) | **556**
- pcc-time-of-day-profiles | **558**
- pcef | **560**
- pcef-profile (Service Set) | **563**
- pcef-profile (TDF Domain) | **564**
- pcef-profile (TDF Domain Selection) | **566**
- peer (Diameter Base Protocol) | **568**
- peer (Diameter Network Element) | **569**

- pending-queue-watermark | **571**
- pending-queue-watermark-abate | **572**
- policy-based-logging (LRF Profile) | **574**
- pool (TDF Domain) | **575**
- port (LRF Profile) | **577**
- port (RADIUS Server) | **578**
- port-range (Application Identification) | **579**
- prefer-framed-ip-address (RADIUS Clients) | **581**
- prefer-framed-ipv6-prefix (RADIUS Clients) | **582**
- priority (Diameter Network Element) | **583**
- priority (RADIUS Network Elements) | **585**
- product-name | **586**
- profile | **587**
- profile (HTTP Header Enrichment) | **589**
- profile (LRF) | **590**
- profile (Services Application Identification) | **593**
- profile (Services PCEF) | **594**
- profiles (AAA) | **595**
- profiles (PCEF) | **597**
- protocol (Application Identification) | **600**
- protocol (Flow Descriptions) | **602**
- realm (Diameter Origin) | **604**
- redirect (PCC Action Profiles) | **605**
- regex (Class Attribute) | **607**
- remote-address | **608**
- remote-port-range | **610**
- remote-ports | **612**
- report (LRF Rule) | **614**
- request-cache-timeout (RADIUS Snoop Segment) | **616**
- request-timeout | **617**
- response-cache-timeout (RADIUS Client) | **618**
- retry (RADIUS Server) | **620**

- revert-interval (RADIUS Server) | **621**
- routing-instance (PCC Action Profiles) | **623**
- rule (HTTP Header Enrichment for Tag Rule Set) | **625**
- rule (LRF) | **626**
- rule-activation-time | **628**
- rule-deactivation-time | **630**
- secret (RADIUS Client) | **632**
- secret (RADIUS Server) | **633**
- server (RADIUS Network Elements) | **634**
- servers (RADIUS) | **636**
- service-mode | **638**
- service-pics | **640**
- service-set (Subscriber-Aware) | **641**
- service-set (TDF Interface) | **643**
- session-pics | **644**
- session-pics (Diameter) | **645**
- shared-secret (RADIUS Snoop Segment) | **647**
- snoop-segment (TDF Domain Selection) | **649**
- snoop-segments (RADIUS) | **650**
- snoop-segments (TDF Gateway) | **652**
- source (Application Identification) | **653**
- source-address (LRF Profile) | **655**
- source-interface | **656**
- source-interface (RADIUS Server) | **657**
- source-interface (RADIUS Snoop Segment) | **659**
- source-ip-address (RADIUS Snoop Segment) | **660**
- static-policy-control | **661**
- steering | **663**
- string | **665**
- subscriber-address | **667**
- subscriber-awareness (Service Set Options) | **668**
- subscriber-aware-services | **669**

- subscriber-exclude-prefix | **670**
- subscriber-type (TDF Domain) | **672**
- subscription-id | **674**
- subscription-id-options | **675**
- subscription-id-type (Class Attribute) | **677**
- tag (HTTP Header Enrichment) | **679**
- tag-attribute (HTTP Header Enrichment) | **680**
- tag-attribute (HTTP Header Enrichment Tag Rule) | **682**
- tag-header (HTTP Header Enrichment) | **683**
- tag-operation (HTTP Header Enrichment) | **685**
- tag-rule (Profiles for HTTP Header Enrichment) | **686**
- tag-rule (HTTP Header Enrichment) | **688**
- tag-rules (Service Set) | **690**
- tag-rule-set (HTTP Header Enrichment) | **692**
- tag-rule-sets (Service Set) | **693**
- tag-separator (HTTP Header Enrichment) | **695**
- tag-value (HTTP Header Enrichment) | **696**
- tags (Application Identification) | **697**
- targets | **699**
- tdf (Unified Edge) | **701**
- tdf-interface | **702**
- template (LRF Profile) | **704**
- template (LRF Rule) | **705**
- template-tx-interval (LRF Profile) | **707**
- template-type (LRF Profile) | **708**
- term (HTTP Header Enrichment) | **711**
- term (TDF Domain Selection) | **713**
- then (HTTP Header Enrichment) | **717**
- then (LRF rule) | **719**
- then (PCC Rules) | **720**
- then (TDF Domain Selection) | **722**
- time | **724**

- time-limit (LRF Rule) | **725**
- timeout (Diameter Network Element) | **727**
- timeout (RADIUS Server) | **728**
- traceoptions (Diameter Base Protocol) | **730**
- traceoptions (PCEF) | **732**
- traceoptions (TDF Gateway) | **735**
- trigger-type (LRF Profile) | **738**
- type (Application Identification) | **740**
- type (ICMP Mapping for Application Identification) | **741**
- unit (TDF Interface) | **743**
- url | **744**
- use-class (Class Attribute) | **746**
- user-name | **747**
- user-password (PCEF Profile) | **749**
- v4address | **750**
- v6address | **752**
- v6prefix | **753**
- vendor-id | **755**
- vendor-id (AAA Profile) | **756**
- vendor-support | **758**
- volume-limit (LRF Rule) | **759**
- watchdog-timeout | **760**

3gpp-imsi

IN THIS SECTION

- Syntax | **263**
- Hierarchy Level | **263**
- Description | **263**

Required Privilege Level | 263
Release Information | 263

Syntax

```
3gpp-imsi {
    equals value;
    has-prefix value;
    has-suffix value;
    matches value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from]
```

Description

Specify the RADIUS AVP 3GPP-IMSI for the incoming RADIUS request from the subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130

Understanding Selection of Properties for an IP-Based TDF Subscriber | 110

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112

IP-Based Subscriber Setup Overview | 107

aaa clients (TDF)

IN THIS SECTION

- Syntax | 264
- Hierarchy Level | 264
- Description | 265
- Options | 265
- Required Privilege Level | 265
- Release Information | 265

Syntax

```
aaa {
    clients client-name;
    apply-groups [group-names];
    apply-groups-except [group-names];
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name]
```

Description

Specify the GGSN, PGW, or BNG RADIUS clients that can send RADIUS requests to a TDF gateway.

Options

client-name RADIUS client name that was previously configured at the **[edit access radius clients]** hierarchy level.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | 128

Configuring a TDF Gateway | 16

aaa-policy-control (PCEF Profile)

IN THIS SECTION

- Syntax | 266
- Hierarchy Level | 266
- Description | 266
- Required Privilege Level | 266
- Release Information | 266

Syntax

```
aaa-policy-control {
    aaa-profile aaa-profile-name;
    pcc-rulebases [rulebase-name];
    user-password password;
}
```

Hierarchy Level

```
[edit unified-edge pcef profiles profile-name]
```

Description

Configure RADIUS-server-controlled policy management for a policy and charging enforcement function (PCEF) profile.

The remaining statements are explained separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Policies That a RADIUS Server Controls | **101**

Configuring an AAA Profile | **96**

aaa-profile (PCEF Profile)

IN THIS SECTION

- Syntax | 267
- Hierarchy Level | 267
- Description | 267
- Options | 267
- Required Privilege Level | 267
- Release Information | 268

Syntax

```
aaa-profile aaa-profile-name;
```

Hierarchy Level

```
[edit unified-edge pcef profiles profile-name aaa-policy-control]
```

Description

Specify the AAA profile that identifies the RADIUS server policy control parameters for the policy and charging enforcement function (PCEF) profile. The AAA profile must already be defined at the **[edit unified-edge aaa]** hierarchy level.

Options

aaa-profile-name	Name of the AAA profile.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Policies That a RADIUS Server Controls | 101

Configuring an AAA Profile | 96

access-interfaces (IFL Subscriber)

IN THIS SECTION

- Syntax | 268
- Hierarchy Level | 268
- Description | 269
- Options | 269
- Required Privilege Level | 269
- Release Information | 269

Syntax

```
access-interfaces [interface-name];
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ifl-subscriber
subscriber-name]
```

Description

Specify one or more interfaces that carry traffic for the subscriber.

Options

interface-name Name of the interface. You can assign only one IFL-based subscriber to an interface. You can specify the following types of interfaces:

- Physical Layer 3 Ethernet interface
- Layer 3 Aggregated Ethernet interface
- IRB interface
- IRB that contains Ether-channel and physical interface members
- Logical Tunnel interface

NOTE: The interfaces and the TDF interface (mif) in the TDF domain must be included in the same VRF routing instance.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | 140

Understanding the Definition of a Set of IFL-Based Subscriber Properties with a TDF Domain | 116

access-interfaces (IP Subscriber)

IN THIS SECTION

- Syntax | 270
- Hierarchy Level | 270
- Description | 270
- Options | 270
- Required Privilege Level | 271
- Release Information | 271

Syntax

```
access-interfaces [interface-name];
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber]
```

Description

Specify at least one interface that faces the access network and that carries traffic for the TDF domain for IP-based subscribers. You can specify multiple interfaces by including the **access-interfaces** statement multiple times.

Options

interface-name	Name of the interface.

NOTE: The access-facing interface and the TDF interface (mif) in the TDF domain must be included in the same VRF routing instance.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108

IP-Based Subscriber Setup Overview | 107

accounting (AAA Profile)

IN THIS SECTION

- Syntax | 272
- Hierarchy Level | 272
- Description | 272
- Required Privilege Level | 272
- Release Information | 272

Syntax

```
accounting {
    network-element network-element-name;
}
```

Hierarchy Level

```
[edit unified-edge aaa profiles aaa-profile-name radius]
```

Description

Specify the network element providing policy management for TDF subscribers. The network element must already be defined at the **[edit access radius]** hierarchy level. This statement is required if the RADIUS servers cannot initiate a CoA request without an accounting record.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring an AAA Profile | **96**
- Understanding AAA Profiles | **73**
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | **64**

accounting (RADIUS Client)

IN THIS SECTION

- Syntax | 273
- Hierarchy Level | 273
- Description | 273
- Required Privilege Level | 273
- Release Information | 274

Syntax

```
accounting {
    secret password;
    response-cache-timeout seconds;
}
```

Hierarchy Level

```
[edit access radius clients client-name]
```

Description

Specify a shared secret and response cache timeout to be used by the MX Series router and the RADIUS client for accounting.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | 128

accounting-port (RADIUS Server)

IN THIS SECTION

- Syntax | 274
- Hierarchy Level | 274
- Description | 274
- Options | 275
- Required Privilege Level | 275
- Release Information | 275

Syntax

```
accounting-port port-number;
```

Hierarchy Level

```
[edit access radius servers name]
```

Description

Specify the RADIUS server port number to which the MX Series router sends RADIUS accounting-start and accounting-stop requests. RADIUS accounting-start and accounting-stop requests are used when

the RADIUS server is not able to initiate a change of authorization request without an accounting record.

Options

port-number Port number to which the RADIUS requests are sent.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring RADIUS Servers | 91
- Understanding Network Elements | 71
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

accounting-secret (RADIUS Server)

IN THIS SECTION

- Syntax | 276
- Hierarchy Level | 276
- Description | 276
- Default | 276
- Options | 276
- Required Privilege Level | 276
- Release Information | 276

Syntax

```
accounting-secret password;
```

Hierarchy Level

```
[edit access radius servers name]
```

Description

Configure the secret password to be used when sending accounting-start requests to the RADIUS server if the accounting secret password is different from the authentication secret password. RADIUS accounting-start requests are used when the RADIUS server is not able to initiate a change of authorization request without an accounting record.

Default

Use the same password that is used for authentication requests.

Options

password Password for accounting requests.

- **Range:** 1 through 64 characters

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Servers | 91

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

activation-attribute (AAA Profile)

IN THIS SECTION

- Syntax | 277
- Hierarchy Level | 277
- Description | 277
- Required Privilege Level | 278
- Release Information | 278

Syntax

```
activation-attribute {
    <code numeric-code;>
    <vendor-id vendor-id;>
}
```

Hierarchy Level

```
[edit unified-edge aaa profiles aaa-profile-name radius policy]
```

Description

Configure the RADIUS attribute that you want to carry the PCC rulebase name for rulebase activations from the RADIUS policy server to the MX Series router. By default, the rulebase name is carried in the ERX-Service-Activate Juniper vendor-specific attribute.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring an AAA Profile | 96
- Understanding AAA Profiles | 73
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

address (Diameter Peer)

IN THIS SECTION

- Syntax | 278
- Hierarchy Level | 279
- Description | 279
- Options | 279
- Required Privilege Level | 279
- Release Information | 279

Syntax

```
address ip-address;
```

Hierarchy Level

```
[edit access diameter peer peer-name]
```

Description

Configure the IP address for the Diameter remote peer.

Options

address—IP address for the Diameter peer.

Required Privilege Level

admin—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

address (LRF Profile)

IN THIS SECTION

- Syntax | 280
- Hierarchy Level | 280
- Description | 280
- Options | 280

Required Privilege Level | 280
Release Information | 280

Syntax

```
address collector-address;
```

Hierarchy Level

```
[edit services lrf profile profile-name collector collector-name destination]
```

Description

Specify the destination IP address of the collector.

Options

collector-address	IP address of the collector.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

address (RADIUS Clients)

IN THIS SECTION

- Syntax | 281
- Hierarchy Level | 281
- Description | 281
- Options | 281
- Required Privilege Level | 282
- Release Information | 282

Syntax

```
address client-address;
```

Hierarchy Level

```
[edit access radius clients client-name]
```

Description

Specify the address from which the GGSN, PGW, or BNG RADIUS client sends the RADIUS requests.

Options

client-address	IP address of the PGW client.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | 128

address (RADIUS Server)

IN THIS SECTION

- Syntax | 282
- Hierarchy Level | 282
- Description | 283
- Options | 283
- Required Privilege Level | 283
- Release Information | 283

Syntax

```
address server-address;
```

Hierarchy Level

```
[edit access radius servers name]
```

Description

Configure the address of the RADIUS server.

Options

server-address	IP address for the RADIUS server.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring RADIUS Servers | 91
- Understanding Network Elements | 71
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

address-mapping (Application Identification)

IN THIS SECTION

- Syntax | 284
- Hierarchy Level | 284
- Description | 284
- Options | 284
- Required Privilege Level | 284
- Release Information | 284

Syntax

```
address-mapping name {
    destination {
        ip ip-address-prefix;
    }
    source {
        ip ip-address-prefix;
    }
    order order;
    order-priority (high | low);
    }
}
```

Hierarchy Level

```
[edit services application-identification application application-name]
```

Description

Define an application signature based on the source or destination IP address.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Options

name Name given to the application associated with the source or destination IP address.

Required Privilege Level

view-level—To view this statement in the configuration.

control-level—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

address-pools

IN THIS SECTION

- Syntax | 285
- Hierarchy Level | 286
- Description | 286
- Options | 286
- Required Privilege Level | 286
- Release Information | 286

Syntax

```
address-pools {
    name {
        default-pool;
        family (inet | inet6) {
            network {
                [network-prefix] {
                    external-assigned;
                }
            }
        }
        service-mode service-mode-options;
    }
}
```

Hierarchy Level

```
[edit access address-assignment]
```

Description

Configure the address pools that the TDF domains use to specify the source IP addresses of packets to undergo TDF processing.

Options

name Name of the address pool.

- **Range:** 1 through 63 alphanumeric characters

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Understanding Source IP Filtering with Address Pools in TDF Domains for IP-Based Subscribers | 110

Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers | 119

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

allow-dynamic-requests (RADIUS Server)

IN THIS SECTION

- Syntax | 287
- Hierarchy Level | 287
- Description | 287
- Required Privilege Level | 287
- Release Information | 287

Syntax

```
allow-dynamic-requests;
```

Hierarchy Level

```
[edit access radius servers name]
```

Description

Allow dynamic requests from the RADIUS server so that change of authorization requests can be received.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Servers | 91

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

alt-name (Application Identification)

IN THIS SECTION

- Syntax | 288
- Hierarchy Level | 288
- Description | 288
- Options | 288
- Required Privilege Level | 289
- Release Information | 289

Syntax

```
alt-name alt-name
```

Hierarchy Level

```
[edit services application-identification application application-name]
```

Description

Provide an alternate name for the application.

Options

alt-name Alternate name for the application.

- **Range:** 1 through 255 characters

Required Privilege Level

view-level—To view this statement in the configuration.

control-level—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

> *Application Identification Overview*
>
> *Configuring Custom Application Signatures*

application (Application Identification)

IN THIS SECTION

- Syntax | 289
- Hierarchy Level | 291
- Description | 291
- Options | 291
- Required Privilege Level | 291
- Release Information | 291

Syntax

```
application application-name <description description> {
   address-mapping name {
       destination {
```

```
            ip ip-address-prefix;
        }
        source {
            ip ip-address-prefix;
        }
        order order;
        order-priority (high | low);
        }
    }
    alt-name alt-name;
    cacheable;
    compatibility junos-compatibility-version;
    description description;
    icmp-mapping {
        code icmp-code;
        order order;
        order-priority (high | low);
        type icmp-type;
    }
    ip-protocol-mapping {
        order order;
        order-priority (high | low);
        protocol protocol-number
    }
    order order;
    over protocol-type {
        signature l4-l7-signature-name {
            chain-order
            member member-name {
                check-bytes  max-bytes-to-check;
                context context;
                pattern pattern;
                direction direction;
            }
            order order;
            order-priority (high | low);
            port-range {
                tcp [port-range];
                udp [port-range];
            }
            protocol (http | ssl | tcp | udp);
        ]
    priority;
```

```
    tags tag-value;
    type type;
}
```

Hierarchy Level

```
[edit services application-identification]
```

Description

Configure identification of an application for which one or more custom signatures are defined.

Options

application-name Name of the application for which one or more custom signatures has been defined.

description (Optional) Textual description of the application for which mappings are provided.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

view-level—To view this statement in the configuration.

control-level—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R2 and 19.4R1 on MX Series MX240, MX480 and MX960.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

application-group

IN THIS SECTION

- Syntax | 292
- Hierarchy Level | 292
- Description | 292
- Options | 293
- Required Privilege Level | 293
- Release Information | 293

Syntax

```
application-group group-name {
    disable;
    application-groups {
        application-group-name;
    }
    applications {
        application-name;
    }
    index number;
}
```

Hierarchy Level

```
[edit services application-identification]
```

Description

Define the properties and contents of the application group.

Options

group-name—Unique identifier for the group.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 9.5.

Support added in Junos OS release 19.3R2 and 19.4r1 for Next Gen Services on MX240, MX480, and MX960.

NOTE: The **disable** and **index** options are not supported for Next Gen Services.

RELATED DOCUMENTATION

Configuring Application Groups

application-groups (PCC Rules)

IN THIS SECTION

- Syntax | **294**
- Hierarchy Level | **294**
- Description | **294**
- Options | **294**
- Required Privilege Level | **294**
- Release Information | **295**

Syntax

```
application-groups [application-group-name];
```

Hierarchy Level

```
[edit unified-edge pcef pcc-rules rule-name from],
[edit services pcef pcc-rules rule-name from]
```

Description

Specify one or more application groups to define the match criteria for the policy and charging control (PCC) rule. You can specify a maximum of 10 application groups in a PCC rule.

NOTE: You must also include the **flows** statement. If you do not want to filter subscriber traffic based on service data flow filters, use **flows any**.

If you are using Junos OS Subscriber Aware, specify the name of the application group at the **[edit unified-edge pcef pcc-rules *rule-name* from]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the name of the application group at the **[edit services pcef pcc-rules *rule-name* from]** hierarchy level.

Options

application-group-name Name of an application group that is used to detect IP packet flows.

- **Range:** 1 through 63 characters.

NOTE: The referenced application groups must have been previously configured in the **[edit services application-identification]** hierarchy level.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-rules *rule-name* from]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

Configuring Policy and Charging Control Rules

application-identification (Application Identification)

IN THIS SECTION

- Syntax | **296**
- Hierarchy Level | **298**
- Description | **298**
- Required Privilege Level | **298**
- Release Information | **298**

Syntax

```
application-identification {
    application application-name <description description> {
        address-mapping name {
            destination {
                ip ip-address-prefix;
            }
            source {
                ip ip-address-prefix;
            }
            order order;
            order-priority (high | low);
            }
        }
        alt-name alt-name;
        cacheable;
        compatibility junos-compatibility-version;
        description description;
        icmp-mapping {
            code icmp-code;
            order order;
            order-priority (high | low);
            type icmp-type;
        }
        ip-protocol-mapping {
            order order;
            order-priority (high | low);
            protocol protocol-number
        }
        order
        over protocol-type {
            signature l4-l7-signature-name {
                chain-order
                member member-name {
                    check-bytes  max-bytes-to-check;
                    context context;
                    pattern pattern;
                    direction direction;
                }
                order order;
                order-priority (high | low);
```

```
                port-range {
                    tcp [port-range];
                    udp [port-range];
                }
                protocol (http | ssl | tcp | udp);
            ]
        }
        priority;
        tags tag-value;
        type type;
    }
    application-group group-name {
        disable;
        application-groups {
            application-group-name;
        }
        applications {
            application-name;
        }
        index number;
    }
    application-system-cache-timeout;
    download  {
    }
    inspection-limit {
        tcp {
            byte-limit byte-limit-number;
            packet-limit packet-limit-number;
        }
        udp {
            byte-limit byte-limit-number;
            packet-limit packet-limit-number;
        }
    }
    micro-apps;
    no-application-system-cache;
    statistics {
        interval minutes;
    }
    traceoptions {
        file {
            filename ;
            files number;
```

```
            match regular-expression;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
        flag flag;
        level [all | error | info | notice | verbose | warning]
        no-remote-trace;
    }
    no-application-system-cache;
    packet-capture
    profile profile-name
}
```

Hierarchy Level

```
[edit services]
```

Description

Configure application identification options to identify the application as it passes through the device.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R2 and 19.4R1 on MX Series routers MX240, MX480 and MX960.

RELATED DOCUMENTATION

Application Identification Overview

application-identification-profile (Service Set)

IN THIS SECTION

- Syntax | 299
- Hierarchy Level | 299
- Description | 299
- Options | 299
- Required Privilege Level | 300
- Release Information | 300

Syntax

```
application-identification-profile app-id-profile-name;
```

Hierarchy Level

```
[edit services service-set service-set-name]
```

Description

Specify the dummy application identification profile that you configured at the **[edit services application-identification profile]** hierarchy level. This profile is a placeholder profile with no configuration options, but it must be specified to enable application identification functionality on the services plane.

Options

app-id-profile-name	Name of the application identification profile.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Applying Services to Subscriber-Aware Traffic with a Service Set

Identifying the Service Interface That Handles Subscriber Management Application-Aware Policy Control

applications (Services Application Identification)

IN THIS SECTION

- Syntax | 300
- Hierarchy Level | 301
- Description | 301
- Options | 301
- Required Privilege Level | 301
- Release Information | 301

Syntax

```
applications {
    application-name;
}
```

Hierarchy Level

```
[edit services application-identification application-group group-name]
```

Description

Identify the list of applications for inclusion in the application group.

Options

application-name—Identifier for the application. Maximum length is 32 characters.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 9.5.

Support added in Junos OS release 19.3R2 and 19.4r1 for Next Gen Services on MX240, MX480, and MX960.

RELATED DOCUMENTATION

Configuring Application Groups

applications (Diameter)

IN THIS SECTION

- Syntax | 302
- Hierarchy Level | 302

- Description | 302
- Options | 302
- Required Privilege Level | 302
- Release Information | 303

Syntax

```
applications {
    pcc-gx {
        maximum-pending-requests requests;
    }
}
```

Hierarchy Level

```
[edit access diameter]
```

Description

Configure the parameters for Diameter applications. Specify the Diameter application for which you are configuring the parameters. The Gx application (**pcc-gx**) is currently supported.

Options

pcc-gx Use the parameters for the Gx application.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

applications (PCC Rules)

IN THIS SECTION

- Syntax | 303
- Hierarchy Level | 303
- Description | 304
- Options | 304
- Required Privilege Level | 304
- Release Information | 304

Syntax

```
applications [application-name];
```

Hierarchy Level

```
[edit unified-edge pcef pcc-rules rule-name from],
[edit services pcef pcc-rules rule-name from]
```

Description

Specify one or more applications to define the match criteria for the policy and charging control (PCC) rule. You can specify a maximum of 10 applications in a PCC rule.

NOTE: You must also include the **flows** statement. If you do not want to filter subscriber traffic based on service data flow filters, use **flows any**.

If you are using Junos OS Subscriber Aware, specify the name of the applications at the **[edit unified-edge pcef pcc-rules *rule-name* from]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the name of the applications at the **[edit services pcef pcc-rules *rule-name* from]** hierarchy level.

Options

application-name Name of one or more applications that is used to detect IP packet flows.

- **Range:** 1 through 63 characters.

NOTE: The referenced application must have been previously configured in the **[edit services application-identification]** hierarchy level.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-rules *rule-name* from]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

Configuring Policy and Charging Control Rules

attribute

IN THIS SECTION

- Syntax | **305**
- Hierarchy Level | **307**
- Description | **307**
- Options | **307**
- Required Privilege Level | **307**
- Release Information | **307**

Syntax

```
attribute name {
    code numeric-code;
    vendor-id vendor-id;
    format {
        integer {
            equals {
                value;
            }
            greater-than value;
            less-than value;
        }
```

```
        string {
            equals {
                value;
            }
            has-prefix{
                value;
            }
            has-suffix {
                value;
            }
            matches {
                value;
            }
        }
        time {
            equals {
                value;
            }
            greater-than value;
            less-than value;
        }
        v4address {
            equals {
                value;
            }
        }
        v6address {
            equals {
                value;
            }
        }
        v6prefix {
            equals {
                value;
            }
        }
    }
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from]
```

Description

Specify a custom RADIUS attribute for the incoming RADIUS request from the subscriber. You can configure up to five attributes.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

Options

name Name for the attribute.

- **Range:** 1 through 50 alphanumeric characters. Allowed characters are [a-z, A-Z, 0-9]

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**

Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**

IP-Based Subscriber Setup Overview | **107**

attributes (Diameter Gx Profiles)

IN THIS SECTION

- Syntax | 308
- Hierarchy Level | 308
- Description | 309
- Required Privilege Level | 309
- Release Information | 309

Syntax

```
attributes {
    exclude {
        an-gw-address;
        default-eps-bearer-qos;
        packet-filter-information;
        packet-filter-operation;
        rat-type;
    }
    include {
        gx-capability-list;
        rule-suggestion;
    }
}
```

Hierarchy Level

```
[edit unified-edge diameter-profiles gx-profile profile-name]
```

Description

Configure attribute-value pairs (AVPs) that are excluded from or included in the credit control request (CCR) messages between the MX Series router and the policy and charging enforcement function (PCEF).

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

gx-profile | 429

authentication (AAA Profile)

IN THIS SECTION

- Syntax | 310
- Hierarchy Level | 310
- Description | 310
- Required Privilege Level | 310
- Release Information | 310

Syntax

```
authentication {
    network-element network-element-name;
}
```

Hierarchy Level

```
[edit unified-edge aaa profiles aaa-profile-name radius]
```

Description

Specify the network element providing policy management for TDF subscribers. The network element must already be defined at the **[edit access radius]** hierarchy level.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring an AAA Profile | 96
- Understanding AAA Profiles | 73
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

burst-size (Default Local Policy)

IN THIS SECTION

- Syntax | 311
- Hierarchy Level | 311
- Description | 311
- Options | 311
- Required Privilege Level | 312
- Release Information | 312

Syntax

```
burst-size uplink uplink-burst-size downlink downlink-burst-size;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber
default-local-policy]
```

Description

Specify the allowed burst size for a subscriber's uplink and downlink traffic during the TDF IP-based subscriber creation process. Uplink traffic originates from the subscriber towards the public data network (PDN), and downlink traffic comes from the PDN and is destined for the subscriber.

Options

uplink-burst-size	Burst size value for the uplink direction. • **Range:** 1500 through 1,500,000,000 bytes.
downlink-burst-size	Burst size value for the downlink direction.

- **Range:** 1500 through 1,500,000,000 bytes

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108

IP-Based Subscriber Setup Overview | 107

burst-size (TDF Domain)

IN THIS SECTION

- Syntax | 313
- Hierarchy Level | 313
- Description | 313
- Options | 313
- Required Privilege Level | 313
- Release Information | 313

Syntax

```
burst-size {
    apply-groups [group-names];
    apply-groups-except [group-names];
    downlink downlink-burst-size;
    uplink uplink-burst-size ;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
```

Description

Configure the TDF domain's default TDF subscriber allowed burst size for uplink and downlink traffic. Uplink traffic originates from the subscriber towards the public data network (PDN), and downlink traffic comes from the PDN and is destined for the subscriber.

Options

downlink-burst-size	Burst size value for the downlink direction. • **Range:** 1500 through 1,500,000,000 bytes.
uplink-burst-size	Burst size value for the uplink direction. • **Range:** 1500 through 1,500,000,000 bytes.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | 140
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based and IFL-Based TDF Subscribers Overview | 107
- IP-Based Subscriber Setup Overview | 107

cac (TDF Gateway)

IN THIS SECTION

- Syntax | 314
- Hierarchy Level | 314
- Description | 315
- Required Privilege Level | 315
- Release Information | 315

Syntax

```
cac {
    cpu cpu-pct;
    maximum-sessions max-sessions;
    maximum-sessions-trap-percentage max-sessions-pct;
    memory memory-pct;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name]
```

Description

Configure the call admissions control (CAC) parameters for the TDF gateway.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a TDF Gateway | 16

cacheable (Application Identification)

IN THIS SECTION

- Syntax | 315
- Hierarchy Level | 316
- Description | 316
- Required Privilege Level | 316
- Release Information | 316

Syntax

```
cacheable;
```

Hierarchy Level

```
[edit services application-identification application application-name]
```

Description

Enable the application system cache (ASC), which saves the mapping between an application type and the corresponding destination IP address, destination port, protocol type, and service. The ASC is disabled by default.

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

call-rate-statistics

IN THIS SECTION

- Syntax | 317
- Hierarchy Level | 317
- Description | 317
- Options | 317
- Required Privilege Level | 317

Release Information | 317

Syntax

```
call-rate-statistics {
    history records;
    interval minutes;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name],
[edit unified-edge gateways tdf gateway-name domains domain-name]
```

Description

Configure call rate statistics for a TDF gateway or a TDF domain.

Options

records Number of call-rate statistics records to save. When the number of call-rate records equals this value and a new record is received, the oldest record is replaced by the new record.

minutes Length of statistics collection interval.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Call-Rate Statistics Collection | 241

called-station-id

IN THIS SECTION

- Syntax | 318
- Hierarchy Level | 318
- Description | 318
- Required Privilege Level | 319
- Release Information | 319

Syntax

```
called-station-id {
    equals value;
    matches value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from]
```

Description

Specify the RADIUS AVP called station ID for the incoming RADIUS request from the IP-based subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130
- Understanding Selection of Properties for an IP-Based TDF Subscriber | 110
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- IP-Based Subscriber Setup Overview | 107

calling-station-id

IN THIS SECTION

- Syntax | 319
- Hierarchy Level | 320
- Description | 320
- Required Privilege Level | 320
- Release Information | 320

Syntax

```
calling-station-id {
    equals value;
```

```
    matches value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from]
```

Description

Specify the RADIUS AVP calling station ID for the incoming RADIUS request from the IP-based subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**

Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**

IP-Based Subscriber Setup Overview | **107**

chain-order (Application Identification)

IN THIS SECTION

- Syntax | 321
- Hierarchy Level | 321
- Description | 321
- Required Privilege Level | 321
- Release Information | 321

Syntax

```
chain-order;
```

Hierarchy Level

```
[edit services application-identification application application-name over
protocol-type signature l4-l7-signature-name]
```

Description

Read members in order. By default, chain ordering is turned off. If there is only one member, this option is ignored.

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Releases 19.3R2 and 19.4R1 on MX Series MX240, MX480 and MX960 using the MX-SPC3 services card.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

check-bytes (Application Identification)

IN THIS SECTION

- Syntax | 322
- Hierarchy Level | 322
- Description | 323
- Options | 323
- Required Privilege Level | 323
- Release Information | 323

Syntax

```
check-bytes max-bytes-to-check;
```

Hierarchy Level

```
[edit services application-identification application application-name over
protocol-type signature l4-l7-signature-name member member-name]
```

Description

Specify the maximum number of bytes to be inspected. This statement applies to TCP and UDP protocols for stream context. It is not considered for other protocols and contexts.

Options

max-bytes-to-check	Number of bytes to be inspected. **Range:** 1 through 5000 **Default:** Not configured

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Releases 19.3R2 and 19.4R1 on MX Series MX240, MX480 and MX960 using the MX-SPC3 services card.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

class

IN THIS SECTION

- Syntax | **324**
- Hierarchy Level | **324**

Description | 324
Required Privilege Level | 324
Release Information | 324

Syntax

```
class {
    equals value;
    has-prefix value;
    has-suffix value;
    matches value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from]
```

Description

Specify the RADIUS AVP class for the incoming RADIUS request from the IP-based subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130

Understanding Selection of Properties for an IP-Based TDF Subscriber | 110

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112

IP-Based Subscriber Setup Overview | 107

client

IN THIS SECTION

- Syntax | 325
- Hierarchy Level | 325
- Description | 325
- Options | 326
- Required Privilege Level | 326
- Release Information | 326

Syntax

```
client client-name;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from]
```

Description

Specify the RADIUS client for the incoming RADIUS request from an IP-based subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

Options

client-name	Name of the RADIUS client.

NOTE: The RADIUS client must have been previously configured at the **[edit access radius]** hierarchy level, and specified as the **aaa-client** at the **[edit unified-edge gateways tdf *gateway-name*]** hierarchy level.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**
- Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**
- IP-Based Subscriber Setup Overview | **107**
- Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | **128**

clients

IN THIS SECTION

- Syntax | 327
- Hierarchy Level | 327
- Description | 327
- Options | 328
- Required Privilege Level | 328
- Release Information | 328

Syntax

```
clients client-name {
    accounting {
        secret password;
        response-cache-timeout seconds;
    }
    address client-address;
    <prefer-framed-ip-address>
    <prefer-framed-ipv6-prefix>
    source-interface interface ipv4-address address;
}
```

Hierarchy Level

```
[edit access radius]
```

Description

Configure a RADIUS client for each GGSN, PGW, or BNG that sends subscriber session requests to the MX Series router and identifies it as a RADIUS server.

Options

client-name Name for the client.

- **Range:** 1 through 50 alphanumeric characters. Allowed characters are a-z, A-Z, 0-9.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | 128

coa-accounting (AAA Profile)

IN THIS SECTION

- Syntax | 329
- Hierarchy Level | 329
- Description | 329
- Options | 329
- Required Privilege Level | 329
- Release Information | 329

Syntax

```
coa-accounting (enable | disable);
```

Hierarchy Level

```
[edit unified-edge aaa profiles aaa-profile-name radius policy]
```

Description

Enable or disable the initiation of a RADIUS accounting start from the MX Series router to the RADIUS server. Enabling this feature is required if the RADIUS server cannot initiate a change of authorization request without an accounting record. Specifying **enable** does not cause the MX Series router to report any billing information.

Options

enable Initiate a RADIUS accounting start from the MX Series Router to the RADIUS server.

disable Do not initiate a RADIUS accounting start from the MX Series Router to the RADIUS server.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring an AAA Profile | 96

Understanding AAA Profiles | 73

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

code

IN THIS SECTION

- Syntax | 330
- Hierarchy Level | 330
- Description | 330
- Options | 330
- Required Privilege Level | 331
- Release Information | 331

Syntax

```
code numeric-code;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name]
```

Description

Specify the custom attribute's AVP code for the incoming RADIUS request from the subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

Options

numeric-code — Numeric value for the code.

- **Range:** 0 through 255.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130
- Understanding Selection of Properties for an IP-Based TDF Subscriber | 110
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- IP-Based Subscriber Setup Overview | 107

code (AAA Profile)

IN THIS SECTION

- Syntax | 331
- Hierarchy Level | 332
- Description | 332
- Options | 332
- Required Privilege Level | 332
- Release Information | 332

Syntax

```
code numeric-code;
```

Hierarchy Level

```
[edit unified-edge aaa profiles aaa-profile-name radius policy activation-
attribute],
[edit unified-edge aaa profiles aaa-profile-name radius policy deactivation-
attribute]
```

Description

Configure the RADIUS attributes that you want to carry the PCC rulebase name for rulebase activations and deactivations from the RADIUS policy server to the MX Series router. By default, the rulebase name is carried in the ERX-Service-Activate Juniper vendor-specific attribute (VSA) for activations and in the ERX-Service-Deactivate Juniper VSA for deactivations.

Options

numeric-code	Numeric value for the RADIUS AVP.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring an AAA Profile | 96
- Understanding AAA Profiles | 73
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

code (Application Identification)

IN THIS SECTION

- Syntax | 333
- Hierarchy Level | 333
- Description | 333
- Options | 333
- Required Privilege Level | 333
- Release Information | 334

Syntax

```
code icmp-code;
```

Hierarchy Level

```
[edit services application-identification application application-name icmp-
mapping]
```

Description

Match the specified ICMP code to create a custom application signature.

Options

value Numeric value for the ICMP code.

- **Range:** 0 through 254

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

collector (LRF Profile)

IN THIS SECTION

- Syntax | 334
- Hierarchy Level | 335
- Description | 335
- Options | 335
- Required Privilege Level | 335
- Release Information | 335

Syntax

```
collector collector-name {
    destination {
        address collector-address;
        port collector-port-number;
    }
    source-address source-address;
}
```

Hierarchy Level

```
[edit services lrf profile profile-name]
```

Description

Configure a collector that receives logging and reporting data. This collector can be specified in LRF rules.

Options

collector-name — Name for the collector.

- **Range:** Up to 32 characters.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

> *Configuring an LRF Profile for Subscribers*
>
> Configuring Logging and Reporting for Junos OS Subscriber Aware
>
> *Configuring Logging and Reporting for Subscriber Management*

collector (LRF Rule)

IN THIS SECTION

- Syntax | 336
- Hierarchy Level | 336
- Description | 336
- Options | 336
- Required Privilege Level | 336
- Release Information | 337

Syntax

```
collector collector-name;
```

Hierarchy Level

```
[edit services lrf profile profile-name rule lrf-rule-name then report]
```

Description

Specify the collector that receives the data if the LRF rule is matched.

Options

collector-name Name of the collector that receives the data. The referenced collector must already be defined at the **[edit services lrf profile *profile-name*]** hierarchy level.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Junos OS Subscriber Aware

Configuring Logging and Reporting for Subscriber Management

compatibility (Application Identification)

IN THIS SECTION

- Syntax | 337
- Hierarchy Level | 337
- Description | 338
- Options | 338
- Required Privilege Level | 338
- Release Information | 338

Syntax

```
compatibility junos-compatibility-version;
```

Hierarchy Level

```
[edit services application-identification application application-name]
```

Description

Specify the Junos OS release for compatibility.

Options

junos-compatibility-version Name of the Junos OS software release compatibility version, such as 17.1.

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

connect-actively

IN THIS SECTION

- Syntax | 339
- Hierarchy Level | 339
- Description | 339
- Options | 339
- Required Privilege Level | 340
- Release Information | 340

Syntax

```
connect-actively {
    <capabilities-exchange-timeout seconds>;
    <port port-number>;
    <repeat-timeout seconds>;
    <retry-timeout seconds>;
    <timeout seconds>;
    transport transport-name;
}
```

Hierarchy Level

```
[edit access diameter peer peer-name]
```

Description

Define the destination port and transport connection used to establish active connections to the Diameter peer.

Options

capabilities-exchange-timeout *seconds*

(Optional) Use the specified amount of time to wait for a Capabilities-Exchange-Answer message.

- **Range:** 1 through 65,535 seconds
- **Default:** 10 seconds

port *port-number*

(Optional) Use the specified destination TCP port.

- **Default:** 3868

repeat-timeout *seconds*

(Optional) Use the specified amount of time to wait before attempting to reconnect to this peer after receiving the DO_NOT_WANT_TO_TALK_TO_YOU value for the Disconnect-Cause AVP in the Disconnect-Peer-Request message. A value of zero means that there is no attempt to reconnect to the peer.

- **Range:** 0 through 65,535 seconds

- **Default:** 0

retry-timeout *seconds*

(Optional) Use the specified amount of time to wait between connection attempts for this peer.

- **Range:** 1 through 65,535 seconds
- **Default:** 30 seconds

timeout *seconds*

(Optional) Use the specified amount of time to wait for connection acknowledgement for this peer.

- **Range:** 1 through 65,535 seconds
- **Default:** 10 seconds

transport *transport-name*

Use the specified name of the transport layer connection.

> **NOTE**: The specified transport must already be configured at the **[edit access diameter transport]** hierarchy level.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

constant

IN THIS SECTION

- Syntax | 341
- Hierarchy Level | 341
- Description | 341
- Options | 341
- Required Privilege Level | 341
- Release Information | 342

Syntax

```
constant value;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber
subscription-id]
```

Description

Specify a constant string for the Subscription-Id-Data value for IP-based subscribers. This constant value is used if none of the **subscription-id-options** methods can be used. In such a case, the Subscription-Id-Type is END_USER_PRIVATE.

Options

value String that is used for the Subscription-Id-Data value.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108

IP-Based Subscriber Setup Overview | 107

context (Application Identification)

IN THIS SECTION

- Syntax | 342
- Hierarchy Level | 342
- Description | 343
- Options | 343
- Required Privilege Level | 344
- Release Information | 344

Syntax

```
context context;
```

Hierarchy Level

```
[edit services application-identification application application-name over
protocol-type signature l4-l7-signature-name member member-name]
```

Description

Define a predefined service-specific context as an additional matching criterion for application identification.

Options

context One of the following predefined contexts:

> **NOTE**: If the MX Series router is running Next Gen Services, then the following restrictions apply:
>
> - Only the http-header context types are available at the **[edit services application-identification application *application-name* over http signature *l4-l7-signature-name* member *member-name*]** hierarchy level.
> - Only the **ssl-server** context type is available at the **[edit services application-identification application *application-name* over ssl signature *l4-l7-signature-name* member *member-name*]** hierarchy level.
> - Only the **stream** context type is available at the **[edit services application-identification application *application-name* over (tcp | udp) signature *l4-l7-signature-name* member *member-name*]** hierarchy level.

- **http-get-url-parsed-param-parsed**—Decoded, normalized GET URL in an HTTP request and the decoded CGI parameters, if any.
- **http-header-content-type**—Content-Type header in an HTTP transaction.
- **http-header-cookie**—Cookie header in an HTTP transaction.
- **http-header-host**—Host header in an HTTP request.
- **http-header-user-agent**—User-agent header in an HTTP transaction.
- **http-post-url-parsed-param-parsed**—Decoded, normalized POST URL in an HTTP request and the decoded CGI parameters, if any.
- **http-post-variable-parsed**—Decoded POST URL or form data variables.
- **http-url-parsed**—Decoded, normalized URL in an HTTP request.

- **http-url-parsed-param-parsed**—Decoded, normalized URL in an HTTP request and the decoded CGI parameters, if any.
- **ssl-server-name**—Server name in the TLS server name extension or in the SSL server certificate.
- **stream**— TCP or UDP stream data.

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Releases 19.3R2 and 19.4R1 on MX Series MX240, MX480 and MX960 using the MX-SPC3 services card.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

count (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 345
- Hierarchy Level | 345
- Description | 345
- Required Privilege Level | 345
- Release Information | 345

Syntax

```
count;
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number then]
```

Description

Enable the collection of statistics for HTTP header enrichment for the tag rule term. The collection of statistics for a term is disabled by default.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Configuring HCM Profiles and Assigning Tag Rules | 49
- Junos Web Aware HTTP Header Enrichment Overview | 34
- show services hcm statistics | 885

cpu (TDF Gateway)

IN THIS SECTION

- Syntax | 346
- Hierarchy Level | 346
- Description | 346
- Options | 346
- Required Privilege Level | 347
- Release Information | 347

Syntax

```
cpu cpu-pct;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name cac]
```

Description

Configure the threshold for the maximum amount of CPU that the TDF gateway can use. If the amount of CPU that the TDF gateway uses reaches the threshold, the SNMP trap **jnxScgSMCPUThreshHigh** is generated.

Options

cpu-pct Maximum percentage of CPU.

- **Range:** 1 through 90.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a TDF Gateway | 16

deactivation-attribute (AAA Profile)

IN THIS SECTION

- Syntax | 347
- Hierarchy Level | 348
- Description | 348
- Required Privilege Level | 348
- Release Information | 348

Syntax

```
deactivation-attribute {
    <code numeric-code;>
    <vendor-id vendor-id;>
}
```

Hierarchy Level

```
[edit unified-edge aaa profiles aaa-profile-name radius policy]
```

Description

Configure the RADIUS attribute that you want to carry the PCC rulebase name for rulebase deactivations from the RADIUS policy server to the MX Series router. By default, the rulebase name is carried in the ERX-Service-Deactivate Juniper vendor-specific attribute.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring an AAA Profile | 96
- Understanding AAA Profiles | 73
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

dead-criteria-retries (RADIUS Server)

IN THIS SECTION

- Syntax | 349
- Hierarchy Level | 349
- Description | 349

- Default | 349
- Options | 349
- Required Privilege Level | 350
- Release Information | 350

Syntax

```
dead-criteria-retries retry-number interval seconds;
```

Hierarchy Level

```
[edit access radius servers name]
```

Description

Configure a limit to the number of times the MX Series router can resend a request to the RADIUS server when no response from the RADIUS server is received. If the number of retries reaches this limit, the RADIUS server is marked as dead, and the MX Series router begins to send requests to other RADIUS servers in the network element.

Default

The dead server detection function is disabled.

Options

retry-number	Number of retries. • **Range:** 10 through 65535
seconds	Time interval in seconds. • **Range:** 5 through 300

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring RADIUS Servers | 91
- Understanding Network Elements | 71
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

default-local-policy

IN THIS SECTION

- Syntax | 350
- Hierarchy Level | 351
- Description | 351
- Required Privilege Level | 351
- Release Information | 351

Syntax

```
default-local-policy {
    flow-action (drop | forward);
    maximum-bit-rate uplink mbr-uplink-value downlink mbr-downlink-value;
    burst-size uplink uplink-burst-size downlink downlink-burst-size;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber]
```

Description

Specify the default local policy, which is applied to the IP-based subscriber's data packets entering the access interface of the TDF domain when a TDF subscriber session does not exist.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based Subscriber Setup Overview | 107

default-pool (Address Pools)

IN THIS SECTION

- Syntax | 352
- Hierarchy Level | 352
- Description | 352

Required Privilege Level | 352
Release Information | 352

Syntax

```
default-pool;
```

Hierarchy Level

```
[edit access address-assignment address-pools name]
```

Description

Configure the address pool as a default pool. A TDF domain uses the default address pool to specify the source IP addresses of packets that undergo TDF processing when an address pool is not specified for the TDF domain.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Understanding Source IP Filtering with Address Pools in TDF Domains for IP-Based Subscribers | 110

Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers | 119

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

description (Application Identification)

IN THIS SECTION

- Syntax | 353
- Hierarchy Level | 353
- Description | 353
- Options | 353
- Required Privilege Level | 353
- Release Information | 354

Syntax

```
description description
```

Hierarchy Level

```
[edit services application-identification application application-name]
```

Description

Provide a description of the application.

Options

description Textual description of the application.

- **Range:** 1 through 255 characters

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

destination (Application Identification)

IN THIS SECTION

- Syntax | 354
- Hierarchy Level | 354
- Description | 355
- Options | 355
- Required Privilege Level | 355
- Release Information | 355

Syntax

```
destination ip ip-address-prefix;
```

Hierarchy Level

```
[edit services application-identification application application-name address-
mapping]
```

Description

Specify the destination IP address for address mapping-based application identification.

Options

ip-address-prefix	IP address and prefix for matching.

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

destination (LRF Profile)

IN THIS SECTION

- Syntax | 356
- Hierarchy Level | 356
- Description | 356
- Required Privilege Level | 356
- Release Information | 356

Syntax

```
destination {
    address collector-address;
    port collector-port-number;
}
```

Hierarchy Level

```
[edit services lrf profile profile-name collector collector-name]
```

Description

Specify the destination IP address and port number of the collector.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

> *Configuring an LRF Profile for Subscribers*
>
> Configuring Logging and Reporting for Junos OS Subscriber Aware
>
> *Configuring Logging and Reporting for Subscriber Management*

destination-address (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 357
- Hierarchy Level | 357
- Description | 357
- Options | 358
- Required Privilege Level | 358
- Release Information | 358

Syntax

```
destination-address {
    (any-ipv4 | any-ipv4 except);
    (any-ipv6 | any-ipv6 except);
    (any-unicast | any-unicast except);
    (prefix | prefix except);
}
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number from]
```

Description

Specify the prefix or address type that the HTTP request destination IP address must match. You can specify multiple prefixes or address types by including the **destination-address** statement multiple times.

After this criterion and the other match criteria specified for the **term** are matched, the HTTP header enrichment actions specified for the **term** are applied to the HTTP traffic.

Options

any-ipv4 Match any IPv4 address.

any-ipv4 except Exclude IPv4 addresses from addresses that are in a **destination-address**, **destination-address-range**, or **destination-prefix-list** statement configured at the **[edit services hcm tag-rule *rule-name* term *term-number* from]** hierarchy level. You cannot use **except** without also configuring addresses that do match.

any-ipv6 Match any IPv6 address.

any-ipv6 except Exclude IPv6 addresses from addresses that are in a **destination-address**, **destination-address-range**, or **destination-prefix-list** statement configured at the **[edit services hcm tag-rule *rule-name* term *term-number* from]** hierarchy level. You cannot use **except** without also configuring addresses that do match.

any-unicast Match any IPv4 unicast address. This option does not match any IPv6 addresses.

any-unicast except Exclude IPv4 unicast addresses from addresses that are in a **destination-address**, **destination-address-range**, or **destination-prefix-list** statement configured at the **[edit services hcm tag-rule *rule-name* term *term-number* from]** hierarchy level. You cannot use **except** without also configuring IPv4 addresses that do match.

prefix IP prefix for the addresses that are matched.

***prefix* except** Exclude the specified IP prefixes from addresses that are in a **destination-address**, **destination-address-range**, or **destination-prefix-list** statement configured at the **[edit services hcm tag-rule *rule-name* term *term-number* from]** hierarchy level. You cannot use **except** without also configuring addresses that do match.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm (HTTP Header Enrichment) | 434

destination-address-range (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 359
- Hierarchy Level | 359
- Description | 359
- Options | 360
- Required Privilege Level | 360
- Release Information | 360

Syntax

```
destination-address-range {
    high address low address <except>;
}
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number from]
```

Description

Specify an IP address range that the HTTP request destination IP address must match. You can specify multiple address ranges by including the **destination-address-range** statement multiple times.

After this criterion and the other match criteria specified for the **term** are matched, the HTTP header enrichment actions specified for the **term** are applied to the HTTP traffic.

Options

except (Optional) Exclude addresses in the specified address range from addresses that are in a **destination-address**, **destination-address-range**, or **destination-prefix-list** statement configured at the **[edit services hcm tag-rule** *rule-name* **term** *term-number* **from]** hierarchy level. You cannot use **except** without also configuring addresses that do match.

high *address* Upper limit of the address range.

low *address* Lower limit of the address range.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm (HTTP Header Enrichment) | 434

destination-ip-address (RADIUS Snoop Segment)

IN THIS SECTION

- Syntax | 361
- Hierarchy Level | 361
- Description | 361
- Options | 361
- Required Privilege Level | 361

Release Information | 361

Syntax

```
destination-ip-address destination-address;
```

Hierarchy Level

```
[edit access radius snoop-segments segment-name]
```

Description

Specify the destination IP address for accounting messages to snoop.

Options

destination-address	Destination IPv4 address of accounting messages.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | 136

Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | 114

IP-Based Subscriber Setup Overview | 107

destination-port (RADIUS Snoop Segment)

IN THIS SECTION

- Syntax | 362
- Hierarchy Level | 362
- Description | 362
- Options | 362
- Required Privilege Level | 363
- Release Information | 363

Syntax

```
destination-port destination-port;
```

Hierarchy Level

```
[edit access radius snoop-segments segment-name]
```

Description

Specify the destination port for accounting messages to snoop.

Options

destination-port

Destination port of accounting messages.

- **Default:** 1813
- **Range:** 1 through 65,535

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | 136
- Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | 114
- IP-Based Subscriber Setup Overview | 107

destination-port-range (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 363
- Hierarchy Level | 364
- Description | 364
- Options | 364
- Required Privilege Level | 364
- Release Information | 364

Syntax

```
destination-port-range {
    high port-number low port-number;
}
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number from]
```

Description

Specify a port range that the HTTP request destination port number must match. You can specify multiple port ranges by including the **destination-port-range** statement multiple times.

After this criterion and the other match criteria specified for the **term** are matched, the HTTP header enrichment actions specified for the **term** are applied to the HTTP traffic.

Options

high *port-number*	Upper limit of the port range.
low *port-number*	Lower limit of the port range.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm (HTTP Header Enrichment) | 434

destination-ports (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 365
- Hierarchy Level | 365
- Description | 365
- Options | 365
- Required Privilege Level | 366
- Release Information | 366

Syntax

```
destination-ports value;
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number from]
```

Description

Specify the HTTP request destination port number that must be matched. You can specify multiple ports by including the **destination-ports** statement multiple times.

After this criterion and the other match criteria specified for the **term** are matched, the HTTP header enrichment actions specified for the **term** are applied to the HTTP traffic.

Options

value—Port number.

- **Range:** 0 through 65,535

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm (HTTP Header Enrichment) | 434

destination-prefix-list (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 366
- Hierarchy Level | 367
- Description | 367
- Options | 367
- Required Privilege Level | 367
- Release Information | 367

Syntax

```
destination-prefix-list {
    (prefix-name | prefix-name except);
}
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number from]
```

Description

Specify the destination prefix list that the HTTP request destination IP address must match. You can specify multiple prefix lists by including the **destination-prefix-list** statement multiple times.

After this criterion and the other match criteria specified for the **term** are matched, the HTTP header enrichment actions specified for the **term** are applied to the HTTP traffic.

Options

prefix-name Name of the prefix list.

> **NOTE**: The prefix list must already be defined at the **[edit policy-options prefix-list]** hierarchy level.

***prefix-name* except** Exclude addresses that are in the specified prefix list from addresses that are in the **destination-address** or **destination-address-range** statement configured at the **[edit services hcm tag-rule *rule-name* term *term-number* from]** hierarchy level. You cannot use **except** without also configuring addresses that do match.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm (HTTP Header Enrichment) | 434

diameter (Subscriber Aware Policy Control)

IN THIS SECTION

- Syntax | 368
- Hierarchy Level | 369
- Description | 369
- Required Privilege Level | 370
- Release Information | 370

Syntax

```
diameter {
    applications {
        pcc-gx {
            <maximum-pending-requests requests>;
        }
    }
    <firmware-revision version>;
    network-element element-name {
        function function-name;
        peer peer-name {
            priority priority-value;
            <timeout seconds>;
        }
    }
    origin {
        host hostname;
        realm realm-name;
    }
    peer peer-name {
        address ip-address;
        connect-actively {
```

```
            <capabilities-exchange-timeout seconds>;
            <port port-number>;
            <repeat-timeout seconds>;
            <retry-timeout seconds>;
            <timeout seconds>;
            transport transport-name;
        }
        <disconnect-peer-timeout seconds>;
        <incoming-queue> {
            size size;
        }
        <outgoing-queue> {
            <high-watermark high-watermark>;
            <low-watermark low-watermark>;
            size size;
        }
        <watchdog-timeout seconds>;
    }
<product-name product-name>;
    traceoptions {
        file diameter;
        flag flag;
        level all;
        peer {
            peer-name;
        }
    }
```

Hierarchy Level

```
[edit access]
```

Description

Configure the Diameter base protocol parameters for subscriber-aware dynamic policy control, so that Diameter applications can connect to remote peers. The Diameter base protocol configuration includes configuration of the endpoint origin, the transport layer connection, the remote peers, and the network elements.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Diameter Profiles | 152

diameter (TDF Gateway)

IN THIS SECTION

- Syntax | 370
- Hierarchy Level | 371
- Description | 371
- Required Privilege Level | 371
- Release Information | 371

Syntax

```
diameter {
    network-element {
        element-name {
            session-pics {
                group {
                    group-name {
                        [session-pic interface-name];
                    }
```

```
                    }
                }
            }
        }
    }
```

Hierarchy Level

```
[edit unified-edge tdf gateway-name]
```

Description

Configure the Diameter protocol parameters associated with Diameter bindings for this TDF gateway.

NOTE: If you want to set up Diameter bindings for session PICs on the TDF gateway, contact Juniper Networks Professional Services for assistance.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Diameter Profiles | 152

diameter-profile (PCEF Profile)

IN THIS SECTION

- Syntax | 372
- Hierarchy Level | 372
- Description | 372
- Options | 372
- Required Privilege Level | 373
- Release Information | 373

Syntax

```
diameter-profile gx-profile-name;
```

Hierarchy Level

```
[edit unified-edge pcef profiles profile-name dynamic-policy-control],
[edit services pcef profiles profile-name dynamic-policy-control]
```

Description

Specify the Diameter Gx profile to use for the PCEF dynamic policy control profile. A PCEF profile with dynamic policy control must reference a defined Diameter Gx profile.

If you are using Junos OS Broadband Subscriber Management, specify the Diameter Gx profile at the **[edit services pcef profiles *profile-name* dynamic-policy-control]** hierarchy level.

If you are using Junos OS Subscriber Aware, specify the Diameter Gx profile at the **[edit unified-edge pcef profiles *profile-name* dynamic-policy-control]** hierarchy level.

Options

gx-profile-name Name of the Diameter Gx profile to use with this dynamic policy control profile.

Required Privilege Level

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef profiles *profile-name* dynamic-policy-control]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 18.2R1 on MX Series.

RELATED DOCUMENTATION

Configuring a Policy and Charging Enforcement Function Profile for Subscriber Management

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Dynamic Policies | **98**

direction (Application Identification)

IN THIS SECTION

- Syntax | **374**
- Hierarchy Level | **374**
- Description | **374**
- Options | **374**
- Required Privilege Level | **374**
- Release Information | **374**

Syntax

```
direction (any | client-to-server | server-to-client);
```

Hierarchy Level

```
[edit services application-identification application application-name over
protocol-type signature l4-l7-signature-name member member-name]
```

Description

Specify the connection direction of the packets to which to apply pattern matching.

Options

any	Apply pattern matching to packets flowing in any direction.
client-to-server	Apply pattern matching only to packets flowing from client to server.
server-to-client	Apply pattern matching only to packets flowing from server to client.

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Releases 19.3R2 and 19.4R1 on MX Series MX240, MX480 and MX960 using the MX-SPC3 services card.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

direction (Service Data Flow Filters)

IN THIS SECTION

- Syntax | 375
- Hierarchy Level | 375
- Description | 375
- Default | 375
- Options | 376
- Required Privilege Level | 376
- Release Information | 376

Syntax

```
direction (uplink | downlink | both);
```

Hierarchy Level

```
[edit unified-edge pcef flow-descriptions flow-identifier],
[edit services pcef flow-descriptions flow-identifier]
```

Description

Specify the direction in which service data flow (SDF) filters will detect service flow IP packets.

If you are using Junos OS Subscriber Aware, specify the direction at the **[edit unified-edge pcef flow-descriptions *flow-identifier*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the direction at the **[edit services pcef flow-descriptions *flow-identifier*]** hierarchy level.

Default

If you do not configure the **direction** statement, the default direction is **both**.

Options

uplink SDF filters are applied in the uplink direction.

downlink SDF filters are applied in the downlink direction.

both SDF filters are applied in both the uplink and downlink directions.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef flow-descriptions *flow-identifier*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

RELATED DOCUMENTATION

Configuring Service Data Flow Filters

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment

Understanding Application-Aware Policy Control for Subscriber Management

disconnect-peer-timeout

IN THIS SECTION

- Syntax | 377
- Hierarchy Level | 377
- Description | 377
- Options | 377
- Required Privilege Level | 378
- Release Information | 378

Syntax

```
disconnect-peer-timeout seconds;
```

Hierarchy Level

```
[edit access diameter peer peer-name]
```

Description

Configure the amount of time to wait in the Closing state while disconnecting this peer.

Options

seconds Amount of time to wait in the Closing state.

- **Range:** 1 through 65,535 seconds
- **Default:** 10 seconds

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

domain (TDF Domain Selection)

IN THIS SECTION

- Syntax | 378
- Hierarchy Level | 379
- Description | 379
- Options | 379
- Required Privilege Level | 379
- Release Information | 379

Syntax

```
domain tdf-domain-name;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
then]
```

Description

Specify the TDF domain to be selected when the criteria specified in the domain selection statement are matched.

NOTE: This statement is required even if you have not specified any match criteria.

Options

tdf-domain-name	Name of the TDF domain to use.

NOTE: The TDF domain must have been previously configured at the **[edit unified-edge gateways tdf *gateway-name* domains]** hierarchy level.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**
- Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**

IP-Based Subscriber Setup Overview | 107

domain-selection

IN THIS SECTION

- Syntax | 380
- Hierarchy Level | 382
- Description | 383
- Required Privilege Level | 383
- Release Information | 383

Syntax

```
domain-selection {
    term term-name {
        from {
            3gpp-imsi {
                equals value;
                has-prefix value;
                has-suffix value;
                matches value;
            }
            attribute name {
                code numeric-code;
                vendor-id vendor-id;
                format {
                    integer {
                        equals {
                            value;
                        }
                        greater-than value;
                        less-than value;
                    }
                    string {
```

```
                        equals {
                            value;
                        }
                        has-prefix {
                            value;
                        }
                        has-suffix {
                            value;
                        }
                        matches {
                            value;
                        }
                    }
                    time {
                        equals {
                            value;
                        }
                        greater-than value;
                        less-than value;
                    }
                    v4address {
                        equals {
                            value;
                        }
                    }
                    v6address {
                        equals {
                            value;
                        }
                    }
                    v6prefix {
                        equals {
                            value;
                        }
                    }
                }
            }
            called-station-id {
                equals value;
                matches value;
            }
            calling-station-id {
                equals value;
```

```
                matches value;
            }
            class {
                equals value;
                has-prefix value;
                has-suffix value;
                matches value;
            }
            client client-name;
            framed-ip-address {
                equals value;
            }
            framed-ipv6-prefix {
                equals value;
            }
            nas-ip-address {
                equals value;
            }
            snoop-segment snoop-segment-name;
            user-name {
                equals value;
                has-prefix value;
                has-suffix value;
                matches value;
            }
        }
        then {
            domain tdf-domain-name;
            pcef-profile pcef-profile-name;
        }
    }
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name]
```

Description

Specify the TDF domain to be used for an IP-based subscriber. You can configure multiple terms under **domain-selection**, and each term is applied in the order in which it is configured. You can specify multiple match conditions within a term and all of the conditions have to match. If the incoming RADIUS request from the subscriber matches the criteria in a term, then the TDF domain specified in the **then** statement of the term is used to create the TDF subscriber.

You can also specify a PCEF profile for an IP-based subscriber. This is required if the TDF domain selected for a subscriber does not specify a PCEF profile or you want to allow different members of the same TDF domain to have different PCEF profiles.

After a term matches and a TDF domain is selected, further terms are not evaluated if the PCEF profile is specified in either the **then** statement or in the selected TDF domain. If a PCEF profile is not specified in either the **then** statement or in the selected TDF domain, further terms are evaluated to find a PCEF profile for the subscriber.

If no TDF domain is selected for a subscriber, then a TDF subscriber session is not created.

NOTE: The TDF domain must have been previously configured at the **[edit unified-edge gateways tdf *gateway-name* domains]** hierarchy level.

The PCEF profile must have been previously configured at the **[edit unified-edge pcef]** hierarchy level.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**

Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112

domains

IN THIS SECTION

- Syntax | 384
- Hierarchy Level | 386
- Description | 386
- Options | 387
- Required Privilege Level | 387
- Release Information | 387

Syntax

```
domains domain-name {
    apply-groups [group-names];
    apply-groups-except [group-names];
    burst-size {
        apply-groups [group-names];
        apply-groups-except [group-names];
        downlink downlink-burst-size;
        uplink uplink-burst-size ;
    }
    ifl-subscriber [subscriber-name] {
        access-interfaces [interface-name];
        apply-groups [group-names];
        apply-groups-except [group-names];
    }
    ip-subscriber {
        access-interfaces [interface-name];
        apply-groups [group-names];
        apply-groups-except [group-names];
        default-local-policy {
            flow-action (drop | forward);
```

```
            maximum-bit-rate {
                uplink mbr-uplink-value ;
                downlink mbr-downlink-value;
            }
            burst-size {
                uplink uplink-burst-size;
                downlink downlink-burst-size;
            }
        }
        idle-timeout idle-timout;
        immediate-accounting-response (enabled | disabled);
        maximum-subscribers number;
        subscriber-address {
            apply-groups [group-names];
            apply-groups-except [group-names];
            inet {
                apply-groups [group-names];
                apply-groups-except [group-names];
                pool pool-name;
            }
            inet6 {
                apply-groups [group-names];
                apply-groups-except [group-names];
                pool pool-name;
            }
        }
        subscription-id {
            apply-groups [group-names];
            apply-groups-except [group-names];
            constant ;
            subscription-id-options {
                entry-name {
                    id-components {
                        use-imsi;
                        use-msisdn;
                        use-nai;
                        use-username;
                        use-realm;
                        use-nas-port;
                        use-nas-port-id;
                    }
                }
            }
```

```
        }
    }
    maximum-bit-rate {
        apply-groups [group-names];
        apply-groups-except [group-names];
        downlink mbr-downlink-value;
        uplink mbr-uplink-value;
    }
    pcef-profile name;
    service-mode service-mode-options;
    subscriber-exclude-prefix {
        apply-groups [group-names];
        apply-groups-except [group-names];
        family {
            inet {
                apply-groups [group-names];
                apply-groups-except [group-names];
                network address net-mask;
            }
            inet6 {
                apply-groups [group-names];
                apply-groups-except [group-names];
                network address net-mask;
            }
        }
    }
    subscriber-type (ip | ifl);
    tdf-interface  mif.number;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name]
```

Description

Configure a TDF domain, which specifies a set of properties for creating TDF subscriber sessions and for handling subscriber traffic.

Options

domain-name Name of the TDF domain.

- **Range:** 1 through 50 alphanumeric characters.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | 140
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- Understanding the Definition of a Set of IFL-Based Subscriber Properties with a TDF Domain | 116

dynamic-policy-control

IN THIS SECTION

- Syntax | 388
- Hierarchy Level | 388
- Description | 388
- Required Privilege Level | 388
- Release Information | 388

Syntax

```
dynamic-policy-control {
    pcc-rules {
        [rule-name  number];
    }
    pcc-rulebases {
        [rulebase-name];
    }
    diameter-profile gx-profile-name;
}
```

Hierarchy Level

```
[edit unified-edge pcef profiles profile-name]
```

Description

Configure the dynamic policy control for the PCC rules, PCC rulebases, or both in a PCEF profile. You can configure a maximum of 32 PCC rules in a PCEF profile. There is no limit to the number of PCC rulebases you can configure in a PCEF profile.

NOTE: If you configure the **dynamic-policy-control** statement for a PCEF profile, you cannot configure the **static-policy-control** statement in the same profile.

The remaining statements are explained separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Dynamic Policies | 98

Understanding How Subscriber-Aware Policy and Charging Control Rules Are Provisioned Dynamically by a PCRF | 58

dynamic-requests-secret (RADIUS Server)

IN THIS SECTION

- Syntax | 389
- Hierarchy Level | 389
- Description | 389
- Default | 390
- Options | 390
- Required Privilege Level | 390
- Release Information | 390

Syntax

```
dynamic-requests-secret password;
```

Hierarchy Level

```
[edit access radius servers name]
```

Description

Configure the secret password to be used for change of authorization requests from the RADIUS server.

Default

Use the same password that is used for authentication requests.

Options

password	Password for dynamic requests.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring RADIUS Servers | 91
- Understanding Network Elements | 71
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

encrypt (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 391
- Hierarchy Level | 391
- Description | 391
- Options | 391
- Required Privilege Level | 391
- Release Information | 391

Syntax

```
encrypt {
    hash algorithm;
    prefix hash-prefix;
}
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name]
```

Description

Specify the transform to be applied to the header for the HTTP header enrichment so that you can add subscriber attributes in a way that is obscured from the user.

NOTE: If you include this statement, then you also must configure **hash** and **prefix** statements.

Options

hash *algorithm* Use the specified hashing algorithm. Currently, only **md5** is supported.

prefix *hash-prefix* Use the specified prefix key (up to 63 alphanumeric characters). The prefix key is concatenated with the specified tag attribute and hashed. The resulting hash value is then inserted into the HTTP header.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Configuring HCM Profiles and Assigning Tag Rules | 49
- Junos Web Aware HTTP Header Enrichment Overview | 34

equals

IN THIS SECTION

- Syntax | 392
- Hierarchy Level | 392
- Description | 393
- Options | 393
- Required Privilege Level | 393
- Release Information | 393

Syntax

```
equals {
    value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from called-station-id],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from calling-station-id],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from class],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
```

```
from framed-ip-address],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from framed-ipv6-prefix],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from 3gpp-imsi],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from nas-ip-address],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format integer],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format string],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format time],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format v4address],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format v6address],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format v6prefix]
```

Description

Specify the value that the RADIUS attribute must equal.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

Options

value Value that the RADIUS attribute must equal.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130

Understanding Selection of Properties for an IP-Based TDF Subscriber | 110

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112

IP-Based Subscriber Setup Overview | 107

exclude (Diameter Gx Profiles)

IN THIS SECTION

- Syntax | 394
- Hierarchy Level | 394
- Description | 395
- Options | 395
- Required Privilege Level | 395
- Release Information | 395

Syntax

```
exclude {
    an-gw-address;
    default-eps-bearer-qos;
    packet-filter-information;
    packet-filter-operation;
    rat-type;
}
```

Hierarchy Level

```
[edit unified-edge diameter-profiles gx-profile profile-name attributes]
```

Description

Configure the attribute-value pairs (AVPs) to be excluded from the credit control request (CCR) messages between the MX Series router and the policy and charging enforcement function (PCEF).

Options

an-gw-address—Exclude the AN-GW-Address AVP.

default-eps-bearer-qos—Exclude the Default-EPS-Bearer-QoS AVP.

packet-filter-information—Exclude the Packet-Filter-Information AVP.

packet-filter-operation—Exclude the Packet-Filter-Operation AVP.

rat-type—Exclude the RAT-Type AVP.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

gx-profile | 429

external-assigned (Address Pools)

IN THIS SECTION

- Syntax | 396
- Hierarchy Level | 396
- Description | 396

Required Privilege Level | 396
Release Information | 396

Syntax

```
external-assigned;
```

Hierarchy Level

```
[edit access address-assignment address-pools name family inet network network-
prefix],
[edit access address-assignment address-pools name family inet6 network network-
prefix]
```

Description

Assign addresses in network prefixes statically.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Understanding Source IP Filtering with Address Pools in TDF Domains for IP-Based Subscribers | 110

Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers | 119

family (Address Pools)

IN THIS SECTION

- Syntax | 397
- Hierarchy Level | 397
- Description | 397
- Options | 398
- Required Privilege Level | 398
- Release Information | 398

Syntax

```
family (inet | inet6) {
    network {
        [network-prefix] {
            external-assigned;
        }
    }
}
```

Hierarchy Level

```
[edit access address-assignment address-pools name]
```

Description

Specify the protocol family information for the address pool. Address pools must have either **inet** (IPv4) or **inet6** (IPv6) configured.

NOTE: A address pool can have either **inet** (IPv4) or **inet6** (IPv6) configured, but not both.

Options

inet IP version 4 (IPv4) suite.

inet6 IP version 6 (IPv6) suite.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Understanding Source IP Filtering with Address Pools in TDF Domains for IP-Based Subscribers | 110

Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers | 119

family (Exclude Prefix)

IN THIS SECTION

- Syntax | 399
- Hierarchy Level | 399
- Description | 399
- Required Privilege Level | 399
- Release Information | 399

Syntax

```
family {
    inet {
        apply-groups [group-names];
        apply-groups-except [group-names];
        network address net-mask;
    }
    inet6 {
        apply-groups [group-names];
        apply-groups-except [group-names];
        network address net-mask;
    }
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name subscriber-
exclude-prefix]
```

Description

Specify the IP version for the network prefix of source IP addresses for uplink packets and destination IP addresses for downlink packets that must not undergo TDF processing.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | 140
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based and IFL-Based TDF Subscribers Overview | 107
- IP-Based Subscriber Setup Overview | 107

family (TDF Interface)

IN THIS SECTION

- Syntax | 400
- Hierarchy Level | 400
- Description | 400
- Options | 401
- Required Privilege Level | 401
- Release Information | 401

Syntax

```
family family-name;
```

Hierarchy Level

```
[edit interfaces mif unit interface-unit-number]
```

Description

Configure the protocol family information for the TDF logical interface.

Options

family-name Protocol family. The following options are supported:

- **inet**—IP version 4 suite.
- **inet6**—IP version 6 suite.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a TDF Logical Interface | 143

flow-action

IN THIS SECTION

- Syntax | 402
- Hierarchy Level | 402
- Description | 402
- Options | 402
- Required Privilege Level | 402
- Release Information | 402

Syntax

```
flow-action  (drop | forward)
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber
default-local-policy]
```

Description

Specify the action to take on a subscriber's data packets entering the access interface of the TDF domain when a TDF IP-based subscriber session does not exist.

Options

drop	Drop the subscriber's packets.
forward	Forward the subscriber's packets.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | **121**

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | **108**

IP-Based Subscriber Setup Overview | **107**

flow-descriptions

IN THIS SECTION

- Syntax | 403
- Hierarchy Level | 403
- Description | 404
- Options | 404
- Required Privilege Level | 404
- Release Information | 404

Syntax

```
flow-descriptions flow-identifier {
    direction (uplink | downlink | both);
    local-port-range {
        low lower-boundary high upper-boundary;
    }
    local-ports number;
    no-send-to-ue;
    protocol protocol-number;
    remote-address (ipv4-address ipv4-address | ipv6-address ipv6-address);
    remote-port-range {
        low lower-boundary high upper-boundary;
    }
    remote-ports number;
}
```

Hierarchy Level

```
[edit unified-edge pcef],
[edit services pcef]
```

Description

Specify a service data flow (SDF) filter (flow identifier) that includes one or more filtering parameters (address, protocol, and port) to identify the subscriber traffic that you want the SDF filter to detect. SDF filters are specified in a PCC rule to identify the Layer 3 or Layer 4 IP packet flows that you want to receive a particular treatment.

> **NOTE**: A PCC rule must include at least one SDF filter and can include a maximum of 15 SDF filters.

If you are using Junos OS Subscriber Aware, specify the name of the SDF filter at the **[edit unified-edge pcef]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the name of the SDF filter at the **[edit services pcef]** hierarchy level.

Options

flow-identifier — Name of the SDF filter.

- **Range:** 1 through 63 characters.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

RELATED DOCUMENTATION

Configuring Service Data Flow Filters

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment

Understanding Application-Aware Policy Control for Subscriber Management

flows (PCC Rules)

IN THIS SECTION

- Syntax | **405**
- Hierarchy Level | **405**
- Description | **406**
- Options | **406**
- Required Privilege Level | **406**
- Release Information | **406**

Syntax

```
flows ([flow-identifier] | any);
```

Hierarchy Level

```
[edit unified-edge pcef pcc-rules rule-name from],
[edit services pcef pcc-rules rule-name from]
```

Description

Specify the service data flow (SDF) filters (flow identifiers) that define the match criteria for the policy and charging control (PCC) rule. You can configure a maximum of 15 SDF filters. You must include the **flows** statement in a PCC rule. If you do not want to filter subscriber traffic based on SDF filters, use the **any** option.

If you are using Junos OS Subscriber Aware, specify the name of the SDF filter at the **[edit unified-edge pcef pcc-rules *rule-name* from]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the name of the SDF filter at the **[edit services pcef pcc-rules *rule-name* from]** hierarchy level.

Options

flow-identifier Name of an SDF filter that is used to detect IP packet flows. You can configure a maximum of 15 SDF filters. The referenced SDF filters must be configured.

- **Range:** 1 through 63 characters.

any All IP packet flows.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-rules *rule-name* from]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

Configuring Policy and Charging Control Rules

Configuring Service Data Flow Filters

format (Unified Edge Gateways)

IN THIS SECTION

- Syntax | 407
- Hierarchy Level | 408
- Description | 408
- Required Privilege Level | 409
- Release Information | 409

Syntax

```
format {
    integer {
        equals {
            value;
        }
        greater-than value;
        less-than value;
    }
    string {
        equals {
            value;
        }
        has-prefix{
            value;
        }
        has-suffix {
            value;
        }
        matches {
```

```
            value;
        }
    }
    time {
        equals {
            value;
        }
        greater-than value;
        less-than value;
    }
    v4address {
        equals {
            value;
        }
    }
    v6address {
        equals {
            value;
        }
    }
    v6prefix {
        equals {
            value;
        }
    }
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name]
```

Description

Specify the custom AVP attribute's format and value to match for the incoming RADIUS request from the IP-based subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | **108**
- IP-Based Subscriber Setup Overview | **107**

format (LRF Profile)

IN THIS SECTION

- Syntax | **409**
- Hierarchy Level | **410**
- Description | **410**
- Required Privilege Level | **410**
- Release Information | **410**

Syntax

```
format ipfix;
```

Hierarchy Level

```
[edit services lrf profile profile-name template template-name]
```

Description

Configure a format for the template. Only the IPFIX format is supported for this release.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Junos OS Subscriber Aware

Configuring Logging and Reporting for Subscriber Management

forwarding-class (PCC Action Profiles)

IN THIS SECTION

- Syntax | 411
- Hierarchy Level | 411
- Description | 411
- Options | 411

Required Privilege Level | 411
Release Information | 412

Syntax

```
forwarding-class class-name;
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name],
[edit services pcef pcc-action-profiles profile-name]
```

Description

Specify the forwarding class to which packets must be assigned.

If you are using Junos OS Subscriber Aware, specify the forwarding class at the **[edit unified-edge pcef pcc-action-profiles *profile-name*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the forwarding class at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level.

Options

class-name	Name of the forwarding class.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

- Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment
- *Understanding Application-Aware Policy Control for Subscriber Management*
- *Configuring Policy and Charging Control Action Profiles for Subscriber Management*

firmware-revision

IN THIS SECTION

- Syntax | **412**
- Hierarchy Level | **413**
- Description | **413**
- Options | **413**
- Required Privilege Level | **413**
- Release Information | **413**

Syntax

```
firmware-revision firmware-revision;
```

Hierarchy Level

```
[edit access diameter]
```

Description

Configure the firmware revision that is advertised in the Capabilities-Exchange-Request or Capabilities-Exchange-Answer message.

Options

firmware-revision Number of the firmware revision that is the advertised value of the Firmware-Revision AVP.

- **Default:** 0
- **Range:** 0 through 4294967295

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

framed-ip-address

IN THIS SECTION

- Syntax | 414
- Hierarchy Level | 414
- Description | 414
- Required Privilege Level | 414
- Release Information | 415

Syntax

```
framed-ip-address {
    equals value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from]
```

Description

Specify the RADIUS AVP Framed-IP-Address (IPv4) for the incoming RADIUS request from the subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130
- Understanding Selection of Properties for an IP-Based TDF Subscriber | 110
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- IP-Based Subscriber Setup Overview | 107

framed-ipv6-prefix

IN THIS SECTION

- Syntax | 415
- Hierarchy Level | 416
- Description | 416
- Required Privilege Level | 416
- Release Information | 416

Syntax

```
framed-ipv6-prefix {
    equals value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from]
```

Description

Specify the RADIUS AVP Framed-IPv6-Prefix for the incoming RADIUS request from the subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130

Understanding Selection of Properties for an IP-Based TDF Subscriber | 110

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112

IP-Based Subscriber Setup Overview | 107

from (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 417
- Hierarchy Level | 417
- Description | 418
- Required Privilege Level | 418
- Release Information | 418

Syntax

```
from {
    destination-address {
        (any-ipv4 | any-ipv4 except);
        (any-ipv6 | any-ipv6 except);
        (any-unicast | any-unicast except);
        (prefix | prefix except);
    }
    destination-address-range {
        high address low address <except>;
    }
    destination-port-range {
        high port-number low port-number;
    }
    destination-ports value;
    destination-prefix-list {
        (prefix-name | prefix-name except);
    }
}
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number]
```

Description

Specify the match criteria for the term in the tag rule. If all the conditions specified in the match criteria are met, then the HTTP header enrichment actions specified in the **then** statement are applied.

If you want the HTTP header enrichment actions specified in the **then** statement to be applied to all HTTP requests, do not include any matching conditions with the **from** statement.

NOTE: You must include a **from** statement in a tag rule.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm (HTTP Header Enrichment) | 434

from (PCC Rules)

IN THIS SECTION

- Syntax | 419
- Hierarchy Level | 419
- Description | 419
- Required Privilege Level | 419

Release Information | 420

Syntax

```
from {
    <application-groups [application-group-name]>;
    <applications [application-name]>;
    flows ([flow-identifier] | any);
}
```

Hierarchy Level

```
[edit unified-edge pcef pcc-rules rule-name],
[edit services pcef pcc-rules rule-name]
```

Description

Specify the match criteria for the policy and charging control (PCC) rules. Any referenced SDF filter, application, or application group in the **from** statement must be configured.

If you are using Junos OS Subscriber Aware, specify the match criteria at the **[edit unified-edge pcef pcc-rules *rule-name*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the match criteria at the **[edit services pcef pcc-rules *rule-name*]** hierarchy level.

NOTE: You must include the **flows** statement. If you do not want to filter subscriber traffic based on service data flow (SDF) filters, use **flows any**.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-rules *rule-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

Configuring Policy and Charging Control Rules

from (TDF Domain Selection)

IN THIS SECTION

- Syntax | **421**
- Hierarchy Level | **423**
- Description | **423**
- Required Privilege Level | **423**
- Release Information | **423**

Syntax

```
from {
    3gpp-imsi {
        equals value;
        has-prefix value;
        has-suffix value;
        matches value;
    }
    attribute name {
        code numeric-code;
        vendor-id vendor-id;
        format {
            integer {
                equals {
                    value;
                }
                greater-than value;
                less-than value;
            }
            string {
                equals {
                    value;
                }
                has-prefix{
                    value;
                }
                has-suffix {
                    value;
                }
                matches {
                    value;
                }
            }
            time {
                equals {
                    value;
                }
                greater-than value;
                less-than value;
            }
            v4address {
```

```
                equals {
                    value;
                }
            }
            v6address {
                equals {
                    value;
                }
            }
            v6prefix {
                equals {
                    value;
                }
            }
        }
    }
    called-station-id {
        equals value;
        matches value;
    }
    calling-station-id {
        equals value;
        matches value;
    }
    class {
        equals value;
        has-prefix value;
        has-suffix value;
        matches value;
    }
    client client-name;
    framed-ip-address {
        equals value;
    }
    framed-ipv6-prefix {
        equals value;
    }
    nas-ip-address {
        equals value;
    }
    snoop-segment snoop-segment-name;
    user-name {
        equals value;
```

```
        has-prefix value;
        has-suffix value;
        matches value;
    }
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
```

Description

Specify the match criteria for the TDF domain selection or PCEF profile selection term.

NOTE: For any term, the subscriber must match all the match conditions specified in a **from** statement. If you do not configure the **from** statement, then all subscribers are considered a match.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**
- Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**
- IP-Based Subscriber Setup Overview | **107**

function (Diameter Network Element)

IN THIS SECTION

- Syntax | 424
- Hierarchy Level | 424
- Description | 424
- Options | 424
- Required Privilege Level | 425
- Release Information | 425

Syntax

```
function function-name;
```

Hierarchy Level

```
[edit access diameter network-element element-name]
```

Description

Specify the function associated with a Diameter network element.

Options

function-name—Function associated with the network element.

Functions currently supported:

- Policy charging and control (**pcc-gx**).
- Diameter credit-control application are the functions currently supported.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

gate-status

IN THIS SECTION

- Syntax | 425
- Hierarchy Level | 426
- Description | 426
- Default | 426
- Options | 426
- Required Privilege Level | 426
- Release Information | 427

Syntax

```
gate-status (uplink | downlink | uplink-downlink | disable-both);
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name],
[edit services pcef pcc-action-profiles profile-name]
```

Description

Configure the gate status in a PCC action profile to enable or disable the forwarding of service flow packets. The gate status determines whether the uplink and downlink gates are opened or closed.

If you are using Junos OS Subscriber Aware, configure the gate status at the **[edit unified-edge pcef pcc-action-profiles *profile-name*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, configure the gate status at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level.

Default

By default, if this statement is not configured, forwarding of service data flow packets is enabled in both the uplink and downlink directions.

Options

disable-both	Disable forwarding of service data flow packets in the uplink and downlink directions.
downlink	Enable forwarding of service data flow packets in the downlink direction.
uplink-downlink	Enable forwarding of service data flow packets in the uplink and downlink directions.
uplink	Enable forwarding of service data flow packets in the uplink direction.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

- Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment
- *Configuring Policy and Charging Control Action Profiles for Subscriber Management*
- *Understanding Application-Aware Policy Control for Subscriber Management*

greater-than

IN THIS SECTION

- Syntax | **427**
- Hierarchy Level | **428**
- Description | **428**
- Options | **428**
- Required Privilege Level | **428**
- Release Information | **428**

Syntax

```
greater-than value;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format integer],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format time]
```

Description

Specify a value for the custom AVP attribute above which the incoming RADIUS request from the subscriber must match.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

Options

value Value that the attribute must be greater than.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**

Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**

IP-Based Subscriber Setup Overview | **107**

gx-profile

IN THIS SECTION

- Syntax | 429
- Hierarchy Level | 430
- Description | 430
- Options | 430
- Required Privilege Level | 430
- Release Information | 430

Syntax

```
gx-profile profile-name {
    <attributes> {
        exclude {
            an-gw-address;
            default-eps-bearer-qos;
            packet-filter-information;
            packet-filter-operation;
            rat-type;
        }
        include {
            gx-capability-list;
            rule-suggestion;
        }
    }
    <request-timeout seconds>;
    targets {
        target-name {
            <destination-host hostname>;
            destination-realm realm-name;
            network-element element-name;
            priority priority-value;
        }
```

```
    }
}
```

Hierarchy Level

```
[edit unified-edge diameter-profiles]
```

Description

Configure the Diameter profile used for Gx applications.

Options

profile-name Name of the Diameter profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Diameter Profiles Overview | 149

has-prefix (Unified Edge Gateways)

IN THIS SECTION

- Syntax | 431
- Hierarchy Level | 431
- Description | 431
- Options | 432
- Required Privilege Level | 432
- Release Information | 432

Syntax

```
has-prefix {
    value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from class],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from 3gpp-imsi],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format string]
```

Description

Specify the prefix that the attribute must have.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

Options

value Prefix string.

- **Range:** 1 through 254 alphanumeric characters.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130

Understanding Selection of Properties for an IP-Based TDF Subscriber | 110

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112

IP-Based Subscriber Setup Overview | 107

has-suffix

IN THIS SECTION

- Syntax | 433
- Hierarchy Level | 433
- Description | 433
- Options | 433
- Required Privilege Level | 433

Release Information | 434

Syntax

```
has-suffix {
    value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from class],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from 3gpp-imsi],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format string]
```

Description

Specify the suffix that the attribute must have.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

Options

value Suffix string.

- **Range:** 1 through 254 alphanumeric characters.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130
- Understanding Selection of Properties for an IP-Based TDF Subscriber | 110
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- IP-Based Subscriber Setup Overview | 107

hcm (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 434
- Hierarchy Level | 436
- Description | 436
- Required Privilege Level | 436
- Release Information | 436

Syntax

```
hcm {
    tag-attribute [tag-attr-name];
    tag-rule rule-name {
        term term-number {
            from {
                destination-address {
                    (any-ipv4 | any-ipv4 except);
```

```
                    (any-ipv6 | any-ipv6 except);
                    (any-unicast | any-unicast except);
                    (prefix | prefix except);
                }
                destination-address-range {
                    high address low address <except>;
                }
                destination-port-range {
                    high port-number low port-number;
                }
                destination-ports value;
            }
            then {
                count;
                tag tag-name {
                    encrypt {
                        hash algorithm;
                        prefix hash-prefix;
                    }
                    ipv4-mask ipv4-mask;
                    ipv6-mask ipv6-mask;
                    ipv4-or-value ipv4-or-value;
                    ipv6-or-value ipv6-or-value;
                    tag-attribute tag-attr-name;
                    tag-header header;
                    tag-separator separator;
                }
            }
        }
    }
    tag-rule-set rule-set-name {
        [rule rule-name];
    }
    profile profile-name {
        tag rule rule-name;
    }
}
```

Hierarchy Level

```
[edit services]
```

Description

Configure the parameters required to support subscriber-aware HTTP header enrichment.

You can add content to the HTTP headers sent back and forth as part of the client-server exchange for subscribers accessing Web-based services. You configure HTTP header enrichment as a service for a subscriber.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 16.1.

Support for Next Gen Services introduced in Junos OS Release 20.2R1 on MX Series routers MX240, MX480 and MX960.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm-profile (HTTP Header Enrichment)

IN THIS SECTION

Syntax | 437

- Hierarchy Level | 437
- Description | 437
- Options | 437
- Required Privilege Level | 437
- Release Information | 437

Syntax

```
hcm-profile hcm-profile-name;
```

Hierarchy Level

```
[edit services service-set]
```

Description

Specify the HTTP header enrichment profile that was configured at the **[edit services hcm]** hierarchy level. This placeholder profile has no configuration options, but it must be specified to enable HTTP header enrichment functionality on the services plane.

Options

hcm-profile-name	Name of the HCM profile.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 20.2R1 on MX Series routers MX240, MX480 and MX960.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm (HTTP Header Enrichment) | 434

hcm-profile (PCC Action Profiles)

IN THIS SECTION

- Syntax | 438
- Hierarchy Level | 438
- Description | 438
- Options | 439
- Required Privilege Level | 439
- Release Information | 439

Syntax

```
hcm-profile hcm-profile-name;
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name]
```

Description

Specify the HCM profile that you want a PCC action profile to use for determining which HTTP header enrichment rules to apply.

NOTE: This PCC action profile can be used in a PCC rule that only includes **applications** or **application-groups** statements in the **from** statement, and these statements must identify HTTP-based applications. The HCM profile must have been previously configured at the **[edit services hcm]** hierarchy level.

Options

hcm-profile-name	Name of the HCM profile.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

Support added in Junos 20.2R1 for Next Gen Services on MX240, MX480, and MX960 routers.

RELATED DOCUMENTATION

Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware | 83

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | 56

host (Diameter Origin)

IN THIS SECTION

Syntax | 440

Hierarchy Level | 440

- Description | 440
- Options | 440
- Required Privilege Level | 440
- Release Information | 440

Syntax

```
host hostname;
```

Hierarchy Level

```
[edit access diameter origin]
```

Description

Specify the name of the host that originates the Diameter message.

Options

hostname Name of the message origin host. Supplied as the value of the Origin-Host AVP for all messages sent by the Diameter instance.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

http-log-multiple-transactions (LRF Profile)

IN THIS SECTION

- Syntax | 441
- Hierarchy Level | 441
- Description | 441
- Required Privilege Level | 442
- Release Information | 442

Syntax

```
http-log-multiple-transactions;
```

Hierarchy Level

```
[edit services lrf profile profile-name]
```

Description

Configure HTTP transaction logging to generate and send HTTP metadata for each transaction of a data session. This option is only relevant if the template specified in an LRF rule includes **http** in the **template-type**.

By default, HTTP transaction logging is disabled, and the HTTP transaction records for a TCP session are sent together as one group of records.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

- *Configuring an LRF Profile for Subscribers*
- Configuring Logging and Reporting for Junos OS Subscriber Aware
- *Configuring Logging and Reporting for Subscriber Management*

icmp-mapping (Application Identification)

IN THIS SECTION

- Syntax | 442
- Hierarchy Level | 443
- Description | 443
- Required Privilege Level | 443
- Release Information | 443

Syntax

```
icmp-mapping {
    code icmp-code;
    order order;
    order-priority (high | low);
```

```
    type icmp-type;
}
```

Hierarchy Level

```
[edit services application-identification application application-name]
```

Description

Match Internet Control Message Protocol (ICMP) messages identified by unique code and type. This classification is intended to identify and differentiate various types of ICMP messages.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

view-level—To view this statement in the configuration.

control-level—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

id-components

IN THIS SECTION

Syntax | 444

- Hierarchy Level | 444
- Description | 444
- Options | 445
- Required Privilege Level | 445
- Release Information | 445

Syntax

```
id-components {
    use-class;
    use-imsi;
    use-msisdn;
    use-nai;
    use-nas-port;
    use-nas-port-id;
    use-realm;
    use-username;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber
subscription-id subscription-id-options entry-name]
```

Description

Specify a method for constructing the Subscription-Id for the Diameter credit control request (CCR) message that is sent from the TDF to the PCRF for IP-based subscribers belonging to the TDF domain. You may specify more than one option, and the order of preference matches the order in which the options appear.

Options

use-class Subscription-Id-Type is configurable and the Subscription-Id-Data is the entire Class attribute value by default. You can configure a regular expression to parse the Class attribute contents, specify characters to insert between the resulting regular expression groups, and specify the subscription ID type with the **use-class** options under the **[edit unified-edge gateways tdf *gateway-name* domains *domain-name* subscription-id]** hierarchy.

use-imsi Subscription-Id-Type is END_USER_IMSI and the Subscription-Id-Data is the 3GPP-IMSI.

use-msisdn Subscription-Id-Type is END_USER_E164 and the Subscription-Id-Data is the Calling-Station-Id.

use-nai Subscription-Id-Type is END_USER_NAI and the Subscription-Id-Data is the entire User-Name.

use-nas-port Subscription-Id-Type is END_USER_PRIVATE and the Subscription-Id-Data is the NAS-Port.

use-nas-port-id Subscription-Id-Type is END_USER_PRIVATE and the Subscription-Id-Data is the NAS-Port-Id.

use-realm Subscription-Id-Type is END_USER_PRIVATE and the Subscription-Id-Data is the realm portion of User-Name in NAI format.

use-username Subscription-Id-Type is END_USER_PRIVATE and the Subscription-Id-Data is the user name portion of User-Name in NAI format.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108

idle-timeout

IN THIS SECTION

- Syntax | 446
- Hierarchy Level | 446
- Description | 446
- Options | 447
- Required Privilege Level | 447
- Release Information | 447

Syntax

```
idle-timeout idle-timeout;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber]
```

Description

Configure the idle timeout for the TDF IP-based subscriber session. The idle timeout is the duration that the subscriber session waits to receive a data packet before timing out. After the idle timeout expires, the TDF takes down the session. Setting the idle timeout ensures that if no data is being sent for the duration specified, then the session can be taken down, and the TDF's resources can be freed.

Options

idle-timeout Number of minutes after which the TDF subscriber session times out.

- **Range:** 0 through 300.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108

IP-Based Subscriber Setup Overview | 107

ifl-subscriber

IN THIS SECTION

- Syntax | 448
- Hierarchy Level | 448
- Description | 448
- Options | 448
- Required Privilege Level | 448
- Release Information | 448

Syntax

```
ifl-subscriber [subscriber-name] {
    access-interfaces [interface-name];
    apply-groups [group-names];
    apply-groups-except [group-names];
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
```

Description

Specify the name of the IFL-based subscriber for traffic that is carried on a particular interface or interfaces. You can configure up to 32 IFL-based subscribers in a TDF domain.

To configure a subscriber name, you must have set the **subscriber-type** to **ifl** at the **[edit unified-edge gateway tdf *gateway-name* domains *domain-name*]** hierarchy.

Options

subscriber-name Name of the subscriber. You can configure up to 32 IFL-based subscribers in a TDF domain.

- **Range:** Up to 63 bytes.

The remaining statements are described separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | 140

Understanding the Definition of a Set of IFL-Based Subscriber Properties with a TDF Domain | 116

immediate-accounting-response

IN THIS SECTION

- Syntax | 449
- Hierarchy Level | 449
- Description | 449
- Default | 450
- Options | 450
- Required Privilege Level | 450
- Release Information | 450

Syntax

```
immediate-accounting-response (enabled | disabled);
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber]
```

Description

Enable or disable the sending of an immediate RADIUS response message to the accounting start message received from a GGSN, PGW, or BNG RADIUS client.

Default

If you do not specify an option, **disabled** is the default.

Options

enabled Enable immediate response.

disabled Disable immediate response. The response is sent after TDF subscriber creation is complete.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | **121**
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | **108**
- IP-Based Subscriber Setup Overview | **107**

include (Diameter Gx Profiles)

IN THIS SECTION

- Syntax | **451**
- Hierarchy Level | **451**
- Description | **451**
- Options | **451**
- Required Privilege Level | **451**

Release Information | 451

Syntax

```
include {
    gx-capability-list;
    rule-suggestion;
}
```

Hierarchy Level

```
[edit unified-edge diameter-profiles gx-profile profile-name attributes]
```

Description

Configure the attribute-value pairs (AVPs) to be included in the credit control request (CCR) messages between the MX Series router and the policy and charging enforcement function (PCEF).

Options

gx-capability-list—Include the Gx-Capability list AVP.

rule-suggestion—Include the Rule-suggestion AVP.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

gx-profile | 429

incoming-queue

IN THIS SECTION

- Syntax | 452
- Hierarchy Level | 452
- Description | 452
- Options | 452
- Required Privilege Level | 453
- Release Information | 453

Syntax

```
incoming-queue {
    size size;
}
```

Hierarchy Level

```
[edit access diameter peer peer-name]
```

Description

Configure the incoming queue properties of this peer.

Options

size *size* Size of the queue. The default is 6000.

- **Range:** 1 through 65,535 packets

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

inet (TDF Subscriber Address)

IN THIS SECTION

- Syntax | 453
- Hierarchy Level | 454
- Description | 454
- Required Privilege Level | 454
- Release Information | 454

Syntax

```
inet {
    apply-groups [group-names];
    apply-groups-except [group-names];
```

```
    pool pool-name;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber
subscriber-address]
```

Description

Specify IP version 4 (IPv4) for the address pool that contains the source IP addresses for IP-based subscriber packets that undergo TDF processing.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108

IP-Based Subscriber Setup Overview | 107

inet (TDF Subscriber Exclude Prefix)

IN THIS SECTION

- Syntax | 455
- Hierarchy Level | 455
- Description | 455
- Required Privilege Level | 455
- Release Information | 456

Syntax

```
inet {
    network address mask;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name subscriber-
exclude-prefix family]
```

Description

Specify IP version 4 (IPv4) for the network prefix of source IP addresses for uplink packets and destination IP addresses for downlink packets that do not undergo TDF processing.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | 140
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based and IFL-Based TDF Subscribers Overview | 107
- IP-Based Subscriber Setup Overview | 107

inet6 (TDF Subscriber Address)

IN THIS SECTION

- Syntax | 456
- Hierarchy Level | 457
- Description | 457
- Required Privilege Level | 457
- Release Information | 457

Syntax

```
inet6 {
    pool pool-name;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber
subscriber-address]
```

Description

Specify IP version 6 (IPv6) for the address pool that contains the source IP addresses for IP-based subscriber packets that undergo TDF processing.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based Subscriber Setup Overview | 107

inet6 (TDF Subscriber Exclude Prefix)

IN THIS SECTION

- Syntax | 458
- Hierarchy Level | 458
- Description | 458

Required Privilege Level | 458
Release Information | 458

Syntax

```
inet6 {
    network address mask;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name subscriber-
exclude-prefix family]
```

Description

Specify IP version 6 (IPv6) for the network prefix of source IP addresses for uplink packets and destination IP addresses for downlink packets that do not undergo TDF processing.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | 140

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
IP-Based and IFL-Based TDF Subscribers Overview | 107
IP-Based Subscriber Setup Overview | 107

integer

IN THIS SECTION

- Syntax | 459
- Hierarchy Level | 459
- Description | 459
- Required Privilege Level | 460
- Release Information | 460

Syntax

```
integer {
    equals value;
    greater-than value;
    less-than value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format]
```

Description

Specify the custom AVP attribute's format as an integer and the value to match for the incoming RADIUS request from the IP-based subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**
- Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**
- IP-Based Subscriber Setup Overview | **107**

interface (Services PIC)

IN THIS SECTION

- Syntax | **461**
- Hierarchy Level | **461**
- Description | **461**
- Options | **462**
- Required Privilege Level | **462**
- Release Information | **462**

Syntax

```
[interface interface-name];
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name system service-pics]
```

Description

Specify one or more of the MS-MPC service interfaces that represent the service PICs used for anchoring subscriber-aware services in the MX Series router. The following conditions are applicable to the services PIC interfaces configured here:

- If an aggregated multiservices interface (ams) is specified in this statement, the ams must already be defined at the **[edit interfaces]** hierarchy level.
- The PIC must have the **jservices-hcm**, **jservices-mss**, **jservices-jdpi**, **jservices-pcef**, and **jservices-crypto-base** packages configured at the **[edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider]** hierarchy level.
- The appropriate services group configuration must be applied to the PIC:
  - For each service PIC that requires application identification but not HTTP header enrichment, apply the **tdf-services-xlp-dpi** group.
  - For each service PIC that requires both application identification and HTTP header enrichment, configure the **tdf-services-xlp-dpi-with-hcm** group.
- If an MS-MPC service interface is a member of an AMS, then that member interface cannot be specified here. For example, if mams-2/0/0 is a member interface of ams0, then ms-2/0/0/ cannot be directly specified here.

NOTE: If an AMS (for example ams0) is used for the services PIC, then load balancing is performed to distribute subscriber-aware services among the member interfaces. Otherwise, load balancing is not performed.

Options

interface-name Name of the interface representing the services PIC.

- **Syntax:** The interface must be a valid multiservices interface (ams*n* or ms-*a*/*b*/0, where *n* is the ams number, *a* is the Flexible PIC Concentrator [FPC] slot number, and *b* is the PIC slot number); for example, ams0 or ms-1/0/0.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Service PICs | 18

TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment | 9

interface (Session PICs)

IN THIS SECTION

- Syntax | 463
- Hierarchy Level | 463
- Description | 463
- Options | 463
- Required Privilege Level | 463
- Release Information | 464

Syntax

```
[interface interface-name];
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name system session-pics]
```

Description

Specify one or more of the MS-MPC service interfaces that represent the session PICs used for the control plane in the TDF gateway. The following conditions are applicable to the session PIC interfaces configured here:

- If an aggregated multiservices interface (ams) is specified in this statement, the ams must already be defined at the **[edit interfaces]** hierarchy level.
- The **tdf-session-xlp** group configuration must be applied to the PIC.
- The session PIC must have the **jservices-mobile** package configured at the **[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]** hierarchy level.
- If a session PIC interface is a member of an AMS, then that member interface cannot be specified here. For example, if mams-2/0/0 is a member interface of ams0, then ms-2/0/0/ cannot be directly specified here.

Options

interface-name Name of the interface representing the services PIC.

- **Syntax:** The interface must be a valid multiservices interface (ams*n* or ms-*a*/*b*/0, where *n* is the ams number, *a* is the Flexible PIC Concentrator [FPC] slot number, and *b* is the PIC slot number); for example, ams0 or ms-1/0/0.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Session PICs | 19

TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment | 9

interface-service (Services Interfaces)

IN THIS SECTION

- Syntax | 464
- Hierarchy Level | 465
- Description | 465
- Options | 465
- Required Privilege Level | 465
- Release Information | 465

Syntax

```
interface-service {
    load-balancing-options {
        hash-keys {
            egress-key (destination-ip | source-ip);
            ingress-key (destination-ip | source-ip);
        }
    }
    service-interface name;
}
```

Hierarchy Level

```
[edit services service-set service-set-name]
```

Description

Specify the device name for the interface service Physical Interface Card (PIC).

Options

service-interface *name*—Name of the service device associated with the interface-wide service set.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

- Configuring Service Sets to be Applied to Services Interfaces

ip-protocol-mapping (Application Identification)

IN THIS SECTION

- Syntax | 466
- Hierarchy Level | 466
- Description | 466
- Options | 466

Required Privilege Level | 466
Release Information | 467

Syntax

```
ip-protocol-mapping {
    order order;
    order-priority (high | low);
    protocol  (http | ssl | tcp | udp)
}
```

Hierarchy Level

```
[edit services application-identification application application-name]
```

Description

For IP traffic, identify an application by matching the IP protocol. This parameter is used to identify an application based on IP and is intended only for IP traffic.

Options

protocol-number Industry-standard numeric protocol value.

- **Range:** 0 through 254

You can find a complete list of industry standard protocol numbers at the IANA website.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

view-level—To view this statement in the configuration.

control-level—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

ip-subscriber

IN THIS SECTION

- Syntax | 467
- Hierarchy Level | 468
- Description | 468
- Required Privilege Level | 469
- Release Information | 469

Syntax

```
ip-subscriber {
    access-interfaces interface-name [interface-name];
    default-local-policy {
        flow-action (drop | forward);
        maximum-bit-rate {
            uplink mbr-uplink-value ;
            downlink mbr-downlink-value;
        }
        burst-size {
            uplink uplink-burst-size;
            downlink downlink-burst-size;
        }
    }
```

```
    idle-timeout idle-timout;
    immediate-accounting-response (enabled | disabled);
    maximum-subscribers number;
    subscriber-address {
        inet {
            pool pool-name;
        }
        inet6 {
            pool pool-name;
        }
    }
    subscription-id {
        constant ;
        subscription-id-options {
            entry-name {
                id-components {
                    use-imsi;
                    use-msisdn;
                    use-nai;
                    use-username;
                    use-realm;
                    use-nas-port;
                    use-nas-port-id;
                }
            }
        }
    }
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
```

Description

Configure TDF domain features that are unique to IP-based subscribers.

The remaining statements are described separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based Subscriber Setup Overview | 107

ipv4-address (Steering Path)

IN THIS SECTION

- Syntax | 469
- Hierarchy Level | 470
- Description | 470
- Options | 470
- Required Privilege Level | 470
- Release Information | 470

Syntax

```
ipv4-address ipv4-address;
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name steering path]
[edit services pcef pcc-action-profiles profile-name]
```

Description

Specify the IPv4 address of a third-party server to which the PCC action profile steers HTTP traffic for applying services. If you configure this, the PCC action profile can only be used in PCC rules that match only HTTP-based applications and all flows.

Options

ipv4-address *ipv4-address* Use the specified IPv4 address of the server.

Required Privilege Level

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

- *Understanding Application-Aware Policy Control for Subscriber Management*
- *Configuring Policy and Charging Control Action Profiles for Subscriber Management*
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment
- Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware

ipv4-mask (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 471
- Hierarchy Level | 471
- Description | 471
- Options | 472
- Required Privilege Level | 472
- Release Information | 472

Syntax

```
ipv4-mask ipv4-mask;
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name]
```

Description

Configure the IPv4 mask to identify a byte of the IPv4 subscriber address that you want to modify in the HTTP header. You must also set the **ipv4-or-value** statement at the **[edit services hcm tag-rule *rule-name* term *term-number* then tag *tag-name*]** hierarchy level to specify the new value you want to put in the byte.

Options

ipv4-mask IPv4 mask. Specify **255** in the byte you want to modify and specify **0** in the bytes that you *do not* want to modify.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- ipv4-or-value (HTTP Header Enrichment) | **472**
- Configuring HTTP Header Enrichment Overview | **41**
- Configuring Tag Rules | **42**
- Configuring HCM Profiles and Assigning Tag Rules | **49**
- Junos Web Aware HTTP Header Enrichment Overview | **34**

ipv4-or-value (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | **473**
- Hierarchy Level | **473**
- Description | **473**
- Options | **473**
- Required Privilege Level | **473**
- Release Information | **473**

Syntax

```
ipv4-or-value ipv4-or-value;
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name]
```

Description

Configure the new IPv4 value for the byte you want to modify in the IPv4 subscriber address in the HTTP header. You must also set the **ipv4-mask** statement at the **[edit services hcm tag-rule *rule-name* term *term-number* then tag *tag-name*]** hierarchy level to clear the existing byte value.

Options

ipv4-or-value IPv4 value. Specify the new value in the byte you are modifying and specify 0 in all other bytes.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- ipv4-mask (HTTP Header Enrichment) | 471
- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Configuring HCM Profiles and Assigning Tag Rules | 49
- Junos Web Aware HTTP Header Enrichment Overview | 34

ipv6-address (Steering Path)

IN THIS SECTION

- Syntax | 474
- Hierarchy Level | 474
- Description | 474
- Options | 474
- Required Privilege Level | 474
- Release Information | 475

Syntax

```
ipv6-address ipv6-address;
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name steering path]
[edit services pcef pcc-action-profiles profile-name]
```

Description

Specify the IPv6 address of a third-party server to which the PCC action profile steers HTTP traffic for applying services. If you configure this, the PCC action profile can only be used in PCC rules that match only HTTP-based applications and all flows.

Options

ipv6-address *ipv6-address* Use the specified IPv6 address of the server.

Required Privilege Level

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

- *Understanding Application-Aware Policy Control for Subscriber Management*
- *Configuring Policy and Charging Control Action Profiles for Subscriber Management*
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment
- Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware

ipv6-mask (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | **476**
- Hierarchy Level | **476**
- Description | **476**
- Options | **476**
- Required Privilege Level | **476**
- Release Information | **476**

Syntax

```
ipv6-mask ipv6-mask;
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name]
```

Description

Configure the IPv6 mask to identify a byte of the IPv6 subscriber address that you want to modify in the HTTP header. You must also set the **ipv6-or-value** statement at the **[edit services hcm tag-rule *rule-name* term *term-number* then tag *tag-name*]** hierarchy level to specify the new value you want to put in the byte.

Options

ipv6-mask IPv6 mask. Specify **ff** in the byte you want to modify and specify **0** in the bytes that you *do not* want to modify.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- ipv6-or-value (HTTP Header Enrichment) | 477
- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Configuring HCM Profiles and Assigning Tag Rules | 49

Junos Web Aware HTTP Header Enrichment Overview | 34

ipv6-or-value (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 477
- Hierarchy Level | 477
- Description | 477
- Options | 477
- Required Privilege Level | 478
- Release Information | 478

Syntax

```
ipv6-or-value ipv6-or-value;
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name]
```

Description

Configure the new IPv6 value for the byte you want to modify in the IPv6 subscriber address in the HTTP header. You must also set the **ipv6-mask** statement at the **[edit services hcm tag-rule *rule-name* term *term-number* then tag *tag-name*]** hierarchy level to clear the existing byte value.

Options

ipv6-or-value IPv6 value. Specify the new value in the byte you are modifying and specify 0 in all other bytes.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- ipv6-mask (HTTP Header Enrichment) | 475
- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Configuring HCM Profiles and Assigning Tag Rules | 49
- Junos Web Aware HTTP Header Enrichment Overview | 34

keep-existing-steering

IN THIS SECTION

- Syntax | 478
- Hierarchy Level | 479
- Description | 479
- Required Privilege Level | 479
- Release Information | 479

Syntax

```
keep-existing-steering;
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name steering],
[edit services pcef pcc-action-profiles profile-name]
```

Description

Specify that the PCC action profile steering attributes that a PCC rule applies at the start of a data flow will continue to be applied to that data flow when the PCC rule match conditions are modified, deleted, or added to.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

- *Understanding Application-Aware Policy Control for Subscriber Management*
- *Configuring Policy and Charging Control Action Profiles for Subscriber Management*
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment
- Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware

less-than

IN THIS SECTION

- Syntax | 480
- Hierarchy Level | 480
- Description | 480
- Options | 480
- Required Privilege Level | 481
- Release Information | 481

Syntax

```
less-than value;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format integer],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format time]
```

Description

Specify a value for the custom AVP attribute below which the incoming RADIUS request from the subscriber must match.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

Options

value	Value that the attribute must be less than.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130
- Understanding Selection of Properties for an IP-Based TDF Subscriber | 110
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- IP-Based Subscriber Setup Overview | 107

local-port-range

IN THIS SECTION

- Syntax | 482
- Hierarchy Level | 482
- Description | 482
- Default | 482
- Options | 482
- Required Privilege Level | 483
- Release Information | 483

Syntax

```
local-port-range {
    low low-value;
    high high-value;
}
```

Hierarchy Level

```
[edit unified-edge pcef flow-descriptions flow-identifier],
[edit services pcef flow-descriptions flow-identifier]
```

Description

Specify the port range to identify the subscriber traffic that you want the service data flow (SDF) filter to detect.

NOTE: You can specify either **local-port-range** or a list of ports with **local-ports**, but not both.

If you are using Junos OS Subscriber Aware, specify the port range at the **[edit unified-edge pcef flow-descriptions *flow-identifier*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the port range at the **[edit services pcef flow-descriptions *flow-identifier*]** hierarchy level.

Default

If the **local-port-range** statement is not configured, the default is any range of local ports.

Options

low-value — Lower boundary for the port range.

- **Range:** 1 through 65,535

high-value — Upper boundary for the port range.

- **Range:** 1 through 65,535

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef flow-descriptions *flow-identifier*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

RELATED DOCUMENTATION

Configuring Service Data Flow Filters

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment

Understanding Application-Aware Policy Control for Subscriber Management

local-ports

IN THIS SECTION

- Syntax | **484**
- Hierarchy Level | **484**
- Description | **484**
- Default | **484**
- Options | **484**
- Required Privilege Level | **485**

Release Information | 485

Syntax

```
local-ports [number];
```

Hierarchy Level

```
[edit unified-edge pcef flow-description flow-identifier],
[edit services pcef flow-description flow-identifier]
```

Description

Specify a port number or list of port numbers to identify the subscriber traffic that you want the service data flow (SDF) filter to detect.

NOTE: You can specify either a list of ports or a port range, but not both.

If you are using Junos OS Subscriber Aware, specify the port numbers at the **[edit unified-edge pcef flow-description *flow-identifier*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the port numbers at the **[edit services pcef flow-description *flow-identifier*]** hierarchy level.

Default

If the **local-ports** statement is not configured, the default is any local ports.

Options

number Number of a port or list of port numbers. You can specify a maximum of three port numbers (separated by a space) in a list.

- **Range:** 1 through 65,535

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef flow-description *flow-identifier*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

RELATED DOCUMENTATION

Configuring Service Data Flow Filters

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment

Understanding Application-Aware Policy Control for Subscriber Management

logging-rule (PCC Action Profile)

IN THIS SECTION

- Syntax | **486**
- Hierarchy Level | **486**
- Description | **486**
- Options | **486**
- Required Privilege Level | **486**
- Release Information | **487**

Syntax

```
logging-rule lrf-rule-name;
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name],
[edit services pcef pcc-action-profiles profile-name]
```

Description

Assign the LRF rule to the PCC action profile of a static PCC rule. When the matching conditions in the PCC rule are met, the LRF rule is activated.

If you are using Junos OS Subscriber Aware, specify the name of the LRF rule at the **[edit unified-edge pcef pcc-action-profiles *profile-name*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the name of the LRF rule at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level.

Options

lrf-rule-name LRF rule name. The referenced LRF rule must be configured in an LRF profile.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

- *Configuring the Activation of an LRF Rule by a PCC Rule*
- Configuring Logging and Reporting for Junos OS Subscriber Aware
- *Configuring Logging and Reporting for Subscriber Management*
- *Configuring an LRF Profile for Subscribers*

lrf-profile (Service Set)

IN THIS SECTION

- Syntax | **487**
- Hierarchy Level | **488**
- Description | **488**
- Options | **488**
- Required Privilege Level | **488**
- Release Information | **488**

Syntax

```
lrf-profile profile-name;
```

Hierarchy Level

```
[edit services service-set service-set-name]
```

Description

Assign the LRF profile to the service set that is that is configured for application-aware policy control.

Options

profile-name LRF profile name. The referenced LRF profile must be configured.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Assigning an LRF Profile to Subscribers | **194**

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Junos OS Subscriber Aware | **186**

Applying Logging and Reporting Configuration to a Subscriber Management Service Set

Configuring Logging and Reporting for Subscriber Management

matches

IN THIS SECTION

- Syntax | 489
- Hierarchy Level | 489
- Description | 490
- Options | 491
- Required Privilege Level | 491
- Release Information | 491

Syntax

```
matches {
    apply-groups [group-names];
    apply-groups-except [group-names];
    value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from called-station-id],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from calling-station-id],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from class],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from 3gpp-imsi],
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format string]
```

Description

Specify the regular expression that the attribute must match.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

Table 12: Regular Expression Operators for the matches Statement

Operator	Matches
. (period)	One instance of any character except the space.
* (asterisk)	Zero or more instances of the immediately preceding term.
+ (plus sign)	One or more instances of the immediately preceding term.
? (question mark)	Zero or one instance of the immediately preceding term.
| (pipe)	One of the terms that appears on either side of the pipe operator.
! (exclamation point)	Any string except the one specified by the expression when the exclamation point appears at the start of the expression. Use of the exclamation point is specific to Junos OS.
^ (caret)	Start of a line when the caret appears outside square brackets. One instance of any character that does not follow it within square brackets when the caret is the first character inside square brackets.
$ (dollar sign)	End of a line.
[ ] (paired square brackets)	One instance of one of the enclosed alphanumeric characters. To indicate a range of characters, use a hyphen (-) to separate the beginning and ending characters of the range. For example, [a-z0-9] matches any letter or number.

Table 12: Regular Expression Operators for the matches Statement *(Continued)*

Operator	Matches
( ) (paired parentheses)	One instance of the evaluated value of the enclosed term. Parentheses are used to indicate the order of evaluation in the regular expression.

Options

value Regular expression to match.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**

Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**

IP-Based Subscriber Setup Overview | **107**

maximum-bit-rate (Default Local Policy)

IN THIS SECTION

- Syntax | 492
- Hierarchy Level | 492
- Description | 492
- Options | 492
- Required Privilege Level | 493
- Release Information | 493

Syntax

```
maximum-bit-rate uplink mbr-uplink-value downlink mbr-downlink-value;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber
default-local-policy]
```

Description

Configure the maximum bit rate (MBR) for a subscriber's uplink and downlink traffic entering or exiting the access interface of the TDF domain when a TDF IP-based subscriber session does not exist. Uplink traffic originates from the subscriber towards the public data network (PDN), and downlink traffic comes from the PDN and is destined for the subscriber.

Options

mbr-uplink-value	MBR value for the uplink direction. • **Range:** 0 through 6144000 Kbps.
mbr-downlink-value	MBR value for the downlink direction.

- **Range:** 0 through 6144000 Kbps.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108

IP-Based Subscriber Setup Overview | 107

maximum-bit-rate (PCC Action Profiles)

IN THIS SECTION

- Syntax | 494
- Hierarchy Level | 494
- Description | 494
- Default | 494
- Options | 494
- Required Privilege Level | 494
- Release Information | 495

Syntax

```
maximum-bit-rate uplink mbr-uplink-value downlink mbr-downlink-value;
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name],
[edit services pcef pcc-action-profiles profile-name]
```

Description

Specify the maximum bit rate (MBR) that you want a PCC action profile to use for uplink and downlink traffic.

If you are using Junos OS Subscriber Aware, specify the MBR at the **[edit unified-edge pcef pcc-action-profiles *profile-name*** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the MBR at the **[edit services pcef pcc-action-profiles *profile-name*** hierarchy level.

Default

If you configure the **maximum-bit-rate** statement but do not specify MBR values for **uplink** and **downlink**, the default value is 0.

Options

mbr-uplink-value — MBR value for the uplink direction.

- **Range:** 1 through 6144000 Kbps.

mbr-downlink-value — MBR value for the downlink direction.

- **Range:** 1 through 6144000 Kbps.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-action-profiles *profile-name*** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

- Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment
- *Configuring Policy and Charging Control Action Profiles for Subscriber Management*
- *Understanding Application-Aware Policy Control for Subscriber Management*

maximum-bit-rate (TDF Domain)

IN THIS SECTION

- Syntax | **496**
- Hierarchy Level | **496**
- Description | **496**
- Options | **496**
- Required Privilege Level | **496**
- Release Information | **496**

Syntax

```
maximum-bit-rate {
    apply-groups [group-names];
    apply-groups-except [group-names];
    downlink mbr-downlink-value;
    uplink mbr-uplink-value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
```

Description

Configure the TDF domain's default TDF subscriber maximum bit rate (MBR) for uplink and downlink traffic. Uplink traffic originates from the subscriber towards the public data network (PDN), and downlink traffic comes from the PDN and is destined for the subscriber.

Options

mbr-downlink-value MBR value for the downlink direction.

- **Range:** 0 through 1,048,000 Kbps.

mbr-uplink-value MBR value for the uplink direction.

- **Range:** 0 through 6,144,000 Kbps.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | 140
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based and IFL-Based TDF Subscribers Overview | 107
- IP-Based Subscriber Setup Overview | 107

maximum-pending-reqs-limit

IN THIS SECTION

- Syntax | 497
- Hierarchy Level | 497
- Description | 497
- Options | 498
- Required Privilege Level | 498
- Release Information | 498

Syntax

```
maximum-pending-reqs-limit number;
```

Hierarchy Level

```
[edit access radius network-element name]
```

Description

Configure the maximum number of requests that can be queued to the network element. When the pending-request queue is full, any additional requests are dropped.

Options

number Maximum number of pending requests.

- **Range:** 512 through 8192

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Network Elements | 94

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

maximum-pending-requests (Diameter)

IN THIS SECTION

- Syntax | 499
- Hierarchy Level | 499
- Description | 499
- Options | 499
- Required Privilege Level | 499
- Release Information | 499

Syntax

```
maximum-pending-requests requests;
```

Hierarchy Level

```
[edit access diameter applications pcc-gx]
```

Description

Configure the maximum number of pending requests parameter for the Diameter application.

Options

requests Maximum number of pending requests.

- **Range:** 1000 through 65,535
- **Default:** 20,000

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

maximum-sessions (TDF Gateway)

IN THIS SECTION

- Syntax | 500
- Hierarchy Level | 500
- Description | 500
- Options | 500
- Required Privilege Level | 500
- Release Information | 501

Syntax

```
maximum-sessions max-sessions;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name cac]
```

Description

Configure the maximum number of TDF subscriber sessions that may be running.

Options

max-sessions Maximum number of TDF subscriber sessions, expressed in thousands.

- **Range:** 10 thousands through 5000 thousands

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a TDF Gateway | 16

maximum-subscribers

IN THIS SECTION

- Syntax | 501
- Hierarchy Level | 501
- Description | 502
- Options | 502
- Required Privilege Level | 502
- Release Information | 502

Syntax

```
maximum-subscribers number;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber]
```

Description

Specify the maximum number of IP-based subscriber sessions that the TDF domain can support.

Options

number Maximum number of subscriber sessions allowed.

- **Range:** 100 thousands through 5000 thousands.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | **121**

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | **108**

IP-Based Subscriber Setup Overview | **107**

maximum-sessions-trap-percentage (TDF Gateway)

IN THIS SECTION

- Syntax | **503**
- Hierarchy Level | **503**
- Description | **503**
- Options | **503**
- Required Privilege Level | **503**

Release Information | 503

Syntax

```
maximum-sessions-trap-percentage max-sessions-pct;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name cac]
```

Description

Configure the trap threshold for the number of TDF subscriber sessions as a percentage of the maximum number of sessions (**maximum-sessions**) that was configured at the **[edit unified-edge gateways tdf *gateway-name* cac]** hierarchy level. If the number of subscriber sessions reaches the threshold, the SNMP trap **jnxScgSMSessionThreshHigh** is generated.

Options

max-sessions-pct Percentage of the maximum number of TDF subscriber sessions.

- **Range:** 1 through 90

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a TDF Gateway | 16

member (Application Identification)

IN THIS SECTION

- Syntax | 504
- Hierarchy Level | 504
- Description | 504
- Options | 505
- Required Privilege Level | 505
- Release Information | 505

Syntax

```
[member member-name];
```

Hierarchy Level

```
[edit services application-identification application application-name over
protocol-type signature l4-l7-signature-name]
```

Description

Define a member name for a custom application definition. Custom definitions can contain multiple members that define attributes for an application. You can define a maximum of four member names.

Options

member-name Name of a member for a custom application definition. You can define a maximum of four member names.

Required Privilege Level

view-level—To view this statement in the configuration.

control-level—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Releases 19.3R2 and 19.4R1 on MX Series MX240, MX480 and MX960 using the MX-SPC3 services card.

RELATED DOCUMENTATION

- *Application Identification Overview*
- *Configuring Custom Application Signatures*
- *Application Identification Overview*
- *Application Identification Overview*

memory (TDF Gateway)

IN THIS SECTION

- Syntax | **506**
- Hierarchy Level | **506**
- Description | **506**
- Options | **506**
- Required Privilege Level | **506**
- Release Information | **506**

Syntax

```
memory memory-pct;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name cac]
```

Description

Configure the threshold for the maximum amount of memory that the TDF gateway may use. If the amount of memory that the TDF gateway uses reaches the threshold, the SNMP trap **jnxScgSMMemoryThreshHigh** is generated.

Options

memory-pct Maximum percentage of memory that can be used.

- **Range:** 1 through 90.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a TDF Gateway | 16

mif (TDF Interface)

IN THIS SECTION

- Syntax | 507
- Hierarchy Level | 507
- Description | 507
- Required Privilege Level | 508
- Release Information | 508

Syntax

```
mif {
    mtu;
    unit interface-unit-number {
        family family-name {
            service {
                input service-set;
                output service-set;
            }
        }
    }
}
```

Hierarchy Level

```
[edit interfaces]
```

Description

Configure the TDF interfaces for the TDF domains. A TDF interface is distinct from other types of interfaces and is used to associate a TDF domain's subscribers with an access interface in a virtual routing and forwarding table (VRF). You need to configure one TDF interface logical interface (unit) for every TDF domain.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring a TDF Logical Interface | 143

monitoring-key (PCC Action Profile)

IN THIS SECTION

- Syntax | 508
- Hierarchy Level | 509
- Description | 509
- Options | 509
- Required Privilege Level | 509
- Release Information | 509

Syntax

```
monitoring-key key_string
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name]
```

Description

Specify the monitoring key that controls TDF subscriber usage monitoring for traffic that matches the data flows or applications identified in the predefined PCC rules containing the PCC action profile. The monitoring key is defined by the PCRF.

Options

key_string	Identifier for the monitoring key.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring TDF Subscriber Usage Monitoring for Traffic That Matches Predefined PCC Rules | 105

Understanding Usage Monitoring for TDF Subscribers | 74

mtu (TDF Interface)

IN THIS SECTION

Syntax | 510

- Hierarchy Level | 510
- Description | 510
- Options | 510
- Required Privilege Level | 510
- Release Information | 511

Syntax

```
mtu mtu-size;
```

Hierarchy Level

```
[edit interfaces mif]
```

Description

Configure the maximum transmission unit (MTU) size for the TDF interface.

Options

mtu-size MTU size.

- **Range:** 256 through 9192 bytes
- **Default:** 500 bytes (inet, inet6, and ISO families), 1448 bytes (MPLS)

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a TDF Logical Interface | 143

nas-ip-address

IN THIS SECTION

- Syntax | 511
- Hierarchy Level | 511
- Description | 511
- Required Privilege Level | 512
- Release Information | 512

Syntax

```
nas-ip-address {
    equals value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from]
```

Description

Specify the RADIUS AVP NAS-IP-Address for the incoming RADIUS request from the subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**
- Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**
- IP-Based Subscriber Setup Overview | **107**

nat-rule-sets (Service Set)

IN THIS SECTION

- Syntax | **513**
- Hierarchy Level | **513**
- Description | **513**
- Options | **513**
- Required Privilege Level | **513**
- Release Information | **513**

Syntax

```
nat-rule-sets rule-set-name;
```

Hierarchy Level

```
[edit services service-set service-set-name]
```

Description

Specify the Network Address Translation (NAT) rule set included in the service set. You can configure only one NAT rule set. If you specify a NAT rule set, you cannot specify a NAT rule.

Options

rule-set-name	Name of the NAT rule set.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

Applying Services to Subscriber-Aware Traffic with a Service Set | 146

nat-rules

IN THIS SECTION

- Syntax | 514
- Hierarchy Level | 514
- Description | 514
- Options | 514
- Required Privilege Level | 514
- Release Information | 515

Syntax

```
(nat-rules rule-name | nat-rule-sets rule-set-name);
```

Hierarchy Level

```
[edit services service-set service-set-name]
```

Description

Specify the Network Address Translation (NAT) rules or rule set included in this service set. You can configure multiple rules, but only one rule set for each service.

Options

rule-name—Identifier for the collection of terms that constitute this rule.

rule-set-name—Identifier for the set of rules to be included.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

Configuring Service Rules

Applying Services to Subscriber-Aware Traffic with a Service Set | 146

network-element (AAA Profile)

IN THIS SECTION

- Syntax | 515
- Hierarchy Level | 515
- Description | 516
- Options | 516
- Required Privilege Level | 516
- Release Information | 516

Syntax

```
network-element network-element-name;
```

Hierarchy Level

```
[edit unified-edge aaa profiles aaa-profile-name radius authentication],
[edit unified-edge aaa profiles aaa-profile-name radius accounting]
```

Description

Specify the network element providing policy management for TDF subscribers. The network element must already be defined at the **[edit access radius]** hierarchy level.

Options

network-element-name	Name of the network element.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring an AAA Profile | 96
- Understanding AAA Profiles | 73
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64
- Configuring RADIUS Network Elements | 94

network-element (Diameter Base Protocol)

IN THIS SECTION

- Syntax | 517
- Hierarchy Level | 517
- Description | 517
- Default | 517

- Options | 517
- Required Privilege Level | 518
- Release Information | 518

Syntax

```
network-element element-name {
    function function-name;
    peer peer-name {
        priority priority-value;
        <timeout seconds>;
    }
}
```

Hierarchy Level

```
[edit access diameter]
```

Description

Configure the Diameter network element, which is similar to a peer group that provides function-specific features including failover and load balancing. Specify the associated function that the network element supports. You can prioritize the peers to support failover or load balancing.

Default

By default, all network elements are available on every session PIC unless Diameter bindings are configured.

Options

element-name—Name of the network element.

- **Range:** Up to 32 alphanumeric characters

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

network-element (Subscriber Aware Policy Control)

IN THIS SECTION

- Syntax | 518
- Hierarchy Level | 519
- Description | 519
- Options | 519
- Required Privilege Level | 519
- Release Information | 519

Syntax

```
network-element {
    element-name {
        session-pics {
            group {
                group-name {
                    [session-pic interface-name];
                }
```

```
                }
            }
        }
    }
```

Hierarchy Level

```
[edit unified-edge tdf gateway-name diameter]
```

Description

Configure the Diameter network element associated with Diameter bindings for this TDF gateway.

NOTE: If you want to set up Diameter bindings for session PICs on the TDF gateway, contact Juniper Networks Professional Services for assistance.

Options

element-name Name of the network element.

- **Range:** Up to 32 alphanumeric characters

  NOTE: The specified network element must already be configured on the TDF gateway at the **[edit access diameter network-element]** hierarchy level.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (TDF Gateway) | 370

network-elements (RADIUS)

IN THIS SECTION

- Syntax | 520
- Hierarchy Level | 520
- Description | 521
- Options | 521
- Required Privilege Level | 521
- Release Information | 521

Syntax

```
network-elements name {
    server name {
        priority priority;
    }
    maximum-pending-reqs-limit number;
    pending-queue-watermark watermark;
    pending-queue-watermark-abate abate-watermark;
}
```

Hierarchy Level

```
[edit access radius]
```

Description

Configure a network element, which is a load-balanced group of RADIUS servers providing policy management for TDF subscribers.

Options

name Name of the network element.

- **Range:** Up to 31 alphanumeric characters.

The remaining statements are described separately.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Network Elements | 94

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

network (Address Pools)

IN THIS SECTION

- Syntax | 522
- Hierarchy Level | 522
- Description | 522

- Options | 522
- Required Privilege Level | 522
- Release Information | 523

Syntax

```
network {
    [network-prefix] {
        external-assigned;
    }
}
```

Hierarchy Level

```
[edit access address-assignment address-pools name family inet],
[edit access address-assignment address-pools name family inet6]
```

Description

Specify the network prefix for the address pool for IPv4 or IPv6 addresses.

NOTE: At least one network prefix must be configured but you can configure more than one prefix.

Options

network-prefix	Network prefix (IPv4 or IPv6).

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Understanding Source IP Filtering with Address Pools in TDF Domains for IP-Based Subscribers | 110

Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers | 119

network (TDF Domain)

IN THIS SECTION

- Syntax | 523
- Hierarchy Level | 523
- Description | 524
- Options | 524
- Required Privilege Level | 524
- Release Information | 524

Syntax

```
network address net-mask;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name subscriber-
exclude-prefix family inet],
```

```
[edit unified-edge gateways tdf gateway-name domains domain-name subscriber-
exclude-prefix family inet6]
```

Description

Specify the network prefix of source IP addresses for uplink packets and destination IP addresses for downlink packets that do not undergo TDF processing.

Options

address	Network address for the network prefix to exclude.
net-mask	Netmask for the network prefix.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | **121**
- Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | **140**
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | **108**
- IP-Based and IFL-Based TDF Subscribers Overview | **107**
- IP-Based Subscriber Setup Overview | **107**

no-application-system-cache

IN THIS SECTION

- Syntax | 525
- Hierarchy Level | 525
- Description | 525
- Required Privilege Level | 525
- Release Information | 526

Syntax

```
no-application-system-cache;
```

Hierarchy Level

```
[edit services application-identification],
[edit services application-identification nested-application-settings]
```

Description

Application identification information is saved in the application system cache to improve performance. This cache is updated when a different application is identified. This caching is turned on by default. Use the **no-application-system-cache** statement to turn it off.

ASC is enabled by default when a session is created. You can manually turn this caching off using the **set services application-identification no-application-system-cache** command. You can re-enable the ASC by using the **set services application-identification application-system-cache** command.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 9.5.

Support for Next Gen Services introduced in Junos OS Release 19.3R2 and 19.4R1 on MX Series routers MX240, MX480 and MX960.

RELATED DOCUMENTATION

Configuring Global APPID Properties

Application Identification for Nested Applications

no-send-to-ue

IN THIS SECTION

- Syntax | **526**
- Hierarchy Level | **526**
- Description | **527**
- Default | **527**
- Required Privilege Level | **527**
- Release Information | **527**

Syntax

```
no-send-to-ue;
```

Hierarchy Level

```
[edit unified-edge pcef flow-description flow-identifier]
```

Description

Specify that signaling information about the service data flow (SDF) filter is not sent to the user equipment.

Default

By default, if this statement is not configured, signaling information about the SDF filter is sent to the user equipment.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Service Data Flow Filters | 79

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | 56

order (Application Identification)

IN THIS SECTION

- Syntax | 528
- Hierarchy Level | 528
- Description | 528
- Options | 528
- Required Privilege Level | 528

Release Information | 529

Syntax

```
order order;
```

Hierarchy Level

```
[edit services application-identification application name address-mapping name],
[edit services application-identification application application-name icmp-
mapping],
[edit services application-identification application application-name ip-
protocol-mapping],
[edit services application-identification application application-name over
protocol-type signature l4-l7-signature-name],
[edit services application-identification application application-name
```

Description

Define application matching priority. For address configurations, the order number resolves the conflict when multiple address entries are matched for a specific session. The lower number has a higher priority.

Options

order Order sequence number. This value is mandatory and must be unique.

- **Default:** 0
- **Range:** 0 through 65,535

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

Support at the **[edit services application-identification application *application-name*]** hierarchy level introduced in Junos OS Releases 19.3R2 and 19.4R1 on MX Series MX240, MX480 and MX960 using the MX-SPC3 services card.

RELATED DOCUMENTATION

- *Application Identification Overview*
- *Configuring Custom Application Signatures*
- *Application Identification Overview*
- *Application Identification Overview*

order-priority (Application Identification)

IN THIS SECTION

- Syntax | **529**
- Hierarchy Level | **530**
- Description | **530**
- Options | **530**
- Required Privilege Level | **530**
- Release Information | **530**

Syntax

```
order-priority (high | low);
```

Hierarchy Level

```
[edit services application-identification application application-name address-
mapping name],
[edit services application-identification application application-name icmp-
mapping],
[edit services application-identification application application-name ip-
protocol-mapping],
[edit services application-identification application application-name over
protocol-type signature l4-l7-signature-name]
```

Description

Define the priority of signatures when both a custom signature and predefined signature apply to a protocol bundle.

Options

high Custom signatures have priority over predefined signatures.

low Predefined signatures have priority over custom signatures.

- **Default:** high

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Releases 19.3R2 and 19.4R1 on MX Series MX240, MX480 and MX960 using the MX-SPC3 services card.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

Application Identification Overview

Application Identification Overview

origin (Diameter Base Protocol)

IN THIS SECTION

- Syntax | 531
- Hierarchy Level | 531
- Description | 531
- Required Privilege Level | 532
- Release Information | 532

Syntax

```
origin {
    host hostname;
    realm realm-name;
}
```

Hierarchy Level

```
[edit access diameter]
```

Description

Specify values of the Origin-Realm AVP and the Origin-Host AVP used in all messages sent by the Diameter instance. These values must be unique for each session PIC.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

outgoing-queue

IN THIS SECTION

- Syntax | 532
- Hierarchy Level | 533
- Description | 533
- Options | 533
- Required Privilege Level | 533
- Release Information | 533

Syntax

```
outgoing-queue {
    <high-watermark high-watermark>;
    <low-watermark low-watermark>;
    size size;
}
```

Hierarchy Level

```
[edit access diameter peer peer-name]
```

Description

Configure the outgoing queue properties for this peer. When the queue size reaches the high watermark, the peer is marked unavailable, any new messages to the Diameter network element are not sent to this peer, and the SNMP trap **Diameter_PeerOutQHiWMarkNotif** is generated. When the queue size descends below the low watermark after reaching the high watermark, the peer becomes available and the SNMP trap **Diameter_PeerLowQHiWMarkNotif** is generated.

Options

high-watermark *high-watermark* (Optional) Use the specified high watermark for this peer.

- **Range:** 1 through 100 percent
- **Default:** 80

low-watermark *low-watermark* (Optional) Use the specified low watermark for this peer.

- **Range:** 1 through 100 percent
- **Default:** 60

size *size* Use the specified size of the queue. The default is 6000.

- **Range:** 1 through 65,535 packets

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Diameter Peers | 158

diameter (Subscriber Aware Policy Control) | 368

over (Application Identification)

IN THIS SECTION

- Syntax | 534
- Hierarchy Level | 535
- Description | 535
- Options | 535
- Required Privilege Level | 535
- Release Information | 535

Syntax

```
over protocol-type {
    signature l4-l7-signature-name {
        chain-order
        member member-name {
            check-bytes  max-bytes-to-check;
            context context;
            pattern pattern;
            direction direction;
        }
        order order;
        order-priority (high | low);
        port-range {
            tcp [port-range];
            udp [port-range];
        }
        protocol (http | ssl | tcp | udp);
```

```
    ]
}
```

Hierarchy Level

```
[edit services application-identification application application-name]
```

Description

Configure a custom signature based on Layer 7 custom signatures that are further differentiated by the Layer 4 protocol type. Users can define their own signatures for deep packet inspection (DPI) that do not exist in the predefined signature database.

Options

l4-l7-signature-name	Name of the signature used for DPI.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Releases 19.3R2 and 19.4R1 on MX Series MX240, MX480 and MX960 using the MX-SPC3 services card.

RELATED DOCUMENTATION

- Application Identification Overview | 23
- Configuring Custom Application Signatures | 26
- Application Identification Overview | 23
- Application Identification Overview | 23

packet-capture (Next Gen Services)

IN THIS SECTION

- Syntax | 536
- Hierarchy Level | 536
- Description | 536
- Options | 537
- Required Privilege Level | 538
- Release Information | 538

Syntax

```
packet-capture {
    buffer-packets-limit bytes;
    capture-interval capture-interval;
    capture-limit capture-limit;
    global;
    max-bytes bytes;
    max-files max-files;
    max-packets max-packets;
    no-decryption;
    no-inconclusive;
    storage-limit bytes;
}
```

Hierarchy Level

```
[edit services application-identification]
```

Description

Specify packet capture options to capture the unknown application traffic. You can use the packet capture details to gather more context related to the unknown application or use the information to

analyze the traffic for potential threats. When you enable packet capture for the unknown application traffic, the system captures the entire packet details and stores information in a packet capture file at **/var/log/pcap/** location.

Options

buffer-packets-limit Maximum memory to buffer packets (bytes). Use this option to limit the maximum disk available in the Packet Forwarding Engine for packet capture files.

- **Default:** 1% of available data in shared memory
- **Range:** 0 through 5% of available data in shared memory
- **Default:** 1 MB (for cSRX)
- **Range:** 0 through 5 MB

capture-interval Timeout value in minutes to avoid repetitive capture of the same traffic. Use this option to set the maximum amount of time the current log file remains open, and receives new statistics before it is closed. The file remains open till it has reached the maximum possible size.

- **Default:** 1440 minutes (24 Hours).
- **Range:** 1 through 525600

capture-limit Number of repetitive captures of the same traffic. Use this option to limit the number of times the same traffic can be repeatedly captured before the cache entry times out.

- **Default:** 4
- **Range:** 1 through 1000

global Enable global capturing of the application traffic. use this option to configure the packet capture globally to capture all unknown traffic. Another option is to enable capturing of unknown application traffic specific to a security policy.

max-bytes Maximum number of TCP bytes per session (bytes). For TCP sessions, the count includes the actual payload data length and excludes IP/TCP headers for the maximum bytes limit.

If you are setting the packet capture at security policy level, the packet capture concludes only after the final policy is applied even if the configured limit is reached.

Limitation—Jumbo frames can have up to 1500 bytes of the payload saved in the capture file.

- **Default:** 6000 bytes
- **Range:** 40 through 1073741824

max-files Maximum number of unique packet capture files to create before the oldest file is overwritten by a new file created.

- **Range:** 1 through 2500

max-packets Maximum number of UDP packets per session.

- **Default:** 10 packets
- **Range:** 1 through 1000

no-decryption Disable capturing of the decrypted traffic.

no-inconclusive Disable packet capturing of the inconclusive traffic. This option disables the packet capture for the following sessions:

- Sessions that are closed before the application identification/classification completes.
- Sessions that ar not getting classified even on reaching the maximum packet capture limit.

If you do not configure this option, by default, the system captures packets for the inconclusive sessions.

storage-limit Maximum disk space (bytes) that can be used in the Routing Engine for packet capture files.

- **Default:** 50 MB
- **Range:** 1048576 through 4294967295 bytes

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 20.2R1.

RELATED DOCUMENTATION

show services application-identification packet-capture counters

path (Steering)

IN THIS SECTION

- Syntax | 539
- Hierarchy Level | 539
- Description | 539
- Required Privilege Level | 540
- Release Information | 540

Syntax

```
path {
    ipv4-address ipv4-address;
    ipv6-address ipv6-address;
}
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name steering],
[edit services pcef pcc-action-profiles profile-name]
```

Description

Specify the IP address of a third-party server to which the PCC action profile steers HTTP traffic for applying services. If you configure this, the PCC action profile can only be used in PCC rules that match only HTTP-based applications and all flows.

The remaining statements are explained separately.

Required Privilege Level

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

Understanding Application-Aware Policy Control for Subscriber Management

Configuring Policy and Charging Control Action Profiles for Subscriber Management

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment

Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware

pattern (Application Identification)

IN THIS SECTION

- Syntax | **541**
- Hierarchy Level | **541**
- Description | **541**

- Options | 541
- Required Privilege Level | 541
- Release Information | 541

Syntax

```
pattern pattern;
```

Hierarchy Level

```
[edit services application-identification application application-name over
protocol-type signature l4-l7-signature-name member member-name]
```

Description

Define an attack pattern to be detected.

Options

pattern User-defined pattern of attack to match, using a regular expression.

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Releases 19.3R2 and 19.4R1 on MX Series MX240, MX480 and MX960 using the MX-SPC3 services card.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

pattern (Class Attribute)

IN THIS SECTION

- Syntax | 542
- Hierarchy Level | 542
- Description | 542
- Options | 543
- Required Privilege Level | 543
- Release Information | 543

Syntax

```
pattern "pattern";
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name subscription-id
use-class]
```

Description

Configure characters to insert between the resulting regular expression groups that are generated from parsing the Class attribute contents of the accounting request from the BNG, PGW, or GGSN. Regular expression groups are identified with **\n** for a group number.

Options

pattern Characters to insert between regular expression groups. A regular expression group number "n" is identified as **\n**.

For example, the following configuration generates **" 000118191129|ALICE:DRAV3:"** out of **" 000118191129#000118191129#ALICE:DRAV3:#7168#nflat#ADSL##"**:

```
[edit unified-edge gateways tdf TDF1 domains domain1 subscription-id]
user@host# set use-class regex "[^#]*#\([^#]*\)\#\([^#]*\)"
user@host# set use-class pattern "\1|\2"
```

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

pcc-action-profile (PCC Rules)

IN THIS SECTION

- Syntax | 544
- Hierarchy Level | 544
- Description | 544
- Options | 544

Required Privilege Level | 544
Release Information | 545

Syntax

```
pcc-action-profile profile-name;
```

Hierarchy Level

```
[edit unified-edge pcef pcc-rules rules-name then],
[edit services pcef pcc-rules rules-name then]
```

Description

Specify the name of the action profile to include in a policy and charging control (PCC) rule configuration. The action profile defines the treatment to be applied to specific service data flows or to packets associated with specific applications.

If you are using Junos OS Subscriber Aware, specify the name of the action profile at the **[edit unified-edge pcef pcc-rules *rules-name* then]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the name of the action profile at the **[edit services pcef pcc-rules *rules-name* then]** hierarchy level.

Options

profile-name Name of the PCC action profile that the PCC rule references. The referenced action profile must be configured.

- **Range:** 1 through 63 characters.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-rules *rules-name* then]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

- *Configuring Policy and Charging Control Rules*
- Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment
- *Configuring Policy and Charging Control Action Profiles for Subscriber Management*
- *Understanding Application-Aware Policy Control for Subscriber Management*

pcc-action-profiles

IN THIS SECTION

- Syntax | **546**
- Hierarchy Level | **546**
- Description | **546**
- Options | **547**
- Required Privilege Level | **547**
- Release Information | **547**

Syntax

```
pcc-action-profiles profile-name {
    forwarding-class class-name;
    gate-status (uplink | downlink | uplink-downlink | disable-both);
    hcm-profile hcm-profile-name;
    logging-rule lrf-rule-name;
    maximum-bit-rate uplink mbr-uplink-value downlink mbr-downlink-value;
    monitoring-key key_string;
    redirect {
        url url-name;
    }
    steering {
        keep-existing-steering;
        path {
            ipv4-address ipv4-address;
            ipv6-address ipv6-address;
        }
        routing-instance {
            downlink downlink-vrf-name;
            uplink uplink-vrf-name;
        }
    }
}
```

Hierarchy Level

```
[edit unified-edge pcef],
[edit services pcef]
```

Description

Configure a PCC action profile. A PCC action profile defines the treatment to be applied to specific service data flows or to packets associated with specific applications. A PCC action profile is specified in the **then** clause of a PCC rule.

If you are using Junos OS Subscriber Aware, configure the PCC action profile at the **[edit unified-edge pcef]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, configure the PCC action profile at the **[edit services pcef]** hierarchy level. The following options are not applicable to subscriber management:

- **hcm-profile**
- **monitoring-key**

Options

profile-name — Name of the PCC action profile.

- **Range:** 1 through 63 characters.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

> *Understanding Application-Aware Policy Control for Subscriber Management*
>
> *Configuring Policy and Charging Control Action Profiles for Subscriber Management*

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment

Configuring TDF Subscriber Usage Monitoring for Traffic That Matches Predefined PCC Rules

Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware

pcc-rule

IN THIS SECTION

- Syntax | 548
- Hierarchy Level | 548
- Description | 548
- Options | 549
- Required Privilege Level | 549
- Release Information | 549

Syntax

```
[pcc-rule rule-name  precedence number];
```

Hierarchy Level

```
[edit unified-edge pcef pcc-rule-bases rulebase-name],
[edit services pcef pcc-rule-bases rulebase-name]
```

Description

Specify one or more policy and charging control (PCC) rules and the rules precedence in a PCC rulebase.

If you are using Junos OS Subscriber Aware, configure the PCC rules at the **[edit unified-edge pcef pcc-rule-bases *rulebase-name*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, configure the PCC rules at the **[edit services pcef pcc-rule-bases *rulebase-name*]** hierarchy level.

Options

rule-name Name of the PCC rule. The referenced PCC rule must be configured.

- **Range:** 1 through 63 characters.

number Precedence value assigned to the PCC rule. The precedence assigned must be unique among the configured PCC rules.

- **Range:** 1 through 65,535

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-rule-bases *rulebase-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

RELATED DOCUMENTATION

Configuring a Policy and Charging Control Rulebase

Configuring Policy and Charging Control Rules

pcc-rulebases (PCEF)

IN THIS SECTION

- Syntax | 550
- Hierarchy Level | 550
- Description | 550
- Options | 551
- Required Privilege Level | 551
- Release Information | 551

Syntax

```
pcc-rulebases rulebase-name {
    [pcc-rule rule-name precedence number];
}
```

Hierarchy Level

```
[edit unified-edge pcef],
[edit services pcef]
```

Description

Configure a policy and charging control (PCC) rulebase. You can specify from 1 through 4000 rules in a rulebase.

If you are using Junos OS Subscriber Aware, configure the PCC rulebase at the **[edit unified-edge pcef]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, configure the PCC rulebase at the **[edit services pcef]** hierarchy level.

Options

rulebase-name Name of the PCC rulebase.

- **Range:** 1 through 63 characters.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

RELATED DOCUMENTATION

Configuring a Policy and Charging Control Rulebase

pcc-rulebases (PCEF Profile)

IN THIS SECTION

Syntax | 552

- Hierarchy Level | 552
- Description | 552
- Options | 552
- Required Privilege Level | 553
- Release Information | 553

Syntax

```
[pcc-rulebases rulebase-name <time-of-day-profile profile-name>];
```

Hierarchy Level

```
[edit unified-edge pcef profiles profile-name aaa-policy-control],
[edit unified-edge pcef profiles profile-name dynamic-policy-control],
[edit unified-edge pcef profiles profile-name static-policy-control],
[edit services pcef profiles profile-name static-policy-control],
[edit services pcef profiles profile-name dynamic-policy-control]
```

Description

Specify a policy and charging control (PCC) rulebase for a policy control profile.

If you are using Junos OS Subscriber Aware, specify the PCC rulebase at the **[edit unified-edge pcef profiles *profile-name* (aaa-policy-control | dynamic-policy-control | static-policy-control)** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the PCC rulebase at the **[edit services pcef profiles *profile-name* (static-policy-control | dynamic-policy-control)]** hierarchy level.

Options

rulebase-name	Name of the PCC rulebase. The referenced PCC rulebase must be configured.
time-of-day-profile *profile-name*	(Optional; only applies to rulebases in static PCEF profiles for Junos OS Subscriber Aware) Use the specified name of the time-of-day profile to apply to the PCC rulebase.

The referenced profile must already be defined at the **[edit unified-edge pcef]** hierarchy level. The time-of-day profile specifies the time of day, day of the week, or day of the month to activate or deactivate the PCC rulebase for subscribers assigned to the PCEF profile.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef profiles *profile-name* static-policy-control]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support at the **[edit services pcef profiles *profile-name* dynamic-policy-control]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 18.2R1 on MX Series.

RELATED DOCUMENTATION

- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Dynamic Policies
- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Static Policies
- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Policies That a RADIUS Server Controls
- Configuring Static Time-of-Day PCC Rule Activation and Deactivation in a Junos OS Subscriber Aware PCEF Profile
- *Configuring a Policy and Charging Control Rulebase*
- *Configuring a Policy and Charging Enforcement Function Profile for Subscriber Management*

pcc-rules (PCEF)

IN THIS SECTION

- Syntax | 554
- Hierarchy Level | 554
- Description | 554
- Options | 555
- Required Privilege Level | 555
- Release Information | 555

Syntax

```
pcc-rules rule-name {
    from {
        <application-groups [application-group-name]>;
        <applications [application-name]>;
        flows ([flow-identifier | any)];
    }
    then {
        pcc-action-profile  profile-name;
    }
}
```

Hierarchy Level

```
[edit unified-edge pcef],
[edit services pcef]
```

Description

Configure the PCC rules. A PCC rule identifies the subscriber IP packets that are associated with a service data flow (SDF) or application and defines the treatment to be applied to the packets.

If you are using Junos OS Subscriber Aware, configure the PCC rule at the **[edit unified-edge pcef]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, configure the PCC rule at the **[edit services pcef]** hierarchy level.

Options

rule-name Name of the PCC rule.

- **Range:** 1 through 63 characters.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

Configuring Policy and Charging Control Rules

Configuring TDF Subscriber Usage Monitoring for Traffic That Matches Predefined PCC Rules

pcc-rules (PCEF Profile)

IN THIS SECTION

- Syntax | 556
- Hierarchy Level | 556
- Description | 556
- Options | 557
- Required Privilege Level | 557
- Release Information | 557

Syntax

```
pcc-rules [rule-name precedence number <time-of-day-profile profile-name>];
```

Hierarchy Level

```
[edit unified-edge pcef profiles profile-name aaa-policy-control],
[edit unified-edge pcef profiles profile-name dynamic-policy-control],
[edit unified-edge pcef profiles profile-name static-policy-control],
[edit services pcef profiles profile-name static-policy-control],
[edit services pcef profiles profile-name dynamic-policy-control]
```

Description

Specify the policy and charging control (PCC) rules for a policy and charging enforcement function (PCEF) profile and assign a precedence to each PCC rule. You can configure up to 32 PCC rules in a PCEF profile.

If you are using Junos OS Subscriber Aware, specify the PCC rules at the **[edit unified-edge pcef profiles *profile-name* (aaa-policy-control | dynamic-policy-control | static-policy-control)** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the PCC rules at the **[edit services pcef profiles *profile-name* (static-policy-control | dynamic-policy-control)]** hierarchy level.

Options

rule-name	Name of the PCC rule. The referenced PCC rule must be configured.
precedence *number*	Use the specified precedence value assigned to a PCC rule. A lower precedence value indicates a higher precedence. • **Range:** 1 through 65,535
time-of-day-profile *profile-name*	(Optional; only applies to rules in static PCEF profiles for Junos OS Subscriber Aware) Use the specified name of the time-of-day profile to apply to the PCC rule. The referenced profile must already be defined at the **[edit unified-edge pcef]** hierarchy level. The time-of-day profile specifies the time of day, day of the week, or day of the month to activate or deactivate the PCC rule for subscribers assigned to the PCEF profile.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef profiles *profile-name* static-policy-control]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support at the **[edit services pcef profiles *profile-name* dynamic-policy-control]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 18.2R1 on MX Series.

RELATED DOCUMENTATION

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Dynamic Policies

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Static Policies

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Policies That a RADIUS Server Controls

Configuring Static Time-of-Day PCC Rule Activation and Deactivation in a Junos OS Subscriber Aware PCEF Profile

Configuring a Policy and Charging Enforcement Function Profile for Subscriber Management

Configuring Policy and Charging Control Rules

pcc-time-of-day-profiles

IN THIS SECTION

- Syntax | 558
- Hierarchy Level | 559
- Description | 559
- Options | 559
- Required Privilege Level | 559
- Release Information | 559

Syntax

```
pcc-time-of-day-profiles profile-name {
    rule-activation-time {
        <day-of-week | day-of-month month>;
        <hour:min>;
    }
    rule-deactivation-time {
        <day-of-week | day-of-month month>;
        <hour:min>;
    }
}
```

Hierarchy Level

```
[edit unified-edge pcef]
```

Description

Configure a PCC time-of-day profile to specify the time of day, day of the week, or day of the month to activate and deactivate a PCC rule or rulebase. A PCC time-of-day profile is applied to a PCC rule or PCC rulebase within a static PCEF profile. If a time zone is configured on the router, the time-of-day settings apply to the configured time zone.

Options

profile-name Name of the PCC time-of-day profile.

- **Range:** 1 through 63 characters.

The remaining statements are explained separately.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Static Time-of-Day PCC Rule Activation and Deactivation in a Junos OS Subscriber Aware PCEF Profile | **103**

Understanding Static Time-of-Day PCC Rule Activation and Deactivation | **74**

pcef

IN THIS SECTION

- Syntax | 560
- Hierarchy Level | 562
- Description | 562
- Required Privilege Level | 562
- Release Information | 562

Syntax

```
pcef {
    flow-descriptions flow-identifier {
        direction (uplink | downlink | both);
        local-port-range {
            low low-value high high-value;
        }
        local-ports number;
        no-send-to-ue;
        protocol number;
        remote-address (ipv4-address ipv4-address | ipv6-address ipv6-address);
        remote-port-range {
            low low-value high high-value;
        }
        remote-ports number;
    }
    pcc-action-profiles profile-name {
        forwarding-class class-name;
        gate-status (uplink | downlink | uplink-downlink | disable-both);
        hcm-profile hcm-profile-name;
        logging-rule lrf-rule-name;
        maximum-bit-rate uplink mbr-uplink-value downlink mbr-downlink-value;
        monitoring-key key_string;
        redirect {
            url url-name;
        }
```

```
        steering {
            keep-existing-steering;
            path {
                ipv4-address ipv4-address;
                ipv6-address ipv6-address;
            }
            routing-instance {
                downlink downlink-vrf-name;
                uplink uplink-vrf-name;
            }
        }
    }
    pcc-rulebases rulebase-name {
        [pcc-rule rule-name precedence number];
    }
    pcc-rules rule-name {
        from {
            <application-groups [application-group-name]>;
            <applications [application-name]>;
            flows ([flow-identifier ] | any);
        }
        then {
            pcc-action-profile  profile-name;
        }
    }
    pcc-time-of-day-profiles profile-name {
        rule-activation-time {
            <day-of-week | day-of-month month>;
            <hour:min>;
        }
        rule-deactivation-time {
            <day-of-week | day-of-month month>;
            <hour:min>;
        }
    }
    profiles profile-name {
        aaa-policy-control {
            aaa-profile aaa-profile-name;
            pcc-rulebases [rulebase-name];
            user-password password;
        }
        dynamic-policy-control {
            pcc-rules {
```

```
                [rule-name  number];
            }
            pcc-rulebases {
                [rulebase-name];
            }
            diameter-profile gx-profile-name;
        }
        static-policy-control {
            pcc-rules {
                [rule-name precedence number <time-of-day-profile profile-name>];
            }
            pcc-rulebases {
                [rulebase-name <time-of-day-profile profile-name>];
            }
        }
    }
}
```

Hierarchy Level

```
[edit unified-edge]
```

Description

Set up the overall policy and control enforcement function (PCEF) configuration.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Understanding Junos Subscriber Aware Policy and Charging Enforcement Function (PCEF) | 52

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment | 56

pcef-profile (Service Set)

IN THIS SECTION

- Syntax | 563
- Hierarchy Level | 563
- Description | 563
- Options | 564
- Required Privilege Level | 564
- Release Information | 564

Syntax

```
pcef-profile pcef-profile-name;
```

Hierarchy Level

```
[edit services service-set service-set-name]
```

Description

Specify the dummy PCEF profile that you configured at the **[edit services pcef]** hierarchy level. This profile is a placeholder profile with no configuration options, but it must be specified to enable PCEF functionality on the services plane.

Options

pcef-profile-name	Name of the PCEF profile.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Applying Services to Subscriber-Aware Traffic with a Service Set
- *Identifying the Service Interface That Handles Subscriber Management Application-Aware Policy Control*
- *Configuring a Policy and Charging Enforcement Function Profile for Subscriber Management*

pcef-profile (TDF Domain)

IN THIS SECTION

- Syntax | 565
- Hierarchy Level | 565
- Description | 565
- Options | 565

Required Privilege Level | 565
Release Information | 566

Syntax

```
pcef-profile name;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
```

Description

Specify the policy and charging enforcement function (PCEF) profile to be applied to subscribers in the TDF domain. This is required for IFL-based subscribers, and optional for IP-based subscribers. If you do not identify a PCEF profile, then the PCEF profile must be assigned under the **[edit unified-edge gateways tdf *gateway-name* domain-selection term]** hierarchy level.

Options

name Name of the PCEF profile.

> **NOTE**: The PCEF profile must have been previously configured at the **[edit unified-edge pcef]** hierarchy level.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | 140
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based and IFL-Based TDF Subscribers Overview | 107
- IP-Based Subscriber Setup Overview | 107
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- Understanding PCEF Profiles | 70

pcef-profile (TDF Domain Selection)

IN THIS SECTION

- Syntax | 566
- Hierarchy Level | 567
- Description | 567
- Options | 567
- Required Privilege Level | 567
- Release Information | 567

Syntax

```
pcef-profile pcef-profile-name;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
then]
```

Description

Specify the policy and charging enforcement function (PCEF) profile to be selected for the IP-based TDF subscriber when the criteria specified in the **domain-selection term *term-name* from** statement are matched. This PCEF profile is required if the TDF domain selected for a subscriber does not specify a PCEF profile or you want to allow different members of the same TDF domain to have different PCEF profiles.

Options

pcef-profile-name Name of the PCEF profile.

> **NOTE**: The PCEF profile must have been previously configured at the **[edit unified-edge pcef]** hierarchy level.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**
- IP-Based Subscriber Setup Overview | **107**

peer (Diameter Base Protocol)

IN THIS SECTION

- Syntax | 568
- Hierarchy Level | 569
- Description | 569
- Options | 569
- Required Privilege Level | 569
- Release Information | 569

Syntax

```
peer peer-name {
    address ip-address;
    connect-actively {
        <capabilities-exchange-timeout seconds>;
        <port port-number>;
        <repeat-timeout seconds>;
        <retry-timeout seconds>;
        <timeout seconds>;
        transport transport-name;
    }
    <disconnect-peer-timeout seconds>;
    <incoming-queue> {
        size size;
    }
    <outgoing-queue> {
        <high-watermark high-watermark>;
        <low-watermark low-watermark>;
        size size;
    }
    <watchdog-timeout seconds>;
}
```

Hierarchy Level

```
[edit access diameter]
```

Description

Configure a remote peer for the Diameter instance. You can configure up to 31 peers.

Options

peer-name—Name of the peer.

- **Range:** 1 through 32 alphanumeric characters

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

peer (Diameter Network Element)

IN THIS SECTION

Syntax | 570
Hierarchy Level | 570

- Description | 570
- Options | 570
- Required Privilege Level | 571
- Release Information | 571

Syntax

```
peer peer-name {
    priority priority-value;
    <timeout seconds>;
}
```

Hierarchy Level

```
[edit access diameter network-element element-name]
```

Description

Define and prioritize a peer associated with a Diameter network element. You must prioritize the associated peer by including the **priority** statement.

Options

peer-name—Name of the peer.

- **Range:** 1 through 32 alphanumeric characters

> **NOTE**: The specified peer must already be configured at the **[edit access diameter peer]** hierarchy level.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

pending-queue-watermark

IN THIS SECTION

- Syntax | 571
- Hierarchy Level | 571
- Description | 572
- Options | 572
- Required Privilege Level | 572
- Release Information | 572

Syntax

```
pending-queue-watermark watermark;
```

Hierarchy Level

```
[edit access radius network-element name]
```

Description

Configure the pending-request queue high watermark for the network element. This is a percentage of the maximum number of requests that can be queued to the network element, which is configured in the **maximum-pending-reqs-limit** *number* statement at the **[edit access radius network-element** *name***]** hierarchy level. When the queue size reaches the high watermark, a **flow control on** message is generated.

Options

watermark High watermark for the network element pending request queue.

- **Range:** 1 through 100 percent.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Network Elements | 94

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

pending-queue-watermark-abate

IN THIS SECTION

Syntax | 573

Hierarchy Level | 573

- Description | 573
- Options | 573
- Required Privilege Level | 573
- Release Information | 574

Syntax

```
pending-queue-watermark-abate abate-watermark;
```

Hierarchy Level

```
[edit access radius network-element name]
```

Description

Configure the low watermark of the pending-request queue for the network element. This is a percentage of the maximum size of the pending-request queue, which is configured in the **maximum-pending-reqs-limit *watermark*** statement at the **[edit access radius network-element *name*]** hierarchy level. When the number of pending requests drops below this low watermark value after having exceeded the high watermark configured in the **pending-queue-watermark *watermark*** statement, a **flow control off** message is generated.

Options

abate-watermark Low watermark for the network element pending request queue.

- **Range:** 1 through 100 percent.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring RADIUS Network Elements | 94
- Understanding Network Elements | 71
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

policy-based-logging (LRF Profile)

IN THIS SECTION

- Syntax | 574
- Hierarchy Level | 574
- Description | 574
- Required Privilege Level | 575
- Release Information | 575

Syntax

```
policy-based-logging;
```

Hierarchy Level

```
[edit services lrf profile profile-name]
```

Description

Configure policy-based logging, which causes the LRF rules to be activated by PCC rules.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

- *Configuring an LRF Profile for Subscribers*
- Configuring Logging and Reporting for Junos OS Subscriber Aware
- *Configuring Logging and Reporting for Subscriber Management*

pool (TDF Domain)

IN THIS SECTION

- Syntax | 575
- Hierarchy Level | 576
- Description | 576
- Options | 576
- Required Privilege Level | 576
- Release Information | 576

Syntax

```
pool pool-name;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber
subscriber-address (inet | inet6)]
```

Description

Specify the address pool that contains the source IP addresses for IP-based subscriber packets that undergo TDF processing.

You can specify only one address pool.

Options

pool-name	Name of the address pool.

NOTE: The address pool must have been previously configured at the **[edit access address-assignment]** hierarchy level.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers | **119**
- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | **121**
- Understanding Source IP Filtering with Address Pools in TDF Domains for IP-Based Subscribers | **110**
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | **108**

port (LRF Profile)

IN THIS SECTION

- Syntax | 577
- Hierarchy Level | 577
- Description | 577
- Options | 577
- Required Privilege Level | 577
- Release Information | 578

Syntax

```
port collector-port-number;
```

Hierarchy Level

```
[edit services lrf profile profile-name collector collector-name destination]
```

Description

Specify the destination port of the collector.

Options

collector-port-number Port number for the destination address of the collector.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Junos OS Subscriber Aware

Configuring Logging and Reporting for Subscriber Management

port (RADIUS Server)

IN THIS SECTION

- Syntax | 578
- Hierarchy Level | 578
- Description | 579
- Options | 579
- Required Privilege Level | 579
- Release Information | 579

Syntax

```
port port-number;
```

Hierarchy Level

```
[edit access radius servers name]
```

Description

Configure the port number to which the RADIUS requests are sent.

Options

port-number Port number to which the RADIUS requests are sent.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Servers | 91

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

port-range (Application Identification)

IN THIS SECTION

- Syntax | 580
- Hierarchy Level | 580
- Description | 580
- Options | 580
- Required Privilege Level | 580
- Release Information | 580

Syntax

```
port-range {
    tcp [port-range];
    udp [port-range];
}
```

Hierarchy Level

```
[edit services application-identification application application-name over
protocol-type signature l4-l7-signature-name]
```

Description

Define TCP or UDP port number range.

Options

port-range Numeric port ranges. The format for numeric port ranges is in the format *minimum-value–maximum-value*.

Required Privilege Level

view-level—To view this statement in the configuration.

control-level—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Releases 19.3R2 and 19.4R1 on MX Series MX240, MX480 and MX960 using the MX-SPC3 services card.

RELATED DOCUMENTATION

Application Identification Overview

prefer-framed-ip-address (RADIUS Clients)

IN THIS SECTION

- Syntax | 581
- Hierarchy Level | 581
- Description | 581
- Required Privilege Level | 581
- Release Information | 582

Syntax

```
prefer-framed-ip-address;
```

Hierarchy Level

```
[edit access radius clients client-name]
```

Description

Specify that the framed-ip-address is used for subscriber creation when both the framed-route and framed-ip-address attributes are in the RADIUS accounting request from the RADIUS client. The framed-ip-netmask is also used for subscriber creation if it is in the request.

By default, the framed-route attribute is used for subscriber creation when both the framed-route and framed-ip-address attributes are in the RADIUS accounting request.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | 128

prefer-framed-ipv6-prefix (RADIUS Clients)

IN THIS SECTION

- Syntax | 582
- Hierarchy Level | 582
- Description | 583
- Required Privilege Level | 583
- Release Information | 583

Syntax

```
prefer-framed-ipv6-prefix;
```

Hierarchy Level

```
[edit access radius clients client-name]
```

Description

Specify that the framed-ipv6-prefix is used for subscriber creation when both the delegated-ipv6-prefix and framed-ipv6-prefix attributes are in the RADIUS accounting request from the RADIUS client.

By default, the delegated-ipv6-prefix attribute is used for subscriber creation when both the delegated-ipv6-prefix and framed-ipv6-prefix attributes are in the RADIUS accounting request.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | 128

priority (Diameter Network Element)

IN THIS SECTION

- Syntax | 584
- Hierarchy Level | 584
- Description | 584
- Options | 584
- Required Privilege Level | 584
- Release Information | 584

Syntax

```
priority priority-value;
```

Hierarchy Level

```
[edit access diameter network-element element-name peer peer-name]
```

Description

Set the priority for a peer within a Diameter network element. A peer with a lower number has a higher priority. For load balancing, configure the peers with the same priority.

Options

priority-value Priority for the peer within the network element.

- **Range:** 1 through 65,535

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

priority (RADIUS Network Elements)

IN THIS SECTION

- Syntax | 585
- Hierarchy Level | 585
- Description | 585
- Options | 585
- Required Privilege Level | 586
- Release Information | 586

Syntax

```
priority priority;
```

Hierarchy Level

```
[edit access radius network-element name server name]
```

Description

Configure a priority for each RADIUS server in the network element. You can have multiple servers with the same priority in a network element. All access requests are load balanced among the highest priority servers. If all the servers with the highest priority in the network element fail, then requests are load balanced among servers with the next highest priority level.

Options

priority Relative priority for a RADIUS server.

- **Range:** 1 through 16.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring RADIUS Network Elements | 94
- Understanding Network Elements | 71
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

product-name

IN THIS SECTION

- Syntax | 586
- Hierarchy Level | 587
- Description | 587
- Options | 587
- Required Privilege Level | 587
- Release Information | 587

Syntax

```
product-name name;
```

Hierarchy Level

```
[edit access diameter]
```

Description

Configure the product name that is advertised in the Capabilities-Exchange-Request or Capabilities-Exchange-Answer message.

Options

name Name of product that is the advertised value of the Product-Name AVP.

- **Default:** Juniper Diameter Client

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

profile

IN THIS SECTION

Syntax | 588
Hierarchy Level | 588

- Description | 588
- Options | 588
- Required Privilege Level | 588
- Release Information | 588

Syntax

```
profile profile-name {
    rule-set rule-set-name;
}
```

Hierarchy Level

```
[edit services application-identification]
```

Description

Define members of the application profile, which consists of one or more rule sets.

Options

profile-name—Identifier for the application profile.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 9.5.

Support added in Junos OS release 19.3R2 and 19.4R1 for Next Gen Services on MX240, MX480, and MX960.

RELATED DOCUMENTATION

Configuring Application Profiles

profile (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 589
- Hierarchy Level | 589
- Description | 590
- Options | 590
- Required Privilege Level | 590
- Release Information | 590

Syntax

```
profile profile-name {
    tag rule rule-name;
}
```

Hierarchy Level

```
[edit services hcm]
```

Description

Configure an HCM profile, which points to one or more tag rules that Junos OS uses to enrich HTTP headers with the appropriate tags. You can configure a maximum of 100 HCM profiles.

For subscriber traffic under static policy control, a tag rule is used if it is included in the HCM profile specified in a PCC rule that the traffic matches. For subscribers under dynamic policy control, a message from the PCRF identifies the configured HCM profile and tag rules to use for HTTP header enrichment.

Options

profile-name	Name of the HCM profile.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

Configuring HCM Profiles and Assigning Tag Rules | 49

profile (LRF)

IN THIS SECTION

Syntax | 591

Hierarchy Level | 592

- Description | 592
- Options | 592
- Required Privilege Level | 592
- Release Information | 592

Syntax

```
profile profile-name {
    collector collector-name {
        destination {
            address collector-address;
            port collector-port-number;
        }
        source-address source-address;
    }
    http-log-multiple-transactions;
    policy-based-logging;
    rule lrf-rule-name {
        then {
            report {
                collector collector-name;
                template template-name;
                time-limit time-interval;
                volume-limit volume;
            }
        }
    }
    template template-name {
        format ipfix;
        template-tx-interval tx-time;
        template-type template-type;
        trigger-type (session-close | time | volume);
    }
    vendor-support ibm;
}
```

Hierarchy Level

```
[edit services lrf]
```

Description

Configure an LRF profile to specify a set of logging and reporting parameters, which includes data templates, collectors, and LRF rules.

For Junos OS Subscriber Aware, you can then assign an LRF profile to a subscriber by assigning the profile to the TDF service set associated with the subscriber's TDF domain.

For Junos OS Broadband Subscriber Management, you can then assign the LRF profile to the service set that is configured for application-aware policy control.

Options

profile-name — Name of the LRF profile.

- **Range:** Up to 63 characters.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

vendor-support option introduced in Junos OS Release 17.2.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Junos OS Subscriber Aware

Configuring Logging and Reporting for Subscriber Management

Logging and Reporting Function for Subscribers

profile (Services Application Identification)

IN THIS SECTION

- Syntax | **593**
- Hierarchy Level | **593**
- Description | **593**
- Options | **593**
- Required Privilege Level | **594**
- Release Information | **594**

Syntax

```
profile app-id-profile-name;
```

Hierarchy Level

```
[edit services application-identification]
```

Description

Configure an application identification profile. This profile is a placeholder profile with no configuration options, but it must be created to enable application identification functionality on the services plane.

Options

app-id-profile-name	Name of the application identification profile.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Applying Services to Subscriber-Aware Traffic with a Service Set | 146

profile (Services PCEF)

IN THIS SECTION

- Syntax | 594
- Hierarchy Level | 594
- Description | 595
- Options | 595
- Required Privilege Level | 595
- Release Information | 595

Syntax

```
profile pcef-profile-name;
```

Hierarchy Level

```
[edit services pcef]
```

Description

Configure a policy and charging enforcement function (PCEF) profile that is a placeholder profile with no configuration options. This profile must be created to enable PCEF functionality on the services plane. You apply this placeholder profile to the subscriber-aware service set.

Options

pcef-profile-name	Name of the PCEF profile.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Applying Services to Subscriber-Aware Traffic with a Service Set

Identifying the Service Interface That Handles Subscriber Management Application-Aware Policy Control

profiles (AAA)

IN THIS SECTION

- Syntax | 596
- Hierarchy Level | 596
- Description | 596
- Options | 597
- Required Privilege Level | 597

Release Information | 597

Syntax

```
profiles aaa-profile-name {
    radius {
        accounting {
            network-element network-element-name;
        }
        authentication {
            network-element network-element-name;
        }
        policy {
            activation-attribute {
                <code numeric-code;>
                <vendor-id vendor-id;>
            }
            deactivation-attribute {
                <code numeric-code;>
                <vendor-id vendor-id;>
            }
            coa-accounting (enable | disable);
        }
    }
}
```

Hierarchy Level

```
[edit unified-edge aaa]
```

Description

Configure a profile of the policy control attributes for RADIUS servers. This profile is used by the policy and charging enforcement function (PCEF) profile.

Options

aaa-profile-name	Name of the AAA profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring an AAA Profile | 96
- Understanding AAA Profiles | 73
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

profiles (PCEF)

IN THIS SECTION

- Syntax | 598
- Hierarchy Level | 598
- Description | 598
- Options | 599
- Required Privilege Level | 599
- Release Information | 599

Syntax

```
profiles profile-name {
    aaa-policy-control {
        aaa-profile aaa-profile-name;
        pcc-rulebases [rulebase-name <time-of-day-profile profile-name>];
        user-password password;
    }
    dynamic-policy-control {
        pcc-rules {
            [rule-name  precedence number <time-of-day-profile profile-name>];
        }
        pcc-rulebases {
            [rulebase-name <time-of-day-profile profile-name>];
        }
        diameter-profile gx-profile-name;
    }
    static-policy-control {
        pcc-rules {
            [rule-name precedence number <time-of-day-profile profile-name>];
        }
        pcc-rulebases {
            [rulebase-name <time-of-day-profile profile-name>];
        }
    }
```

Hierarchy Level

```
[edit unified-edge pcef],
[edit services pcef]
```

Description

Set up the overall policy and charging enforcement function (PCEF) configuration that can be applied to subscribers.

NOTE: You can configure only one of the following statements in a PCEF profile: **aaa-policy-control**, **static-policy-control**, or **dynamic-policy-control**.

You can configure a maximum of 32 policy and charging control (PCC) rules in a PCEF profile. There is no limit to the number of PCC rulebases you can configure in a PCEF profile.

If you are using Junos OS Subscriber Aware, configure the PCEF profile at the **[edit unified-edge pcef]** hierarchy level. You then assign this profile to the subscriber's TDF domain or to the domain selection configuration.

If you are using Junos OS Broadband Subscriber Management, configure the PCEF profile at the **[edit services pcef]** hierarchy level. The **static-policy-control** option is applicable to PCC rule activation through a dynamic profile, and you assign the PCEF profile to the dynamic profile. Starting in Junos OS Release 18.2R1, the **dynamic-policy-control** option is also available and is applicable to direct rule activation by a policy and charging rules function (PCRF) server; you assign the PCEF profile to the access profile. The **aaa-policy-control** option is not applicable to subscriber management.

Options

profile-name — Name of the PCEF profile.

- **Range:** 1 through 63 characters.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

RELATED DOCUMENTATION

- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Dynamic Policies
- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Static Policies
- Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Policies That a RADIUS Server Controls
- *Configuring a Policy and Charging Enforcement Function Profile for Subscriber Management*

protocol (Application Identification)

IN THIS SECTION

- Syntax | **600**
- Hierarchy Level | **601**
- Description | **601**
- Options | **601**
- Required Privilege Level | **601**
- Release Information | **601**

Syntax

```
protocol (http | ssl | tcp | udp);
```

Hierarchy Level

```
[edit services application-identification application application-name over
protocol-type signature l4-l7-signature-name]
```

Description

Identify the protocol bundles to be monitored to classify applications. This statement is not available if the MX Series router is running Next Gen Services.

Options

http	Use the HTTP protocol .
ssl	Use the SSL protocol.
tcp	Use the TCP protocol.
udp	Use the UDP protocol.

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

protocol (Flow Descriptions)

IN THIS SECTION

- Syntax | 602
- Hierarchy Level | 602
- Description | 602
- Default | 603
- Options | 603
- Required Privilege Level | 603
- Release Information | 603

Syntax

```
protocol number;
```

Hierarchy Level

```
[edit unified-edge pcef flow-description flow-identifier],
[edit services pcef flow-description flow-identifier]
```

Description

Specify a protocol type to identify the subscriber traffic that you want the service data flow (SDF) filter to detect. If you specify the **protocol** statement, you must specify a protocol number.

If you are using Junos OS Subscriber Aware, specify the protocol type at the **[edit unified-edge pcef flow-description *flow-identifier*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the protocol type at the **[edit services pcef flow-description *flow-identifier*]** hierarchy level.

Default

If you do not specify the **protocol** statement, the default is any protocol.

Options

number Number that specifies the IP protocol type.

- **Range:** 1 through 255

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef flow-description *flow-identifier*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

RELATED DOCUMENTATION

> *Configuring Service Data Flow Filters*
>
> Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment
>
> *Understanding Application-Aware Policy Control for Subscriber Management*

realm (Diameter Origin)

IN THIS SECTION

- Syntax | 604
- Hierarchy Level | 604
- Description | 604
- Options | 604
- Required Privilege Level | 604
- Release Information | 605

Syntax

```
realm realm-name;
```

Hierarchy Level

```
[edit access diameter origin]
```

Description

Specify the realm of the host that originates the Diameter message.

Options

realm-name Name of the message origin realm. Supplied as the value of Origin-Realm AVP for all messages sent by the Diameter instance.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- diameter (Subscriber Aware Policy Control) | 368

redirect (PCC Action Profiles)

IN THIS SECTION

- Syntax | 605
- Hierarchy Level | 605
- Description | 606
- Required Privilege Level | 606
- Release Information | 606

Syntax

```
redirect {
    url url-name;
}
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name],
[edit services pcef pcc-action-profiles profile-name]
```

Description

Specify HTTP redirection to a URL. If you configure this, the PCC action profile can only be used in PCC rules that match only HTTP-based applications and all flows.

If you are using Junos OS Subscriber Aware, specify the redirection at the **[edit unified-edge pcef pcc-action-profiles *profile-name*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the redirection at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware

Configuring Policy and Charging Control Action Profiles for Subscriber Management

regex (Class Attribute)

IN THIS SECTION

- Syntax | 607
- Hierarchy Level | 607
- Description | 607
- Options | 607
- Required Privilege Level | 608
- Release Information | 608

Syntax

```
regex "value";
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name subscription-id
use-class]
```

Description

Configure a regular expression to parse the Class attribute contents of the accounting request from the BNG, PGW, or GGSN.

Options

value Regular expression that parses the contents of the Class attribute.

For example, the following configuration generates **" 000118191129ALICE:DRAV3:"** out of **" 000118191129#000118191129#ALICE:DRAV3:#7168#nflat#ADSL##"**:

```
[edit unified-edge gateways tdf TDF1 domains domain1 subscription-id ]
user@host# set use-class regex "[^#]*#\([^#]*\)\#\([^#]*\)"
```

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | **121**

remote-address

IN THIS SECTION

- Syntax | **609**
- Hierarchy Level | **609**
- Description | **609**
- Options | **609**
- Required Privilege Level | **609**
- Release Information | **610**

Syntax

```
remote-address (ipv4-address ipv4-address | ipv6-address ipv6-address);
```

Hierarchy Level

```
[edit unified-edge pcef flow-descriptions flow-identifier],
[edit services pcef flow-descriptions flow-identifier]
```

Description

Specify a remote IP address for the service data flow (SDF) filter.

If you are using Junos OS Subscriber Aware, specify the remote IP address at the **[edit unified-edge pcef flow-descriptions *flow-identifier*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the remote IP address at the **[edit services pcef flow-descriptions *flow-identifier*]** hierarchy level.

Options

ipv4-address	IPv4 address.
ipv6-address	IPv6 address.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef flow-descriptions *flow-identifier*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

RELATED DOCUMENTATION

Configuring Service Data Flow Filters

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment

Understanding Application-Aware Policy Control for Subscriber Management

remote-port-range

IN THIS SECTION

- Syntax | **610**
- Hierarchy Level | **611**
- Description | **611**
- Default | **611**
- Options | **611**
- Required Privilege Level | **611**
- Release Information | **612**

Syntax

```
remote-port-range {
    low low-value;
    high high-value;
}
```

Hierarchy Level

```
[edit unified-edge pcef flow-descriptions flow-identifier],
[edit services pcef flow-descriptions flow-identifier]
```

Description

Specify the remote port range to identify the subscriber traffic that you want the service data flow (SDF) filter to detect.

If you are using Junos OS Subscriber Aware, specify the remote port range at the **[edit unified-edge pcef flow-descriptions *flow-identifier*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the remote port range at the **[edit services pcef flow-descriptions *flow-identifier*]** hierarchy level.

NOTE: You can specify either a remote port range or a list of remote ports, but not both.

Default

If you configure neither the **remote-port-range** nor the **remote-ports** statement, the default is any remote port.

Options

high-value — Upper boundary for the remote port range.

- **Range:** 1 through 65,535

low-value — Lower boundary for the remote port range.

- **Range:** 1 through 65,535

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef flow-descriptions *flow-identifier*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

RELATED DOCUMENTATION

Configuring Service Data Flow Filters

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment

Understanding Application-Aware Policy Control for Subscriber Management

remote-ports

IN THIS SECTION

- Syntax | **613**
- Hierarchy Level | **613**
- Description | **613**
- Default | **613**
- Options | **613**
- Required Privilege Level | **613**
- Release Information | **614**

Syntax

```
remote-ports [number];
```

Hierarchy Level

```
[edit unified-edge pcef flow-description flow-identifier],
[edit services pcef flow-description flow-identifier]
```

Description

Specify a remote port or list of remote ports to identify the subscriber traffic that you want the service data flow (SDF) filter to detect.

If you are using Junos OS Subscriber Aware, specify the remote ports at the **[edit unified-edge pcef flow-descriptions *flow-identifier*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the remote ports at the **[edit services pcef flow-descriptions *flow-identifier*]** hierarchy level.

NOTE: You can specify either a list of remote ports or a remote port range, but not both.

Default

If you configure neither the **remote-ports** nor the **remote-port-range** statement, the default is any remote port.

Options

number Port number or list of port numbers. You can specify a maximum of three port numbers in a list.

- **Range:** 1 through 65,535

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef flow-descriptions *flow-identifier*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

RELATED DOCUMENTATION

- *Configuring Service Data Flow Filters*
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment
- *Understanding Application-Aware Policy Control for Subscriber Management*

report (LRF Rule)

IN THIS SECTION

- Syntax | **615**
- Hierarchy Level | **615**
- Description | **615**
- Required Privilege Level | **615**
- Release Information | **615**

Syntax

```
report {
    collector collector-name;
    template template-name;
    time-limit time-interval;
    volume-limit volume;
}
```

Hierarchy Level

```
[edit services lrf profile profile-name rule lrf-rule-name then]
```

Description

Configure the actions to take if the LRF rule is matched.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Junos OS Subscriber Aware

Configuring Logging and Reporting for Subscriber Management

request-cache-timeout (RADIUS Snoop Segment)

IN THIS SECTION

- Syntax | 616
- Hierarchy Level | 616
- Description | 616
- Options | 616
- Required Privilege Level | 616
- Release Information | 617

Syntax

```
request-cache-timeout timeout;
```

Hierarchy Level

```
[edit access radius snoop-segments segment-name]
```

Description

Configure the length of time to cache the accounting request that was snooped. If the same request is received by the MX Series router within this time, the duplicate request is dropped.

Options

timeout Length of time, in seconds.

- **Range:** 1 through 30

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | 136
- Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | 114
- IP-Based Subscriber Setup Overview | 107

request-timeout

IN THIS SECTION

- Syntax | 617
- Hierarchy Level | 617
- Description | 618
- Options | 618
- Required Privilege Level | 618
- Release Information | 618

Syntax

```
request-timeout seconds;
```

Hierarchy Level

```
[edit unified-edge diameter-profiles gx-profile profile-name]
```

Description

Configure the time to wait for a response from the server.

Options

seconds Length of timeout interval.

- **Range:** 0 through 65,535 seconds.

> **NOTE**: 0 seconds indicates that the request timeout is not be enabled.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

gx-profile | 429

response-cache-timeout (RADIUS Client)

IN THIS SECTION

- Syntax | 619
- Hierarchy Level | 619
- Description | 619
- Options | 619

Required Privilege Level | 619
Release Information | 619

Syntax

```
response-cache-timeout seconds;
```

Hierarchy Level

```
[edit access radius clients client-name accounting]
```

Description

Configure the timeout for the RADIUS response cache. This timeout indicates how long to store the RADIUS response messages (sent for request messages) in the MX Series router response cache.

Options

seconds Length of timeout interval.

- **Range:** 5 through 20 seconds
- **Default:** 15 seconds

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | 128

retry (RADIUS Server)

IN THIS SECTION

- Syntax | 620
- Hierarchy Level | 620
- Description | 620
- Options | 621
- Required Privilege Level | 621
- Release Information | 621

Syntax

```
retry attempts;
```

Hierarchy Level

```
[edit access radius servers name]
```

Description

Configure a limit to the number of times the MX Series router can resend a request to the RADIUS server when no response from the RADIUS server is received. If the number of retries reaches this limit, the RADIUS server is marked as dead, and the MX Series router begins to send requests to other RADIUS servers in the network element.

Options

attempts Number of attempts allowed.

- **Range:** 1 through 10
- **Default:** 3

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Servers | 91

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

revert-interval (RADIUS Server)

IN THIS SECTION

- Syntax | 622
- Hierarchy Level | 622
- Description | 622
- Options | 622
- Required Privilege Level | 622
- Release Information | 622

Syntax

```
revert-interval seconds;
```

Hierarchy Level

```
[edit access radius servers name]
```

Description

Configure the amount of time that must pass after a RADIUS server is first marked dead until it is marked as alive by Junos OS. When Junos OS marks the RADIUS server as alive, it can again send requests to the RADIUS server.

Options

seconds Number of seconds after which a dead server is marked active.

- **Range:** 0 through 4,294,967,295
- **Default:** 300 seconds

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Servers | 91

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

routing-instance (PCC Action Profiles)

IN THIS SECTION

- Syntax | 623
- Hierarchy Level | 623
- Description | 623
- Options | 623
- Required Privilege Level | 624
- Release Information | 624

Syntax

```
routing-instance {
    downlink downlink-vrf-name;
    uplink uplink-vrf-name;
}
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name steering],
[edit services pcef pcc-action-profiles profile-name steering]
```

Description

Specify the routing instance that a PCC action profile uses for steering traffic.

Options

downlink *downlink-vrf-name* Use the specified name of the routing instance for downlink traffic (to the access side) or the predefined dynamic interface variable .

uplink ***uplink-vrf-name*** Use the specified name of the routing instance for uplink traffic (from the access side).

NOTE: The routing instances must have been previously configured.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

Support at the **[edit services pcef pcc-action-profiles** ***profile-name*** **steering]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

- Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware
- Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment
- *Configuring Policy and Charging Control Action Profiles for Subscriber Management*
- *Understanding Application-Aware Policy Control for Subscriber Management*

rule (HTTP Header Enrichment for Tag Rule Set)

IN THIS SECTION

- Syntax | 625
- Hierarchy Level | 625
- Description | 625
- Options | 625
- Required Privilege Level | 626
- Release Information | 626

Syntax

```
rule rule-name;
```

Hierarchy Level

```
[edit services hcm tag-rule-set]
```

Description

Specify the tag rule that you want to be a part of the tag rule set.

NOTE: The tag rule must already be defined at the **[edit services hcm]** hierarchy level.

Options

rule-name	Name of the tag rule.

To specify multiple tag rules, include the **rule** statement multiple times.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm (HTTP Header Enrichment) | 434

rule (LRF)

IN THIS SECTION

- Syntax | 626
- Hierarchy Level | 627
- Description | 627
- Options | 627
- Required Privilege Level | 627
- Release Information | 627

Syntax

```
rule lrf-rule-name {
    then {
        report {
            collector collector-name;
            template template-name;
            time-limit time-interval;
```

```
            volume-limit volume;
        }
    }
}
```

Hierarchy Level

```
[edit services lrf profile profile-name]
```

Description

Configure an LRF rule, which controls how data sessions are logged and reported. In this release, the matching conditions for an LRF rule are identified in a static PCC rule, not in the LRF rule.

Options

lrf-rule-name Name of the LRF rule.

- **Range:** Up to 63 characters.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

> *Configuring an LRF Profile for Subscribers*
>
> Configuring Logging and Reporting for Junos OS Subscriber Aware

rule-activation-time

IN THIS SECTION

- Syntax | 628
- Hierarchy Level | 628
- Description | 628
- Options | 629
- Required Privilege Level | 629
- Release Information | 629

Syntax

```
rule-activation-time {
    <day-of-week | day-of-month month>;
    <hour:min>;
}
```

Hierarchy Level

```
[edit unified-edge pcef pcc-time-of-day-profiles profile-name]
```

Description

Specify the time of day, day of the week or day of the month, or month of the year to activate a PCC rule or rulebase. You can specify the time of day, the day, or both. If you specify the day of the month, you can also specify the month of the year, which results in the yearly activation of the rule or rulebase. Use the same combination of options in the **rule-deactivation-time** statement. If a time zone is configured on the router, the time-of-day settings apply to the configured time zone.

If a day is not specified and the activation time of day setting is later than the deactivation time of day setting, then a rule is deactivated the day after it is activated.

Options

day-of-week	(Optional) Day of the week on which to activate a PCC rule or rulebase.
day-of-month	(Optional) Day of the month on which to activate a PCC rule or rulebase. • **Syntax: DAY*n***, where *n* can be from 1 through 31, or **Last-day-of-month**, which depends on the current month.
month	(Optional) Month of the year in which to activate a PCC rule or rulebase.
hour	(Optional) Hour at which to activate a PCC rule or rulebase as a two-digit number from 00 through 23.
min	(Optional) Minute at which to activate a PCC rule or rulebase as a two-digit number from 00 through 59.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Static Time-of-Day PCC Rule Activation and Deactivation in a Junos OS Subscriber Aware PCEF Profile | **103**

Understanding Static Time-of-Day PCC Rule Activation and Deactivation | **74**

rule-deactivation-time

IN THIS SECTION

- Syntax | 630
- Hierarchy Level | 630
- Description | 630
- Options | 631
- Required Privilege Level | 631
- Release Information | 631

Syntax

```
rule-deactivation-time {
    <day-of-week | day-of-month month>;
    <hour:min>;
}
```

Hierarchy Level

```
[edit unified-edge pcef pcc-time-of-day-profiles profile-name]
```

Description

Specify the time of day, day of the week or day of the month, or month of the year to deactivate a PCC rule or rulebase. You can specify the time of day, the day, or both. If you specify the day of the month, you can also specify the month of the year, which results in the yearly deactivation of the rule or rulebase. Use the same combination of options as in the **rule-activation-time** statement. If a time zone is configured on the router, the time-of-day settings apply to the configured time zone.

If a day is not specified and the deactivation time of day setting is earlier than the activation time of day setting, then a rule is deactivated the day after it is activated.

Options

day-of-week	(Optional) Day of the week on which to deactivate a PCC rule or rulebase.
day-of-month	(Optional) Day of the month on which to deactivate a PCC rule or rulebase. • **Syntax: DAY*n***, where *n* can be from 1 through 31, or **Last-day-of-month**, which depends on the current month.
month	(Optional) Month of the year in which to deactivate a PCC rule or rulebase.
hour	(Optional) Hour at which to deactivate a PCC rule or rulebase as a two-digit number from 00 through 23.
min	(Optional) Minute at which to deactivate a PCC rule or rulebase as a two-digit number from 00 through 59.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Static Time-of-Day PCC Rule Activation and Deactivation in a Junos OS Subscriber Aware PCEF Profile | **103**

Understanding Static Time-of-Day PCC Rule Activation and Deactivation | **74**

secret (RADIUS Client)

IN THIS SECTION

- Syntax | 632
- Hierarchy Level | 632
- Description | 632
- Options | 632
- Required Privilege Level | 632
- Release Information | 633

Syntax

```
secret password;
```

Hierarchy Level

```
[edit access radius clients client-name accounting]
```

Description

Specify a shared secret to be used by the MX Series router and the RADIUS client for accounting.

Options

password Shared secret to use ; it can include spaces if the character string is enclosed in quotation marks. Maximum length is 256 characters.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | 128

secret (RADIUS Server)

IN THIS SECTION

- Syntax | 633
- Hierarchy Level | 633
- Description | 633
- Options | 634
- Required Privilege Level | 634
- Release Information | 634

Syntax

```
secret password;
```

Hierarchy Level

```
[edit access radius servers name]
```

Description

Configure a shared secret to be used by the MX Series router and the RADIUS server.

Options

password Shared secret to use.

- **Range:** 1 through 64 characters

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Servers | 91

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

server (RADIUS Network Elements)

IN THIS SECTION

- Syntax | 635
- Hierarchy Level | 635
- Description | 635
- Options | 635
- Required Privilege Level | 635
- Release Information | 635

Syntax

```
server name {
    priority priority;
}
```

Hierarchy Level

```
[edit access radius network-element name]
```

Description

Configure a RADIUS server for the network element, which is a load-balanced group of RADIUS servers providing policy management for TDF subscribers. The RADIUS server must already be defined at the **[edit access radius]** hierarchy level. You can configure multiple RADIUS servers under a network element.

Options

name	Name of the RADIUS server.

The remaining statement is described separately.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Network Elements | 94

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

Configuring RADIUS Servers | 91

servers (RADIUS)

IN THIS SECTION

- Syntax | 636
- Hierarchy Level | 637
- Description | 637
- Options | 637
- Required Privilege Level | 637
- Release Information | 637

Syntax

```
servers name {
    accounting-port port-number;
    accounting-secret password;
    address server-address;
    allow-dynamic-requests;
    dead-criteria-retries retry-number interval seconds;
    dynamic-requests-secret password;
    port port-number;
    retry attempts;
    revert-interval seconds;
    secret password;
    source-interface interface [ipv4-address address];
    timeout seconds;
}
```

Hierarchy Level

```
[edit access radius]
```

Description

Configure a RADIUS server that provides policy management for TDF subscribers.

Options

name Name of the RADIUS server.

- **Range:** 1 through 32 characters

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Servers | 91

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

service-mode

IN THIS SECTION

- Syntax | 638
- Hierarchy Level | 638
- Description | 638
- Options | 639
- Required Privilege Level | 639
- Release Information | 639

Syntax

```
service-mode service-mode-options;
```

Hierarchy Level

```
[edit routing-instance vrf-name access address-assignment address-pools juniper-
pool],
[edit unified-edge gateways tdf gateway-name],
[edit unified-edge gateways tdf gateway-name domains domain-name],
[edit unified-edge tdf gateway-name system interface interface-name],
[unified-edge gateways tdf gateway-name system session-pics interface interface-
name]
```

Description

Set maintenance mode for a network element so that you can carry out maintenance tasks such as deleting or modifying the element, for example, an address pool.

When in the maintenance mode active phase, you can modify all the valid attributes on the network element. In other cases, you can modify only the non-maintenance mode attributes.

The following network elements must be in maintenance mode before you can modify or delete them:

- Address pools
- AMS interfaces
- PCEF profiles
- Session PICs
- Service PICs
- Static time-of-day settings
- TDF domains
- TDF interfaces
- TDF gateways

Options

service-mode-options Type of the service mode. Currently, only **maintenance** mode is supported.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Maintenance Mode Overview for Subscriber Aware Policy Enforcement | **200**

service-pics

IN THIS SECTION

- Syntax | 640
- Hierarchy Level | 640
- Description | 640
- Required Privilege Level | 640
- Release Information | 641

Syntax

```
service-pics {
    [interface interface-name];
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name system]
```

Description

Specify the service interfaces that represent the service PICs used for anchoring subscriber-aware services in the TDF Gateway.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Service PICs | 18

TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment | 9

service-set (Subscriber-Aware)

IN THIS SECTION

- Syntax | 641
- Hierarchy Level | 642
- Description | 642
- Options | 642
- Required Privilege Level | 642
- Release Information | 642

Syntax

```
service-set service-set-name {
    service-set-options {
        subscriber-awareness;
    }
    lrf-profile profile-name;
    pcef-profile pcef-profile-name;
    application-identification-profile app-id-profile-name;
    hcm profilehcm-profile--name;
    nat-rules rule-name;
    nat-rule-sets rule-set-name;
    disable-replication-capability;
    }
```

```
    interface-service {
        service-interface interface-name;
    }
}
```

Hierarchy Level

```
[edit services]
```

Description

Configure subscriber-aware services by creating a subscriber-aware service set to be applied to a TDF interface.

Options

service-set-name	Name of the service set.

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.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Applying Services to Subscriber-Aware Traffic with a Service Set | 146

Configuring Logging and Reporting for Junos OS Subscriber Aware | 186

service-set (TDF Interface)

IN THIS SECTION

- Syntax | 643
- Hierarchy Level | 643
- Description | 643
- Options | 643
- Required Privilege Level | 644
- Release Information | 644

Syntax

```
service-set service-set-name;
```

Hierarchy Level

```
[edit interfaces mif unit number family inet service input],
[edit interfaces mif unit number family inet service output]
```

Description

Apply the service set to the service input and output of the TDF interface (mif) that is part of a TDF domain.

The output service set for the mif is not used by the MX Series router, but it must be configured so that the configuration commit does not fail.

Options

service-set-name	Name of the service set that is being applied to the TDF interface.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Applying Services to Subscriber-Aware Traffic with a Service Set | 146

session-pics

IN THIS SECTION

- Syntax | 644
- Hierarchy Level | 645
- Description | 645
- Required Privilege Level | 645
- Release Information | 645

Syntax

```
session-pics {
    [interface interface-name];
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name system]
```

Description

Specify the service interfaces that represent the session PICs used for the control plane in the TDF gateway.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Session PICs | 19

TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment | 9

session-pics (Diameter)

IN THIS SECTION

- Syntax | 646
- Hierarchy Level | 646
- Description | 646
- Options | 646

Required Privilege Level | 647
Release Information | 647

Syntax

```
session-pics {
    group {
        group-name {
            [session-pic interface-name];
        }
    }
}
```

Hierarchy Level

```
[edit unified-edge tdf gateway-name diameter network-element element-name]
```

Description

Configure the session PICs that are serving this Diameter network element for Diameter bindings on this TDF gateway.

NOTE: If you want to set up Diameter bindings for session PICs on the TDF gateway, contact Juniper Networks Professional Services for assistance.

Options

group-name	Name of the session PIC group that is serving the Diameter network element.
interface-name	Name of interface representing session PIC.

- **Syntax:** The interface must be a valid multiservices interface (ams or ms-*a*/*b*/0, where *a* is the Flexible PIC Concentrator [FPC] slot number and *b* is the PIC slot number); for example, ams0, ams1, or ms-1/0/0.

  NOTE: The specified interface for the session PIC must already be configured for this TDF gateway.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (TDF Gateway) | 370

shared-secret (RADIUS Snoop Segment)

IN THIS SECTION

- Syntax | 648
- Hierarchy Level | 648
- Description | 648
- Options | 648
- Required Privilege Level | 648
- Release Information | 648

Syntax

```
shared-secret secret;
```

Hierarchy Level

```
[edit access radius snoop-segments segment-name]
```

Description

Configure a shared secret to be used by the MX Series router and the RADIUS client. If the shared secrets do not match, the subscriber session is not set up.

Options

secret Shared secret. The maximum length is 64 characters.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | **136**

Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | **114**

IP-Based Subscriber Setup Overview | **107**

snoop-segment (TDF Domain Selection)

IN THIS SECTION

- Syntax | 649
- Hierarchy Level | 649
- Description | 649
- Options | 649
- Required Privilege Level | 650
- Release Information | 650

Syntax

```
snoop-segment snoop-segment-name;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from]
```

Description

Specify the snoop segment that matches the RADIUS request.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

Options

snoop-segment-name	Name of the snoop segment.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | **130**
- Understanding Selection of Properties for an IP-Based TDF Subscriber | **110**
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | **112**
- IP-Based Subscriber Setup Overview | **107**
- Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | **136**

snoop-segments (RADIUS)

IN THIS SECTION

- Syntax | **651**
- Hierarchy Level | **651**
- Description | **651**
- Options | **651**
- Required Privilege Level | **651**
- Release Information | **651**

Syntax

```
snoop-segments snoop-segment-name {
    destination-ip-address destination-address;
    <destination-port destination-port;>
    <request-cache-timeout timeout;>
    shared-secret secret;
    source-interface source-interface;
    <source-ip-address source-address;>
}
```

Hierarchy Level

```
[edit access radius]
```

Description

Specify which accounting messages to snoop. You must specify at least the destination IP address for the accounting messages, the shared secret, and the source interface.

Options

snoop-segment-name Name for the snoop segment. The maximum length is 32 characters.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | 136

Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | 114

IP-Based Subscriber Setup Overview | 107

snoop-segments (TDF Gateway)

IN THIS SECTION

- Syntax | 652
- Hierarchy Level | 652
- Description | 652
- Options | 653
- Required Privilege Level | 653
- Release Information | 653

Syntax

```
snoop-segments [snoop-segment-name];
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name aaa]
```

Description

Specify one or more snoop segments that control RADIUS accounting request snooping for the TDF gateway. The snoop segments must already be configured at the **[edit access radius]** hierarchy level.

Options

snoop-segment-name	Name of a snoop segment.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | 136
- Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | 114
- IP-Based Subscriber Setup Overview | 107

source (Application Identification)

IN THIS SECTION

- Syntax | 654
- Hierarchy Level | 654
- Description | 654
- Options | 654
- Required Privilege Level | 654
- Release Information | 654

Syntax

```
source ip ip-address-prefix;
```

Hierarchy Level

```
[edit services application-identification application application-name address-
mapping]
```

Description

Specify the source IP address for address mapping-based application identification.

Options

ip-address-prefix	IP address and prefix for matching.

Required Privilege Level

view-level—To view this statement in the configuration.

control-level—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- *Application Identification Overview*
- *Configuring Custom Application Signatures*
- *Application Identification Overview*

source-address (LRF Profile)

IN THIS SECTION

- Syntax | 655
- Hierarchy Level | 655
- Description | 655
- Options | 655
- Required Privilege Level | 655
- Release Information | 656

Syntax

```
source-address source-address;
```

Hierarchy Level

```
[edit services lrf profile profile-name collector collector-name]
```

Description

Configure the source address to be used when exporting data to the collector.

Options

source-address IP address to be used as the source address.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Junos OS Subscriber Aware

Configuring Logging and Reporting for Subscriber Management

source-interface

IN THIS SECTION

- Syntax | **656**
- Hierarchy Level | **656**
- Description | **657**
- Options | **657**
- Required Privilege Level | **657**
- Release Information | **657**

Syntax

```
source-interface interface ipv4-address address;
```

Hierarchy Level

```
[edit access radius clients client-name]
```

Description

Configure the MX Series router interface and IPv4 address that receive RADIUS requests from the GGSN, PGW, or BNG RADIUS client.

Options

interface	Name of the interface.
address	IPv4 address on the MX Series router.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Clients That Send Accounting Requests for IP-Based Subscribers | 128

source-interface (RADIUS Server)

IN THIS SECTION

- Syntax | 658
- Hierarchy Level | 658
- Description | 658
- Options | 658
- Required Privilege Level | 658
- Release Information | 658

Syntax

```
source-interface interface [ipv4-address address];
```

Hierarchy Level

```
[edit access radius servers name]
```

Description

Specify the source interface and one or more IPv4 addresses on the MX Series router that receive RADIUS requests from which the RADIUS requests are sent to the RADIUS server.

Options

interface Source interface that sends the RADIUS requests.

address Source IPv4 address that sends the RADIUS requests. You can specify multiple source IPv4 addresses.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Servers | 91

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

source-interface (RADIUS Snoop Segment)

IN THIS SECTION

- Syntax | 659
- Hierarchy Level | 659
- Description | 659
- Options | 659
- Required Privilege Level | 659
- Release Information | 660

Syntax

```
source-interface source-interface;
```

Hierarchy Level

```
[edit access radius snoop-segments segment-name]
```

Description

Specify the interface of the MX Series router that receives accounting packets from the access network to be snooped.

Options

source-interface	Name of the interface.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | 136

Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | 114

IP-Based Subscriber Setup Overview | 107

source-ip-address (RADIUS Snoop Segment)

IN THIS SECTION

- Syntax | 660
- Hierarchy Level | 660
- Description | 661
- Options | 661
- Required Privilege Level | 661
- Release Information | 661

Syntax

```
source-ip-address source-address;
```

Hierarchy Level

```
[edit access radius snoop-segments segment-name]
```

Description

Specify the source IP address of accounting requests from a GGSN, PGW, or BNG to snoop. If you do not enter a source IP address, accounting requests from any IP address can be snooped.

Options

source-address	Source IPv4 address.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | **136**
- Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | **114**
- IP-Based Subscriber Setup Overview | **107**

static-policy-control

IN THIS SECTION

- Syntax | **662**
- Hierarchy Level | **662**
- Description | **662**
- Required Privilege Level | **662**
- Release Information | **663**

Syntax

```
static-policy-control {
    pcc-rules {
        [rule-name precedence number <time-of-day-profile profile-name>];
    }
    pcc-rulebases {
        [rulebase-name <time-of-day-profile profile-name>];
    }
}
```

Hierarchy Level

```
[edit unified-edge pcef profiles profile-name],
[edit services pcef profiles profile-name]
```

Description

Configure static policy control for the policy and charging control (PCC) rules or PCC rulebase in a policy and charging enforcement function (PCEF) profile. You can configure a maximum of 32 PCC rules in a PCEF profile. There is no limit to the number of PCC rulebases you can configure in a PCEF profile.

NOTE: For Junos OS Subscriber Aware, you can configure only one of the following statements in a PCEF profile: **aaa-policy-control**, **static-policy-control**, or **dynamic-policy-control**. For Junos OS Subscriber Management, you can configure only **static-policy-control**.

If you are using Junos OS Subscriber Aware, configure static policy control at the **[edit unified-edge pcef profiles *profile-name*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, configure static policy control at the **[edit services pcef profiles *profile-name*]** hierarchy level.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef profiles *profile-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

RELATED DOCUMENTATION

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Static Policies

Configuring a Policy and Charging Enforcement Function Profile for Subscriber Management

steering

IN THIS SECTION

- Syntax | **664**
- Hierarchy Level | **664**
- Description | **664**
- Required Privilege Level | **664**
- Release Information | **665**

Syntax

```
steering {
    keep-existing-steering;
    path {
        ipv4-address ipv4-address;
        ipv6-address ipv6-address;
    }
    routing-instance {
        downlink downlink-vrf-name;
        uplink uplink-vrf-name;
    }
}
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name],
[edit services pcef pcc-action-profiles profile-name]
```

Description

Specify the method that a PCC action profile uses for steering traffic

If you are using Junos OS Subscriber Aware, configure steering at the **[edit unified-edge pcef pcc-action-profiles *profile-name*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, configure the PCC action profile at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-action-profiles *profile-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

Understanding Application-Aware Policy Control for Subscriber Management

Configuring Policy and Charging Control Action Profiles for Subscriber Management

Understanding Predefined Policy and Charging Control Rules for Subscriber-Aware Traffic Treatment

Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware

string

IN THIS SECTION

- Syntax | **666**
- Hierarchy Level | **666**
- Description | **666**
- Required Privilege Level | **666**
- Release Information | **666**

Syntax

```
string {
    equals;
    has-prefix;
    has-suffix;
    matches;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format]
```

Description

Specify the custom AVP attribute's format as a string and the value to match for the incoming RADIUS request from the IP-based subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130

Understanding Selection of Properties for an IP-Based TDF Subscriber | 110

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112

IP-Based Subscriber Setup Overview | 107

subscriber-address

IN THIS SECTION

- Syntax | 667
- Hierarchy Level | 667
- Description | 667
- Required Privilege Level | 668
- Release Information | 668

Syntax

```
subscriber-address {
    inet {
        pool pool-name;
    }
    inet6 {
        pool pool-name;
    }
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber]
```

Description

Specify the address pool that contains the source IP addresses for IP-based subscriber packets that can undergo TDF processing.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based Subscriber Setup Overview | 107

subscriber-awareness (Service Set Options)

IN THIS SECTION

- Syntax | 668
- Hierarchy Level | 669
- Description | 669
- Default | 669
- Required Privilege Level | 669
- Release Information | 669

Syntax

```
subscriber-awareness;
```

Hierarchy Level

```
[edit services service-set service-set-name service-set-options]
```

Description

Enable subscriber awareness on the service set.

Default

If you do not include the **subscriber-awareness** statement, then subscriber-aware services cannot be provided.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Applying Services to Subscriber-Aware Traffic with a Service Set | 146

subscriber-aware-services

IN THIS SECTION

- Syntax | 670
- Hierarchy Level | 670
- Description | 670

- Required Privilege Level | 670
- Release Information | 670

Syntax

```
subscriber-aware-services;
```

Hierarchy Level

```
[edit chassis fpc name pic name]
```

Description

Enable subscriber-aware services.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS 20.2R1 for Next Gen Services on MX240, MX480 and MX960.

subscriber-exclude-prefix

IN THIS SECTION

- Syntax | 671
- Hierarchy Level | 671

- Description | 671
- Required Privilege Level | 672
- Release Information | 672

Syntax

```
subscriber-exclude-prefix {
    apply-groups [group-names];
    apply-groups-except [group-names];
    family {
        inet {
            apply-groups [group-names];
            apply-groups-except [group-names];
            network address net-mask;
        }
        inet6 {
            apply-groups [group-names];
            apply-groups-except [group-names];
            network address net-mask;
        }
    }
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
```

Description

Specify the network prefix of source IP addresses for uplink packets and destination IP addresses for downlink packets that do not undergo TDF processing.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | 140
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based and IFL-Based TDF Subscribers Overview | 107
- IP-Based Subscriber Setup Overview | 107

subscriber-type (TDF Domain)

IN THIS SECTION

- Syntax | 672
- Hierarchy Level | 673
- Description | 673
- Options | 673
- Required Privilege Level | 673
- Release Information | 673

Syntax

```
subscriber-type (ip | ifl);
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
```

Description

Configure the type of subscriber that this domain is applied to — an IP-based subscriber or an IFL-based (interface-based) subscriber. If you do not include this statement, **subscriber-type ip** is used.

Options

ip (Default) Apply the TDF domain to IP-based subscribers, for which a RADIUS accounting request is sent to the MX Series router. An individual subscriber session is created for each unique source IP address.

ifl Apply the TDF domain to IFL-based subscribers, which are defined by a set of interfaces. One subscriber session is created for all traffic that is received on those interfaces.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | **121**

Configuring IFL-Based TDF Subscribers and Properties with a TDF Domain | **140**

Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | **108**

Understanding the Definition of a Set of IFL-Based Subscriber Properties with a TDF Domain | **116**

subscription-id

IN THIS SECTION

- Syntax | 674
- Hierarchy Level | 675
- Description | 675
- Required Privilege Level | 675
- Release Information | 675

Syntax

```
subscription-id {
    constant value;
    subscription-id-options {
        entry-name {
            id-components {
                use-class;
                use-imsi;
                use-msisdn;
                use-nai;
                use-nas-port;
                use-nas-port-id;
                use-realm;
                use-username;
            }
        }
    }
    use-class {
        regex "value";
        pattern "pattern";
        subscription-id-type (imsi | msisdn | nai | private | sip-uri);
    }
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber]
```

Description

Specify how the Subscription-Id is constructed for the Diameter credit control request (CCR) message that is sent from the TDF to the PCRF for IP-based subscribers belonging to the TDF domain.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based Subscriber Setup Overview | 107

subscription-id-options

IN THIS SECTION

- Syntax | 676
- Hierarchy Level | 676
- Description | 676

- Options | 677
- Required Privilege Level | 677
- Release Information | 677

Syntax

```
subscription-id-options {
    [entry-name] {
        id-components {
            use-class;
            use-imsi;
            use-msisdn;
            use-nai;
            use-nas-port;
            use-nas-port-id;
            use-realm;
            use-username;
        }
    }
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name ip-subscriber
subscription-id]
```

Description

Specify a method for constructing the Subscription-Id for the RADIUS credit control request (CCR) message that is sent from the TDF to the PCRF for IP-based subscribers belonging to the TDF domain. To specify multiple methods, include the *entry-name* option multiple times.

Options

entry-name Identifier for the Subscription-Id construction method.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | 108
- IP-Based Subscriber Setup Overview | 107

subscription-id-type (Class Attribute)

IN THIS SECTION

- Syntax | 678
- Hierarchy Level | 678
- Description | 678
- Options | 678
- Required Privilege Level | 678
- Release Information | 678

Syntax

```
subscription-id-type (imsi | msisdn | nai | private | sip-uri);
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name subscription-id
use-class]
```

Description

Configure the subscription ID type when the Class attribute is used for the subscription ID.

Options

imsi Use the IMSI subscriber type.

msisdn Use the MSISDN (E164) subscriber type.

nai Use the NAI subscriber type.

private Use the Private subscriber type.

sip-uri Use the SIP URI name subscriber type.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

tag (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 679
- Hierarchy Level | 679
- Description | 680
- Options | 680
- Required Privilege Level | 680
- Release Information | 680

Syntax

```
tag tag-name {
    encrypt {
        hash algorithm;
        prefix hash-prefix;
    }
    ipv4-mask ipv4-mask;
    ipv6-mask ipv6-mask;
    ipv4-or-value ipv4-or-value;
    ipv6-or-value ipv6-or-value;
    tag-attribute tag-attr-name;
    tag-header header;
    tag-separator separator;
}
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number then]
```

Description

Configure the tags to be applied to the HTTP headers. If you configure a tag, you must include the **tag-header** statement.

Options

tag-name	Name of the tag.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Configuring HCM Profiles and Assigning Tag Rules | 49
- Junos Web Aware HTTP Header Enrichment Overview | 34

tag-attribute (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 681
- Hierarchy Level | 681
- Description | 681

Options | 681
Required Privilege Level | 681
Release Information | 682

Syntax

```
tag-attribute [tag-attr-name];
```

Hierarchy Level

```
[edit services hcm]
```

Description

Specify one or more tag attributes that can be used in tag rules for HTTP header enrichment.

These attributes are stored in the subscriber database for subscribers. After these attributes are configured, they can be used in the tag rules. HTTP tag rules can be configured to choose one or more of these attributes to insert in the HTTP header.

Options

tag-attr-name—Tag attribute. To specify multiple attributes at one time, include the attributes in square brackets ([]). The supported attributes are **apn**, **ggsnipv4**, **ggsnipv6**, **imei**, **imsi**, **ipv4addr**, **ipv6addr**, and **msisdn**.

- **Range:** 1 through 63 alphanumeric characters

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Junos Web Aware HTTP Header Enrichment Overview | 34

tag-attribute (HTTP Header Enrichment Tag Rule)

IN THIS SECTION

- Syntax | 682
- Hierarchy Level | 682
- Description | 683
- Options | 683
- Required Privilege Level | 683
- Release Information | 683

Syntax

```
tag-attribute [tag-attr-name];
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name]
```

Description

Specify one or more tag attributes (for the tag header and separator) to insert into the HTTP header.

> **NOTE**: The tag attribute specified here must already be defined at the **[edit services hcm]** hierarchy level.

Options

tag-attr-name—Tag attribute. To specify multiple attributes at one time, include the attributes in square brackets ([]). The supported attributes are **apn**, **ggsnipv4**, **ggsnipv6**, **imei**, **imsi**, **ipv4addr**, **ipv6addr**, and **msisdn**.

- **Range:** 1 through 63 alphanumeric characters

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

Configuring Tag Rules | 42

tag-header (HTTP Header Enrichment)

IN THIS SECTION

Syntax | 684

- Hierarchy Level | 684
- Description | 684
- Options | 684
- Required Privilege Level | 684
- Release Information | 685

Syntax

```
tag-header header;
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name]
```

Description

Specify the tag header for the tag to be inserted into the HTTP header. This is a required configuration.

You can configure a total of 16 unique tag headers for all the tag rules you configure.

Options

header—Tag header.

- **Values:** You *cannot* use the following values: **accept**, **accept-charset**, **accept-encoding**, **accept-language**, **authorization**, **expect**, **host**, **if-match**, **if-modified-since**, **if-none-match**, **if-range**, **if-unmodified-since**, **max-forwards**, **proxy-authorization**, **referer**, **user-agent**, or **x-moz**. These header values are reserved; you cannot configure them.
- **Range:** 1 through 63 alphanumeric characters

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Configuring HCM Profiles and Assigning Tag Rules | 49
- Junos Web Aware HTTP Header Enrichment Overview | 34

tag-operation (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 685
- Hierarchy Level | 685
- Description | 686
- Options | 686
- Required Privilege Level | 686
- Release Information | 686

Syntax

```
tag-operation (add | delete | modify);
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-name then tag tag-name]
```

Description

Specify the operation to be performed on the specified tag of the tag rule set.

NOTE: The tag rule must already be defined at the **[edit services hcm]** hierarchy level.

Options

add Add the specified tag with previously existing tag in the tag rule set.

delete Delete the specified tag from the tag rule set.

modify Modify the existing tag in the tag rule set.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm (HTTP Header Enrichment) | 434

tag-rule (Profiles for HTTP Header Enrichment)

IN THIS SECTION

Syntax | 687

- Hierarchy Level | 687
- Description | 687
- Options | 687
- Required Privilege Level | 687
- Release Information | 688

Syntax

```
tag-rule rule-name;
```

Hierarchy Level

```
[edit services hcm profile profile-name]
```

Description

Specify the tag rule to be associated with the HCM profile.

NOTE: The tag rule specified here must already be defined at the **[edit services hcm]** hierarchy level.

Options

rule-name Name of the tag rule.

- **Range:** 1 through 63 alphanumeric characters

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

Configuring HCM Profiles and Assigning Tag Rules | 49

tag-rule (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 688
- Hierarchy Level | 689
- Description | 689
- Options | 690
- Required Privilege Level | 690
- Release Information | 690

Syntax

```
tag-rule rule-name {
    term term-number {
        from {
            destination-address {
                (any-ipv4 | any-ipv4 except);
                (any-ipv6 | any-ipv6 except);
                (any-unicast | any-unicast except);
                (prefix | prefix except);
            }
            destination-address-range {
                high address low address <except>;
            }
```

```
            destination-port-range {
                high port-number low port-number;
            }
            destination-ports value;
            destination-prefix-list {
                (prefix-name | prefix-name except);
            }
        }
        then {
            count;
            tag tag-name {
                encrypt {
                    hash algorithm;
                    prefix hash-prefix;
                }
                ipv4-mask ipv4-mask;
                ipv6-mask ipv6-mask;
                ipv4-or-value ipv4-or-value;
                ipv6-or-value ipv6-or-value;
                tag-attribute tag-attr-name;
                tag-header header;
                tag-separator separator;
            }
        }
    }
}
```

Hierarchy Level

```
[edit services hcm]
```

Description

Configure the tag rules that enrich HTTP headers with the appropriate tags.

You must configure at least one term for a tag rule, but you can configure multiple terms. Terms are evaluated in the order they are configured. If a data packet matches all the criteria in the **from** statement in any of the terms, then the actions specified in the **then** statement are applied. If the **from** statement does not identify any criteria, then all traffic matches. After a term matches a data packet, further terms are not evaluated. If no terms match, then the HTTP header is not enriched.

For subscriber traffic under static policy control, a tag rule is used if it is included in the HCM profile specified in a PCC rule that the traffic matches. For subscribers under dynamic policy control, a message from the PCRF identifies the configured HCM profile and tag rules to use for HTTP header enrichment.

Options

rule-name—Name of the tag rule.

- **Range:** 1 through 63 alphanumeric characters

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

Configuring Tag Rules | 42

Configuring HCM Profiles and Assigning Tag Rules | 49

Junos Web Aware HTTP Header Enrichment Overview | 34

tag-rules (Service Set)

IN THIS SECTION

- Syntax | 691
- Hierarchy Level | 691
- Description | 691

Options | 691
Required Privilege Level | 691
Release Information | 691

Syntax

```
[tag-rules rule-name;]
```

Hierarchy Level

```
[edit services service-set service-set-name]
```

Description

Specify one or more HTTP header enrichment tag rules to include in the service set. You can configure multiple tag rules. If you specify any tag rules, you cannot specify a tag rule set.

Options

rule-name Name of the tag rule.

- **Range:** 1 through 63 alphanumeric characters

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Applying Services to Subscriber-Aware Traffic with a Service Set | 146

Configuring HTTP Header Enrichment Overview | 41

tag-rule-set (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 692
- Hierarchy Level | 692
- Description | 692
- Options | 693
- Required Privilege Level | 693
- Release Information | 693

Syntax

```
tag-rule-set rule-set-name {
    [rule rule-name];
}
```

Hierarchy Level

```
[edit services hcm]
```

Description

Configure the tag rule set for HTTP header enrichment so that you can group multiple configured tag rules into one tag rule set.

Options

rule-set-name	Name of the tag rule set.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm (HTTP Header Enrichment) | 434

tag-rule-sets (Service Set)

IN THIS SECTION

- Syntax | 694
- Hierarchy Level | 694
- Description | 694
- Options | 694
- Required Privilege Level | 694
- Release Information | 694

Syntax

```
tag-rule-sets rule-set-name;
```

Hierarchy Level

```
[edit services service-set service-set-name]
```

Description

Specify the HTTP header enrichment tag rule set included in the service set. You can configure only one tag rule set. If you specify a tag rule set, you cannot specify a tag rule.

Options

rule-set-name	Name of the tag rule set.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Applying Services to Subscriber-Aware Traffic with a Service Set | 146

Configuring HTTP Header Enrichment Overview | 41

tag-separator (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 695
- Hierarchy Level | 695
- Description | 695
- Options | 695
- Required Privilege Level | 695
- Release Information | 696

Syntax

```
tag-separator separator;
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number then tag tag-name]
```

Description

Specify the tag separator for the tag to be inserted into the HTTP header.

Options

separator Tag separator. You may use a forward slash (/) or pipe (|).

- **Default:** / (forward slash)

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Configuring HCM Profiles and Assigning Tag Rules | 49
- Junos Web Aware HTTP Header Enrichment Overview | 34

tag-value (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 696
- Hierarchy Level | 696
- Description | 697
- Options | 697
- Required Privilege Level | 697
- Release Information | 697

Syntax

```
tag-value value;
```

Hierarchy Level

```
[edit services hcm tag-rule then tag]
```

Description

Specify the tag value for the specified tag name.

NOTE: The tag rule must already be defined at the **[edit services hcm]** hierarchy level.

Options

value String of up to 16 alphanumeric characters

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring HTTP Header Enrichment Overview | 41

hcm (HTTP Header Enrichment) | 434

tags (Application Identification)

IN THIS SECTION

- Syntax | 698
- Hierarchy Level | 698
- Description | 698
- Options | 698

Required Privilege Level | 698
Release Information | 698

Syntax

```
tags tag-name tag-value;
```

Hierarchy Level

```
[edit services application-identification application application-name]
```

Description

Specify an application tag that provides general information about the application, such as associated risk factors, technology, and the type of traffic. The tag consists of a user-defined name and value.

Options

tag-name	Name for the tag, which is a textual string.
tag-value	Value for the tag.

Required Privilege Level

view-level—To view this statement in the configuration.

control-level—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- *Application Identification Overview*
- *Configuring Custom Application Signatures*
- *Application Identification Overview*
- *Application Identification Overview*

targets

IN THIS SECTION

- Syntax | 699
- Hierarchy Level | 699
- Description | 700
- Options | 700
- Required Privilege Level | 700
- Release Information | 700

Syntax

```
targets {
    target-name {
        <destination-host hostname>;
        destination-realm realm-name;
        network-element element-name;
        priority priority-value;
    }
}
```

Hierarchy Level

```
[edit unified-edge diameter-profiles gx-profile profile-name]
```

Description

Configure the targets for this Diameter profile.

Options

target-name Name of the target.

destination-host ***hostname*** (Optional) Use the name of the destination host associated with this target.

destination-realm ***realm-name*** Use the name of the destination realm associated with this target.

network-element ***element-name*** Use the name of the network element.

> **NOTE**: The Diameter network element must be previously configured at the **[edit access diameter network-element]** hierarchy level.

- **Range:** 1 through 32 characters

priority ***priority-value*** Use the specified priority for the target within the Diameter profile. A value with a lower number has a higher priority. For load balancing, configure the targets with the same priority.

> **NOTE**: Failover handling depends on how the policy for the application is configured. For example, switching between the primary and secondary online charging servers set with the appropriate priority can occur only when the failover handling policy is configured to do so.

- **Range:** 1 through 65,535

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

gx-profile | 429

tdf (Unified Edge)

IN THIS SECTION

- Syntax | 701
- Hierarchy Level | 701
- Description | 701
- Options | 701
- Required Privilege Level | 702
- Release Information | 702

Syntax

```
tdf gateway-name;
```

Hierarchy Level

```
[edit unified-edge gateways]
```

Description

Specify the name to be used for the traffic detection function (TDF) gateway.

Options

gateway-name Name of the gateway.

- **Range:** 1 through 16 characters.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

TDF Gateway Service PICs and Session PICs for Subscriber-Aware Traffic Treatment | 9

tdf-interface

IN THIS SECTION

- Syntax | 702
- Hierarchy Level | 702
- Description | 703
- Options | 703
- Required Privilege Level | 703
- Release Information | 703

Syntax

```
tdf-interface mif.number;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name]
```

Description

Specify the TDF interface that the TDF domain uses. A TDF interface is different from other types of interfaces, and is associated with the TDF service set that is used for the TDF subscriber.

NOTE: The TDF interface must have been previously configured at the **[edit interfaces]** hierarchy level.

The TDF interface and the access-facing interfaces in the TDF domain must be included in the same VRF routing instance.

Options

mif.*number*	Use the specified TDF interface unit number.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | **121**
- Understanding the Definition of a Set of IP-Based Subscriber Properties with a TDF Domain | **108**
- IP-Based Subscriber Setup Overview | **107**
- Configuring TDF Interface to Access Interface Associations in VRFs | **144**
- Configuring TDF Interface to Access Interface Associations in VRFs | **144**
- Configuring a TDF Logical Interface | **143**

template (LRF Profile)

IN THIS SECTION

- Syntax | 704
- Hierarchy Level | 704
- Description | 704
- Options | 704
- Required Privilege Level | 705
- Release Information | 705

Syntax

```
template template-name {
    format ipfix;
    template-tx-interval tx-time;
    template-type template-type;
    trigger-type (session-close | volume);
}
```

Hierarchy Level

```
[edit services lrf profile profile-name]
```

Description

Configure a template, which specifies a set of data to be transmitted. This template can be specified in LRF rules.

Options

template-name	Name for the template.

- **Range:** Up to 32 characters.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Junos OS Subscriber Aware

Configuring Logging and Reporting for Subscriber Management

template (LRF Rule)

IN THIS SECTION

- Syntax | **706**
- Hierarchy Level | **706**
- Description | **706**
- Options | **706**
- Required Privilege Level | **706**
- Release Information | **706**

Syntax

```
template template-name;
```

Hierarchy Level

```
[edit services lrf profile profile-name rule lrf-rule-name then report]
```

Description

Specify the template that identifies the type of data to report if the LRF rule is matched.

Options

template-name Name of the template that is used. The referenced template must be configured.

- **Range:** Up to 32 characters.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Junos OS Subscriber Aware

Configuring Logging and Reporting for Subscriber Management

template-tx-interval (LRF Profile)

IN THIS SECTION

- Syntax | 707
- Hierarchy Level | 707
- Description | 707
- Options | 707
- Required Privilege Level | 708
- Release Information | 708

Syntax

```
template-tx-interval tx-time;
```

Hierarchy Level

```
[edit services lrf profile profile-name template template-name]
```

Description

Configure the interval at which to retransmit the template to the collector.

Options

tx-time Time interval in seconds.

- **Default:** 60
- **Range:** 10 through 600

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

- *Configuring an LRF Profile for Subscribers*
- Configuring Logging and Reporting for Junos OS Subscriber Aware
- *Configuring Logging and Reporting for Subscriber Management*

template-type (LRF Profile)

IN THIS SECTION

- Syntax | **708**
- Hierarchy Level | **709**
- Description | **709**
- Options | **709**
- Required Privilege Level | **710**
- Release Information | **710**

Syntax

```
template-type template-type;
```

Hierarchy Level

```
[edit services lrf profile profile-name template template-name]
```

Description

Configure the template types for the template, which specify the data fields to include. You must configure at least one type, and you can configure multiple types.

If Next Gen Services is enabled, then the template types **dns**, **ifl-subscriber**, **ipv4-extended**, **ipv6-extended**, **mobile-subscriber**, **video**, and **wireline-subscriber** are not available.

Options

template-type Template type. You must configure at least one of the following types, and you can configure multiple types:

- **device-data**—Use data fields specific to the device collecting the logging feed.
- **dns**—(Not available if Next Gen Services is enabled) Use the DNS response time data field.
- **flow-id**—Use the Flow ID data field.
- **http**—Use data fields for the HTTP metadata from header fields.
- **ifl-subscriber**—(Not available if Next Gen Services is enabled) Use data fields specific to interface-based subscribers.
- **ipflow**—Use data fields for the uplink and downlink octets and bytes.
- **ipflow-extended**—Use data fields for the service set name, routing instance, and payload timestamps.
- **ipflow-tcp**—Use data fields for TCP-related timestamps.
- **ipflow-tcp-ts**—Use IBM-specific data fields for TCP-related timestamps.When configuring a **ipflow-tcp-ts** template, configure **vendor-support ibm** at the **[edit services lrf profile *profile-name*]** hierarchy level to avoid a commit warning.
- **ipflow-ts**—Use data fields for the flow start and end timestamps.
- **ipv4**—Use data fields for the basic source and destination IPv4 information.

- **ipv4-extended**—(Not available if Next Gen Services is enabled) Use data fields for the elements of IPv4 extended fields.
- **ipv6**—Use data fields for the basic source and destination IPv6 information.
- **ipv6-extended**—(Not available if Next Gen Services is enabled) Use data fields for the elements of IPv6 extended fields.
- **l7-app**—Use data fields for the Layer 7 application.
- **mobile-subscriber**—(Not available if Next Gen Services is enabled) Use data fields specific to mobile subscribers.
- **pcc**—Use the PCC rule name data field.
- **status-code-dist**—Use data fields for the HTTP or DNS status codes.
- **subscriber-data**—Use data fields for Generic Subscriber information that can be included with wireless (mobile) subscribers or wireline subscribers.
- **transport-layer**—Use data fields for the transport layer.
- **video**—(Not available if Next Gen Services is enabled) Use data fields for video traffic.
- **wireline-subscriber**—(Not available if Next Gen Services is enabled) Use the UserName data field for wireline subscribers.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

> *Configuring an LRF Profile for Subscribers*
>
> Configuring Logging and Reporting for Junos OS Subscriber Aware
>
> *Configuring Logging and Reporting for Subscriber Management*

term (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 711
- Hierarchy Level | 712
- Description | 712
- Options | 712
- Required Privilege Level | 713
- Release Information | 713

Syntax

```
term term-number {
    from {
        destination-address {
            (any-ipv4 | any-ipv4 except);
            (any-ipv6 | any-ipv6 except);
            (any-unicast | any-unicast except);
            (prefix | prefix except);
        }
        destination-address-range {
            high address low address <except>;
        }
        destination-port-range {
            high port-number low port-number;
        }
        destination-ports value;
        destination-prefix-list {
            (prefix-name | prefix-name except);
        }
    }
    then {
        count;
        tag tag-name {
            encrypt {
                hash algorithm;
```

```
                prefix hash-prefix;
            }
            ipv4-mask ipv4-mask;
            ipv6-mask ipv6-mask;
            ipv4-or-value ipv4-or-value;
            ipv6-or-value ipv6-or-value;
            tag-attribute tag-attr-name;
            tag-header header;
            tag-separator separator;
        }
    }
}
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name]
```

Description

Configure a term in a tag rule, which is used to enrich HTTP headers with the appropriate tags. You must configure at least one term for a tag rule, but you can configure multiple terms. Terms are evaluated in the order they are configured. If a data packet matches all the criteria in the **from** statement in any of the terms, then the actions specified in the **then** statement are applied. If the **from** statement does not identify any criteria, then all traffic matches. After a term matches a data packet, further terms are not evaluated. If no terms match, then the HTTP header is not enriched.

For subscriber traffic under static policy control, a tag rule is used if it is included in the HCM profile specified in a PCC rule that the traffic matches. For subscribers under dynamic policy control, a message from the PCRF identifies the configured HCM profile and tag rules to use for HTTP header enrichment.

Options

term-number Number for the term.

- **Range:** 1 through 32,767

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Configuring HCM Profiles and Assigning Tag Rules | 49
- Junos Web Aware HTTP Header Enrichment Overview | 34

term (TDF Domain Selection)

IN THIS SECTION

- Syntax | 713
- Hierarchy Level | 716
- Description | 716
- Options | 716
- Required Privilege Level | 717
- Release Information | 717

Syntax

```
term term-name {
    from {
        3gpp-imsi {
```

```
            equals value;
            has-prefix value;
            has-suffix value;
            matches value;
        }
        attribute name {
            code numeric-code;
            vendor-id vendor-id;
            format {
                integer {
                    equals {
                        value;
                    }
                    greater-than value;
                    less-than value;
                }
                string {
                    equals {
                        value;
                    }
                    has-prefix{
                        value;
                    }
                    has-suffix {
                        value;
                    }
                    matches {
                        value;
                    }
                }
                time {
                    equals {
                        value;
                    }
                    greater-than value;
                    less-than value;
                }
                v4address {
                    equals {
                        value;
                    }
                }
                v6address {
```

```
                    equals {
                        value;
                    }
                }
                v6prefix {
                    equals {
                        value;
                    }
                }
            }
        }
        called-station-id {
            equals value;
            matches value;
        }
        calling-station-id {
            equals value;
            matches value;
        }
        class {
            equals value;
            has-prefix value;
            has-suffix value;
            matches value;
        }
        client client-name;
        framed-ip-address {
            equals value;
        }
        framed-ipv6-prefix {
            equals value;
        }
        nas-ip-address {
            equals value;
        }
        snoop-segment snoop-segment-name;
        user-name {
            equals value;
            has-prefix value;
            has-suffix value;
            matches value;
        }
    }
```

```
    then {
        domain tdf-domain-name;
        pcef-profile pcef-profile-name;
    }
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection]
```

Description

Configure a term that can be used to select the TDF domain for an IP-based subscriber. You can configure multiple terms (up to 10 terms) for the TDF domain selection, and each term is applied in the order in which it is configured. You can specify multiple match conditions within the **from** statement of a term, and all of the conditions have to match. If the incoming RADIUS request from the subscriber matches the criteria in a term, then the TDF domain specified in the **then** statement of the term is used to create the TDF subscriber session.

A term can also be used to select a PCEF profile for a an IP-based subscriber. Setting up a term so that it is used to select a profile is required if the TDF domain selected for a subscriber does not specify a PCEF profile or you want to allow different members of the same TDF domain to have different PCEF profiles.

After a term matches and a TDF domain is selected, further terms are not evaluated when the PCEF profile is specified in either the **then** statement or in the selected TDF domain. If a PCEF profile is not specified in either the **then** statement or in the selected TDF domain, further terms are evaluated to find a PCEF profile for the subscriber.

If no TDF domain is selected for a subscriber, then a TDF subscriber session is not created.

NOTE: The TDF domain must have been previously configured at the **[edit unified-edge gateways tdf *gateway-name* domains]** hierarchy level.

The PCEF profile must have been previously configured at the **[edit unified-edge pcef]** hierarchy level.

Options

term-name	Identifier for the term.

- **Range:** 1 through 50 alphanumeric characters.

The remaining statements are explained separately. See CLI Explorer.

NOTE: You must configure at least one term.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130
- Understanding Selection of Properties for an IP-Based TDF Subscriber | 110
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- IP-Based Subscriber Setup Overview | 107

then (HTTP Header Enrichment)

IN THIS SECTION

- Syntax | 718
- Hierarchy Level | 718
- Description | 718
- Required Privilege Level | 718
- Release Information | 719

Syntax

```
then {
    count;
    tag tag-name {
        encrypt {
            hash algorithm;
            prefix hash-prefix;
        }
        ipv4-mask ipv4-mask;
        ipv6-mask ipv6-mask;
        ipv4-or-value ipv4-or-value;
        ipv6-or-value ipv6-or-value;
        tag-attribute tag-attr-name;
        tag-header header;
        tag-separator separator;
    }
}
```

Hierarchy Level

```
[edit services hcm tag-rule rule-name term term-number]
```

Description

Specify the actions to be taken if the criteria for the tag rule are matched. For subscribers under static policy control, the matching conditions for a tag rule are determined by the PCC rule that uses the HCM profile specifying the tag rule. For subscribers under dynamic policy control, a message from the PCRF identifies the configured HCM profile to use for HTTP header enrichment.

NOTE: You must configure this statement and include at least one action to be taken for the tag rule term.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring HTTP Header Enrichment Overview | 41
- Configuring Tag Rules | 42
- Configuring HCM Profiles and Assigning Tag Rules | 49
- Junos Web Aware HTTP Header Enrichment Overview | 34

then (LRF rule)

IN THIS SECTION

- Syntax | 719
- Hierarchy Level | 720
- Description | 720
- Required Privilege Level | 720
- Release Information | 720

Syntax

```
then {
    report {
        collector collector-name;
        template template-name;
        time-limit time-interval;
        volume-limit volume;
    }
}
```

Hierarchy Level

```
[edit services lrf profile profile-name rule lrf-rule-name]
```

Description

Configure the actions to take if the LRF rule is matched.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

- *Configuring an LRF Profile for Subscribers*
- Configuring Logging and Reporting for Junos OS Subscriber Aware
- *Configuring Logging and Reporting for Subscriber Management*

then (PCC Rules)

IN THIS SECTION

- Syntax | **721**
- Hierarchy Level | **721**

- Description | 721
- Required Privilege Level | 721
- Release Information | 722

Syntax

```
then {
    pcc-action-profile  profile-name;
}
```

Hierarchy Level

```
[edit unified-edge pcef pcc-rules rule-name],
[edit services pcef pcc-rules rule-name]
```

Description

Specify the policy and charging control (PCC) action profile for a PCC rule. The PCC action profile specifies the actions to apply to subscriber traffic that matches any of the **from** statements in the PCC rule. A PCC rule configuration must include the **then** statement and a PCC action profile. The referenced PCC action profile must be configured.

If you are using Junos OS Subscriber Aware, specify the name of the PCC action profile at the **[edit unified-edge pcef pcc-rules *rule-name*]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the name of the PCC action profile at the **[edit services pcef pcc-rules *rule-name*]** hierarchy level.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-rules *rule-name*]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

Configuring Policy and Charging Control Rules

Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware

Configuring Policy and Charging Control Action Profiles for Subscriber Management

then (TDF Domain Selection)

IN THIS SECTION

- Syntax | **723**
- Hierarchy Level | **723**
- Description | **723**
- Required Privilege Level | **723**
- Release Information | **723**

Syntax

```
then {
    domain tdf-domain-name;
    pcef-profile pcef-profile-name;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name]
```

Description

Specify the TDF domain or the PCEF profile to be selected when the criteria specified in the domain selection statement match.

NOTE: This statement is required even if you have not specified any match criteria. The TDF domain must have been previously configured at the **[edit unified-edge gateways tdf *gateway-name* domains]** hierarchy level.

The PCEF profile must have been previously configured at the **[edit unified-edge pcef]** hierarchy level.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130

Understanding Selection of Properties for an IP-Based TDF Subscriber | 110

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112

IP-Based Subscriber Setup Overview | 107

time

IN THIS SECTION

- Syntax | 724
- Hierarchy Level | 724
- Description | 725
- Required Privilege Level | 725
- Release Information | 725

Syntax

```
time {
    equals {
        value;
    }
    greater-than value;
    less-than value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format]
```

Description

Specify the custom AVP attribute's format as time and the value to match for the incoming RADIUS request from the IP-based subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130
- Understanding Selection of Properties for an IP-Based TDF Subscriber | 110
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- IP-Based Subscriber Setup Overview | 107

time-limit (LRF Rule)

IN THIS SECTION

- Syntax | 726
- Hierarchy Level | 726
- Description | 726
- Options | 726

Required Privilege Level | 726
Release Information | 726

Syntax

```
time-limit time-interval;
```

Hierarchy Level

```
[edit services lrf profile profile-name rule lrf-rule-name then report]
```

Description

Configure the time limit to be used for reporting. The template that the LRF rule is using must have **trigger-type time** configured.

Options

time-interval

The time limit in seconds.

- **Range:** 60 through 1800
- **Default:** 300

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Subscriber Management

Configuring Logging and Reporting for Junos OS Subscriber Aware

timeout (Diameter Network Element)

IN THIS SECTION

- Syntax | 727
- Hierarchy Level | 727
- Description | 727
- Options | 728
- Required Privilege Level | 728
- Release Information | 728

Syntax

```
timeout seconds;
```

Hierarchy Level

```
[edit access diameter network-element element-name peer peer-name]
```

Description

Configure the amount of time to wait for a response from this peer before transmitting the request to another peer.

Options

seconds Amount of time to wait before transmitting the request.

- **Range:** 1 through 100 seconds
- **Default:** 4 seconds

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

timeout (RADIUS Server)

IN THIS SECTION

- Syntax | 729
- Hierarchy Level | 729
- Description | 729
- Options | 729
- Required Privilege Level | 729
- Release Information | 729

Syntax

```
timeout seconds;
```

Hierarchy Level

```
[edit access radius servers name]
```

Description

Configure the amount of time that the MX Series router waits to receive a response from a RADIUS server before retrying the request.

Options

seconds Number of seconds to wait.

- **Range:** 1 through 90
- **Default:** 3

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring RADIUS Servers | 91

Understanding Network Elements | 71

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

traceoptions (Diameter Base Protocol)

IN THIS SECTION

- Syntax | 730
- Hierarchy Level | 730
- Description | 730
- Options | 731
- Required Privilege Level | 732
- Release Information | 732

Syntax

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

Hierarchy Level

```
[edit access diameter]
```

Description

Define tracing options for Diameter peers.

Options

file *filename* Use the specified file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory **/var/log**.

files *number* (Optional) Create the specified maximum number of trace files before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

- **Range:** 2 through 1000
- **Default:** 3 files

flag *flag* Use the specified tracing operation. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **receive**—Trace received packets.
- **receive-detail**—Trace received packets in detail.
- **send**—Trace transmitted packets.
- **send-detail**—Trace transmitted packets in detail.
- **state**—Trace Diameter peer state changes.
- **timeout**—Trace timeout events.

level Use the specified level of tracing. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

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

no-remote-trace Disable remote tracing.

no-world-readable	(Optional) Disable unrestricted file access.
peer *peer-name*	(Optional) Trace packets sent to or received from the specified peer. The specified peer must be defined at the **[edit access diameter peer]** hierarchy level.
size *maximum-file-size*	(Optional) Use the specified maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option. • **Syntax:** ***size*k** to specify KB, ***size*m** to specify MB, or ***size*g** to specify GB • **Range:** 10240 through 1073741824 • **Default:** 128 KB
world-readable	(Optional) Enable unrestricted file access.

Required Privilege Level

trace—To view this statement in the configuration.

trace-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

traceoptions (PCEF)

IN THIS SECTION

Syntax | 733
Hierarchy Level | 733

- Description | 733
- Options | 733
- Required Privilege Level | 735
- Release Information | 735

Syntax

```
traceoptions {
    file file-name <files number> <no-word-readable | world-readable> <size
size>;
    flag flag;
    level (all | critical | error | info | notice | verbose | warning);
    no-remote-trace;
}
```

Hierarchy Level

```
[edit unified-edge pcef]
```

Description

Specify tracing options for policy and charging enforcement functions (PCEF).

Options

file *file-name* Use the specified name of the file to receive the output of the tracing operation.

files *number* (Optional) Use the specified maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- **Range:** 2 through 1000
- **Default:** 3 files

flag *flag* Specify which operations are to be traced. To specify more than one operation, include multiple flag statements.

> **BEST PRACTICE**: You might want to enable traceoptions only when you want to debug specific charging operations. Enabling the traceoption flags might have an impact on the system performance.

- **all**—Trace all operations.
- **config**—Trace configuration events.
- **debug**—Trace debug internal events.
- **fsm**—Trace finite state machine events.
- **general**—Trace general events that do not fit in any specific traces.
- **high-availability**—Trace high-availability events.
- **init**—Trace initialization events.
- **tftmgr**—Trace tftmgr events.

level Use the specified level of tracing. You can specify any of the following levels:

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

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

no-world-readable (Optional) Disable unrestricted file access.

size *size* (Optional) Use the specified maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named trace-file reaches this size, it is renamed trace-

file.0. When the trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the size option.

- **Syntax:** *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB.
- **Range:** 10,240 through 1,073,741,824 bytes
- **Default:** 128 KB

word-readable (Optional) Enable unrestricted file access.

Required Privilege Level

trace and unified-edge—To view this statement in the configuration.

trace-control and unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Tracing for PCEF Operations | 239

traceoptions (TDF Gateway)

IN THIS SECTION

- Syntax | 736
- Hierarchy Level | 736
- Description | 736
- Options | 736

Required Privilege Level | 738
Release Information | 738

Syntax

```
traceoptions {
    file file-name <files number> <no-word-readable | world-readable> <size
size>;
    flag flag;
    level (all | critical | error | info | notice | verbose | warning);
    no-remote-trace;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name]
```

Description

Specify tracing options for the TDF gateway.

Options

file *file-name* Use the specified name of the file to receive the output of the tracing operation.

files *number* (Optional) Use the specified maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

- **Range:** 2 through 1000 files
- **Default:** 3 files

flag *flag* Specify which operations are to be traced. To specify more than one operation, include multiple flag statements.

- **all**—Trace everything.
- **bulkjob**—Trace events that are handled by bulk jobs in order to prevent system overload.
- **config**—Trace configuration events.
- **cos-cac**—Trace class of service (CoS) and call admission control (CAC) events.
- **ctxt**—Trace user equipment, Packet Data Network (PDN), or bearer context events.
- **fsm**—Trace mobile subscriber finite state machine (FSM) events.
- **gtpu**—Trace GPRS tunneling protocol, user plane (GTP-U) events.
- **ha**—Trace high availability events.
- **init**—Trace initialization events.
- **pfem**—Trace Packet Forwarding Engine Manager events.
- **stats**—Trace **stats** events. This flag is used internally by Juniper Networks engineers.
- **waitq**—Trace **waitq** events. This flag is used internally by Juniper Networks engineers.

level Use the specified level of tracing. You can specify any of the following levels:

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

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

no-world-readable (Optional) Disable unrestricted file access.

size *size* (Optional) Use the specified maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When the trace-file again reaches its maximum size, trace-file.0 is renamed trace-

file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the size option.

- **Syntax:** *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB.
- **Range:** 10,240 through 1,073,741,824 bytes.
- **Default:** 128 KB

word-readable (Optional) Enable unrestricted file access.

Required Privilege Level

trace and unified-edge—To view this statement in the configuration.

trace-control and unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Tracing for TDF Gateway | 20

trigger-type (LRF Profile)

IN THIS SECTION

- Syntax | 739
- Hierarchy Level | 739
- Description | 739
- Default | 739
- Options | 739

Required Privilege Level | 739
Release Information | 740

Syntax

```
trigger-type  (session-close | volume);
```

Hierarchy Level

```
[edit services lrf profile profile-name template template-name]
```

Description

Configure the type of trigger that causes the generation of data records and transmission to the collector. You can only configure one type of trigger.

Default

If you do not include the **trigger-type** statement, the default trigger is **session-close**.

Options

session-close	Use the closing of the data session to cause the generation of data records and transmission to the collector.
volume	Use a data volume limit to cause the generation of data records and transmission to the collector. The data volume limit value is configured in the LRF rule.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Junos OS Subscriber Aware

Configuring Logging and Reporting for Subscriber Management

type (Application Identification)

IN THIS SECTION

- Syntax | **740**
- Hierarchy Level | **740**
- Description | **741**
- Options | **741**
- Required Privilege Level | **741**
- Release Information | **741**

Syntax

```
type type;
```

Hierarchy Level

```
[edit services application-identification application application-name]
```

Description

Specify the type of application, such as FTP or HTTP.

Options

type Type of application such as FTP or HTTP.

Required Privilege Level

system—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

type (ICMP Mapping for Application Identification)

IN THIS SECTION

- Syntax | 742
- Hierarchy Level | 742
- Description | 742
- Options | 742
- Required Privilege Level | 742
- Release Information | 742

Syntax

```
type icmp-type;
```

Hierarchy Level

```
[edit services application-identification application application-name icmp-
mapping]
```

Description

Match an ICMP type value to create a custom application signature.

Options

value ICMP code value.

- **Range:** 0 through 254

Required Privilege Level

view-level—To view this statement in the configuration.

control-level—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

unit (TDF Interface)

IN THIS SECTION

- Syntax | 743
- Hierarchy Level | 743
- Description | 743
- Options | 743
- Required Privilege Level | 744
- Release Information | 744

Syntax

```
unit interface-unit-number {
    family family-name;
}
```

Hierarchy Level

```
[edit interfaces mif]
```

Description

Configure the logical interface on the TDF interface. You must configure a logical interface to be able to use the TDF interface.

Options

interface-unit-number — Number of the logical unit.

- **Range:** 0 through 16,384

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- Configuring a TDF Logical Interface | 143

url

IN THIS SECTION

- Syntax | 744
- Hierarchy Level | 745
- Description | 745
- Options | 745
- Required Privilege Level | 745
- Release Information | 745

Syntax

```
url url-name;
```

Hierarchy Level

```
[edit unified-edge pcef pcc-action-profiles profile-name redirect],
[edit services pcef pcc-action-profiles profile-name redirect]
```

Description

Specify the URL name that you want a PCC action profile to use for performing HTTP redirection. If you configure this, the PCC action profile can only be used in PCC rules that match only HTTP-based applications and all flows.

If you are using Junos OS Subscriber Aware, specify the URL name at the **[edit unified-edge pcef pcc-action-profiles *profile-name* redirect]** hierarchy level.

If you are using Junos OS Broadband Subscriber Management, specify the URL name at the **[edit services pcef pcc-action-profiles *profile-name* redirect]** hierarchy level.

Options

url-name	URL for the HTTP redirect.

Required Privilege Level

For Junos OS Subscriber Aware:

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

For Junos OS Broadband Subscriber Management:

services—To view this statement in the configuration.

services–control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

Support at the **[edit services pcef pcc-action-profiles *profile-name* redirect]** hierarchy level introduced for Junos OS Broadband Subscriber Management in Junos OS Release 17.2 on MX Series.

Support for Next Gen Services for Junos OS Broadband Subscriber Management introduced in Junos OS Release 19.3R2 on MX Series.

RELATED DOCUMENTATION

Configuring Policy and Charging Control Action Profiles For Junos OS Subscriber Aware

Configuring Policy and Charging Control Action Profiles for Subscriber Management

use-class (Class Attribute)

IN THIS SECTION

- Syntax | 746
- Hierarchy Level | 746
- Description | 747
- Required Privilege Level | 747
- Release Information | 747

Syntax

```
use-class {
    regex "value";
    pattern "pattern";
    subscription-id-type (imsi | msisdn | nai | private | sip-uri);
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domains domain-name subscription-id]
```

Description

Configure a regular expression to parse the Class attribute contents, specify characters to insert between the resulting regular expression groups, and specify the subscription ID type if you configured **subscription-id-options** ***entry-name*** **use-class** under **[edit unified-edge gateways tdf** ***gateway-name*** **domains** ***domain-name*** **subscription-id]**.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a Set of IP-Based TDF Subscriber Properties with a TDF Domain | 121

user-name

IN THIS SECTION

- Syntax | 748
- Hierarchy Level | 748
- Description | 748
- Required Privilege Level | 748
- Release Information | 748

Syntax

```
user-name {
    equals value;
    has-prefix value;
    has-suffix value;
    matches value;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from]
```

Description

Specify the RADIUS AVP User-Name for the incoming RADIUS request from the subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130

Understanding Selection of Properties for an IP-Based TDF Subscriber | 110

Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112

IP-Based Subscriber Setup Overview | 107

user-password (PCEF Profile)

IN THIS SECTION

- Syntax | 749
- Hierarchy Level | 749
- Description | 749
- Options | 749
- Required Privilege Level | 750
- Release Information | 750

Syntax

```
user-password password;
```

Hierarchy Level

```
[edit unified-edge  pcef profiles profile-name aaa-policy-control]
```

Description

Configure the user password for subscribers assigned to the parent PCEF profile.

Options

password Password for access requests to the RADIUS server.

- **Range:** 1 through 32 characters

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring a Policy and Charging Enforcement Function Profile for Junos OS Subscriber Aware Policies That a RADIUS Server Controls | 101

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

v4address

IN THIS SECTION

- Syntax | 750
- Hierarchy Level | 751
- Description | 751
- Required Privilege Level | 751
- Release Information | 751

Syntax

```
v4address {
    equals;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format]
```

Description

Specify the custom AVP attribute's format as an IPv4 address and the value to match for the incoming RADIUS request from the IP-based subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130
- Understanding Selection of Properties for an IP-Based TDF Subscriber | 110
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- IP-Based Subscriber Setup Overview | 107

v6address

IN THIS SECTION

- Syntax | 752
- Hierarchy Level | 752
- Description | 752
- Required Privilege Level | 752
- Release Information | 753

Syntax

```
v6address {
    equals;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format]
```

Description

Specify the custom AVP attribute's format as an IPv6 address and the value to match for the incoming RADIUS request from the IP-based subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130
- Understanding Selection of Properties for an IP-Based TDF Subscriber | 110
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- IP-Based Subscriber Setup Overview | 107

v6prefix

IN THIS SECTION

- Syntax | 753
- Hierarchy Level | 754
- Description | 754
- Required Privilege Level | 754
- Release Information | 754

Syntax

```
v6prefix {
    apply-groups [group-names];
    apply-groups-except [group-names];
    equals;
}
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name format]
```

Description

Specify the custom AVP attribute's format as an IPv6 address prefix and the value to match for the incoming RADIUS request from the IP-based subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130
- Understanding Selection of Properties for an IP-Based TDF Subscriber | 110
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- IP-Based Subscriber Setup Overview | 107

vendor-id

IN THIS SECTION

- Syntax | 755
- Hierarchy Level | 755
- Description | 755
- Options | 755
- Required Privilege Level | 756
- Release Information | 756

Syntax

```
vendor-id vendor-id;
```

Hierarchy Level

```
[edit unified-edge gateways tdf gateway-name domain-selection term term-name
from attribute name]
```

Description

Specify the custom attribute's AVP vendor identification number for the incoming RADIUS request from the subscriber.

After this criterion and the other match criteria specified for the TDF domain or PCEF profile selection term are matched, the specified TDF domain or PCEF profile is selected.

Options

vendor-id AVP vendor identification number.

- **Range:** 0 through 65,534.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

- Configuring Assignment of TDF Subscriber Properties and Policy-Control Properties to IP-Based Subscribers | 130
- Understanding Selection of Properties for an IP-Based TDF Subscriber | 110
- Understanding Selection of Policy-Control Properties for an IP-based TDF Subscriber | 112
- IP-Based Subscriber Setup Overview | 107

vendor-id (AAA Profile)

IN THIS SECTION

- Syntax | 756
- Hierarchy Level | 757
- Description | 757
- Options | 757
- Required Privilege Level | 757
- Release Information | 757

Syntax

```
vendor-id vendor-id;
```

Hierarchy Level

```
[edit unified-edge aaa profiles aaa-profile-name radius policy activation-
attribute],
[edit unified-edge aaa profiles aaa-profile-name radius policy deactivation-
attribute]
```

Description

Configure the vendor identification when a vendor-specific RADIUS attribute is used to carry the policy and charging control (PCC) rulebase name for rulebase activations or deactivations. By default, the rulebase name is carried in the ERX-Service-Activate Juniper vendor-specific attribute (VSA) for activations and in the ERX-Service-Deactivate Juniper VSA for deactivations.

Options

vendor-id Vendor identification number for the RADIUS AVP.

Required Privilege Level

unified-edge—To view this statement in the configuration.

unified-edge-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring an AAA Profile | 96

Understanding AAA Profiles | 73

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

vendor-support

IN THIS SECTION

- Syntax | 758
- Hierarchy Level | 758
- Description | 758
- Required Privilege Level | 758
- Release Information | 758

Syntax

```
vendor-support ibm;
```

Hierarchy Level

```
[edit services lrf profile profile-name]
```

Description

Configure support for any vendor-specific template types. Currently, the only vendor-specific template type is **ipflow-tcp-ts**, for which you configure **vendor-specific ibm**.

If you do not configure **vendor-specific ibm**, a warning appears when you commit the configuration.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.2.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Junos OS Subscriber Aware

Configuring Logging and Reporting for Subscriber Management

Logging and Reporting Function for Subscribers

volume-limit (LRF Rule)

IN THIS SECTION

- Syntax | 759
- Hierarchy Level | 759
- Description | 760
- Options | 760
- Required Privilege Level | 760
- Release Information | 760

Syntax

```
volume-limit volume;
```

Hierarchy Level

```
[edit services lrf profile profile-name rule lrf-rule-name then report]
```

Description

Configure the data volume limit to be used for reporting. The template that the LRF rule is using must have **trigger-type volume** configured.

Options

volume Data volume, in megabytes.

- **Range:** 1 through 1024

Required Privilege Level

interface—To view this statement in the configuration.

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

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R1 on MX Series.

RELATED DOCUMENTATION

Configuring an LRF Profile for Subscribers

Configuring Logging and Reporting for Junos OS Subscriber Aware

Configuring Logging and Reporting for Subscriber Management

watchdog-timeout

IN THIS SECTION

- Syntax | **761**
- Hierarchy Level | **761**
- Description | **761**

Options | 761
Required Privilege Level | 761
Release Information | 761

Syntax

```
watchdog-timeout seconds;
```

Hierarchy Level

```
[edit access diameter peer peer-name]
```

Description

Configure the amount of time to wait for a Device-Watchdog-Answer message.

Options

seconds Amount of time to wait.

- **Range:** 1 through 65,535 seconds
- **Default:** 30 seconds

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

diameter (Subscriber Aware Policy Control) | 368

CHAPTER 13

Operational Commands

IN THIS CHAPTER

- clear services application-identification application-system-cache | 765
- clear services application-identification statistics | 767
- clear services lrf collector statistics | 769
- clear services lrf statistics | 771
- clear services sessions | 772
- clear unified-edge tdf aaa radius client statistics | 777
- clear unified-edge tdf aaa radius network-element statistics | 779
- clear unified-edge tdf aaa radius server statistics | 781
- clear unified-edge tdf aaa radius snoop-segment statistics | 782
- clear unified-edge tdf aaa statistics | 784
- clear unified-edge tdf address-assignment pool | 786
- clear unified-edge tdf address-assignment statistics | 788
- clear unified-edge tdf call-admission-control statistics | 790
- clear unified-edge tdf diameter network-element statistics | 791
- clear unified-edge tdf diameter pcc-gx statistics | 793
- clear unified-edge tdf diameter peer statistics | 795
- clear unified-edge tdf statistics | 797
- clear unified-edge tdf subscribers | 798
- clear unified-edge tdf subscribers peer | 800
- request interface load-balancing revert (Aggregated Multiservices) | 802
- request interface load-balancing switchover (Aggregated Multiservices) | 804
- request services application-identification application | 806
- request services application-identification download | 808
- request services application-identification download status | 809
- request services application-identification group | 811
- request services application-identification install | 813

- request services application-identification install status | **814**
- request services application-identification proto-bundle-status | **816**
- request services application-identification uninstall | **817**
- request services application-identification uninstall status | **819**
- request unified-edge tdf call-trace clear | **820**
- request unified-edge tdf call-trace show | **822**
- request unified-edge tdf call-trace start | **826**
- request unified-edge tdf call-trace stop | **829**
- show interfaces anchor-group (Aggregated Packet Forwarding Engine) | **831**
- show interfaces load-balancing (Aggregated Multiservices) | **836**
- show services application-identification application | **841**
- show services application-identification application-system-cache | **850**
- show services application-identification counter | **856**
- show services application-identification group | **860**
- show services application-identification statistics application-groups | **865**
- show services application-identification statistics applications | **868**
- show services application-identification status | **870**
- show services application-identification version | **873**
- show services ha detail | **874**
- show services ha statistics | **877**
- show services hcm statistics | **885**
- show services hcm pic-statistics | **888**
- show services lrf collector statistics | **896**
- show services lrf rule statistics | **898**
- show services lrf statistics | **901**
- show services lrf template | **903**
- show services traffic-detection-function hcm statistics | **906**
- show services traffic-detection-function sessions | **911**
- show unified-edge tdf aaa radius client statistics | **915**
- show unified-edge tdf aaa radius client status | **923**
- show unified-edge tdf aaa radius network-element statistics | **925**
- show unified-edge tdf aaa radius server statistics | **930**

- show unified-edge tdf aaa radius server status | 936
- show unified-edge tdf aaa radius snoop-segment statistics | 940
- show unified-edge tdf aaa statistics | 945
- show unified-edge tdf address-assignment pool | 958
- show unified-edge tdf address-assignment service-mode | 964
- show unified-edge tdf address-assignment statistics | 967
- show unified-edge tdf call-admission-control statistics | 970
- show unified-edge tdf call-rate statistics | 974
- show unified-edge tdf diameter network-element statistics | 978
- show unified-edge tdf diameter network-element status | 981
- show unified-edge tdf diameter pcc-gx statistics | 984
- show unified-edge tdf diameter peer statistics | 992
- show unified-edge tdf diameter peer status | 999
- show unified-edge tdf domain service-mode | 1004
- show unified-edge tdf domain statistics | 1007
- show unified-edge tdf resource-manager clients | 1014
- show unified-edge tdf service-mode | 1017
- show unified-edge tdf statistics | 1020
- show unified-edge tdf status | 1032
- show unified-edge tdf subscribers | 1038
- show unified-edge tdf system interfaces | 1059
- show unified-edge tdf system interfaces service-mode | 1061

clear services application-identification application-system-cache

IN THIS SECTION

- Syntax | 766
- Description | 766
- Options | 766

- Required Privilege Level | 766
- Output Fields | 766
- Sample Output | 766
- Release Information | 766

Syntax

```
clear services application-identification application-system-cache
```

Description

Clear entries from the application system cache.

Options

This command has no options.

Required Privilege Level

clear

Output Fields

When you enter this command, you are provided no feedback on the status of your request.

Sample Output

clear services application-identification application-system-cache

```
user@host> clear services application-identification application-system-cache
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show services application-identification application-system-cache

clear services application-identification statistics

IN THIS SECTION

- Syntax | 767
- Description | 767
- Options | 767
- Required Privilege Level | 768
- Output Fields | 768
- Sample Output | 768
- Release Information | 769

Syntax

```
clear services application-identification statistics
<cumulative>
<interval>
<logical-system (logical-system-name | all | root-logical-system)>
<tenant (tenant-name | all)>
```

Description

Clears all Junos OS application statistics such as cumulative, interval, applications, and application groups.

Options

cumulative (Optional) Clears the cumulative application statistics.

interval	(Optional) Clears the application interval statistics. Interval statistics are displayed in Top-N format, such that the first application group displayed has the largest byte count. If this parameter is not specified, then the default is 1, which is the current interval.
logical-system ***logical-system-name***	(Optional) Clears application identification statistics of the specified logical system.
logical-system ***all***	(Optional) Clears application identification statistics of all the logical systems.
root-logical-system	(Optional) Clears application identification statistics of the root logical system.
tenant ***tenant-name***	(Optional) Clears application identification statistics of the specified tenant system.
tenant ***all***	(Optional) Clears application identification statistics of all the tenant systems.

Required Privilege Level

clear

Output Fields

When you enter this command, you are provided no feedback on the status of your request.

Sample Output

clear services application-identification statistics

```
user@host> clear services application-identification statistics
appid statistics cleared
```

clear services application-identification statistics logical-system all

```
user@host> clear services application-identification statistics logical-system all
appid statistics cleared
```

clear services application-identification statistics cumulative tenant TSYS1

```
user@host> clear services application-identification statistics cumulative tenant TSYS1
appid statistics cleared
```

clear services application-identification statistics cumulative tenant all

```
user@host> clear services application-identification statistics cumulative tenant all
appid statistics cleared
```

clear services application-identification statistics cumulative

```
user@host:TSYS1> clear services application-identification statistics cumulative
appid statistics cleared
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

logical-system option introduced in Junos OS Release 18.3R1 on SRX Series.

tenant option introduced in Junos OS Release 19.4R1 on SRX Series.

RELATED DOCUMENTATION

show services application-identification statistics applications

show services application-identification statistics application-groups

clear services lrf collector statistics

IN THIS SECTION

Syntax | 770

- Description | 770
- Options | 770
- Required Privilege Level | 770
- Output Fields | 770
- Sample Output | 771
- Release Information | 771

Syntax

```
clear services lrf collector statistics
<collector-name>
```

Description

Clear all the LRF statistics for the specified collector. If a collector is not specified, statistics are cleared for all collectors.

Options

none	Clear LRF statistics for all collectors.
collector-name	(Optional) Clear LRF statistics for the specified collector.

Required Privilege Level

clear

Output Fields

A message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear services lrf collector statistics

```
user@host> clear services lrf collector statistics coll1
Interface: ms-0/1/0, Status: LRF collector statistics successfully cleared
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show services lrf collector statistics

clear services lrf statistics

IN THIS SECTION

- Syntax | 771
- Description | 772
- Required Privilege Level | 772
- Output Fields | 772
- Sample Output | 772
- Release Information | 772

Syntax

```
clear services lrf statistics
```

Description

Clear all the LRF statistics.

Required Privilege Level

clear

Output Fields

A message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear services lrf statistics

```
user@host> clear services lrf statistics
Interface: ms-0/1/0, Status: LRF statistics successfully cleared
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show services lrf statistics

clear services sessions

IN THIS SECTION

- Syntax | 773
- Description | 773

- Options | 773
- Required Privilege Level | 776
- Output Fields | 776
- Sample Output | 776
- Release Information | 777

Syntax

```
clear services sessions
<application-protocol protocol>
<destination-port destination-port>
<destination-prefix destination-prefix>
<interface interface-name>
<ip-action>
<protocol protocol>
<service-set service-set>
<source-port source-port>
<source-prefix source-prefix>
```

Description

Clear services sessions currently active on the embedded PIC or MIC. When you enter this command, the sessions are marked for deletion and are cleared thereafter. The time that is taken to clear the currently active sessions varies, depending on the scaled nature of the environment.

Options

none Clear all sessions.

application-protocol *protocol* (Optional) Clear sessions for one of the following application protocols:

- **bootp**—Bootstrap protocol
- **dce-rpc**—Distributed Computing Environment-Remote Procedure Call protocols

- **dce-rpc-portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—Domain Name System protocol
- **exec**—Exec
- **ftp**—File Transfer Protocol
- **h323**—H.323 standards
- **icmp**—Internet Control Message Protocol
- **iiop**—Internet Inter-ORB Protocol
- **ip**—IP
- **login**—Login
- **netbios**—NetBIOS
- **netshow**—NetShow
- **pptp**—Point-to-Point Tunneling Protocol
- **realaudio**—RealAudio
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol
- **shell**—Shell
- **sip**—Session Initiation Protocol
- **snmp**—Simple Network Management Protocol
- **sqlnet**—SQLNet
- **talk**—Talk Program
- **tftp**—Trivial File Transfer Protocol
- **traceroute**—Traceroute
- **winframe**—WinFrame

destination-port *destination-port*
(Optional) Clear sessions for the specified destination port. The range of values is from 0 to 65535.

destination-prefix *destination-prefix*
(Optional) Clear sessions for the specified destination prefix.

interface *interface-name*
(Optional) Clear sessions for the specified interface. On M Series and T Series routers, the *interface-name* can be **ms-***fpc/ pic/ port* or **rsp***number*.

ip-action
(Optional) Clear **ip-action** entries generated by the router to log, drop, or block traffic based on previous matches. The IP action options and targets are configured at the **{edit security idp idp-policy** *policy-name* **rulebase-ips rule** *rule-name* **then]** hierarchy level.

protocol *protocol*
(Optional) Clear sessions for one of the following IP types:

- *number*—Numeric protocol value from **0** to **255**
- **ah**—IPsec Authentication Header protocol
- **egp**—An exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload protocol
- **gre**—A generic routing encapsulation protocol
- **icmp**—Internet Control Message Protocol
- **icmp6**—Internet Control Message Protocol version 6
- **igmp**—Internet Group Management Protocol
- **ipip**—IP-over-IP Encapsulation Protocol
- **ospf**—Open Shortest Path First protocol
- **pim**—Protocol Independent Multicast protocol
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

service-set *service-set*
(Optional) Clear sessions for the specified service set.

source-port *source-port* (Optional) Clear sessions for the specified source port. The range of values is from 0 through 65535.

source-prefix *source-prefix* (Optional) Clear sessions for the specified source prefix.

Required Privilege Level

clear

Output Fields

Table 13 on page 776 lists the output fields for the **clear services sessions** command. Output fields are listed in the approximate order in which they appear.

Table 13: clear services sessions Output Fields

Field Name	Field Description
Interface	Name of an interface.
Service set	Name of the service set from which sessions are being cleared.
Sessions marked for deletion	Number of sessions that are marked for deletion and are subsequently cleared.

Sample Output

clear services sessions

```
user@host>clear services sessions
Interface   Service set           Sessions marked for deletion
ms-0/0/0    sset                        10
```

Release Information

Command introduced in Junos OS Release 13.1.

RELATED DOCUMENTATION

show services sessions

clear unified-edge tdf aaa radius client statistics

IN THIS SECTION

- Syntax | 777
- Description | 778
- Options | 778
- Required Privilege Level | 778
- Output Fields | 778
- Sample Output | 778
- Release Information | 779

Syntax

```
clear unified-edge tdf aaa radius client statistics
<all>
<client name>
<fpc-slot fpc-slot>
<gateway gateway>
<pic-slot pic-slot>
```

Description

Clear statistics for the accounting requests and responses transmitted and received by the RADIUS client for one or more TDF gateways. If a TDF gateway is not specified, then information for all TDF gateways is cleared.

Options

none	(Same as all) Clear statistics for all clients on all TDF gateways.
all	(Optional) Clear statistics for all the clients.
client *name*	(Optional) Clear statistics for the specified client.
fpc-slot *fpc-slot*	(Optional) Clear statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway*	(Optional) Clear statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Clear statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

clear, unified-edge

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear unified-edge tdf aaa radius client statistics all

```
user@host> clear unified-edge tdf aaa radius client statistics all

Cleared all RADIUS statistics
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf aaa radius client statistics | 915

clear unified-edge tdf aaa radius network-element statistics

IN THIS SECTION

- Syntax | 779
- Description | 779
- Options | 780
- Required Privilege Level | 780
- Output Fields | 780
- Sample Output | 780
- Release Information | 780

Syntax

```
clear unified-edge tdf aaa radius network-element statistics
<fpc-slot fpc-slot>
<gateway gateway>
<pic-slot pic-slot>
<name name>
```

Description

Clear all the statistics for the specified network element.

Options

none	Clear statistics for all network elements for all TDF gateways.
fpc-slot *fpc-slot*	(Optional) Clear statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway*	(Optional) Clear statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Clear statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.
name *name*	(Optional) Clear statistics for the specified network element.

Required Privilege Level

clear, unified-edge

Output Fields

No message is displayed on successful execution of this command; otherwise, an error message is displayed.

Sample Output

clear unified-edge tdf aaa radius network-element statistics

```
user@host> clear unified-edge tdf aaa radius network-element statistics
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf aaa radius network-element statistics | 925

Understanding Network Elements | 71

clear unified-edge tdf aaa radius server statistics

IN THIS SECTION

- Syntax | 781
- Description | 781
- Options | 781
- Required Privilege Level | 782
- Output Fields | 782
- Sample Output | 782
- Release Information | 782

Syntax

```
clear unified-edge tdf aaa radius server statistics
<fpc-slot fpc-slot>
<gateway gateway>
<pic-slot pic-slot>
<name name>
```

Description

Clear all the statistics for the specified RADIUS server.

Options

none	Clear statistics for all RADIUS servers for all TDF gateways.
fpc-slot *fpc-slot*	(Optional) Clear statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway*	(Optional) Clear statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Clear statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

name *name* (Optional) Clear statistics for the specified RADIUS server.

Required Privilege Level

clear, unified-edge

Output Fields

No message is displayed on successful execution of this command; otherwise, an error message is displayed.

Sample Output

clear unified-edge tdf aaa radius server statistics

```
user@host> clear unified-edge tdf aaa radius server statistics
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf aaa radius server statistics | 930

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

clear unified-edge tdf aaa radius snoop-segment statistics

IN THIS SECTION

- Syntax | 783
- Description | 783
- Options | 783

- Required Privilege Level | 783
- Output Fields | 784
- Sample Output | 784
- Release Information | 784

Syntax

```
clear unified-edge tdf aaa radius snoop-segment  statistics
<fpc-slot fpc-slot>
<gateway gateway>
<pic-slot pic-slot>
<segment snoop-segment-name>
```

Description

Clear all snoop segment statistics for FPCs, PICs, TDF gateways, or snoop segments that you specify.

Options

none	Clear all snoop-segment statistics for all TDF gateways.
fpc-slot *fpc-slot*	(Optional) Clear statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway*	(Optional) Clear statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Clear statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.
segment *snoop-segment-name*	(Optional) Clear statistics for the specified snoop segment.

Required Privilege Level

clear, unified-edge

Output Fields

A message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear unified-edge tdf aaa radius snoop-segment statistics

```
user@host> clear unified-edge tdf aaa radius snoop-segment statistics
Cleared Radius snoop-segment Statistics
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf aaa radius snoop-segment statistics | 940

Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | 114

clear unified-edge tdf aaa statistics

IN THIS SECTION

- Syntax | 785
- Description | 785
- Options | 785
- Required Privilege Level | 785
- Output Fields | 785
- Sample Output | 786
- Release Information | 786

Syntax

```
clear unified-edge tdf aaa statistics
<all>
<fpc-slot fpc-slot>
<gateway gateway>
<pic-slot pic-slot>
```

Description

Clear global authentication, authorization, and accounting (AAA) statistics for one or more TDF gateways. If a TDF gateway is not specified, then information for all TDF gateways is cleared.

Options

none	(Same as all) Clear AAA statistics for all TDF gateways.
all	(Optional) Clear AAA statistics for all the TDF gateways.
fpc-slot *fpc-slot*	(Optional) Clear AAA statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway*	(Optional) Clear AAA statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Clear AAA statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

clear, unified-edge

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear unified-edge tdf aaa statistics all

```
user@host> clear unified-edge tdf aaa statistics all

Cleared all AAA statistics
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf aaa statistics | 945

clear unified-edge tdf address-assignment pool

IN THIS SECTION

- Syntax | 787
- Description | 787
- Options | 787
- Required Privilege Level | 787
- Output Fields | 787
- Sample Output | 787
- Release Information | 788

Syntax

```
clear unified-edge tdf address-assignment pool name pool-name
<gateway gateway>
<routing-instance routing-instance>
```

Description

Clear the sessions that have been assigned addresses from the specified mobile pool for one or more TDF gateways. If a TDF gateway is not specified, then the sessions for all TDF gateways are cleared.

Options

none	Clear the sessions for all TDF gateways associated with the specified mobile pool.
name *pool-name*	Clear the sessions for the specified mobile pool.
gateway *gateway*	(Optional) Clear the sessions on the specified TDF gateway.
routing-instance *routing-instance*	(Optional) Clear the sessions on the specified routing instance.

Required Privilege Level

clear, unified-edge

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear unified-edge tdf address-assignment pool name

```
user@host> clear unified-edge tdf address-assignment pool name pool-1

Initiated clearing of sessions in the pool
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf address-assignment pool | 958

clear unified-edge tdf address-assignment statistics

IN THIS SECTION

- Syntax | 788
- Description | 788
- Options | 789
- Required Privilege Level | 789
- Output Fields | 789
- Sample Output | 789
- Release Information | 789

Syntax

```
clear unified-edge tdf address-assignment statistics
<fpc-slot fpc-slot>
<gateway gateway>
<pic-slot pic-slot>
```

Description

Clear the global address assignment statistics for one or more TDF gateways. If a TDF gateway is not specified, then the statistics for all TDF gateways are cleared.

Options

none	Clear statistics for all TDF gateways.
fpc-slot *fpc-slot*	(Optional) Clear the statistics for the session PIC in the specified FPC slot.
gateway *gateway*	(Optional) Clear the statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Clear information about the session PIC in this particular PIC slot. For routers, replace *pic-slot* with a value from 0 through 3.

Required Privilege Level

clear, unified-edge

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear unified-edge tdf address-assignment statistics

```
user@host> clear unified-edge tdf address-assignment statistics

Cleared address-assignment statistics
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf address-assignment statistics | 967

clear unified-edge tdf call-admission-control statistics

IN THIS SECTION

- Syntax | 790
- Description | 790
- Options | 790
- Required Privilege Level | 790
- Output Fields | 791
- Sample Output | 791
- Release Information | 791

Syntax

```
clear unified-edge tdf call-admission-control statistics gateway gateway-name
<fpc-slot fpc-slot>
<pic-slot pic-slot>
```

Description

Clear call admission control (CAC) statistics for the specified TDF gateway.

Options

fpc-slot *fpc-slot*	(Optional) Clear statistics for the session PIC in the specified FPC slot.
gateway *gateway-name*	Clear CAC statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Clear statistics for the session PIC in the specified PIC slot.

Required Privilege Level

clear, unified-edge

Output Fields

No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear unified-edge tdf call-admission-control statistics gateway

```
user@host> clear unified-edge tdf call-admission-control statistics gateway TDF
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf call-admission-control statistics | 970

clear unified-edge tdf diameter network-element statistics

IN THIS SECTION

- Syntax | 792
- Description | 792
- Options | 792
- Required Privilege Level | 792
- Output Fields | 792
- Sample Output | 793
- Release Information | 793

Syntax

```
clear unified-edge tdf diameter network-element statistics
<fpc-slot fpc-slot>
<gateway gateway-name>
<network-element-name network-element-name>
<pic-slot pic-slot>
```

Description

Clear the statistics for network elements for one or more TDF gateways. If a network element is not specified, then statistics for all network elements are cleared. If a TDF gateway is not specified, then statistics for all TDF gateways are cleared.

Options

none	Clear statistics for all network elements and TDF gateways.
fpc-slot ***fpc-slot***	(Optional) Clear statistics for the specified Flexible PIC Concentrator (FPC).
gateway ***gateway-name***	(Optional) Clear statistics for the specified TDF gateway.
network-element-name ***network-element-name***	(Optional) Clear statistics for the specified network element.
pic-slot ***pic-slot***	(Optional) Clear statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

clear, unified-edge

Output Fields

No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear unified-edge tdf diameter network-element statistics

```
user@host> clear unified-edge tdf diameter network-element statistics
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf diameter network-element statistics | 978

clear unified-edge tdf diameter pcc-gx statistics

IN THIS SECTION

- Syntax | 793
- Description | 794
- Options | 794
- Required Privilege Level | 794
- Output Fields | 794
- Sample Output | 794
- Release Information | 794

Syntax

```
clear unified-edge tdf diameter pcc-gx statistics
<fpc-slot fpc-slot>
```

```
<gateway gateway-name>
<pic-slot pic-slot>
```

Description

Clear all statistics for the Gx application for one or more TDF gateways. If a TDF gateway is not specified, then statistics for all TDF gateways are cleared.

Options

none	Clear Gx application statistics for all TDF gateways.
fpc-slot *fpc-slot*	(Optional) Clear statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway-name*	(Optional) Clear statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Clear statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

clear, unified-edge

Output Fields

No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear unified-edge tdf diameter pcc-gx statistics

```
user@host> clear unified-edge tdf diameter pcc-gx statistics
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf diameter pcc-gx statistics | 793

clear unified-edge tdf diameter peer statistics

IN THIS SECTION

- Syntax | 795
- Description | 795
- Options | 795
- Required Privilege Level | 796
- Output Fields | 796
- Sample Output | 796
- Release Information | 796

Syntax

```
clear unified-edge tdf diameter peer statistics
<fpc-slot fpc-slot>
<gateway gateway-name>
<peer-name peer-name>
<pic-slot pic-slot>
```

Description

Clear statistics for Diameter peers for one or more TDF gateways. If a peer is not specified, then statistics for all peers are cleared. If a TDF gateway is not specified, then statistics for all TDF gateways are cleared.

Options

none	Clear Diameter peer statistics for all TDF gateways.

fpc-slot *fpc-slot*	(Optional) Clear statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway-name*	(Optional) Clear statistics for the specified TDF gateway.
peer-name *peer-name*	(Optional) Clear statistics for the specified peer.
pic-slot *pic-slot*	(Optional) Clear statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

clear, unified-edge

Output Fields

No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear unified-edge tdf diameter peer statistics

```
user@host> clear unified-edge tdf diameter peer statistics
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf diameter peer statistics | 992

clear unified-edge tdf statistics

IN THIS SECTION

- Syntax | 797
- Description | 797
- Options | 797
- Required Privilege Level | 798
- Output Fields | 798
- Sample Output | 798
- Release Information | 798

Syntax

```
clear unified-edge tdf statistics
<data-plane>
<gateway gateway-name>
<domain domain-name
```

Description

Clear all the statistics for the specified TDF gateway, domain, or control plane.

Options

none	Clear statistics for all TDF control planes, domains, and gateways.
data-plane	(Optional) Clear statistics for the data plane.
domain *domain-name*	(Optional) Clear statistics for the specified TDF domain.
gateway *gateway-name*	(Optional) Clear statistics for the specified TDF gateway.

Required Privilege Level

clear, unified-edge

Output Fields

No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear unified-edge tdf statistics gateway

```
user@host> clear unified-edge tdf statistics gateway TDF
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf statistics | 1020

clear unified-edge tdf subscribers

IN THIS SECTION

- Syntax | 799
- Description | 799
- Options | 799
- Required Privilege Level | 800
- Output Fields | 800

Sample Output | 800
Release Information | 800

Syntax

```
clear unified-edge tdf subscribers [option]
```

Description

Clear the subscribers identified by the option values. You must include at least one option. For IFL-based subscribers, use the **revert** option to re-create the cleared subscribers identified by the option values.

Options

option One or more of the following options:

- **domain** ***domain-name***—Clear the subscribers for the specified TDF domain.
- **gateway** ***gateway-name***—Clear the subscribers for the specified TDF gateway.
- **interface** ***interface-name***—Clear the subscribers on the specified multiservices interface, aggregated multiservices interface, Packet Forwarding Engine interface, or aggregated Packet Forwarding Engine interface names.
- **peer** ***peer-name***—Clear the subscriber matching GPRS tunneling protocol (GTP) peer on the specified TDF gateway.
- **revert**—For an IFL-based subscriber, recreate an IFL-subscriber that was cleared.
- **routing-instance** ***routing-instance***—Clear the subscriber information for the specified routing instance.
- **subscriber-name** ***subscriber-name***—Clear the specified IFL-based subscriber.
- **v4-addr** ***v4-addr***—Clear the subscriber information for the specified IPv4 address of the IP-based subscriber's user equipment (UE).
- **v6-addr** ***v6-addr***—Clear the subscriber information for the specified IPv6 address of the IP-based subscriber's user equipment.

Required Privilege Level

clear, unified-edge

Output Fields

No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear unified-edge tdf subscribers gateway tdf

```
user@host> clear unified-edge tdf subscribers gateway tdf
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- clear unified-edge tdf statistics | 797
- clear unified-edge tdf subscribers peer | 800
- show unified-edge tdf subscribers | 1038
- IP-Based and IFL-Based TDF Subscribers Overview | 107
- Understanding IFL-Based Subscriber Setup | 115

clear unified-edge tdf subscribers peer

IN THIS SECTION

- Syntax | 801

- Description | **801**
- Options | **801**
- Required Privilege Level | **802**
- Output Fields | **802**
- Sample Output | **802**
- Release Information | **802**

Syntax

```
clear unified-edge tdf subscribers peer
<gateway gateway>
<remote-addr remote-addr>
<nas-id nas-id
<routing-instance routing-instance>
```

Description

Clear the information for IP-based subscribers anchored on the specified RADIUS client, TDF gateway, or both, or for IP-based subscribers matching the specified routing instance.

Options

none	Clear information for all IP-based subscribers.
gateway *gateway*	(Optional) Clear IP-based subscriber information for the TDF gateway.
nas-id *nas-id*	(Optional) Clear IP-based subscriber information for the specified NAS identifier of the RADIUS client.
remote-addr *remote-addr*	(Optional) Clear IP-based subscriber information for the specified IPv4 address of the RADIUS client.
routing-instance *routing-instance*	(Optional) Clear IP-based subscriber information for the specified routing instance.

Required Privilege Level

clear, unified-edge

Output Fields

No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear unified-edge tdf subscribers peer gateway remote-addr

```
user@host> clear unified-edge tdf subscribers peer gateway TDF remote-addr 198.0.2.2
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf subscribers | 798

show unified-edge tdf subscribers | 1038

request interface load-balancing revert (Aggregated Multiservices)

IN THIS SECTION

- Syntax | 803
- Description | 803
- Options | 803
- Required Privilege Level | 803

- Output Fields | 803
- Sample Output | 803
- Release Information | 804

Syntax

```
request interface load-balancing revert interface-name
```

Description

Revert the aggregated multiservices member interface (mams-) from the inactive state to the active or backup state based on the configuration and the operational state of the aggregated multiservices interface.

Options

interface-name	Name of the member interface. The member interface format is mams-*a*/*b*/0, where *a* is the FPC slot number and *b* is the PIC slot number.

Required Privilege Level

view

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request interface load-balancing revert

```
user@host> request interface load-balancing revert mams-4/0/0
request succeeded
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

request interface load-balancing switchover (Aggregated Multiservices) | 804

request interface load-balancing switchover (Aggregated Multiservices)

IN THIS SECTION

- Syntax | 804
- Description | 804
- Options | 805
- Required Privilege Level | 805
- Output Fields | 805
- Sample Output | 805
- Release Information | 805

Syntax

request interface load-balancing switchover ***interface-name***
<force>

Description

Switch the active member interface to the backup state.

In the case of mobile control plane redundancy, the behavior depends on the replication state of the member interface:

- If the sync state is **in-sync**, then the active member is rebooted and the backup member becomes the new active member.
- If the sync-state is **in-progress**, then the **force** option must be used to force the switchover.

> ⚠ **CAUTION**: In this case, there is a risk of losing subscriber information because the synchronization has not yet been completed.

Options

interface-name	Name of the member interface. The member interface format is mams-*a*/*b*/0, where *a* is the FPC slot number and *b* is the PIC slot number.
force	(Optional) Force the switchover from the active member to the backup member.

Required Privilege Level

view

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request interface load-balancing switchover force

```
user@host> request interface load-balancing switchover force mams-4/0/0
Switchover Initiated
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

request interface load-balancing revert (Aggregated Multiservices) | 802

request services application-identification application

IN THIS SECTION

- Syntax | 806
- Description | 806
- Options | 806
- Required Privilege Level | 807
- Output Fields | 807
- Sample Output | 807
- Release Information | 807

Syntax

```
request services application-identification application <disable | enable>
predefined-application-name
```

Description

Disable or enable a predefined application signature.

Options

predefined-application-name—Application name; a maximum of up to 31 characters. Predefined applications have the prefix **junos-** to avoid conflict with user-defined ones. Do not name your custom application signature with the **junos** prefix; this prefix is reserved for predefined application signatures.

disable— (Optional) Disable a predefined application signature, initiate signature recompilation, and commit all pending uncompiled signatures to the configuration.

The following conditions apply:

- You cannot disable a predefined application signature that is referenced by an active security policy or custom application signature. First modify or deactivate the policy or custom application signature.
- If you disable an application signature, for example, junos:HTTP, that has nested applications, the nested applications are not recognized.

enable—(Optional) Enable a predefined application signature, initiate signature recompilation, and commit all pending uncompiled signatures to the configuration. Include the **no-commit** keyword to defer signature recompilation.

Required Privilege Level

maintenance

Output Fields

When you enter this command, the system provides feedback on the status of your request.

Sample Output

request services application-identification application disable

```
user@host> request services application-identification application disable junos:163

 Please wait while we are re-compiling signatures ..
 Please wait while we are re-compiling signatures ..
 Please wait while we are re-compiling signatures ..
 Please wait while we are re-compiling signatures ..
 Disable application junos:163 succeed.
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show services application-identification application

request services application-identification download

IN THIS SECTION

- Syntax | 808
- Description | 808
- Options | 808
- Required Privilege Level | 808
- Output Fields | 808
- Sample Output | 809
- Release Information | 809

Syntax

```
request services application-identification download <version version-number>;
```

Description

Manually download the application package for Junos OS application identification. The application package is extracted from the IDP signature database and contains signature definitions for known applications, such as DNS, Facebook, FTP, Skype, and SNMP.

Options

version *version-number*—(Optional) Download the specified version of the application package from the Juniper Networks website. If you do not enter a version, the most recent version is downloaded.

Required Privilege Level

maintenance

Output Fields

When you enter this command, you are shown the command to use to check the status of your download.

Sample Output

request services application-identification download

```
user@host> request services application-identification download
Please use command "request services application-identification download status"
 to check status
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

RELATED DOCUMENTATION

- *request services application-identification install*
- *request services application-identification download status*

request services application-identification download status

IN THIS SECTION

- Syntax | 810
- Description | 810
- Required Privilege Level | 810
- Output Fields | 810
- Sample Output | 810
- Release Information | 810

Syntax

```
request services application-identification download status
```

Description

Check the download status of the application signature package. The downloaded application package is saved under **/var/db/appid/sec-download/**.

Required Privilege Level

maintenance

Output Fields

When you enter this command, the system provides feedback on the status of your request.

Sample Output

request services application-identification download status

```
user@host> request services application-identifications download status
Application package 1608 is downloaded successfully.
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

RELATED DOCUMENTATION

request services application-identification download

request services application-identification group

IN THIS SECTION

- Syntax | 811
- Description | 811
- Options | 811
- Required Privilege Level | 812
- Output Fields | 812
- Sample Output | 812
- Release Information | 812

Syntax

```
request services application-identification group (copy | disable | enable)
predefined-application-group-name
```

Description

Copy, disable, or enable a predefined application signature group.

Options

predefined-application-group-name—Identifier for the application group. Maximum length is 32 characters.

copy—Copy the specified predefined application signature group from the database to the configuration and change the name (for example, my:FTP). The ID and order are generated automatically. You can copy the same predefined application signature group only once. You cannot copy duplicate custom signature groups.

NOTE: In configuration mode, if an uncommitted action is pending, the **request services application-identification group copy** command fails.

disable—Disable the specified predefined application signature group.

> **NOTE**: You cannot disable a predefined application signature group that is referenced by an active security policy or custom application signature group. First modify or deactivate the policy or custom application signature group.

enable—Enable the specified predefined application signature group.

Required Privilege Level

maintenance

Output Fields

When you enter this command, the system provides feedback on the status of your request.

Sample Output

request services application-identification group copy

```
user@host> request services application-identification group copy junos:SYBASE
group 1040 copied successfully.
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show services application-identification group

request services application-identification install

IN THIS SECTION

- Syntax | 813
- Description | 813
- Required Privilege Level | 813
- Output Fields | 813
- Sample Output | 814
- Release Information | 814

Syntax

```
request services application-identification install
```

Description

Install the downloaded predefined application signature package.

The install operation fails if any custom application signatures or custom application signature groups have been manually inserted before any predefined application signatures or predefined application signature groups in the Junos OS configuration. Remove any insert-before signatures, then retry the install operation. This command does not display the installation status and only provides an informational message on the types of commands to use to verify the installation status of the application signature package and the protocol bundle.

Required Privilege Level

maintenance

Output Fields

When you enter this command, you are shown the command to use to check the status of your installation request.

Sample Output

request services application-identification install

```
user@host> request services application-identification install
Please use command "request services application-identification install status"
to check status and use command "request services application-identification
proto-bundle-status" to check protocol bundle status
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

RELATED DOCUMENTATION

request services application-identification download

request services application-identification install status

request services application-identification install status

IN THIS SECTION

- Syntax | 815
- Description | 815
- Required Privilege Level | 815
- Output Fields | 815
- Sample Output | 815
- Release Information | 815

Syntax

```
request services application-identification install status
```

Description

Display the status of the install operation.

Required Privilege Level

maintenance

Output Fields

When you enter this command, the system provides feedback on whether your request succeeded or failed.

Sample Output

request services application-identification install status

```
user@host> request services application-identification install status
Install application package version (1776) succeed.
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

RELATED DOCUMENTATION

request services application-identification install

request services application-identification proto-bundle-status

IN THIS SECTION

- Syntax | 816
- Description | 816
- Required Privilege Level | 816
- Output Fields | 816
- Sample Output | 817
- Release Information | 817

Syntax

```
request services application-identification proto-bundle-status
```

Description

Display the status of the install operation of the protocol bundle. This command provides feedback on whether your request succeeded or failed.

Required Privilege Level

maintenance

Output Fields

When you enter this command, the system provides feedback on whether your request succeeded or failed.

Sample Output

request services application-identification proto-bundle-status

```
user@host> request services application-identification proto-bundle-status
Protocol Bundle Version (1.30.4-22.005 (build date Jan 17 2014)) and application
secpack version (2345) is loaded and activated.
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

RELATED DOCUMENTATION

request services application-identification install

request services application-identification uninstall

IN THIS SECTION

- Syntax | **817**
- Description | **818**
- Required Privilege Level | **818**
- Output Fields | **818**
- Sample Output | **818**
- Release Information | **818**

Syntax

```
request services application-identification uninstall
```

Description

Uninstall the predefined application package.

The uninstall operation fails if any active security policies, custom application signatures, or custom application signature groups reference predefined application signatures or predefined application signature groups in the Junos OS configuration. This command does not display the uninstallation status and only provides an informational message on the types of commands to use to verify the uninstallation status of the application signature package and the protocol bundle.

Required Privilege Level

maintenance

Output Fields

When you enter this command, you are shown the command to use to check the status of your uninstall request.

Sample Output

request services application-identification uninstall

```
user@host> request services application-identification uninstall
Please use command "request services application-identification uninstall
status" to check status and use command "request services application-
identification proto-bundle-status" to check protocol bundle status
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

RELATED DOCUMENTATION

request services application-identification install

request services application-identification uninstall status

IN THIS SECTION

- Syntax | 819
- Description | 819
- Required Privilege Level | 819
- Output Fields | 819
- Sample Output | 820
- Release Information | 820

Syntax

```
request services application-identification uninstall status
```

Description

Display the status of the uninstall operation. This command provides information on whether the uninstall operation succeeded or failed.

Required Privilege Level

maintenance

Output Fields

When you enter this command, the system provides feedback on whether the request succeeded or failed..

Sample Output

request services application-identification uninstall status

```
user@host> request services application-identification uninstall status
Uninstall application package version (1776) succeed.
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

RELATED DOCUMENTATION

request services application-identification uninstall

request unified-edge tdf call-trace clear

IN THIS SECTION

- Syntax | 820
- Description | 821
- Options | 821
- Required Privilege Level | 821
- Output Fields | 821
- Sample Output | 821
- Release Information | 821

Syntax

```
request unified-edge tdf call-trace clear
```

Description

Clear the completed or duplicate subscriber call traces on one or more TDF gateways.

Options

This command has no options.

Required Privilege Level

unified-edge

Output Fields

No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

request unified-edge tdf call-trace clear

```
user@host> request unified-edge tdf call-trace clear
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

request unified-edge tdf call-trace show | 822

request unified-edge tdf call-trace start | 826

request unified-edge tdf call-trace stop | 829

request unified-edge tdf call-trace show

IN THIS SECTION

- Syntax | 822
- Description | 822
- Options | 822
- Required Privilege Level | 823
- Output Fields | 823
- Sample Output | 824
- Release Information | 825

Syntax

```
request unified-edge tdf call-trace show
<all | completed | current>
<brief | detail>
```

Description

Display the information related to subscriber call tracing on one or more TDF gateways.

Options

none	(Same as brief) Display information related to subscriber call tracing in brief.
all | completed | current	(Optional) Display call trace information for the following: • **all**—All calls. • **completed**—Completed calls only. • **current**—Call traces that are currently active.
brief | detail	(Optional) Display the specified level of output.

Required Privilege Level

unified-edge

Output Fields

Table 14 on page 823 lists the output fields for the **request unified-edge tdf call-trace show** command. Output fields are listed in the approximate order in which they appear.

Table 14: request unified-edge tdf call-trace show Output Fields

Field Name	Field Description	Level of Output
Identifier	Identifier for the call trace.	All levels
File name	Name of the call trace file.	none **brief**
Trace file	Name of the call trace file.	**detail**
Status	Status of the call trace: • **done**—Call trace complete. • **not-done**—Call trace in progress. • **duplicate**—Another call trace record is present that has the same attributes.	All levels
SPIC Mask create	Internal mask of the services PIC where this call trace was enabled.	none **brief**
Create Mask	Internal mask of the services PIC where this call trace was enabled.	**detail**
SPIC Mask complete	Internal mask of the services PIC where this call trace was completed.	none **brief**

Table 14: request unified-edge tdf call-trace show Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Complete Mask	Internal mask of the services PIC where this call trace was completed.	**detail**
IMSI	International Mobile Subscriber Identity (IMSI) of the subscriber's user equipment (UE).	**detail**
MSISDN	Mobile station ISDN of the subscriber's user equipment.	
Calls Traced	Number of calls traced.	**detail**
Next Call	Number of next calls to be traced. For example, a value of 10 indicates that the next 10 calls are traced.	**detail**
TDF domain	TDF domain pertaining to the subscriber's call.	**detail**
FPC	FPC slot on which the call trace was enabled. This field is displayed only if the call trace is enabled on the FPC slot.	**detail**
PIC	PIC slot on which the call trace was enabled. This field is displayed only if the call trace is enabled on the PIC slot.	**detail**

Sample Output

request unified-edge tdf call-trace show brief

```
user@host> request unified-edge tdf call-trace show brief
  Identifier           File name           Status       SPIC Mask   SPIC Mask
                                                         create      complete
 call_trace_id_2 call_trace_id_2_02112012_060450        done 0x10   0x10
 call_trace_id_3 call_trace_id_3_02112012_070614        done 0x10   0x10
 call_trace_id_4 call_trace_id_4_02112012_071342   duplicate 0x0    0x0
 call_trace_id_5 call_trace_id_5_02112012_201317   duplicate 0x0    0x0
```

```
 call_trace_id_6 call_trace_id_6_02112012_201649   duplicate 0x0    0x0
 call_trace_id_7 call_trace_id_7_02112012_202501        done 0x0    0x0
 call_trace_id_8 call_trace_id_8_02112012_204718   duplicate 0x0    0x0
 call_trace_id_9 call_trace_id_9_02112012_204759    not-done 0x10   0x0
```

request unified-edge tdf call-trace show detail

```
user@host> request unified-edge tdf call-trace show detail
 Call trace information :

  Identifier : call_trace_id_13        Trace file :
call_trace_id_13_02292012_001343
  Status : not-done    Create Mask : 0x200      Complete Mask : 0x0
  IMSI : 29299
  Calls Traced : 0
  Identifier : call_trace_id_14        Trace file :
call_trace_id_14_02292012_001348
  Status : not-done    Create Mask : 0x200      Complete Mask : 0x0
                                                     MS-ISDN: 2929910000000000
  Calls Traced : 0
  Identifier : call_trace_id_15        Trace file :
call_trace_id_15_02292012_001408
  Status : not-done    Create Mask : 0x200      Complete Mask : 0x0
  Next Call : 1                        TDF domain : jnpr-sunnyvale
  Calls Traced : 0
  Identifier : call_trace_id_16        Trace file :
call_trace_id_16_02292012_001416
  Status : not-done    Create Mask : 0x200      Complete Mask : 0x0
  Calls Traced : 0                     FPC : 3   PIC : 1
  Identifier : call_trace_id_17        Trace file :
call_trace_id_17_02292012_001424
  Status : done        Create Mask : 0x200      Complete Mask : 0x200
  Next Call : 2
  Calls Traced : 2
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

request unified-edge tdf call-trace clear | 820
request unified-edge tdf call-trace start | 826
request unified-edge tdf call-trace stop | 829

request unified-edge tdf call-trace start

IN THIS SECTION

- Syntax | 826
- Description | 826
- Options | 827
- Required Privilege Level | 827
- Output Fields | 827
- Sample Output | 828
- Release Information | 828

Syntax

```
request unified-edge tdf call-trace start
<imsi imsi>
<msisdn msisdn>
<next-call next-call>
<routing-instance routing-instance>
<subscriber-name string>
<user-name string>
<v4-addr v4-addr>
<v6-addr v6-addr>
```

Description

Start TDF subscriber call tracing.

Options

none	Start call tracing for all TDF subscribers.
imsi *imsi*	(Optional) Start the call tracing for subscribers with the specified International Mobile Subscriber Identity (IMSI) number.
msisdn *msisdn*	(Optional) Start call tracing for subscribers with the specified Mobile station ISDN (MSIDSN) number.
next-call *next-call*	(Optional) Start call tracing for the specified number of next call events (1 through 50). For example, if you specify 10, then the next 10 calls are traced. **NOTE**: If you do not include the **next-call** keyword while tracing subscribers on a domain, the default value of 1 is used.
routing-instance *routing-instance*	(Optional) Start call tracing for subscribers for the specified routing instance.
subscriber-name *string*	(Optional) Start call tracing for the specified IFL-based subscriber.
user-name *string*	(Optional) Start call tracing for the specified IP-based subscriber.
v4-addr *v4-addr*	(Optional) Start call tracing for subscribers for the specified IPv4 address of the subscriber's user equipment (UE).
v6-addr *v6-addr*	(Optional) Start call tracing for subscribers for the specified IPv6 address of the subscriber's user equipment.

Required Privilege Level

unified-edge

Output Fields

Table 15 on page 828 lists the output fields for the **request unified-edge tdf call-trace start** command. Output fields are listed in the approximate order in which they appear.

Table 15: request unified-edge tdf call-trace start Output Fields

Field Name	Field Description
Session PIC	Identifier of the session PIC for which the call trace status is displayed.
Status	Status of the call trace: • **duplicate**—Another call trace record is present that has the same attributes. • **success**—Call trace started successfully. • **fail**—Call tracing cannot be started.

Sample Output

request unified-edge tdf call-trace start next-call

```
user@host> request unified-edge tdf call-trace start next-call 10
       Session PIC            Status
       ms-0/1/0             success
       ms-1/1/0             success
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

request unified-edge tdf call-trace clear | 820
request unified-edge tdf call-trace show | 822
request unified-edge tdf call-trace stop | 829

request unified-edge tdf call-trace stop

IN THIS SECTION

- Syntax | 829
- Description | 829
- Options | 829
- Required Privilege Level | 829
- Output Fields | 830
- Sample Output | 830
- Release Information | 830

Syntax

```
request unified-edge tdf call-trace stop
<all>
<identifier call-trace-identifier>
```

Description

Stop the previously configured subscriber call tracing on one or more TDF gateways.

Options

none	(Same as all) Stop all subscriber call tracing.
all	(Optional) Stop all subscriber call tracing.
identifier *call-trace-identifier*	(Optional) Stop call tracing for the specified call trace identifier.

Required Privilege Level

unified-edge

Output Fields

Table 16 on page 830 lists the output fields for the **request unified-edge tdf call-trace stop** command. Output fields are listed in the approximate order in which they appear.

Table 16: request unified-edge tdf call-trace stop Output Fields

Field Name	Field Description
Session PIC	Identifier of session PIC for which the call trace status is displayed.
Status	Status of the call trace: • **success**—Call trace stopped successfully. • **fail**—Call tracing cannot be stopped.

Sample Output

request unified-edge tdf call-trace stop

```
user@host> request unified-edge tdf call-trace stop
       Session PIC            Status
       ms-0/1/0              success
       ms-1/1/0              success
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

request unified-edge tdf call-trace clear | 820
request unified-edge tdf call-trace show | 822
request unified-edge tdf call-trace start | 826

show interfaces anchor-group (Aggregated Packet Forwarding Engine)

IN THIS SECTION

- Syntax | 831
- Description | 831
- Options | 831
- Required Privilege Level | 832
- Output Fields | 832
- Sample Output | 834
- Release Information | 835

Syntax

show interfaces anchor-group
<brief | detail>
interface-name

Description

Display interface information for the aggregated Packet Forwarding Engine group.

Options

none (Same as brief) Display a summary of the aggregated Packet Forwarding Engine interface information.

brief | detail (Optional) Display the specified level of output.

interface-name Name of the interface within the anchor Packet Forwarding Engine group.

> **NOTE**: The interface must be an aggregated Packet Forwarding Engine interface (apfe-).

Required Privilege Level

view

Output Fields

Table 17 on page 832 lists the output fields for the **show interfaces anchor-group** command. Output fields are listed in the approximate order in which they appear.

Table 17: show interfaces anchor-group Output Fields

Field Name	Field Description	Level of Output
Active	Anchor Packet Forwarding Engine is operational.	All levels
Inactive	Anchor Packet Forwarding Engine is not operational.	All levels
PF	Primary Packet Forwarding Engine anchor has failed.	All levels
MS	Primary Packet Forwarding Engine is protected by a secondary Packet Forwarding Engine in manually switched mode for primary role change.	All levels
HS	Primary Packet Forwarding Engine is protected by a secondary Packet Forwarding Engine in hot standby mode.	All levels
WS	Primary Packet Forwarding Engine is protected by a secondary Packet Forwarding Engine in warm standby mode.	All levels
Group	Name of the aggregated Packet Forwarding Engine group.	**brief** none
Mode	Redundancy mode in which the aggregated Packet Forwarding Engine group operates. Currently, only warm standby mode is supported.	**brief** none

Table 17: show interfaces anchor-group Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Sub-group ID	Redundancy subgroups within the anchor Packet Forwarding Engine group configuration that has FPCs as members. This is derived out of the Packet Forwarding Engines on a given FPC. For example, if the first Packet Forwarding Engine is assigned the number 0, then all the other Packet Forwarding Engines with sub-group ID 0 form the N:1 redundancy group.	**brief** none
Interface	Anchor Packet Forwarding Engine interface (**pfe-**).	All levels
Configured State	State in which the anchor Packet Forwarding Engine was configured. • **Primary**—Anchor Packet Forwarding Engine is in the pool of primary members. • **Secondary**—Anchor Packet Forwarding Engine is a backup to all the primary members.	All levels
Operational State	Indication whether the anchor Packet Forwarding Engine is operational (**Active**) or not operational (**Inactive**).	All levels
Redundancy State	Redundancy state (primary or secondary) in which the anchor Packet Forwarding Engine was configured.	All levels
Group Name	Name of the aggregated Packet Forwarding Engine group.	**detail**
Group Mode	Redundancy mode in which the aggregated Packet Forwarding Engine group operates. Currently, only warm standby mode is supported.	**detail**
Group Id	Internal ID generated for the group.	**detail**

Table 17: show interfaces anchor-group Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Switchover information	Switchover details, if any.	**detail**
Subgroup identifier	Number of redundancy subgroups within the anchor Packet Forwarding Engine group configuration that has FPCs as members. This is derived out of the Packet Forwarding Engines on a given FPC. For example, if the first Packet Forwarding Engine is assigned the number 0, then all the other Packet Forwarding Engines with subgroup ID 0 form the N:1 redundancy group.	**detail**

Sample Output

show interfaces anchor-group brief

```
user@host> show interfaces anchor-group brief
Redundancy Status Legend:

Active: Operational               Inactive: Non-operational
MS: Manually switched             PF: Primary failed
HS: Hot standby                   WS: Warm standby

Group     Mode  Sub-group  Interface  Configured  Operational    Redundancy
                   ID                    State       State          State

apfe0     WS       0       pfe-4/0/0  Primary     Active         Primary
                           pfe-5/0/0  Secondary   Active         Secondary
                   2       pfe-4/2/0  Primary     Active         Primary
                           pfe-5/2/0  Secondary   Active         Secondary
```

show interfaces anchor-group detail

```
user@host> show interfaces anchor-group detail
Active: Operational                Inactive: Non-operational
MS: Manually switched              PF: Primary failed
HS: Hot standby                    WS: Warm standby

Group Name: apfe0
  Group Mode: WS                         Group Id: 65
  Switchover information: None
  Interface pfe-4/2/0
    Configured state: Primary            Operational state: Active
    Redundancy state: Primary
    Subgroup identifier: 2
  Interface pfe-4/0/0
    Configured state: Primary            Operational state: Active
    Redundancy state: Primary
    Subgroup identifier: 0
  Interface pfe-5/0/0
    Configured state: Secondary          Operational state: Active
    Redundancy state: Secondary
    Subgroup identifier: 0
  Interface pfe-5/2/0
    Configured state: Secondary          Operational state: Active
    Redundancy state: Secondary
    Subgroup identifier: 2
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf system interfaces | 1059

show interfaces load-balancing (Aggregated Multiservices)

IN THIS SECTION

- Syntax | 836
- Description | 836
- Options | 836
- Required Privilege Level | 837
- Output Fields | 837
- Sample Output | 839
- Release Information | 841

Syntax

```
show interfaces load-balancing
<detail>
<interface-name>
```

Description

Display information about the aggregated multiservices interface (AMS) as well as its individual member interfaces and the status of the replication state.

Options

none	Display standard information about status of all AMS interfaces.
detail	(Optional) Display detailed status of all AMS interfaces.
interface-name	(Optional) Name of the aggregated multiservices interface (**ams**). If this is omitted, then the information for all the aggregated multiservices interfaces, including those used in control plane redundancy and high availability (HA) for service applications, is displayed.

Required Privilege Level

view

Output Fields

Table 18 on page 837 lists the output fields for the **show interfaces load-balancing** (aggregated multiservices interfaces) command. Output fields are listed in the approximate order in which they appear.

Table 18: Aggregated Multiservices show interfaces load-balancing Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the aggregated multiservices (AMS) interface.	**detail** none
State	Status of AMS interfaces: • **Coming Up**—Interface is becoming operational. • **Members Seen**—Member interfaces (mams) are available. • **Up**—Interface is configured and operational. • **Wait for Members**—Member interfaces (mams) are not available. • **Wait Timer**—Interface is waiting for member interfaces (mams) to come online.	**detail** none
Last change	Time (in *hh:mm:ss* [*hours:minutes:seconds*] format) when the state last changed.	**detail** none
Members	Number of member interfaces (mams-).	none specified
Member count	Number of member PICs (mams) that are part of the aggregated interface.	**detail** none

Table 18: Aggregated Multiservices show interfaces load-balancing Output Fields *(Continued)*

Field Name	Field Description	Level of Output
HA Model	High availability (HA) model supported on the interface. • **Many-to-One**—The preferred backup Multiservices PIC, in hot standby mode, backs up one or more (N) active Multiservices PICs. • **One-to-One**—–The preferred backup Multiservices PIC, in hot standby mode, backs up only one active Multiservices PIC. **NOTE**: **One-to-One** is not supported on MX-SPC3 cards.	**detail** none

Members	Information about the member interfaces:
	• **Interface**—Name of the member interface.
	• **Weight**—Not applicable for the current release.
	• **State**—State of the member interface (mams-).
	  • **Active**—Member is an active member.
	  • **Backup**—Member is a backup.
	  • **Discard**—Member has not yet rejoined the ams interface after failure.
	  • **Down**—Member has not yet powered on.
	  • **Inactive**—Member has failed to rejoin the ams interface within the configured **rejoin-timeout**.
	  • **Invalid**—Multiservices PIC corresponding to the member interface has been configured but is not physically present in the chassis.
		detail

Table 18: Aggregated Multiservices show interfaces load-balancing Output Fields *(Continued)*

Field Name	Field Description	Level of Output

Sync-state	Synchronization (sync) status of the control plane redundancy. The sync state is displayed only when the ams interface is **Up**.
	• **Interface**—Name of the member interface.
	• **Status**—Synchronization status of the member interfaces.
	  • **In progress**—The active member is currently synchronizing its state information with the backup member.
	  • **In sync**—The active member has finished synchronizing its state information with the backup and the backup is ready to take over if the active member fails.
	  • **NA (Not applicable)**—The backup member is not yet ready to synchronize with the active (primary) member. This condition may occur if the backup is still powered off or still booting.
	  • **Unknown**—The daemons are still initializing and the state information is unavailable.
		detail

Sample Output

show interfaces load-balancing

```
user@host> show interfaces load-balancing
Interface  State       Last change  Members  HA Model
ams0       Up          00:10:02     4        Many-to-One
```

show interfaces load-balancing detail

```
user@host> show interfaces load-balancing detail
Load-balancing interfaces detail
Interface        : ams0
```

```
  State          : Up
  Last change    : 00:10:23
  Member count   : 4
  HA Model       : Many-to-One
  Members        :
      Interface    Weight   State
      mams-4/0/0   10       Active
      mams-4/1/0   10       Active
      mams-5/0/0   10       Active
      mams-5/1/0   10       Backup
  Sync-state     :
      Interface    Status
      mams-4/0/0   Unknown
      mams-4/1/0   Unknown
      mams-5/0/0   Unknown
```

show interfaces load-balancing detail (Specific Interface)

```
user@host> show interfaces load-balancing ams0 detail
Load-balancing interfaces detail
Interface        : ams0
  State          : Up
  Last change    : 00:11:28
  Member count   : 4
  HA Model       : Many-to-One
  Members        :
      Interface    Weight   State
      mams-4/0/0   10       Active
      mams-4/1/0   10       Active
      mams-5/0/0   10       Active
      mams-5/1/0   10       Backup
  Sync-state     :
      Interface    Status
      mams-4/0/0   Unknown
      mams-4/1/0   Unknown
      mams-5/0/0   Unknown
```

Release Information

Command introduced in Junos OS Release 11.4.

interface-name option added in Junos OS Release 16.1.

Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces

Understanding Aggregated Multiservices Interfaces for Next Gen Services

Example: Configuring an Aggregated Multiservices Interface (AMS)

show services application-identification application

IN THIS SECTION

- Syntax | **841**
- Description | **842**
- Options | **842**
- Required Privilege Level | **842**
- Output Fields | **842**
- Sample Output | **844**
- Release Information | **850**

Syntax

```
show services application-identification application
<detail <application-name> | summary >
```

Description

Display detailed information about a specified application signature, all application signatures, or a summary of the existing application signatures and nested application signatures. Both custom and predefined application signatures and nested application signatures can be displayed.

Options

none	(Same as summary) Display a summary of the application identification application information.
detail <*application-name*> | summary	(Optional) Display the specified level of output.
application-name	(Optional) Display detailed information for the specified application name; maximum 31 characters. Predefined applications have the prefix **junos-** to avoid conflict with user-defined ones.

Required Privilege Level

view

Output Fields

Table 19 on page 842 lists the output fields for the **show services application-identification application** command. Output fields are listed in the approximate order in which they appear.

Table 19: show services application-identification application Output Fields

Field Name	Field Description	Level of Output
Application(s)	Number of applications present.	none **summary**
Application	Name of the predefined application.	none **summary**

Table 19: show services application-identification application Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Disabled	Status (**Yes** or **No**) of the application and whether the mapping method is currently used to identify this application.	none **summary**
Application ID	Unique ID number of an application. ID numbers 1 through 32,767 are automatically generated for predefined applications; these IDs do not change.	none **summary**
Order	Unique number used to specify priority when multiple applications match the traffic. The lowest order number takes the highest priority. The order attribute is applicable only for custom signatures.	none **summary**
Application Name	Name of the predefined application.	**detail**
Application type	Basic application type, such as HTTP.	**detail**
Description	Description of the predefined application.	**detail**
Number of Parent Group(s)	Number of parent groups associated with this application.	**detail**

Table 19: show services application-identification application Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Application Tags	Category specifying one or more following attributes of the application: **characteristic**: One or more characteristics of the application. **risk**: Level of risk of the application. **subcategory**: Subcategory of the application. **category**: Technology of the application.	**detail**
Layer-7 Protocol(s)	Layer 7 protocols associated with the application.	**detail**
Port Mapping Default port	Ports associated with the application.	**detail**
Signature	Signature mapping criteria for application identification: **Port range**, **Client-to-server**, and **Order**.	**detail**

Sample Output

show services application-identification application summary

```
user@host> show services application-identification application summary
Application(s): 2564
  Applications                                Disabled         ID      Order
  junos:DOT-NET                                No               10182   2564
  junos:ICMP-PHOTURIS-NEED-AUTHOR              No               11377   2563
  junos:MYSPACE-TAG-ME                         No               10683   2562
  junos:SLACKER                                No               1179    2561
  junos:ICMP-TYPE-55                           No               11392   2560
```

```
  junos:FLIPDRIVE-SSL                          No              10939   2559
  junos:ICMP-MOBILE-HOST-REDIR                 No              11363   2558
  junos:TWITPIC                                No              864     2557
  junos:ICMP-TYPE-245                          No              11582   2556
```

show services application-identification application detail

```
user@host> show services application-identification application detail
re0:
--------------------------------------------------------------------------
Application Name: junos:dot-net
Application type: DOT-NET
Description: .Net Remoting
Application ID: 10182
Disabled: No
Number of Parent Group(s): 1
Application Groups:
    junos:infrastructure:rpc
Port Mapping:
    Default ports: N/A
Signature:
    Port range: N/A
    Client-to-server
    Order: 1
Application Name: junos:icmp-photuris-need-author
Application type: ICMP-PHOTURIS-NEED-AUTHOR
Description: ICMP Type 40 Code 5 - Photuris (Need Authorization)
Application ID: 11377
Disabled: No
Number of Parent Group(s): 1
Application Groups:
    junos:infrastructure:networking
Port Mapping:
    Default ports: N/A
Signature:
    Port range: N/A
    Client-to-server
    Order: 5
Application Name: junos:myspace-tag-me
Application type: MYSPACE-TAG-ME
Description: This signature detects Tag Me by BitRhymes on MySpace Apps.  Tag
```

```
             Me by BitRhymes on MySpace Apps is a Web-based entertainment
             application on the popular social network MySpace.
Application ID: 10683
Disabled: No
Number of Parent Group(s): 1
Application Groups:
    junos:web:social-networking
Port Mapping:
    Default ports: N/A
Signature:
    Port range: N/A
    Client-to-server
    Order: 4
Application Name: junos:slacker
Application type: SLACKER
Description: This protocol plug-in classifies the http traffic to the host
             .slacker.com.
Application ID: 1179
Disabled: No
Number of Parent Group(s): 2
Application Groups:
    junos:multimedia:divers
    junos:multimedia
Port Mapping:
    Default ports: N/A
Signature:
    Port range: N/A
    Client-to-server
    Order: 3
Application Name: junos:icmp-type-55
Application type: ICMP-TYPE-55
Description: ICMP Type 55 - Unassigned
Application ID: 11392
Disabled: No
Number of Parent Group(s): 1
Application Groups:
    junos:infrastructure:networking
Port Mapping:
    Default ports: N/A
Signature:
    Port range: N/A
    Client-to-server
    Order: 2
```

```
Application Name: junos:flipdrive-ssl
Application type: FLIPDRIVE-SSL
Description: This signature detects logins to FlipDrive, a cloud-based
             file-sharing and backup service.
Application ID: 10939
Disabled: No
Number of Parent Group(s): 1
Application Groups:
    junos:web:file-sharing
Port Mapping:
    Default ports: N/A
Signature:
    Port range: N/A
    Client-to-server
    Order: 1
Application Name: junos:icmp-mobile-host-redir
Application type: ICMP-MOBILE-HOST-REDIR
Description: ICMP Type 32 - Mobile Host Redirect
Application ID: 11363
Disabled: No
Number of Parent Group(s): 1
Application Groups:
    junos:infrastructure:networking
Port Mapping:
    Default ports: N/A
Signature:
    Port range: N/A
    Client-to-server
    Order: 5
Application Name: junos:twitpic
Application type: TWITPIC
Description: This signature detects Twitpic, a Web site that allows users to
             easily post pictures to the Twitter microblogging and social media
             service.
Application ID: 864
Disabled: No
Number of Parent Group(s): 1
Application Groups:
    junos:web:social-networking
Port Mapping:
    Default ports: N/A
Signature:
    Port range: N/A
```

```
    Client-to-server
    Order: 4
Application Name: junos:icmp-type-245
Application type: ICMP-TYPE-245
Description: ICMP Type 245 - Unassigned
Application ID: 11582
Disabled: No
Number of Parent Group(s): 1
Application Groups:
    junos:infrastructure:networking
Port Mapping:
    Default ports: N/A
Signature:
    Port range: N/A
    Client-to-server
    Order: 3

---(more)---
```

show services application-identification application detail (Specific Application)

```
user@host> show services application-identification application detail junos:SKYPE
Application Name: junos:SKYPE
Application type: SKYPE
Description: This signature detects Skype, which is a proprietary P2P VOIP
             network. It is a "complete black box" for both users and
             analyzers. It uses security through obscurity to make itself
             troublesome to analyze or reverse-engineer without a significant
             amount of work, or use of emulation. It uses AES block cipher, the
             RSA public key cryptosystem, the ISO 9796-2 signature padding
             scheme, the SHA-1 hash function, and the RC4 stream cipher through
             the communications between the client to client, client to
             supernodes and supernode to supernode.
Application ID: 183
Disabled: No
Number of Parent Group(s): 1
Application Groups:
    junos:web:infrastructure:voip
Application Tags:
    characteristic        : Supports File Transfer
    characteristic        : Evasive
```

```
    characteristic        : Bandwidth Consumer
    risk                  : 4
    subcategory           : VOIP
    category              : Infrastructure
Layer-7 Protocol(s): UDP         / 216
                     TCP         / 205
                     SSL         / 199
                     HTTPS       / 68
                     HTTP        / 67
Port Mapping:
    Default ports: N/A
Signature:
    Port range: N/A
    Client-to-server
    Order: 20
```

show services application-identification application detail (Specific Application)

```
user@host> show services application-identification detail junos:http
re0:
--------------------------------------------------------------------------
Application Name: junos:http
Application type: HTTP
Description: This signature detects HyperText Transfer Protocol (HTTP), which
             is a protocol used by the World Wide Web. It defines how messages
             are formatted and transmitted and what actions Web servers and
             browsers should take in response to various commands. HTTP usually
             runs on TCP port 80.
Application ID: 67
Disabled: No
Number of Parent Group(s): 1
Application Groups:
    junos:web
Port Mapping:
    Default ports: TCP/80,3128,8000,8080
Signature:
    Port range: N/A
    Client-to-server
    Order: 3
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

request services application-identification install

request services application-identification application

show services application-identification application-system-cache

IN THIS SECTION

- Syntax | 850
- Description | 850
- Options | 851
- Required Privilege Level | 851
- Output Fields | 851
- Sample Output | 854
- Release Information | 856

Syntax

show services application-identification application-system-cache
<interface *interface-name*>

Description

Display the database of cached values stored by the application identification system.

NOTE: The **show services application-identification application-system-cache** command gives the information only when the application identifier (AI) is matched with the signature.

Options

none	Display the database of cached values for the all services interfaces.
interface ***interface-name***	(Optional) Display the database of cached values for the specified services interface.

Required Privilege Level

view

Output Fields

Table 20 on page 851 lists the output fields for the **show services application-identification application-system-cache** command. Output fields are listed in the approximate order in which they appear.

Table 20: show services application-identification application-system-cache Output Fields

Field Name	Field Description
application-cache	Status (**on** or **off**) of the application cache.
cache-entry-timeout	Number of seconds the mapping information is saved.
pic	PIC number of the accumulated statistics.
IP address	IP address of the traffic flow for which application-identification is enabled.
Port	Port number of the traffic flow for which application-identification is enabled.

Table 20: show services application-identification application-system-cache Output Fields *(Continued)*

Field Name	Field Description
Protocol	Protocol name of the flow for which application-identification is enabled.
Application	Application number, which is a unique identifier that denotes the application or service for which identification of traffic flows is enabled.
Classification Path	Protocols or nested applications that denote the paths traversed for classified packets.
PIC	PIC number of the accumulated statistics. For the interface on which deep packet inspection (DPI) application is not running, that detail is also displayed for the corresponding interface.
Unknown applications	Number of unknown applications.
Cache hits	Number of sessions that matched the application in the application identification cache.
Cache misses	Number of sessions that did not find the application in the application identification cache.
Client-to-server packets processed	Number of client-to-server packets processed.
Server-to-client packets processed	Number of server-to-client packets processed.
Client-to-server bytes processed	Number of client-to-server payload bytes processed.

Table 20: show services application-identification application-system-cache Output Fields *(Continued)*

Field Name	Field Description
Server-to-client layer bytes processed	Number of server-to-client payload bytes processed.
Client-to-server packets processed	Number of client-to-server packets processed.
Server-to-client packets processed	Number of server-to-client packets processed.
Client-to-server bytes processed	Number of client-to-server payload bytes processed.
Server-to-client layer bytes processed	Number of server-to-client payload bytes processed.
Sessions bypassed due to resource allocation failure	Number of sessions bypassed due to resource allocation failure.
Segment case 1 - New segment to left	Number of TCP segments contained before the previous segment.

Table 20: show services application-identification application-system-cache Output Fields *(Continued)*

Field Name	Field Description
Segment case 2 - New segment overlap right	Number of TCP segments that start before the previous segment and are contained in it.
Segment case 3 - Old segment overlapped	Number of TCP segments that start before the previous segment and extend beyond it.
Segment case 4 - New segment overlapped	Number of TCP segments that start and end within the previous segment.
Segment case 5 - New segment overlap left	Number of TCP segments that start within the previous segments and extend beyond it.
Segment case 6 - New segment to right	Number of TCP segments that start after the previous segment. This is the normal case.

Sample Output

show services application-identification application-system-cache

```
user@host> show services application-identification application-system-cache
Application System Cache Configurations:
  application-cache: on
  cache-entry-timeout: 3600 seconds
```

```
pic: ams0
pic: ms-0/3/0
ms-0/3/0 is not running DPI engine
pic: ams1
pic: ms-0/0/0
IP address: 192.0.2.2                                Port: 80     Protocol: TCP
Application: HTTP:YOUTUBE
Classification Path: IP:TCP:HTTP:YOUTUBE
```

show services application-identification application-system-cache interface

```
user@host> show services application-identification application-system-cache interface ms-1/0/0
Application System Cache Configurations:
  application-cache: on
  cache-entry-timeout: 3600 seconds
pic: ms-0/0/0
IP address: 192.0.2.2                                Port: 80     Protocol: TCP
Application: HTTP:YOUTUBE
Classification Path: IP:TCP:HTTP:YOUTUBE
user@host> show services application-identification counter

pic: ams0
ms-0/3/0 is not running DPI engine

pic: ams1
  Counter type                                                    Value
Unknown applications                                                32682
Cache hits                                                          323504
Cache misses                                                        400
Client-to-server packets processed                                  2034
Server-to-client packets processed                                  1982
Client-to-server bytes processed                                    258786
Server-to-client bytes processed                                    1314722
Sessions bypassed due to resource allocation failure                0
Segment case 1 - New segment to left                                0
Segment case 2 - New segment overlap right                          0
Segment case 3 - Old segment overlapped                             0
Segment case 4 - New segment overlapped                             0
Segment case 5 - New segment overlap left                           0
```

```
Segment case 6 - New segment to right                                    0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

request services application-identification application

show services application-identification counter

IN THIS SECTION

- Syntax | **856**
- Description | **856**
- Options | **857**
- Required Privilege Level | **857**
- Output Fields | **857**
- Sample Output | **858**
- Release Information | **859**

Syntax

show services application-identification counter
<interface *interface-name*>

Description

Display application identification counter statistics.

Options

none	Display counter statistics for all services interfaces.
interface *interface-name*	(Optional) Display counter statistics for the specified services interface.

Required Privilege Level

view

Output Fields

Table 21 on page 857 lists the output fields for the **show services application-identification counter** command. Output fields are listed in an approximate order in which they appear.

Table 21: show services application-identification counter Output Fields

Field Name	Field Description
PIC	PIC number of the accumulated statistics.
Unknown applications	Number of unknown applications.
Cache hits	Number of sessions that matched the application in the application identification cache.
Cache misses	Number of sessions that did not find the application in the application identification cache.
Client-to-server packets processed	Number of client-to-server packets processed.
Server-to-client packets processed	Number of server-to-client packets processed.
Client-to-server bytes processed	Number of client-to-server payload bytes processed.

Table 21: show services application-identification counter Output Fields *(Continued)*

Field Name	Field Description
Server-to-client layer bytes processed	Number of server-to-client payload bytes processed.
Sessions bypassed due to resource allocation failure	Number of sessions bypassed due to resource allocation failure.
Segment case 1 - New segment to left	Number of TCP segments contained before the previous segment.
Segment case 2 - New segment overlap right	Number of TCP segments that start before the previous segment and are contained in it.
Segment case 3 - Old segment overlapped	Number of TCP segments that start before the previous segment and extend beyond it.
Segment case 4 - New segment overlapped	Number of TCP segments that start and end within the previous segment.
Segment case 5 - New segment overlap left	Number of TCP segments that start within the previous segments and extend beyond it.
Segment case 6 - New segment to right	Number of TCP segments that start after the previous segment. This is the normal case.

Sample Output

show services application-identification counter

```
user@host> show services application-identification counter


pic: 5/0
```

```
  Counter type                                                    Value
 Unknown applications                                                0
 Cache hits                                                          0
 Cache misses                                                       36
 Client-to-server packets processed                                 16
 Server-to-client packets processed                                101
 Client-to-server bytes processed                                 3494
 Server-to-client bytes processed                               112493
 Sessions bypassed due to resource allocation failure                0
 Segment case 1 - New segment to left                               11
 Segment case 2 - New segment overlap right                          8
 Segment case 3 - Old segment overlapped                             0
 Segment case 4 - New segment overlapped                             0
 Segment case 5 - New segment overlap left                           0
 Segment case 6 - New segment to right                               7

pic: 5/1
  Counter type                                                    Value
 Unknown applications                                                0
 Cache hits                                                          0
 Cache misses                                                        0
 Client-to-server packets processed                                  0
 Server-to-client packets processed                                  0
 Client-to-server bytes processed                                    0
 Server-to-client bytes processed                                    0
 Sessions bypassed due to resource allocation failure                0
 Segment case 1 - New segment to left                                0
 Segment case 2 - New segment overlap right                          0
 Segment case 3 - Old segment overlapped                             0
 Segment case 4 - New segment overlapped                             0
 Segment case 5 - New segment overlap left                           0
 Segment case 6 - New segment to right                               0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

show services application-identification group

IN THIS SECTION

- Syntax | 860
- Description | 860
- Options | 860
- Required Privilege Level | 861
- Output Fields | 861
- Sample Output | 862
- Release Information | 865

Syntax

```
show services application-identification group [detail application-group name |
summary]
```

Description

Display detailed or summary information about a specified application signature group or all application signature groups. Both custom and predefined application signature groups can be displayed.

Options

none	Display summary information for all application signature groups.
detail | summary	Display the specified level of output.

application-name Application name; maximum 31 characters. Predefined applications have the prefix **junos-** to avoid conflict with user-defined ones.

Required Privilege Level

view

Output Fields

Table 22 on page 861 lists the output fields for the **show services application-identification group** command. Output fields are listed in the approximate order in which they appear.

Table 22: show services application-identification group Output Fields

Field Name	Field Description	Level of Output
Group ID	Unique ID number of an application signature group. ID numbers 1 through 32,767 are automatically generated for predefined application signatures and application signature groups; these IDs do not change. ID numbers for custom application signatures and application signature groups use ID numbers 32,768 through 65,534.	none **detail** **summary**
Disabled	Status of the application signature group and whether the signature method is currently used to identify this application. The default is No.	none **summary**
Application Group(s)	Number of application signature groups present.	none **summary**

Table 22: show services application-identification group Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Applications	Names of application signatures associated with this application signature group.	none **detail** **summary**
Group Name	Name of an application signature or application signature group.	**detail**
Description	Description of the specified application in the detailed display. If a description is not previously specified, **N/A** is displayed for this field.	**detail**
Number of Applications	Total number of applications contained in the group.	**detail**
Number of Sub-Groups	Total number of sub-groups associated with this application signature group.	**detail**
Number of Parent-Groups	Total number of parent groups in this application signature group or cluster.	**detail**
Sub-Group(s)	Application signature sub-groups present.	**detail**

Sample Output

show services application-identification group summary

```
user@host> show services application-identification group summary

Application Group(s): 66
```

```
Application Groups                                  Disabled  ID
  junos:web:social-networking:facebook               No        68
  junos:web:reference                                No        67
  junos:infrastructure:legacy                        No        66
  junos:web:cdn                                      No        65
  junos:infrastructure:scada                         No        64
  junos:web:real-estate                              No        63
  junos:web:finance                                  No        62
  junos:multimedia:audio-streaming                   No        61
  junos:web:remote-access                            No        60
  junos:web:p2p                                      No        59
  junos:remote-access:backdoors                      No        58
  junos:infrastructure:authentication                No        57
  junos:web:forums                                   No        56
  junos:remote-access:command                        No        55
  junos:infrastructure:scm                           No        54
  junos:web:portal                                   No        53
  junos:web:shopping                                 No        52
  junos:infrastructure:rpc                           No        51
  junos:messaging:mail                               No        50
  junos:web:search                                   No        49
  junos:infrastructure:encryption                    No        48
  junos:gaming:divers                                No        47
  junos:p2p:file-sharing                             No        46
  junos:infrastructure:backup                        No        45
  junos:multimedia:transport                         No        44
  junos:gaming:protocols                             No        43
  junos:web:advertisements                           No        42
  junos:infrastructure:monitoring                    No        41
  junos:infrastructure:mobile                        No        40
  junos:infrastructure:file-servers                  No        39
  junos:web:infrastructure                           No        38
  junos:web:wiki                                     No        37
  junos:web:image-sharing                            No        36
  junos:infrastructure:directory                     No        35
  junos:infrastructure:database                      No        34
  junos:remote-access:tunneling                      No        33
  junos:remote-access:interactive-desktop            No        32
  junos:web:gaming                                   No        31
  junos:web:anonymizer                               No        30
  junos:web:blogging                                 No        29
  junos:remote-access:divers                         No        28
  junos:remote-access                                No        27
```

```
  junos:p2p:divers                                No        26
  junos:p2p                                       No        25
  junos:web:news                                  No        24
  junos:gaming:web-based                          No        23
  junos:gaming                                    No        22
  junos:web:messaging                             No        21
  junos:multimedia:web-based                      No        20
  junos:web:file-sharing                          No        19
  junos:web:travel                                No        18
  junos:multimedia:video-streaming                No        17
  junos:messaging:instant-messaging               No        16
  junos:web:multimedia                            No        15
  junos:infrastructure:voip                       No        14
  junos:messaging:divers                          No        13
  junos:messaging                                 No        12
  junos:web:applications                          No        11
  junos:multimedia:divers                         No        10
  junos:multimedia                                No        9
  junos:web:divers                                No        8
  junos:web:social-networking                     No        7
  junos:web                                       No        6
  junos:infrastructure:networking                 No        5
  junos:infrastructure:divers                     No        4
  junos:infrastructure                            No        3
```

show services application-identification group detail

```
user@host> show services application-identification group detail junos:social-networking
Group Name: junos:web
Group ID: 15
Description: N/A
Disabled: No
Number of Applications: 1
Number of Sub-Groups: 21
Number of Parent-Groups: 1
Applications:
    junos:http
Sub Groups:
    junos:web:forums
    junos:web:travel
    junos:web:reference
```

```
    junos:web:portal
    junos:web:blogging
    junos:web:shopping
    junos:web:search
    junos:web:anonymizer
    junos:web:image-sharing
    junos:web:file-sharing
    junos:web:remote-access
    junos:web:real-estate
    junos:web:news
    junos:web:gaming
    junos:web:p2p
    junos:web:applications
    junos:web:multimedia
    junos:web:divers
    junos:web:messaging
    junos:web:social-networking
    junos:web:infrastructure
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

request services application-identification group

show services application-identification statistics application-groups

IN THIS SECTION

- Syntax | 866
- Description | 866

- Options | 866
- Required Privilege Level | 866
- Output Fields | 866
- Sample Output | 867
- Release Information | 867

Syntax

```
show services application-identification statistics application-groups
```

Description

Display cumulative session and byte statistics per application group. Statistics are displayed in alphabetical order.

Options

This command has no options.

Required Privilege Level

view

Output Fields

Table 23 on page 867 lists the output fields for the **show services application-identification statistics application-groups** command. Output fields are listed in the approximate order in which they appear.

Table 23: show services application-identification statistics application-groups Output Fields

Field Name	Field Description
Last Reset	Date, time, and how long ago the statistics for the sessions were cleared. The format None specified is *year-month-day hour:minute:second timezone*. If you did not clear the statistics previously at any point, **Never** is displayed.
Application Group	Name of the application group.
Sessions	Number of sessions for the application group.
Kilo Bytes	Size of the application group in kilobytes.

Sample Output

show services application-identification statistics application-groups

```
user@host> show services application-identification statistics application-groups

Last Reset: 2014-02-19 00:38:01 PST
                Application Group           Sessions         Kilo Bytes
             junos:infrastructure                  2                 18
  junos:infrastructure:monitoring                  2                 18
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

RELATED DOCUMENTATION

clear services application-identification statistics

show services application-identification statistics applications

IN THIS SECTION

- Syntax | 868
- Description | 868
- Options | 868
- Required Privilege Level | 868
- Output Fields | 868
- Sample Output | 869
- Release Information | 869

Syntax

```
show services application-identification statistics applications
```

Description

Display cumulative session and byte statistics per application. Statistics are displayed in alphabetical order.

Options

This command has no options.

Required Privilege Level

view

Output Fields

Table 24 on page 869 lists the output fields for the **show services application-identification statistics applications** command. Output fields are listed in the approximate order in which they appear.

Table 24: show services application-identification statistics applications Output Fields

Field Name	Field Description
Last Reset	Date, time, and how long ago the statistics for the sessions were cleared in the format *year-month-day hour:minute:second timezone* . If you did not clear the statistics previously at any point, **Never** is displayed.
Application	Name of the application.
Sessions	Number of sessions for the application.
Bytes	Size of the application in bytes.

Sample Output

show services application-identification statistics applications

```
user@host> show services application-identification statistics applications

Last Reset: 2014-01-26 18:32:36 PST
         Application           Sessions              Bytes
          junos:http                  4              24009
          junos:https                 1             101823
          junos:hulu                  1              48329
      junos:linkedin                  1               2650
       junos:netflix                  2              32747
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

RELATED DOCUMENTATION

clear services application-identification statistics

show services application-identification status

IN THIS SECTION

- Syntax | 870
- Description | 870
- Required Privilege Level | 870
- Output Fields | 870
- Sample Output | 872
- Release Information | 873

Syntax

```
show services application-identification status
```

Description

Display detailed information about application identification status.

Required Privilege Level

view

Output Fields

Table 25 on page 871 lists the output fields for the **show services application-identification status** command. Output fields are listed in the approximate order in which they appear.

Table 25: show services application-identification status Output Fields

Field Name	Field Description
Application Identification	Details of the application-identification engine and the processing details of sessions.
Status	Status of application identification: **Enabled** or **Disabled**.
Sessions under app detection	Number of sessions undergoing application identification detection.
Engine Version	Application identification detector engine version.
Max TCP session packet memory	Maximum number of TCP sessions that application identification maintains.
Force packet plugin	Force packet plugin status: **Enabled** or **Disabled**.
Force stream plugin	Force stream plugin status: **Enabled** or **Disabled**.
Statistics collection interval	Frequency (in minutes) for collecting statistics.
Application System Cache	Details of entries in the application system cache.
Status	Status of application system cache: **Enabled** or **Disabled**.
Max Number of entries in cache	Maximum number of cache entries.
Cache timeout	Number of seconds after which the cache entries expires.
Protocol Bundle	Information regarding application package downloads.

Table 25: show services application-identification status Output Fields *(Continued)*

Field Name	Field Description
Download Server CGI	URL of the server from where protocol bundle was downloaded.
Auto Update	Status of auto update to receive protocol bundle updates from the server: **Enabled** or **Disabled**.
Slot	Number of the slot pertaining to the packets for which application-identification is associated.
Status	Status of protocol bundle: **Active** or **Free**.
Version	Version of protocol bundle.
Session	Number of active sessions.

Sample Output

show services application-identification status

```
user@host> show services application-identification status
pic: 5/0

Application Identification
 Status                          Enabled
 Sessions under app detection    0
 Engine Version                  4.18.1-20 (build date Feb 15 2014)
 Max TCP session packet memory   30000
 Force packet plugin             Disabled
 Force stream plugin             Disabled
 Statistics collection interval  1 (in minutes)

Application System Cache
 Status                          Enabled
 Max Number of entries in cache  131072
```

```
 Cache timeout                    3600 (in seconds)

Protocol Bundle
 Download Server                  https://services.netscreen.com/cgi-bin/
index.cgi
 AutoUpdate                       Disabled
Slot 1:
 Status                           Active
 Version                          1.30.4-22.005 (build date Jan 17 2014)
 Sessions                         0
Slot 2
 Status                           Free
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

RELATED DOCUMENTATION

Application Identification Overview

Configuring Custom Application Signatures

request services application-identification application

show services application-identification version

IN THIS SECTION

- Syntax | **874**
- Description | **874**
- Required Privilege Level | **874**
- Sample Output | **874**
- Release Information | **874**

Syntax

```
show services application-identification version
```

Description

Display the Junos OS application package version.

Required Privilege Level

view

Sample Output

show services application-identification version

```
user@host> show services application-identification version
Application package version: 1608
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

request services application-identification download

show services ha detail

IN THIS SECTION

- Syntax | 875
- Description | 875

- Options | 875
- Required Privilege Level | 875
- Output Fields | 875
- Sample Output | 877
- Release Information | 877

Syntax

```
show services ha detail
<interface interface-name>
```

Description

Display detailed information for stateful sync processing for a specified interface or for all interfaces.

Options

none	Display detailed information for stateful sync processing for all interfaces.
interface-name	(Optional) Name of a specific interface.

Required Privilege Level

view

Output Fields

Table 26 on page 876 lists the output fields for the **show services ha detail** command. Output fields are listed in the approximate order in which they appear.

Table 26: show services ha detail Output Fields

Field Name	Field Description
Interface	Name of the interface for which information is reported.
Inter-chassis	
Role	Role of the interface. • **active**—Active interface. • **backup**–Backup interface.
Connection	Status of the peer connection. • Up • Down
Synchronization	Synchronization state of peers. • Off–Peers are not currently engaged in synchronization.. • Cold–Peers are in a pre-synchronization state. • Hot—Peers are ready for synchronization.
Peers	
Local	Local peer IP address.
Port	Local peer port number.
Remote	Remote peer IP address.
Port	Remote peer port number.

Sample Output

show services ha detail

```
user@host> show services ha detail
Interface:        ms-7/0/0
Inter-chassis:    Role: active, Connection: Up, Synchronization: Hot
Peers:            Local: 192.0.2.1 Port: 4001, Remote: 192.0.2.2 Port: 4001

Interface:        ms-7/1/0
Inter-chassis:    Role: active, Connection: Down, Synchronization: Off
Peers:            Local: 198.51.100.1 Port: 4001, Remote: 198.51.100.2 Port: 4001

Interface:        ms-8/0/0
Inter-chassis:    Role: active, Connection: Up, Synchronization: Cold
Peers:            Local: 203.0.113.1 Port: 4001, Remote: 203.0.113.2 Port: 4001

Interface:        ms-8/1/0
Inter-chassis:    Role: active, Connection: Up, Synchronization: Hot
Peers:            Local: 10.10.10.1 Port: 4001, Remote: 10.10.10.2 Port: 4001
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

> *Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) Overview (Release 16.1 and later)*

show services ha statistics

IN THIS SECTION

Syntax | 878

- Description | 878
- Options | 878
- Required Privilege Level | 878
- Output Fields | 878
- Sample Output | 884
- Release Information | 885

Syntax

```
show services ha statistics
<interface interface-name>
```

Description

Display detailed statistics for stateful sync processing for a specified interface or for all interfaces.

Options

none	Display detailed statistics for stateful sync processing for all interfaces.
interface-name	(Optional) Name of a specific interface.

Required Privilege Level

view

Output Fields

Table 27 on page 879 lists the output fields for the **show services ha statistics** command. Output fields are listed in the approximate order in which they appear.

Table 27: show services ha statistics Output Fields

Field Name	Field Description
Interface	Interface name.
Inter-chassis	
Role	Role of the interface. • **active**—Active interface. • **backup**–Backup interface.
Connection	Status of the peer connection. • Up • Down
Synchronization	Synchronization state of peers. • Off–Peers are not currently engaged in synchronization. • Cold–Peers are in a pre-synchronization state. • Hot—Peers are ready for synchronization.
Peers	
Local	Local peer IP address.
Port	Local peer port number.
Remote	Remote peer IP address.
Port	Remote peer port number.
Connection Status	

Table 27: show services ha statistics Output Fields *(Continued)*

Field Name	Field Description
TCP connection establish	Number of times a TCP connection is established.
TCP connection teardown	Number of times a TCP connection is torn down.
UDP address exchange sent	Number of times a UDP address is sent.
Stateful sync start sent	Number of stateful sync start messages sent by the backup PIC, indicating the start of the cold sync phase.
Stateful sync start received	Number of stateful sync start messages received by active PIC, indicating the start of the cold sync phase.
Cold sync completed count	Number of times the PIC has successfully completed the cold sync phase.
Session Add Statistics	
Sent	Number of session add statistics sent by the active PIC.
Received	Number of session add statistics received by the backup PIC.
Completed	Number of session adds completed on the active and backup PICs.
rate	Number of sessions currently added per second.
Nack sent	Number of times that a session add failed on the backup PIC, resulting in the sending of a Nack message to the active PIC.
Nack received	Number of Nack messages received from backup PIC due to session add failure.

Table 27: show services ha statistics Output Fields *(Continued)*

Field Name	Field Description
Add pending	Number of sessions eligible for synchronization, but not yet synchronized.
Session Delete Statistics	
Sent	Number of session deletes sent by the active PIC.
Received	Number of session deletes received by the backup PIC.
Completed	Number of session deletes completed on the active and backup PICs.
rate	Number of sessions currently deleted per second.
Nack sent	Number of times that a session add failed on the backup PIC, resulting in the sending of a Nack message to the active PIC.
Nack received	Number of Nack messages received from backup PIC due to session add failure.
Session not found	Number of sessions not found when session delete was attempted.
Session Error Statistics	
Session attach failures	Number of high-availability extension creation failures on the active PIC.
Session detach failures	Number of high-availability extension deletion failures on the active PIC.

Table 27: show services ha statistics Output Fields *(Continued)*

Field Name	Field Description
Session extension get failures	Number of times that the high-availability extension is not available when requested.
Session nullify	Number of times the high-availability session creation failed on the active PIC.
Lookup fail	Number of times session lookup failed because the session has already been released by the infrastructure.
Initiate fail	Number of times session creation failed on the backup PIC.
Activate fail	Number of times session activation failed on the backup PIC.
Illegal flow type	Number of times an illegal flow type occurred on the active and backup PICs.
Illegal service set	Number of times service set extraction failed on backup and active PICs.
Unsupported protocol	Number of times that a session was not backed up because the protocol was neither TCP or UDP.
Send overflow	Number of times buffer overflowed when the high-availability session was created on the active PIC.
Send discard	Number of sessions that not synchronized to the backup, even though they were eligible for synchronization. This occurs whe at least one plugin in the service set indicates that a session should not be synchronized.

Table 27: show services ha statistics Output Fields *(Continued)*

Field Name	Field Description
Spurious	Number of packets received on the backup PIC for which there are no existing sessions
Process incoming failed	Number of times JMUX header processing failed.
Session ignored	Number of sessions that were eligible for synchronization, but are ignored because stateful sync is not supported for them, such as ALG sessions
JMUX Error Statistics	Synchronization statistics related to the JMUX library.
JMUX begin fail	Number of times that JMUX key verification or header creation failed.
JMUX commit fail	Number of times addition of JMUX data failed.
JMUX flush fail	Number of times a send of JMUX data failed.
Invalid plugin header	Number of times stateful sync messages were rejected due to an invalid plugin header (internal error).
Invalid plugin name	Number of times stateful sync messages were rejected due to an invalid plugin name (internal error).
Invalid plugin length	Number of times stateful sync messages were rejected due to invalid plugin length (internal error).
Plugin receive error	Number of times installation of plugin information failed on the backup.
Plugin send error	Number of times the plugin failed to pack the extension.

Table 27: show services ha statistics Output Fields *(Continued)*

Field Name	Field Description
IDL Error Statistics	Statistics concerning encode or decode errors at the backup.
IDL encode fail	Number of times IDL encoding failed on the active and backup PICs.
IDL decode fail	Number of times IDL decoding failed on the active and backup PICs.

Sample Output

show services ha statistics

```
user@host> show services ha statistics
Interface:        ms-5/0/0
Inter-chassis:    Role: active, Connection: Up, Synchronization: Hot
Peers:            Local: 192.0.2.2 Port: 4001, Remote: 192.0.2.1 Port: 4001
Connection Status:
    TCP connection establish: 8, Teardown: 8
    UDP address exchange sent: 8, Received: 8
    Stateful sync start sent: 0, Received: 8
    Cold sync completed count: 0
Session Add Statistics:
    Sent: 255, Received: 0
    Completed: 255, Rate: 0
    Nack sent: 0, Nack received: 0
    Add pending: 0
Session Delete Statistics:
    Sent: 255, Received: 0
    Completed: 255, Rate: 0
    Nack sent: 0, Nack received: 0
    Session not found: 0
Session Error Statistics:
   Session attach failures: 0, Session detach failures: 0
    Session extension get failures: 0, Session nullify: 0
```

```
    Lookup fail: 0, Initiate fail: 0, Activate fail: 0
    Illegal flow type: 0, Illegal service set: 0
    Unsupported protocol: 0, Send overflow: 0, Send discard: 0
    Spurious: 0, Process incoming failed: 0, Session ignored: 0
JMUX Error Statistics:
    JMUX begin fail: 0, JMUX commit fail: 0, JMUX flush fail: 0
    Invalid plugin header: 0, Invalid plugin name: 0
    Invalid plugin length: 0, Plugin receive error: 0, Plugin send error: 0
IDL Error Statistics:
    IDL encode fail: 0, IDL decode fail: 0
```

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) Overview (Release 16.1 and later)

show services hcm statistics

IN THIS SECTION

- Syntax | 886
- Description | 886
- Options | 886
- Required Privilege Level | 886
- Output Fields | 886
- Sample Output | 887
- Release Information | 887

Syntax

```
show services hcm statistics rule rule-name
```

Description

Display the statistics collected for HTTP header enrichment for a specified tag rule.

NOTE: This command displays output only if the **count** statement is configured for the term in a tag rule at the **[edit services hcm tag-rule *rule-name* term *term-name* then]** hierarchy level.

If you change the configuration of tag rules during an existing subscriber data session and commit the change, the tag rule statistics are reset to 0 and stop incrementing for the existing TCP sessions.

Options

none	Display detailed statistics about stateful sync processing for all interfaces.
rule *rule-name*	Display statistics for the specified tag rule.

Required Privilege Level

view

Output Fields

Table 28 on page 886 lists the output fields for the **show services hcm statistics** command. Output fields are listed in the approximate order in which they appear.

Table 28: show services hcm statistics Output Fields

Field Name	Field Description
Interface	Name of the interface for which the statistics are displayed.

Table 28: show services hcm statistics Output Fields *(Continued)*

Field Name	Field Description
Term id	Identifier for the term (in the tag rule) for which the statistics are displayed.
Hits	Number of times that the term was matched. This field displays the aggregate number of occurrences in service sets that include the term.

Sample Output

show services hcm statistics rule

```
user@host> show services hcm statistics rule rule1
Interface: mams-3/1/0
Term id              Hits
1                   58
Interface: mams-4/1/0
Term id              Hits
1                   144
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- count (HTTP Header Enrichment) | 344
- Configuring HTTP Header Enrichment Overview | 41
- show services hcm pic-statistics | 888

show services hcm pic-statistics

IN THIS SECTION

- Syntax | 888
- Description | 888
- Options | 888
- Required Privilege Level | 888
- Output Fields | 889
- Sample Output | 893
- Sample Output | 894
- Release Information | 896

Syntax

```
show services hcm pic-statistics
<interface interface-name>
```

Description

Display the statistics collected (from the services PICs) for HTTP header enrichment.

Options

none	Display the statistics for all the services PICs.
interface *interface-name*	(Optional) Display the statistics for the specified services PIC.

Required Privilege Level

view

Output Fields

Table 29 on page 889 lists the output fields for the **show services hcm pic-statistics** command. Output fields are listed in the approximate order in which they appear.

Table 29: show services hcm pic-statistics Output Fields

Field Name	Field Description
Interface	Name of the services PIC interface for which statistics are displayed.
Session statistics—For each services PIC.	
Number of Session Interest events	Number of Session Interest events.
Number of Session Create events	Number of Session Create events.
Number of Session Close events	Number of Session Close events.
Number of Session Destroy events	Number of Session Destroy events.
Number of Session Data events	Number of Session Data events.
Number of Session Handle failures	Number of Session Handle failures.
Number of Session Extension allocations	Number of Session Extension allocations that were successful.
Number of Session Extension alloc failures	Number of Session Extension allocations that failed.
Number of Session Extension frees	Number of Session Extension frees (memory releases).
TCP Proxy statistics	

Table 29: show services hcm pic-statistics Output Fields *(Continued)*

Field Name	Field Description
Number of missing stbuf	Number of missing stream buffers.
Number of stbuf initializations	Number of stream buffer initializations that were successful.
Number of stbuf initialization failures	Number of stream buffer initializations that failed.
Number of stbuf store failures	Number of stream buffer store failures.
Number of stbuf frees	Number of stream buffer frees (memory releases) that were successful.
Number of stbuf free failures	Number of stream buffer frees that failed.
Number of stbuf sends	Number of stream buffer sends that were successful.
Number of stbuf send failures	Number of stream buffer sends that failed.
Number of stbuf receives	Number of stream buffer receives that were successful.
Number of stbuf throttles	Number of stream buffer throttles. Throttles are done when the stream buffer queue is full.
Number of invalid stbuf	Number of invalid stream buffers.
THR statistics	
Number of THR creates	Number of successful TCP Header Rewriter (THR) Create Requests.

Table 29: show services hcm pic-statistics Output Fields *(Continued)*

Field Name	Field Description
Number of missing THR handles	Number of missing THR handles.
Number of THR create failures	Number of THR Create Requests that failed.
Number of THR store failures	Number of THR store failures.
Number of THR short circuit failures	Number of THR short circuit (packet bypass) failures.
Number of THR update failures	Number of THR updates that failed.
Number of THR state updates	Number of THR state updates.
Number of THR destroy failures	Number of THR destroys that failed.
Number of THR destroys	Number of THR Cleanup Requests that were successful.
JCPP statistics	
Number of JCPP handle allocations	Number of Juniper Content and Protocol Parsers (JCPP) handle allocations that were successful.
Number of JCPP handle allocation failures	Number of JCPP handle allocations that failed.
Header Insertion statistics	
Number of HCM Header Insertions	Number of times that tags were successfully inserted into HTTP headers.

Table 29: show services hcm pic-statistics Output Fields *(Continued)*

Field Name	Field Description
Number of HCM Header Insertion failures	Number of times that the insertion of tags into HTTP headers failed.
Number of HCM Header Renamed	Number of times that HTTP headers were successfully renamed.
Number of HCM Header Rename failures	Number of times that HTTP header rename attempts failed.
Number of HCM IPV4 Mask modifications	Number of times IPv4 address mask was inserted.
Number of HCM IPV6 Mask modifications	Number of times IPv6 address mask was inserted.
Number of HCM Tags too large	Number of tags that were not inserted into HTTP headers because the tag size was larger than the maximum allowed size.
Number of HCM Tag encryption failures	Number of times that the encryption of HTTP tags used for header insertion failed.
Number of HCM requests	Number of HTTP header enrichment requests.
Number of missing Subscribers in HCM	Number of times that tags were not inserted because subscriber was missing.
Number of HCM missing subscriber attributes	Number of times that tags were not inserted because subscriber attributes were missing.

Table 29: show services hcm pic-statistics Output Fields *(Continued)*

Field Name	Field Description
Number of HCM missing IPV4 attributes	Number of times that tags were not inserted because subscriber IPv4 user address attributes were missing.
Number of HCM missing IPV6 attributes	Number of times that tags were not inserted because subscriber IPv6 user address attributes were missing.
Number of HCM IPV4 / IPV6 tag insertions	Number of times that an IPv4 or an IPv6 user address tag was successfully inserted into HTTP headers when the tag rule included both IPv4 and IPv6 user address tags.

Sample Output

show services hcm pic-statistics (mams interface)

```
user@host> show services hcm pic-statistics
Interface: mams-3/0/0
Session statistics
    Number of Session Interest events              :224590
    Number of Session Create events                :224590
    Number of Session Close events                 :224590
    Number of Session Destroy events               :224590
    Number of Session Data events                  :224589
    Number of Session Handle failures              :0
    Number of Session Extension allocations        :224590
    Number of Session Extension alloc failures     :0
    Number of Session Extension frees              :224590
TCP Proxy statistics
    Number of missing stbuf                        :0
    Number of stbuf initializations                :0
    Number of stbuf initialization failures        :0
    Number of stbuf store failures                 :0
    Number of stbuf frees                          :0
    Number of stbuf free failures                  :0
    Number of stbuf sends                          :0
```

```
    Number of stbuf send failures                   :0
    Number of stbuf receives                        :0
    Number of stbuf throttles                       :0
    Number of invalid stbuf                         :0
THR statistics
    Number of THR creates                           :224590
    Number of missing THR handles                   :0
    Number of THR create failures                   :0
    Number of THR store failures                    :0
    Number of THR short circuit failures            :0
    Number of THR update failures                   :0
    Number of THR state updates                     :449180
    Number of THR destroy failures                  :0
    Number of THR destroys                          :0
JCPP statistics
    Number of JCPP handle allocations               :0
    Number of JCPP handle allocation failures       :0
Header Insertion statistics
    Number of HCM Header Insertions                 :224589
    Number of HCM Header Insertion failures         :0
    Number of HCM Header Renamed                    :0
    Number of HCM Header Rename failures            :0
    Number of HCM IPV4 Mask modifications           :0
    Number of HCM IPV6 Mask modifications           :0
    Number of HCM Tags too large                    :0
    Number of HCM Tag encryption failures           :0
    Number of HCM requests                          :224589
    Number of missing Subscribers in HCM            :0
    Number of HCM missing subscriber attributes     :0
    Number of HCM missing IPV4 attributes           :0
    Number of HCM missing IPV6 attributes           :0
    Number of HCM IPV4 / IPV6 tag insertions        :0
```

Sample Output

show services hcm pic-statistics (vms- interface)

```
user@host> show services hcm pic-statistics
Interface: vms-5/2/0
Session statistics
```

```
    Number of Session Interest events               :90064
    Number of Session Create events                 :90064
    Number of Session Close events                  :90064
    Number of Session Destroy events                :90064
    Number of Session Data events                   :90064
    Number of Session Handle failures               :0
    Number of Session Extension allocations         :90064
    Number of Session Extension alloc failures      :0
    Number of Session Extension frees               :90064
TCP Proxy statistics
    Number of missing stbuf                         :0
    Number of stbuf initializations                 :0
    Number of stbuf initialization failures         :0
    Number of stbuf store failures                  :0
    Number of stbuf frees                           :0
    Number of stbuf free failures                   :0
    Number of stbuf sends                           :0
    Number of stbuf send failures                   :0
    Number of stbuf receives                        :0
    Number of stbuf throttles                       :0
    Number of invalid stbuf                         :0
THR statistics
    Number of THR creates                           :90064
    Number of missing THR handles                   :0
    Number of THR create failures                   :0
    Number of THR store failures                    :0
    Number of THR short circuit failures            :0
    Number of THR update failures                   :0
    Number of THR state updates                     :180128
    Number of THR destroy failures                  :0
    Number of THR destroys                          :0
JCPP statistics
    Number of JCPP handle allocations               :0
    Number of JCPP handle allocation failures       :0
Header Insertion statistics
    Number of HCM Header Insertions                 :90061
    Number of HCM IP Mask modifications             :90061
    Number of HCM Header Insertion failures         :0
    Number of HCM Tags too large                    :0
    Number of HCM Tag encryption failures           :0
    Number of HCM requests                          :90061
    Number of missing Subscribers in HCM            :90061
```

Release Information

Statement introduced in Junos OS Release 17.1.

Support for Next Gen Services introduced in Junos OS Release 19.3R2 and 19.4R1 on MX Series routers MX240, MX480 and MX960.

RELATED DOCUMENTATION

show services hcm statistics | 885

show services lrf collector statistics

IN THIS SECTION

- Syntax | 896
- Description | 896
- Options | 897
- Required Privilege Level | 897
- Output Fields | 897
- Sample Output | 898
- Release Information | 898

Syntax

```
show services lrf collector statistics
<collector-name>
```

Description

Display LRF statistics for one or more collectors. If a collector is not specified, statistics are displayed for all collectors.

Options

none	Display LRF statistics for all collectors.
collector-name	(Optional) Display LRF statistics for the specified collector.

Required Privilege Level

view

Output Fields

Table 30 on page 897 lists the output fields for the **show services lrf collector statistics** command. Output fields are listed in the approximate order in which they appear.

Table 30: show services lrf collector statistics Output Fields

Field Name	Field Description
Interface	Name of the interface from which data records are sent to the collector.
Templates registered	Number of templates registered with the collector.
Template registration failures	Number of template registration failures.
Templates active	Number of active templates.
Sessions received	Number of data sessions received for logging of data.
Sessions ignored	Number of data sessions received for logging of data that were ignored.
Records logged	Number of logs sent to the collector.
Records exported	Number of data records exported to the collector.

Table 30: show services lrf collector statistics Output Fields *(Continued)*

Field Name	Field Description
Record export failures	Number of data record export attempts that failed.

Sample Output

show services lrf collector statistics

```
user@host> show services lrf collector statistics
LRF Collector Statistics
    Interface: ms-2/1/0
    Templates registered: 0, Template registration failures: 0, Templates
active: 1
    Sessions received: 0, Sessions ignored: 0, Records logged: 0
    Records exported: 0, Record export failures: 0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Logging and Reporting Function for Subscribers

show services lrf rule statistics

IN THIS SECTION

- Syntax | 899
- Description | 899

- Options | 899
- Required Privilege Level | 899
- Output Fields | 899
- Sample Output | 901
- Release Information | 901

Syntax

```
show services lrf rule statistics
<rule-name>
```

Description

Display LRF statistics for one or more LRF rules. If an LRF rule is not specified, statistics are displayed for all LRF rules.

Options

none	Display LRF statistics for all LRF rules.
rule-name	(Optional) Display LRF statistics for the specified LRF rule.

Required Privilege Level

view

Output Fields

Table 31 on page 900 lists the output fields for the **show services lrf rule statistics** command. Output fields are listed in the approximate order in which they appear.

Table 31: show services lrf rule statistics Output Fields

Field Name	Field Description
Interface	Name of the interface from which data records are sent to the collector.
Rule	Name of the LRF rule that caused data records to be exported to the collector.
Template	Name of the template that was used to export data records to the collector.
Templates registered	Number of templates registered with the collector.
Template registration failures	Number of template registration failures.
Collector	Name of the collector to which data records were sent.
Sessions received	Number of data sessions received for logging of data.
Sessions ignored	Number of data sessions received for logging of data that were ignored.
Sessions logged	Number of data sessions that had data records exported to the collector.
Records exported	Number of data records exported to the collector.
Record export failures	Number of data record export attempts that failed.

Sample Output

show services lrf rule statistics

```
user@host> show services lrf rule statistics
  LRF Rule Statistics
    Interface: ms-3/1/0
    Rule: r1
    Template: temp1
    Templates registered: 2, Template registration failures: 0
    Collector: coll1
    Sessions received: 115, Sessions ignored: 0, Sessions logged: 134
    Records exported: 134, Record export failures: 0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Logging and Reporting Function for Subscribers

show services lrf statistics

IN THIS SECTION

- Syntax | 902
- Description | 902
- Required Privilege Level | 902
- Output Fields | 902
- Sample Output | 903
- Release Information | 903

Syntax

```
show services lrf statistics
```

Description

Display number of bytes, packets, and flows for carrying data records to the collector.

Required Privilege Level

view

Output Fields

Table 32 on page 902 lists the output fields for the **show services lrf statistics** command. Output fields are listed in the approximate order in which they appear.

Table 32: show services lrf statistics Output Fields

Field Name	Field Description
Interface	Name of the interface from which data records are sent to the collector.
Flow packets	Number of packets carrying data records to the collector.
Flow bytes	Number of bytes carrying data records to the collector.
Active flows	Number of active flows carrying data records to the collector.
Total flows	Total number of flows for carrying data records to the collector.

Sample Output

show services lrf statistics

```
user@host> show services lrf statistics
LRF Statistics
    Interface: ms-3/1/0
    Flow packets: 31125, Flow bytes: 15335751
    Active flows: 0, Total flows: 1887

    Interface: ms-3/2/0
    Flow packets: 0, Flow bytes: 0
    Active flows: 0, Total flows: 0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Logging and Reporting Function for Subscribers

show services lrf template

IN THIS SECTION

- Syntax | 904
- Description | 904
- Options | 904
- Required Privilege Level | 905
- Sample Output | 905
- Release Information | 906

Syntax

```
show services lrf template option
```

Description

Display the fields for a template type. You must specify a template type.

Options

option Specify one of the following template types:

- device-data—Display the fields for the Device Data template type.
- flow-id—Display the fields for the Flow ID template type.
- http—Display the fields for the HTTP template type.
- ifl-subscriber—Display the fields for the IFL Subscriber template type.
- ipflow—Display the fields for the IPFlow template type.
- ipflow-extended—Display the fields for the IPFlow Extended template type.
- ipflow-tcp—Displays the fields for the IPFlow TCP template type.
- ipflow-tcp-ts—Displays the fields for the IPFlow TCP Timestamp template type.
- ipflow-ts—Display the fields for the IPFlow Timestamp template type.
- ipv4—Display the fields for the IPv4 template type.
- ipv4-extended—Display the fields for the IPv4 Extended template type.
- ipv6—Display the fields for the IPv6 template type.
- ipv6-extended—Display the fields for the IPv6 Extended template type.
- l7-app—Display the fields for the L7 Application template type.
- mobile-subscriber—Display the fields for the Mobile Subscriber template type.
- pcc—Display the fields for the PCC template type.
- subscriber-data—Display the fields for the Subscriber Data template type.

- wireline-subscriber—Display the fields for the Wireline Subscriber template type.

Required Privilege Level

view

Sample Output

show services lrf template ipv4

```
user@host> show services lrf template ipv4
LRF Template fields
    Ipv4 source address
    Ipv4 destination address
    TCP/UDP source port
    TCP/UDP destination port
```

show services lrf template ipflow-extended

```
user@host> show services lrf template ipflow-extended
Field                   Element Id       Length(bytes)      Vendor
Service set name        520              16                 Juniper
Routing-instance        521              16                 Juniper
```

show services lrf template ipflow-tcp-ts

```
user@host> show services lrf template ipflow-tcp-ts
Field                           Element Id    Length(bytes)  Vendor
Smooth RTT uplink               10000         4              Juniper
Smooth RTT downlink             10001         4              Juniper
Client setup Time               10002         4              Juniper
Server Setup time               10003         4              Juniper
Client first payload timestamp  10004         8              Juniper
Upload time                     10005         4              Juniper
Server first payload timestamp  10006         8              Juniper
Download time                   10007         4              Juniper
```

```
Acknowledged volumes uplink      10008         8              Juniper
Acknowledged volumes downlink    10009         8              Juniper
```

show services lrf template ipflow-tcp

```
user@host> show services lrf template ipflow-tcp
Field                             Element Id  Length(bytes)  Vendor
Retransmitted TCP packets uplink  115         4              Juniper
Retransmitted TCP packets downlink 116        4              Juniper
TCP flow creation timestamp       121         8              Juniper
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Logging and Reporting Function for Subscribers

show services traffic-detection-function hcm statistics

IN THIS SECTION

- Syntax | **907**
- Description | **907**
- Options | **907**
- Required Privilege Level | **907**
- Output Fields | **907**
- Sample Output | **910**
- Sample Output | **910**
- Release Information | **911**

Syntax

```
show services traffic-detection-function hcm statistics
<ipv4-address v4-addr>
<ipv6-address v6-addr>
<routing-instance routing-instance>
```

Description

Display the statistics related to HTTP header enrichment for all the active HTTP sessions for the TDF subscriber.

Options

none	Display HTTP header enrichment statistics for all active HTTP sessions.
ipv4-address *v4-addr*	(Optional) Display HCM statistics for the specified IPv4 address of the subscriber's user equipment (UE).
ipv6-address *v6-addr*	(Optional) Display HCM statistics for the specified IPv6 address of the subscriber's user equipment.
routing-instance *routing-instance*	(Optional) Display HCM statistics for the specified routing instance of the subscriber's user equipment.

Required Privilege Level

view

Output Fields

Table 33 on page 908 lists the output fields for the **show services traffic-detection-function hcm statistics** command. Output fields are listed in the approximate order in which they appear.

Table 33: show services traffic-detection-function hcm statistics Output Fields

Field Name	Field Description
Interface Name	Name of the services PIC on which data sessions are being serviced. The HTTP header enrichment statistics sessions are displayed per services PIC.
Session id	Identifier for the session.
Subscriber-type	Type of subscriber: • **ip**—IP-based subscriber. • **ifl**—Interface-based subscriber.
IMSI	International Mobile Subscriber Identity (IMSI) of the subscriber's user detail equipment (UE).
MSISDN	Mobile station ISDN of the subscriber's user equipment.
Header inserted	Number of times that tags were successfully inserted into HTTP headers for the data session.
Header insert failed	Number of times that the insertion of tags into HTTP headers failed for the data session.
Header renamed	Number of times an HTTP header was renamed.
Header rename fail	Number of times an attempt to rename an HTTP header failed.
IPV4 mask modification	Number of times IPv4 address mask was inserted.
IPV6 mask modification	Number of times IPv6 address mask was inserted.

Table 33: show services traffic-detection-function hcm statistics Output Fields *(Continued)*

Field Name	Field Description
Tag too large	Number of tags that cannot be inserted into HTTP headers because the tag size was larger than the maximum configured size for the data session.
Tag encryption failed	Number of times that the encryption of HTTP tags used for header insertion failed for the data session.
Total Get request	Total number of HTTP Get Requests received for the data session.
Subscriber info unavailable	Number of times that subscriber attributes were missing during attempted header insertions for the data session.
Subscriber attribute missing	Number of times that tags were not inserted because subscriber attributes were missing.
IPV4 attribute missing	Number of times that tags were not inserted because subscriber IPv4 user address attributes were missing.
IPV6 attribute missing	Number of times that tags were not inserted because subscriber IPv6 user address attributes were missing.
IPV4 / IPV6 attribute	Number of times that IPv4 and IPv6 user address tags were successfully inserted into HTTP headers.

Sample Output

show services traffic-detection-function hcm statistics routing-instance

```
user@host> show services traffic-detection-function hcm statistics routing-instance r1
Interface Name: mams-2/3/0 (ams1)
Session id: 134217730, Subscriber-type: ip
    Header inserted              : 6
    Header insert failed         : 0
    Header renamed               : 36
    Header rename fail           : 0
    IPV4 mask modification       : 3
    IPV6 mask modification       : 0
    Tag too large                : 0
    Tag encryption failed        : 0
    Total Get request            : 3
    Subscriber info unavailable  : 9
    Subscriber attribute missing : 9
    IPV4 attribute missing       : 0
    IPV6 attribute missing       : 3
    IPV4 / IPV6 attributes       : 0
```

Sample Output

show services traffic-detection-function hcm statistics ipv4-address routing-instance

```
user@host> show services traffic-detection-function hcm statistics ipv4-address 192.0.2.1 routing-
instance default
Interface Name: mams-2/0/0 (ams1)
Session id: 67108865, Subscriber Type: IP, IMSI: 324234324, MSISDN: 0
    Header inserted              : 0
    Header insert failed         : 0
    Header renamed               : 0
    Header rename fail           : 0
    IPV4 mask modification       : 0
    IPV6 mask modification       : 0
    Tag too large                : 0
    Tag encryption failed        : 0
    Total Get request            : 0
```

```
    Subscriber info unavailable  : 0
    Subscriber attribute missing : 0
    IPV4 attribute missing       : 0
    IPV6 attribute missing       : 0
    IPV4 / IPV6 attributes       : 0
```

Release Information

Statement introduced in Junos OS Release 17.1.

This statement is not supported for Next Gen Services.

RELATED DOCUMENTATION

show services traffic-detection-function sessions | 911

show services traffic-detection-function sessions

IN THIS SECTION

- Syntax | 911
- Description | 912
- Options | 912
- Required Privilege Level | 912
- Output Fields | 912
- Sample Output | 914
- Sample Output | 914
- Release Information | 914

Syntax

```
show services traffic-detection-function sessions
<ipv4-address v4-addr>
```

```
<ipv6-address v6-addr>
<routing-instance routing-instance>
```

Description

Display the active data sessions (TCP or UDP flows) that are being serviced (passing through a services PIC) for a specified TDF subscriber.

Options

none	No output is displayed.
ipv4-address *v4-addr*	(Optional) Display subscriber sessions for the specified IPv4 address of the subscriber's user equipment (UE).
ipv6-address *v6-addr*	(Optional) Display subscriber sessions for the specified IPv6 address of the subscriber's user equipment.
routing-instance *routing-instance*	(Optional) Display subscriber sessions for the specified routing instance.

Required Privilege Level

view

Output Fields

Table 34 on page 912 lists the output fields for the **show services traffic-detection-function sessions** command. Output fields are listed in the approximate order in which they appear.

Table 34: show services traffic-detection-function sessions Output Fields

Field Name	Field Description
Interface Name	Name of the service PIC on which data sessions are being serviced. The data sessions are displayed per services PIC.

Table 34: show services traffic-detection-function sessions Output Fields *(Continued)*

Field Name	Field Description
Service Set	Name of the service set on which the data session is being serviced.
Session	Identifier for the data session.
ALG	Identifier for the application-level gateway (ALG).
Subscriber-type	Type of subscriber: • **ip**—IP-based subscriber. • **ifl**—Interface-based subscriber.
IMSI	International Mobile Subscriber Identity (IMSI) of the subscriber's user detail equipment (UE).
MSISDN	Mobile station ISDN of the subscriber's user equipment.
For each session, the following information, pertaining to the flow, is displayed: • Flow protocol: **TCP**, **UDP**, or **ICMP** • Flow source IP address and source port address • Flow destination IP address and destination port address • Flow state: **Forward** or **Drop** • Flow direction: input (**I**) or output (**O**) • Number of packets transmitted	

Sample Output

show services traffic-detection-function sessions routing-instance

```
user@host> show services traffic-detection-function sessions routing-instance r1
Interface Name: mams-5/1/0 (ams1)
Service Set: set-hcm, Session: 67258263, ALG: none, Subscriber-type: ip
TCP         192.0.2.8:17751 ->     198.51.100.5:80    Forward  I              31
TCP         198.51.100.5:80    ->     192.0.2.8:17751 Forward  O              53
Service Set: set-hcm, Session: 67269654, ALG: none, Subscriber-type: ifl
TCP         192.0.2.8:18572 ->     198.51.100.5:80    Forward  I              31
TCP         198.51.100.5:80    ->     192.0.2.8:18572 Forward  O              54
Service Set: set-hcm, Session: 83939629, ALG: none, Subscriber-type: ifl
TCP         192.0.2.8:20826 ->     198.51.100.5:80    Forward  I              31
TCP         198.51.100.5:80    ->     192.0.2.8:20826 Forward  O              53
```

Sample Output

show services traffic-detection-function sessions ipv4-address routing-instance

```
user@host> show services traffic-detection-function sessions ipv4-address 203.0.113.1 routing-instance
default
Interface Name: mams-2/0/0 (ams1)
Service Set: tdf-service-set, Session: 33554433, ALG: none, Subscriber Type: IP,
IMSI: 324234324, MSISDN: 0
ICMP           203.0.113.1     ->    10.11.0.1     Forward  I              81
ICMP          10.11.0.1     ->    203.0.113.1      Forward  O               0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf subscribers | 1038

show unified-edge tdf aaa radius client statistics

IN THIS SECTION

- Syntax | 915
- Description | 915
- Options | 915
- Required Privilege Level | 916
- Output Fields | 916
- Sample Output | 918
- Release Information | 923

Syntax

```
show unified-edge tdf aaa radius client statistics
<brief | detail>
<fpc-slot fpc-slot>
<gateway gateway>
<client name>
<pic-slot pic-slot>
```

Description

Display the statistics for the accounting packets transmitted and received from the RADIUS client for one or more TDF gateways. If a TDF gateway is not specified, then information for all TDF gateways is displayed.

Options

none	Display statistics for all TDF gateways.
brief | detail	(Optional) Display the specified level of output.
client *name*	(Optional) Display statistics for the specified RADIUS client.

fpc-slot *fpc-slot* (Optional) Display statistics for the specified Flexible PIC Concentrator (FPC).

gateway *gateway* (Optional) Display statistics for the specified TDF gateway.

pic-slot *pic-slot* (Optional) Display statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

view

Output Fields

Table 35 on page 916 lists the output fields for the **show unified-edge tdf aaa radius client statistics** command. Output fields are listed in the approximate order in which they appear.

Table 35: show unified-edge tdf aaa radius client statistics Output Fields

Field Name	Field Description	Level of Output
Client	Name of the RADIUS client.	All levels
Gateway Name	Name of the TDF gateway.	All levels
FPC/PIC	FPC and PIC slot numbers for which the statistics are displayed.	**detail**

Table 35: show unified-edge tdf aaa radius client statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Accounting Requests	Number of accounting requests sent to the RADIUS server from the FPC slot and PIC slot. The following information is displayed about each request type: • **Start**—Number of Accounting Start requests sent. • **Stop**—Number of Accounting Stop requests sent. • **Interim**—Number of Accounting Interim-Update requests sent. • **On**—Number of Accounting On requests sent. • **Off**—Number of Accounting Off requests sent.	All levels
Accounting Responses	Number of accounting responses sent to the RADIUS server from the FPC slot and PIC slot. The following information is displayed about each request type: • **Start**—Number of Accounting Start responses sent. • **Stop**—Number of Accounting Stop responses sent. • **Interim**—Number of Accounting Interim-Update responses sent. • **On**—Number of Accounting On responses sent. • **Off**—Number of Accounting Off responses sent.	All levels
Duplicate Requests	Number of duplicate accounting requests sent to the RADIUS server.	All levels
Malformed Requests	Number of malformed accounting requests sent to the RADIUS server.	All levels

Table 35: show unified-edge tdf aaa radius client statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Bad Authenticators	Number of responses received from the RADIUS server with bad authenticators.	All levels
Unknown Types	Number of unknown type responses (that the TDF gateway does not recognize) received from the RADIUS server.	All levels
Dropped Packets	Number of packets dropped.	All levels

Sample Output

show unified-edge tdf aaa radius client statistics brief

```
user@host> show unified-edge tdf aaa radius client statistics brief
Client: pgwclient
Gateway Name: TDF
    Accounting Requests: 8
        Start: 8
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Accounting Responses: 8
        Start: 8
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
    Dropped Packets: 0
```

```
Client: pgwclient_jrad
Gateway Name: TDF
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Accounting Responses: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
    Dropped Packets: 0

Client: pgwclient_jrad1
Gateway Name: TDF
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Accounting Responses: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
    Dropped Packets: 0
```

show unified-edge tdf aaa radius client statistics detail

```
user@host> show unified-edge tdf aaa radius client statistics detail
Client: pgwclient
Gateway Name: TDF
FPC/PIC: 2/0
    Accounting Requests: 8
        Start: 8
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Accounting Responses: 8
        Start: 8
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
    Dropped Packets: 0

Client: pgwclient
Gateway Name: TDF
FPC/PIC: 2/1
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Accounting Responses: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
```

```
    Unknown Types: 0
    Dropped Packets: 0

Client: pgwclient_jrad
Gateway Name: TDF
FPC/PIC: 2/0
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Accounting Responses: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
    Dropped Packets: 0

Client: pgwclient_jrad
Gateway Name: TDF
FPC/PIC: 2/1
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Accounting Responses: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
```

```
    Dropped Packets: 0

Client: pgwclient_jrad1
Gateway Name: TDF
FPC/PIC: 2/0
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Accounting Responses: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
    Dropped Packets: 0

Client: pgwclient_jrad1
Gateway Name: TDF
FPC/PIC: 2/1
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Accounting Responses: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
```

```
    Unknown Types: 0
    Dropped Packets: 0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- clear unified-edge tdf aaa radius client statistics | 777
- show unified-edge tdf aaa statistics | 945

show unified-edge tdf aaa radius client status

IN THIS SECTION

- Syntax | 923
- Description | 924
- Options | 924
- Required Privilege Level | 924
- Output Fields | 924
- Sample Output | 925
- Release Information | 925

Syntax

```
show unified-edge tdf aaa radius client status
<fpc-slot fpc-slot>
<gateway gateway>
<client name>
<pic-slot pic-slot>
```

Description

Display the status of the RADIUS client for one or more TDF gateways. If a TDF gateway is not specified, then information for all TDF gateways is displayed.

Options

none	Display RADIUS client status for all TDF gateways.
client *name*	(Optional) Display the status for the specified RADIUS client.
fpc-slot *fpc-slot*	(Optional) Display the status for the specified Flexible PIC Concentrator (FPC).
gateway *gateway*	(Optional) Display the status for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Display the status for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

view

Output Fields

Table 36 on page 924 lists the output fields for the **show unified-edge tdf aaa radius client status** command. Output fields are listed in the approximate order in which they appear.

Table 36: show unified-edge tdf aaa radius client status Output Fields

Field Name	Field Description
Client	Name of the RADIUS client.
FPC/PIC	FPC and PIC slot numbers for which the statistics are displayed.
Address	IP address of the RADIUS client.

Table 36: show unified-edge tdf aaa radius client status Output Fields *(Continued)*

Field Name	Field Description
Last activity	Day of the week, month, date, time, and year when the last operation occurred on the RADIUS client. The term **No activity** is displayed if no communication occurred between the RADIUS client and the TDF gateway.

Sample Output

show unified-edge tdf aaa radius client status

```
user@host> show unified-edge tdf aaa radius statistics accounting brief
Client       FPC/PIC  Address              Last activity
-----------------------------------------------------------------
pgwclient    2/0      192.0.2.3           Mon Jul 21 11:00:16 2014
pgwclient_j  2/0      198.51.100.2            No activity
pgwclient_j  2/0      203.0.113.1            No activity
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf aaa radius client statistics | 777

show unified-edge tdf aaa statistics | 945

show unified-edge tdf aaa radius network-element statistics

IN THIS SECTION

Syntax | 926

- Description | 926
- Options | 926
- Required Privilege Level | 927
- Output Fields | 927
- Sample Output | 928
- Release Information | 929

Syntax

```
show unified-edge tdf aaa radius network-element statistics
<brief | detail>
<fpc-slot fpc-slot>
<gateway gateway>
<name name>
<pic-slot pic-slot>
```

Description

Display RADIUS network element statistics. If a TDF gateway is not specified, then statistics for all TDF gateways are displayed.

Options

none	Display statistics for all TDF gateways.
brief | detail	(Optional) Display the specified level of output. The **brief** option is the default and displays the consolidated statistics for all TDF gateways, and the **detail** option displays the statistics for each Services PIC on the configured TDF gateways.
fpc-slot *fpc-slot*	(Optional) Display statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway*	(Optional) Display statistics for the specified TDF gateway.
name *name*	(Optional) Display statistics for the specified network element.

pic-slot *pic-slot* (Optional) Display statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

view

Output Fields

Table 37 on page 927 lists the output fields for the **show unified-edge tdf aaa radius network-element statistics** command. Output fields are listed in the approximate order in which they appear.

Table 37: show unified-edge tdf aaa radius network-element statistics Output Fields

Field Name	Field Description	Level of Output
Network-element	Name of the network element to which the statistics belong.	All levels
FPC/PIC	FPC and PIC slot numbers for which statistics are displayed.	**detail**
Requests Attempted	Number of access and accounting requests that were attempted.	All levels
Access Requests Sent	Number of access requests sent.	All levels
Accounting Requests Sent	Number of accounting requests sent.	All levels
Responses Received	Number of access and accounting response messages received.	All levels

Table 37: show unified-edge tdf aaa radius network-element statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Request Timeouts	Number of access and accounting requests to the RADIUS server that timed out.	All levels
Memory Failures	Number of internal memory allocation failures.	All levels
Invalid State Errors	Number of access requests and accounting requests that were attempted in non-operational state.	All levels
No Radius Server Found	Number of access requests and accounting requests that failed because no more RADIUS servers were available.	All levels
Source Port allocation Errors	Number of access and accounting requests that failed because of source port allocation failure for outgoing RADIUS messages.	All levels
Send Failures	Total number of failed attempts to send access requests and accounting requests.	All levels

Sample Output

show unified-edge tdf aaa radius network-element statistics detail

```
user@host> show unified-edge tdf aaa radius network-element statistics detail
  Network-element: ne1
```

```
FPC/PIC:         5/2
  Requests Attempted:            0
  Access Requests Sent:          0
  Accounting Requests Sent:      0
  Responses Received:            0
  Request Timeouts:              0
  Memory Failures:               0
  Invalid State Errors:          0
  No Radius Server Found:        0
  Source Port allocation Errors: 0
  Send Failures:                 0

Network-element: ne2
FPC/PIC:         5/2
  Requests Attempted:            0
  Access Requests Sent:          0
  Accounting Requests Sent:      0
  Responses Received:            0
  Request Timeouts:              0
  Memory Failures:               0
  Invalid State Errors:          0
  No Radius Server Found:        0
  Source Port allocation Errors: 0
  Send Failures:                 0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf aaa radius network-element statistics | 779

Understanding Network Elements | 71

show unified-edge tdf aaa radius server statistics

IN THIS SECTION

- Syntax | 930
- Description | 930
- Options | 930
- Required Privilege Level | 931
- Output Fields | 931
- Sample Output | 935
- Release Information | 936

Syntax

```
show unified-edge tdf aaa radius server statistics
<brief | detail>
<fpc-slot fpc-slot>
<gateway gateway>
<name name>
<pic-slot pic-slot>
```

Description

Display RADIUS server statistics. If a TDF gateway is not specified, then statistics for all TDF gateways are displayed.

Options

none Display the same output as the **brief** option.

brief | detail (Optional) Display the specified level of output.

The **brief** option is the default and displays the consolidated statistics for all TDF gateways, and the **detail** option displays the statistics for each Services PIC on the configured TDF gateways.

fpc-slot *fpc-slot* (Optional) Display statistics for the specified Flexible PIC Concentrator (FPC).

gateway *gateway* (Optional) Display statistics for the specified TDF gateway.

name *name* (Optional) Display statistics for the specified RADIUS server.

pic-slot *pic-slot* (Optional) Display statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

view

Output Fields

Table 38 on page 931 lists the output fields for the **show unified-edge tdf aaa radius server statistics** command. Output fields are listed in the approximate order in which they appear.

Table 38: show unified-edge tdf aaa radius server statistics Output Fields

Field Name	Field Description	Level of Output
RADIUS server	Name of the RADIUS server.	All levels
Address	IP address of the RADIUS server.	All levels
Routing-instance	Routing-instance of RADIUS server's source address.	**detail**
Authentication Statistics		
Port	RADIUS server port number to which access requests are sent.	All levels
FPC/PIC	FPC and PIC slot numbers for which the statistics are displayed.	**detail**

Table 38: show unified-edge tdf aaa radius server statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Access requests	Number of access requests sent to the RADIUS server.	All levels
Access req retransmissions	Number of access requests retransmitted to the RADIUS server.	All levels
Access accepts	Number of access accepts sent by the RADIUS server.	All levels
Access rejects	Number of access requests rejected by the RADIUS server.	All levels
Malformed responses	Number of malformed access responses received from the RADIUS server.	All levels
Bad authenticators	Number of bad authentication responses received for access-requests.	All levels
Timeouts	Number of access requests to the RADIUS server that timed out.	All levels
Unknown types	Number of unknown type responses received from the RADIUS server for access requests.	All levels
Packets dropped	Number of packets dropped for access requests and responses.	All levels
Accounting Statistics		
Port	RADIUS server port number to which accounting requests are sent.	All levels

Table 38: show unified-edge tdf aaa radius server statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Accounting requests	Number of accounting requests sent to the RADIUS server. The following information is displayed about each request type for the **detail** level: • **Start**—Number of accounting start requests sent. • **Stop**—Number of accounting stop requests sent. • **Interim**—Number of accounting interim-update requests sent. • **On**—Number of accounting on requests sent. • **Off**—Number of accounting off requests sent.	All levels
Accounting req retransmissions	Number of accounting requests retransmitted to the RADIUS server.	All levels
Accounting responses	Number of accounting responses received from the RADIUS server.	All levels
Malformed responses	Number of malformed accounting responses received from the RADIUS server.	All levels
Bad authenticators	Number of bad accounting responses received for accounting requests.	All levels
Timeouts	Number of accounting requests to the RADIUS server that timed out.	All levels
Unknown types	Number of unknown type responses (that the TDF gateway does not recognize) received from the RADIUS server for accounting requests.	All levels

Table 38: show unified-edge tdf aaa radius server statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Packets dropped	Number of packets dropped for accounting requests and responses.	All levels
Dynamic Authorization Request Statistics		
CoA requests received	Number of change of authorization (CoA) requests received from the RADIUS server.	All levels
DM requests received	Number of Disconnect Message (DM) requests received from the RADIUS server.	All levels
CoA Acks sent	Number of CoA acknowledgements sent to the RADIUS server.	All levels
CoA Nacks sent	Number of CoA negative acknowledgements sent to the RADIUS server.	All levels
DM Acks sent	Number of DM acknowledgements sent to the RADIUS server.	All levels
DM Nacks sent	Number of DM negative acknowledgements sent to the RADIUS server.	All levels
Dropped	Number of dynamic authorization requests dropped.	All levels

Sample Output

show unified-edge tdf aaa radius server statistics detail

```
user@host> show unified-edge tdf aaa radius server statistics detail
RADIUS server: radius1 (FPC/PIC: 5/2)
Address: 192.0.2.2
Routing-instance: default
Authentication Statistics:
    Port: 1812
    Access requests: 0
    Access req retransmissions: 0
    Access accepts: 0
    Access rejects: 0
    Malformed responses: 0
    Bad authenticators: 0
    Timeouts: 0
    Unknown types: 0
    Packets dropped: 0
Accounting Statistics:
    Port: 1813
    Accounting requests: 0
      Start: 0      Stop: 0      Interim: 0      On: 0      Off: 0
    Accounting req retransmissions: 0
    Accounting responses: 0
    Malformed responses: 0
    Bad authenticators: 0
    Timeouts: 0
    Unknown types: 0
    Packets dropped: 0
Dynamic Authorization Request Statistics:
    CoA requests received: 0
    DM requests received: 0
    CoA Acks sent: 0
    CoA Nacks sent: 0
    DM Acks sent: 0
    DM Nacks sent: 0
    Dropped: 0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf aaa radius server statistics | 781

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

show unified-edge tdf aaa radius server status

IN THIS SECTION

- Syntax | 936
- Description | 937
- Options | 937
- Required Privilege Level | 937
- Output Fields | 937
- Sample Output | 939
- Release Information | 940

Syntax

```
show unified-edge tdf aaa radius server status
<brief | detail>
<fpc-slot fpc-slot>
<gateway gateway>
<name name>
<pic-slot pic-slot>
```

Description

Display RADIUS server status. If a TDF gateway is not specified, then statistics for all TDF gateways are displayed.

Options

none	(Same as brief) Display consolidated statistics for all TDF gateways.
brief | detail	(Optional) Display the specified level of output. The **brief** option is the default.
fpc-slot *fpc-slot*	(Optional) Display statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway*	(Optional) Display statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Display statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

view

Output Fields

Table 39 on page 937 lists the output fields for the **show unified-edge tdf aaa radius server status** command. Output fields are listed in the approximate order in which they appear.

Table 39: show unified-edge tdf aaa radius server status Output Fields

Field Name	Field Description	Level of Output
Server	Name of the RADIUS server.	**brief**
RADIUS Server	Name of the RADIUS server.	**detail**
FPC/PIC	FPC and PIC slot numbers for which the statistics are displayed.	All levels

Table 39: show unified-edge tdf aaa radius server status Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Address	IP address of the RADIUS server.	All levels
State	State of the RADIUS server: **Active** or **Inactive** (dead).	All levels
Duration	Duration, in *weeks:days:MM:SS* format, for which the RADIUS server has been in the current state.	All levels
Previous duration	Duration, in *HH:MM:SS* format, for which the RADIUS server was in the previous state.	All levels
Flaps	Number of times that the RADIUS server transitioned from the active to inactive state.	All levels
Authentication Information		
Pending requests	Number of access requests waiting for responses from the RADIUS server.	**detail**
Round trip time (ms)	Time taken to receive the response from the RADIUS server for access requests. The minimum, maximum, and average round-trip times are also displayed.	**detail**
Accounting Information		

Table 39: show unified-edge tdf aaa radius server status Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Pending requests	Number of accounting requests waiting for responses from the RADIUS server.	**detail**
Round trip time (ms)	Time taken to receive the response from the RADIUS server for accounting requests. The minimum, maximum, and average round-trip times are also displayed.	**detail**

Sample Output

show unified-edge tdf aaa radius server status brief

```
user@host> show unified-edge tdf aaa radius server status brief
             FPC/                                    Previous
Server       PIC     Address          State    Duration      Duration    Flaps
-------------------------------------------------------------------------------
radius1      5/2     192.0.2.2        Active   1w5d 23:12    00:00:00    0
radius2      5/2     198.51.100.100   Active   1w5d 23:12    00:00:00    0
radius3      5/2     203.0.113.100     Active   1w5d 23:12    00:00:00    0
radius4      5/2     203.0.113.100     Active   1w5d 23:12    00:00:00    0
```

show unified-edge tdf aaa radius server status detail

```
user@host> show unified-edge tdf aaa radius server status detail
RADIUS server: pgwcl (FPC/PIC: 4/0)
Address            : 198.51.100.100
State              : Active
Duration           : 1w6d 11:29
Previous Duration : 00:00:00
Flaps              : 0
Authentication Information:
    Pending requests     : 0
```

```
    Round trip time (ms) : 1 (Min: 1 Max: 1 Avg: 1)
Accounting Information:
    Pending requests     : 0
    Round trip time (ms) : 0 (Min: 0 Max: 0 Avg: 0)
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf aaa radius server statistics | 930

Understanding How a RADIUS Server Controls Policy and Charging Control Rules | 64

show unified-edge tdf aaa radius snoop-segment statistics

IN THIS SECTION

- Syntax | 940
- Description | 941
- Options | 941
- Required Privilege Level | 941
- Output Fields | 941
- Sample Output | 943
- Release Information | 945

Syntax

```
show unified-edge tdf aaa radius snoop-segment statistics
<brief | detail>
<fpc-slot fpc-slot>
<gateway gateway>
```

```
<pic-slot pic-slot>
<segment snoop-segment-name>
```

Description

Display statistics for snoop segments. If a snoop segment is not specified, then statistics for all snoop segments are displayed.

Options

none	(Same as brief) Display statistics for all snoop segments for all TDF gateways.
brief | detail	(Optional) Display the specified level of output. The **brief** option displays the consolidated statistics for all TDF gateways, and the **detail** option displays the statistics for each Services PIC on the configured TDF gateways.
fpc-slot *fpc-slot*	(Optional) Display statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway*	(Optional) Display statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Display statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.
segment *snoop-segment-name*	(Optional) Display statistics for the specified snoop segment.

Required Privilege Level

view

Output Fields

Table 40 on page 942 lists the output fields for the **show unified-edge tdf aaa radius snoop-segment statistics** command. Output fields are listed in the approximate order in which they appear.

Table 40: show unified-edge tdf aaa radius snoop-segment statistics Output Fields

Field Name	Field Description	Level of Output
Snoop-segment	Name of the snoop-segment for which statistics are displayed.	All levels
Gateway Name	Name of the TDF gateway. If the statistics for all TDF gateways are displayed, then **All** is displayed.	All levels
FPC/PIC	FPC and PIC slot numbers for which the statistics are displayed.	**detail**
Accounting Requests	The following information is displayed for each category: • **Start**—Number of snooped Accounting Start requests. • **Interim**—Number of snooped Accounting Interim-Update requests. • **Stop**—Number of snooped Accounting Stop requests. • **On**—Number of snooped Accounting On requests. • **Off**—Number of snooped Accounting Off requests.	All levels
Duplicate Requests	Number of duplicate snooped accounting requests.	All levels
Malformed Requests	Number of snooped malformed accounting requests.	All levels
Bad Authenticators	Number of snooped acccounting requests with bad authenticators.	All levels
Unknown Types	Number of snooped accounting requests of unknown type.	All levels
Dropped Packets	Number of snooped packets dropped.	All levels

Sample Output

show unified-edge tdf aaa radius snoop-segment statistics brief

```
user@host> show unified-edge tdf aaa radius snoop-segment statistics brief

Snoop-segment: 123
Gateway Name: TDF
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
    Dropped Packets: 0

Snoop-segment: dummy
Gateway Name: TDF
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
    Dropped Packets: 0
```

show unified-edge tdf aaa radius snoop-segment statistics detail

```
user@host> show unified-edge tdf aaa radius snoop-segment statistics detail
Snoop-segment: 123
Gateway Name: TDF
FPC/PIC: 4/0
```

```
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
    Dropped Packets: 0

Snoop-segment: 123
Gateway Name: TDF
FPC/PIC: 4/1
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
    Dropped Packets: 0

Snoop-segment: dummy
Gateway Name: TDF
FPC/PIC: 4/0
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
    Dropped Packets: 0

Snoop-segment: dummy
```

```
Gateway Name: TDF
FPC/PIC: 4/1
    Accounting Requests: 0
        Start: 0
        Stop: 0
        Interim: 0
        On: 0
        Off: 0
    Duplicate Requests: 0
    Malformed Requests: 0
    Bad Authenticators: 0
    Unknown Types: 0
    Dropped Packets: 0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf aaa radius snoop-segment statistics | 782

Configuring Snooping of RADIUS Accounting Requests for IP-Based Subscribers | 136

Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | 114

show unified-edge tdf aaa statistics

IN THIS SECTION

- Syntax | 946
- Description | 946
- Options | 946
- Required Privilege Level | 946
- Output Fields | 947
- Sample Output | 953

Release Information | 958

Syntax

```
show unified-edge tdf aaa statistics
<brief | detail>
<fpc-slot fpc-slot>
<gateway gateway>
<pic-slot pic-slot>
```

Description

Display global statistics for accounting requests and responses for one or more TDF gateways. If a TDF gateway is not specified, then statistics for all TDF gateways are displayed.

Options

none	(Same as brief) Display statistics for all TDF gateways.
brief | detail	(Optional) Display the specified level of output. The **brief** option displays the consolidated statistics for all TDF gateways, and the **detail** option displays the statistics for each Services PIC on the configured TDF gateways.
fpc-slot *fpc-slot*	(Optional) Display statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway*	(Optional) Display statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Display statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

view

Output Fields

Table 41 on page 947 lists the output fields for the **show unified-edge tdf aaa statistics** command. Output fields are listed in the approximate order in which they appear.

Table 41: show unified-edge tdf aaa statistics Output Fields

Field Name	Field Description	Level of Output
Gateway Name	Name of the TDF gateway. If the statistics for all TDF gateways are displayed, then **All** is displayed.	All levels
FPC/PIC	FPC and PIC slot numbers for which the statistics are displayed.	**detail**
Total Messages	Total number of all RADIUS requests and responses for the following categories: • **Received** • **Sent** • **Snooped**—Snooped by the MX Series router. • **Forwarded In**—Forwarded into the interface. • **Forwarded Out**—Forwarded out of the interface.	All levels **Forwarded In** and **Forwarded Out** are displayed only with the **detail** option.
Access Requests	Number of access requests for the following category: • **Sent**—Sent to the RADIUS server from the FPC slot and PIC slot.	All levels

Table 41: show unified-edge tdf aaa statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Access Responses	Number of access responses for the following category: • **Received**—Received from the RADIUS server for the FPC slot and PIC slot. The following information is displayed: • **Accept**—Number of access accepts sent by the RADIUS server. • **Reject**—Number of access requests rejected by the RADIUS server.	All levels
Accounting Requests	Number of accounting requests for the following categories: • **Received** • **Sent** • **Snooped**—Snooped by the MX Series router. • **Forwarded In**—Forwarded into the interface. • **Forwarded Out**—Forwarded out of the interface. The following information is displayed for each category: • **Start**—Number of Accounting Start requests. • **Interim**—Number of Accounting Interim-Update requests. • **Stop**—Number of Accounting Stop requests. • **On**—Number of Accounting On requests. • **Off**—Number of Accounting Off requests.	All levels **Forwarded In** and **Forwarded Out** are displayed only with the **detail** option.

Table 41: show unified-edge tdf aaa statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Accounting Responses	Number of accounting responses for the following categories: • **Received** • **Sent** • **Snooped**—Snooped by the MX Series router. • **Forwarded In**—Forwarded into the interface. • **Forwarded Out**—Forwarded out of the interface. The following information is displayed for each category: • **Start**—Number of Accounting Start responses. • **Interim**—Number of Accounting Interim-Update responses. • **Stop**—Number of Accounting Stop responses. • **On**—Number of Accounting On responses. • **Off**—Number of Accounting Off responses.	All levels **detail**—Number of responses that are forwarded into the interface and forwarded out of the interface is displayed only with the **detail** option.
Change of Auth Requests	Number of change of authorization (CoA) requests for the following categories: • **Received**—Received from the RADIUS server. • **Forwarded In**—Forwarded into the interface. • **Forwarded Out**—Forwarded out of the interface.	All levels **Forwarded In** and **Forwarded Out** are displayed only with the **detail** option.

Table 41: show unified-edge tdf aaa statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Change of Auth Responses	Number of CoA responses for the following category: • **Sent**—Sent to the RADIUS server from the FPC slot and PIC slot. • **Forwarded In**—Forwarded into the interface. • **Forwarded Out**—Forwarded out of the interface. The following information is displayed: • **Ack**—Number of CoA acknowledgements sent to the RADIUS server. • **Nack**—Number of CoA negative acknowledgements sent to the RADIUS server.	All levels **Forwarded In** and **Forwarded Out** are displayed only with the **detail** option.
Disconnect Message Requests	Number of Disconnect Message requests for the following categories: • **Received**—Received from the RADIUS server. • **Forwarded In**—Forwarded into the interface. • **Forwarded Out**—Forwarded out of the interface.	All levels **Forwarded In** and **Forwarded Out** are displayed only with the **detail** option.

Table 41: show unified-edge tdf aaa statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Disconnect Message Responses	Number of Disconnect Message responses for the following categories: • **Sent**—Sent to the RADIUS server. • **Forwarded In**—Forwarded into the interface. • **Forwarded Out**—Forwarded out of the interface. The following information is displayed: • **Ack**—Number of Disconnect Message acknowledgements sent to the RADIUS server. • **Nack**—Number of Disconnect Message negative acknowledgements sent to the RADIUS server.	All levels **Forwarded In** and **Forwarded Out** are displayed only with the **detail** option.
Duplicates	Number of duplicate requests received from RADIUS clients.	All levels
Request Processing errors	Number of errors that occurred during the processing of accounting requests.	All levels
Response Processing errors	Number of errors that occurred during the processing of access and accounting response packets from the RADIUS server.	All levels
Request Transmit errors	Number of errors that occurred during the transmission of access and accounting requests.	All levels
Response Transmit errors	Number of errors that occurred during the transmission of access and accounting responses to the RADIUS server.	All levels
Request Enqueue Errors	Number of errors that occurred while trying to place an access or accounting request packet in the queue.	All levels

Table 41: show unified-edge tdf aaa statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Response Enqueue Errors	Number of errors that occurred while trying to place an access or accounting response packet in the queue.	All levels
Request Timeouts	Number of access and accounting requests to the RADIUS server that timed out.	All levels
Request Retransmissions	Number of access and accounting requests that were retransmitted to the RADIUS server because they did not receive a response.	All levels
Dropped Requests	Number of accounting requests that were dropped.	All levels
Dropped Responses	Number of access or accounting responses from the RADIUS server that were dropped.	All levels
Missing TDF Domain	Number of accounting requests from the GGSN, PGW, or BNG for which the TDF domain corresponding to the subscriber was not available.	All levels
Missing PCEF profile	Number of accounting requests from the GGSN, PGW, or BNG for which the PCEF profile corresponding to the subscriber was not available.	All levels
Server Initiated Request Processing Errors	Number of processing errors of CoA and Disconnect Message requests from the RADIUS server.	All levels
Dropped Server Initiated Requests	Number of CoA and Disconnect Message requests from the RADIUS server that were dropped.	All levels
Duplicate Server Initiated Requests	Number of duplicate requests received from RADIUS servers.	All levels

Table 41: show unified-edge tdf aaa statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Cached Reply Sent	Number of RADIUS cached responses sent for RADIUS accounting request messages from the GGSN, PGW, or BNG. RADIUS replies are stored in the MX Series router response cache.	All levels

Sample Output

show unified-edge tdf aaa statistics brief

```
user@host> show unified-edge tdf aaa statistics brief


Gateway Name: TDF
Messages                        Received        Sent        Snooped
-------------------------------------------------------------------------
Total Messages                  15              15          0
Access Requests                 0               7           0
Access Responses                7               0           0
    Accept                      7               0           0
    Reject                      0               0           0
Accounting Requests             8               0           0
    Start                       8               0           0
    Interim                     0               0           0
    Stop                        0               0           0
    On                          0               0           0
    Off                         0               0           0
Accounting Responses            0               8           0
    Start                       0               8           0
    Interim                     0               0           0
    Stop                        0               0           0
    On                          0               0           0
    Off                         0               0           0
Change of Auth Requests         0               0           0
Change of Auth Responses        0               0           0
    Ack                         0               0           0
```

```
    Nak                       0               0           0
Disconnect Message Requests   0               0           0
Disconnect Message Responses  0               0           0
    Ack                       0               0           0
    Nak                       0               0           0

Duplicates:                                    0
Request Processing Errors:                     0
Response Processing Errors:                    0
Request Transmit Errors :                      0
Response Transmit Errors:                      0
Request Enqueue Errors:                        0
Response Enqueue Errors:                       0
Request Timeouts:                              0
Request Retransmissions:                       0
Missing TDF Domain:                            0
Missing PCEF profile:                          0
Dropped Requests:                              0
Dropped Responses:                             0
Server Initiated Request Processing Errors:    0
Dropped Server Initiated Requests:             0
Duplicate Server Initiated Requests:           0
Cached Reply Sent:                             0
```

show unified-edge tdf aaa statistics detail

```
user@host> show unified-edge tdf aaa statistics detail


Gateway Name: TDF
FPC/PIC: 2/0
Messages                  Received        Sent        Forwarded In     Forwarded
Out   Snooped
-------------------------------------------------------------------------------
-------------

Total Messages               2               2           0
0            0
Access Requests              0               0           0
0            0
```

```
Access Responses              0               0           0
0            0
    Accept                    0               0           0
0            0
    Reject                    0               0           0
0            0
Accounting Requests           2               0           0
0            0
    Start                     2               0           0
0            0
    Interim                   0               0           0
0            0
    Stop                      0               0           0
0            0
    On                        0               0           0
0            0
    Off                       0               0           0
0            0
Accounting Responses          0               2           0
0            0
    Start                     0               2           0
0            0
    Interim                   0               0           0
0            0
    Stop                      0               0           0
0            0
    On                        0               0           0
0            0
    Off                       0               0           0
0            0
Change of Auth Requests       0               0           0
0            0
Change of Auth Responses      0               0           0
0            0
    Ack                       0               0           0
0            0
    Nak                       0               0           0
0            0
Disconnect Message Requests   0               0           0
0            0
Disconnect Message Responses  0               0           0
0            0
    Ack                       0               0           0
```

```
0            0
    Nak                       0               0           0
0            0

Duplicates:                                    0
Request Processing Errors:                     0
Response Processing Errors:                    0
Request Transmit Errors :                      0
Response Transmit Errors:                      0
Request Enqueue Errors:                        0
Response Enqueue Errors:                       0
Request Timeouts:                              0
Request Retransmissions:                       0
Missing TDF Domain:                            0
Missing PCEF profile:                          0
Dropped Requests:                              0
Dropped Responses:                             0
Server Initiated Request Processing Errors:    0
Dropped Server Initiated Requests:             0
Duplicate Server Initiated Requests:           0
Cached Reply Sent:                             0

Gateway Name: TDF
FPC/PIC: 2/1
Messages                     Received        Sent        Forwarded In
Forwarded Out   Snooped
-------------------------------------------------------------------------------
-----------------
Total Messages                 0               0             0
0            0
Access Requests                0               0             0
0            0
Access Responses               0               0             0
0            0
    Accept                     0               0             0
0            0
    Reject                     0               0             0
0            0
Accounting Requests            0               0             0
0            0
    Start                      0               0             0
0            0
    Interim                    0               0             0
```

```
0            0
    Stop                        0              0              0
0            0
    On                          0              0              0
0            0
    Off                         0              0              0
0            0
Accounting Responses            0              0              0
0            0
    Start                       0              0              0
0            0
    Interim                     0              0              0
0            0
    Stop                        0              0              0
0            0
    On                          0              0              0
0            0
    Off                         0              0              0
0            0
Change of Auth Requests         0              0              0
0            0
Change of Auth Responses        0              0              0
0            0
    Ack                         0              0              0
0            0
    Nak                         0              0              0
0            0
Disconnect Message Requests     0              0              0
0            0
Disconnect Message Responses    0              0              0
0            0
    Ack                         0              0              0
0            0
    Nak                         0              0              0
0            0

Duplicates:                                 0
Request Processing Errors:                  0
Response Processing Errors:                 0
Request Transmit Errors :                   0
Response Transmit Errors:                   0
Request Enqueue Errors:                     0
Response Enqueue Errors:                    0
```

```
Request Timeouts:                              0
Request Retransmissions:                       0
Missing TDF Domain:                            0
Missing PCEF profile:                          0
Number of Dropped Requests:                                  0
Dropped Responses:                             0
Server Initiated Request Processing Errors:    0
Dropped Server Initiated Requests:             0
Duplicate Server Initiated Requests:           0
Cached Reply Sent:                             0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- clear unified-edge tdf aaa statistics | **784**
- show unified-edge tdf aaa radius client statistics | **915**
- show unified-edge tdf aaa radius server statistics | **930**
- Understanding How a RADIUS Server Controls Policy and Charging Control Rules | **64**
- IP-Based Subscriber Setup Overview | **107**
- Snooping RADIUS Accounting Requests for IP-Based Subscribers Overview | **114**

show unified-edge tdf address-assignment pool

IN THIS SECTION

- Syntax | **959**
- Description | **959**
- Options | **959**
- Required Privilege Level | **960**
- Output Fields | **960**

Sample Output | 962
Release Information | 964

Syntax

```
show unified-edge tdf address-assignment pool
<brief | detail | summary>
<fpc-slot fpc-slot>
<gateway gateway-name>
<name pool-name>
<pic-slot pic-slot>
<routing-instance routing-instance>
```

Description

Display information about the address pools for one or more TDF gateways. If a TDF gateway is not specified, then information for all TDF gateways is displayed.

Options

none	(Same as brief) Display address information about the address pools in brief for all TDF gateways.
brief | detail | summary	(Optional) Display the specified level of output.
fpc-slot *fpc-slot*	(Optional) Display address pool information for the session PIC in the specified FPC slot.
gateway *gateway-name*	(Optional) Display address pool information for the specified TDF gateway.
name *pool-name*	(Optional) Display information for the specified address pool.
pic-slot *pic-slot*	(Optional) Display address pool information for the session PIC in the specified PIC slot.
routing-instance *routing-instance*	(Optional) Display the address pool information for the specified routing instance.

Required Privilege Level

view

Output Fields

Table 42 on page 960 lists the output fields for the **show unified-edge tdf address-assignment pool** command. Output fields are listed in the approximate order in which they appear.

Table 42: show unified-edge tdf address-assignment pool Output Fields

Field Name	Field Description	Level of Output
Pool or **Name**	Name of the address pool.	All levels
FPC/PIC	FPC and PIC slots of the session PIC for which the address pool information is displayed.	**detail**
Total addresses	Total number of addresses available in the address pool.	**brief** **detail**
Total	Total number of addresses available in the address pool.	**summary**
Addresses in use	Number of addresses that have been allocated.	**brief** **detail**
In-use	Number of addresses that have been allocated.	**summary**
Addresses skipped	Number of addresses that are excluded from allocation.	**brief** **detail**

Table 42: show unified-edge tdf address-assignment pool Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Address usage (percent)	Percentage of the total addresses used.	**brief** **detail**
Util (%)	Percentage of the total addresses used.	**summary**
Addresses in aging period	Number of addresses that are currently being released and that cannot be allocated.	**brief** **detail**
Routing Instance	Name of the routing instance to which the address pool belongs.	All levels
Gateway	TDF gateway to which the session PIC belongs.	**detail**
Pool Maintenance Mode	Service mode of the address pool; for example, Operational or Maintenance.	**detail**
Address chunks	Number of chunks of IP addresses in the address pool (for the session PIC) that are currently being assigned	**detail**
Total address chunk size	Total number of addresses in the address chunk (for the session PIC).	**detail**
Total allocation failures	Total number of addresses that were not allocated.	**detail**

Sample Output

show unified-edge tdf address-assignment pool brief

```
user@host> show unified-edge tdf address-assignment pool brief


Pool: pool1
  Total addresses:           16777215
  Addresses in use:          1600
  Addresses skipped:         416
  Address usage (percent):   0
  Addresses in aging period: 1600
  Routing instance:          default


Pool: pool2
  Total addresses:           256
  Addresses in use:          254
  Addresses skipped:         2
  Address usage (percent):   99
  Addresses in aging period: 0
  Routing instance:          default

[...output truncated...]
```

show unified-edge tdf address-assignment pool detail

```
user@host> show unified-edge tdf address-assignment pool detail

Pool: pool1 (FPC/PIC: 4/0)
  Pool Maintenance Mode:     Operational
  Total addresses:           16777215
  Addresses in use:          822
  Addresses skipped:         208
  Address usage (percent):   0
  Addresses in aging period: 822
  Routing instance:          default
  Gateway:                   TDF
  Address chunks:            26
```

```
  Total address chunk size:  26416
  Total allocation failures: 0

Pool: pool1 (FPC/PIC: 4/1)
  Pool Maintenance Mode:     Operational
  Total addresses:           16777215
  Addresses in use:          778
  Addresses skipped:         208
  Address usage (percent):   0
  Addresses in aging period: 778
  Routing instance:          default
  Gateway:                   TDF
  Address chunks:            26
  Total address chunk size:  26416
  Total allocation failures: 0

Pool: pool2 (FPC/PIC: 4/0)
  Pool Maintenance Mode:     Operational
  Total addresses:           256
  Addresses in use:          0
  Addresses skipped:         0
  Address usage (percent):   0
  Addresses in aging period: 0
  Routing instance:          default
  Gateway:                   TDF
  Address chunks:            0
  Total address chunk size:  0
  Total allocation failures: 0

[...output truncated...]
```

show unified-edge tdf address-assignment pool summary

```
user@host> show unified-edge tdf address-assignment pool summary
                                                 Util
Name                          Total       In-use     (%)  Routing instance
pool1                         16777215    1600       0    default
pool2                         256         254        99   default
pool3                         256         47         18   default
v4_pool                       16777216    0          0    default
v4_pool1                      16777215    0          0    default
```

```
v6_pool                        16777215     0           0     default
v6_pool1                       16777215     0           0     default
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf address-assignment pool | 786

show unified-edge tdf address-assignment service-mode

IN THIS SECTION

- Syntax | 964
- Description | 965
- Options | 965
- Required Privilege Level | 965
- Output Fields | 965
- Sample Output | 966
- Release Information | 967

Syntax

```
show unified-edge tdf address-assignment service-mode
<brief | detail>
<pool pool-name>
<routing-instance routing-instance-name>
```

Description

Display service mode information about address pools.

Options

none	(Same as brief) Display service mode information in brief.
brief | detail	(Optional) Display the specified level of output.
pool *pool-name*	(Optional) Display service mode information for the specified address pool.
routing-instance *routing-instance-name*	(Optional) Display service mode information about the address pools that are part of the specified routing instance.

Required Privilege Level

view

Output Fields

Table 43 on page 965 lists the output fields for the **show unified-edge tdf address-assignment service-mode** command. Output fields are listed in the approximate order in which they appear.

Table 43: show unified-edge tdf address-assignment service-mode Output Fields

Field Name	Field Description	Level of Output
Maintenance Mode	Phases applicable when the address pool is in maintenance mode. • **MM - Active Phase**—All the attributes of the address pool can be modified. • **MM - In/Out Phase**—Only the non-maintenance mode attributes of the address pool can be modified.	None specified
Pool Name	Name of the address pool.	All levels

Table 43: show unified-edge tdf address-assignment service-mode Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Routing Instance	Routing instance to which the address pool belongs.	All levels
Service Mode	Service mode for the address pool: • **Operational**—Address pool is in operational mode. • **Maintenance**—Address pool is in maintenance mode. • **Maintenance - Active Phase**—All the attributes of the address pool can be modified. • **Maintenance - In/Out Phase**—Only the non-maintenance mode attributes of the address pool can be modified.	All levels

Sample Output

show unified-edge tdf address-assignment service-mode brief

```
user@host> show unified-edge tdf address-assignment service-mode brief
Maintenance Mode
    MM Active Phase - System is ready to accept configuration changes for all
                      attributes of this object and its sub-hierarchies.
    MM In/Out Phase - System is ready to accept configuration changes only for
                      non-maintenance mode attributes of this object and
                      its sub-hierarchies.

Routing-Instance               Pool Name                      Service Mode

default                        my_pool                        Operational
default                        v6_pool                        Operational
```

show unified-edge tdf address-assignment service-mode detail

```
user@host> show unified-edge tdf address-assignment service-mode detail
Routing Instance: default
Pool Name       : my_pool
Service Mode    : Operational

Routing Instance: default
Pool Name       : v6_pool
Service Mode    : Operational
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Address Pools for Source-IP Filtering of IP-Based Subscribers | 119

show unified-edge tdf address-assignment statistics

IN THIS SECTION

- Syntax | 968
- Description | 968
- Options | 968
- Required Privilege Level | 968
- Output Fields | 968
- Sample Output | 969
- Release Information | 970

Syntax

```
show unified-edge tdf address-assignment statistics
<brief | detail>
<fpc-slot fpc-slot>
<gateway gateway-name>
<pic-slot pic-slot>
```

Description

Display address assignment statistics for one or more TDF gateways. If a TDF gateway is not specified, then the consolidated statistics for all TDF gateways are displayed.

Options

none	(Same as brief) Display address assignment statistics in brief for all TDF gateways.
brief | detail	(Optional) Display the specified level of output.
fpc-slot *fpc-slot*	(Optional) Display statistics for the session PIC in the specified FPC slot.
gateway *gateway-name*	(Optional) Display consolidated statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Display statistics for the session PIC in the specified PIC slot.

Required Privilege Level

view

Output Fields

Table 44 on page 969 lists the output fields for the **show unified-edge tdf address-assignment statistics** command. Output fields are listed in the approximate order in which they appear.

Table 44: show unified-edge tdf address-assignment statistics Output Fields

Field Name	Field Description	Level of Output
FPC/PIC	FPC and PIC slots for which the statistics are displayed.	**detail**
Gateway	Name of the TDF gateway.	**detail**
Total address allocations	Total number of addresses allocated.	All levels
Total allocation failures	Total number of address allocations that failed.	All levels
Total address releases	Total number of addresses that were released.	All levels

Sample Output

show unified-edge tdf address-assignment statistics

```
user@host> show unified-edge tdf address-assignment statistics


Address assignment statistics
  Total address allocations: 1101
  Total allocation failures: 0
  Total address releases:    800
```

show unified-edge tdf address-assignment statistics detail

```
user@host> show unified-edge tdf address-assignment statistics detail


Address assignment statistics   (FPC/PIC: 4/0)
  Gateway:                    TDF
  Total address allocations: 416
  Total allocation failures: 0
```

```
  Total address releases:    416

Address assignment statistics   (FPC/PIC: 4/1)
  Gateway:                   TDF
  Total address allocations: 685
  Total allocation failures: 0
  Total address releases:    384
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf address-assignment statistics | 788

show unified-edge tdf call-admission-control statistics

IN THIS SECTION

- Syntax | 970
- Description | 971
- Options | 971
- Required Privilege Level | 971
- Output Fields | 971
- Sample Output | 973
- Release Information | 974

Syntax

```
show unified-edge tdf call-admission-control statistics
<detail>
```

```
<fpc-slot fpc-slot>
<gateway gateway-name>
<pic-slot pic-slot>
```

Description

Display call admission control (CAC) statistics for one or more TDF gateways. If a TDF gateway is not specified, then statistics for all TDF gateways are displayed.

NOTE: CAC statistics are not stored on the Routing Engine. When this command is executed, the Routing Engine fetches the statistics from the active session PICs and displays the consolidated statistics for one or more TDF gateways.

Options

none	Display CAC statistics for all TDF gateways.
detail	(Optional) Display detailed CAC statistics for the specified FPC and PIC slot numbers. **NOTE**: The **detail** option is valid only when you specify an FPC and PIC slot number configured on the TDF gateway.
fpc-slot *fpc-slot*	(Optional) Display statistics for the session PIC in the specified FPC slot.
pic-slot *pic-slot*	(Optional) Display statistics for the session PIC in the specified PIC slot.
gateway *gateway-name*	(Optional) Display CAC statistics for the specified TDF gateway.

Required Privilege Level

view

Output Fields

Table 45 on page 972 lists the output fields for the **show unified-edge tdf call-admission-control statistics** command. Output fields are listed in the approximate order in which they appear.

Table 45: show unified-edge tdf call-admission-control statistics Output Fields

Field Name	Field Description	Level of Output
Gateway: TDF	Output is displayed for TDF gateways.	**detail** none
GW CAC Statistics	Statistical details are displayed at the TDF gateway level.	**detail** none
Memory High Rejects	Number of subscribers or PDP contexts that were rejected because the memory load or utilization (at the session PIC level) was high.	**detail** none
Memory High Redirects	Number of subscribers or PDP contexts that were redirected because the memory load or utilization (at the session PIC level) was high.	**detail** none
CPU High Rejects	Number of subscribers or PDP contexts that were rejected because the CPU load or utilization (at the session PIC level) was high.	**detail** none
CPU High Redirects	Number of subscribers or PDP contexts that were redirected because the CPU load or utilization (at the session PIC level) was high.	**detail** none
Session Reservation Rejects	Number of sessions that were rejected for reservation of TDF subscribers on a particular TDF gateway or domain.	**detail** none
Session Reservation Redirects	Number of sessions that were redirected to a different TDF gateway or domain for reservation of TDF subscribers.	**detail** none

Table 45: show unified-edge tdf call-admission-control statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Gateway Subscriber Count	Total number of subscribers that are connected to the TDF gateway.	**detail** none
TDF DOMAIN CAC Statistics	Statistical details are displayed at the TDF domain level.	**detail** none
Session Reservation Rejects	Number of sessions that were rejected for reservation of TDF subscribers on a particular TDF gateway or domain.	**detail** none
Session Reservation Redirects	Number of sessions that were redirected to a different TDF gateway or domain for reservation of TDF subscribers.	**detail** none

Sample Output

show unified-edge tdf call-admission-control statistics

```
user@host> show unified-edge tdf call-admission-control statistics
Gateway: TDF

GW CAC Statistics:
  Memory High Rejects                     :   0
  Memory High Redirects                   :   0
  CPU High Rejects                        :   0
  CPU High Redirects                      :   0
  Session Reservation Rejects             :   0
  Session Reservation Redirects           :   0
  Gateway Subscriber Count                :   1

Domain CAC Statistics:
  Session Reservation Rejects             :   0
  Session Reservation Redirects           :   0
```

show unified-edge tdf call-admission-control statistics fpc-slot pic-slot detail

```
user@host> show unified-edge tdf call-admission-control statistics fpc-slot 3 pic-slot 1 detail

Gateway: TDF

GW CAC Statistics:
  Memory High Rejects                       :   0
  Memory High Redirects                     :   0
  CPU High Rejects                          :   0
  CPU High Redirects                        :   0
  Session Reservation Rejects               :   0
  Session Reservation Redirects             :   0
  Gateway Subscriber Count                  :   1

Domain CAC Statistics:
  Session Reservation Rejects               :   0
  Session Reservation Redirects             :   0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf call-admission-control statistics | 790

show unified-edge tdf call-rate statistics

IN THIS SECTION

Syntax | 975

- Description | 975
- Options | 975
- Required Privilege Level | 975
- Output Fields | 975
- Sample Output | 977
- Release Information | 977

Syntax

```
show unified-edge tdf call-rate statistics (domain domain-name | gateway gateway-name)
```

Description

Display call-rate statistics for the specified TDF domain or specified TDF gateway.

Options

domain *domain-name*	Display call-rate statistics for the specified TDF domain.
gateway *gateway-name*	Display call-rate statistics for the specified TDF gateway.

Required Privilege Level

view

Output Fields

Table 46 on page 976 lists the output fields for the **show unified-edge tdf call-rate statistics** command. Output fields are listed in the approximate order in which they appear.

Table 46: show unified-edge tdf call-rate statistics Output Fields

Field Name	Field Description
Gateway	Name of the TDF gateway.
TDF domain name	Name of the TDF domain. This is displayed only when the **domain** option is used.
Record *n*	Displays statistics for the most recent *n* number of intervals.
Number of Activations	Number of successful subscriber logins for this record.
Number of Deactivations	Number of subscriber logouts for this record.
Activations processing time (in ms)	Average subscriber login activation processing time.
Subscriber session duration (in mins)	Average subscriber session duration.
Statistics collection time	Time at which the statistics were collected.
Control Plane Standard Deviation	Standard deviations for the following: • **Number of Activations**—Number of subscriber logins • **Number of Deactivations**—Number of subscriber logouts • **Activations processing time**—Length of time of subscriber login • **Subscriber session duration**—Length of time of subscriber logout

Sample Output

show unified-edge tdf call-rate statistics gateway

```
user@host> show unified-edge tdf call-rate statistics gateway TDF
Gateway: TDF
Record 1 (Call-rate statistics for the past 1 min):
Control Plane:
        Number of Activations:                  0
        Number of Deactivations:                0
        Activations processing time (in ms):    0
        Subscriber session duration (in mins):  0

Statistics collection time: 2014-03-04 11:45:44 UTC (00:03:06 ago)

Record 2 (Call-rate statistics for the past 2 min):
Control Plane:
        Number of Activations:                  0
        Number of Deactivations:                0
        Activations processing time (in ms):    0
        Subscriber session duration (in mins):  0

Control Plane Standard Deviation:
        Number of Activations:                  0
        Number of Deactivations:                0
        Activations processing time:            0
        Subscriber session duration:            0

Statistics collection time: 2014-03-04 11:44:44 UTC (00:04:06 ago)
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

Configuring Call-Rate Statistics Collection | 241

show unified-edge tdf diameter network-element statistics

IN THIS SECTION

- Syntax | 978
- Description | 978
- Options | 978
- Required Privilege Level | 979
- Output Fields | 979
- Sample Output | 980
- Release Information | 981

Syntax

```
show unified-edge tdf diameter network-element statistics
<brief | detail>
<fpc-slot fpc-slot>
<gateway gateway-name>
<network-element-name network-element-name>
<pic-slot pic-slot>
```

Description

Display statistics for network elements for one or more TDF gateways. If a network element is not specified, then statistics for all network elements are displayed. If a TDF gateway is not specified, then statistics for all TDF gateways are displayed.

Options

none	Display statistics for network elements for all TDF gateways.
brief | detail	(Optional) Display the specified level of output. The **brief** output is displayed by default.
fpc-slot *fpc-slot*	(Optional) Display statistics for the specified Flexible PIC Concentrator (FPC).

gateway *gateway-name*	(Optional) Display statistics for the specified TDF gateway.
network-element-name *network-element-name*	(Optional) Display statistics for the specified network element.
pic-slot *pic-slot*	(Optional) Display the statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

view

Output Fields

Table 47 on page 979 lists the output fields for the **show unified-edge tdf diameter network-element statistics** command. Output fields are listed in the approximate order in which they appear.

Table 47: show unified-edge tdf diameter network-element statistics Output Fields

Field Name	Field Description	Level of Output
Name	Name of the network element.	All levels
FPC/PIC	FPC and PIC slot numbers through which the network element was reached.	**detail**
Packets Received	Number of incoming packets.	All levels
Packets Transmitted	Number of outgoing packets.	All levels
Request Timeouts	Number of request timeouts.	All levels
Credit Control Request Transmitted	Number of outgoing Credit-Control-Request messages.	All levels
Credit Control Answer Received	Number of incoming Credit-Control-Answer messages.	All levels

Sample Output

show unified-edge tdf diameter network-element statistics

```
user@host> show unified-edge tdf diameter network-element statistics

  Name:   pcrf-dne
     Packets Received :                       0
     Packets Transmitted :                    0
     Request Timeouts :                       0
     Credit Control Request Transmitted :     0
     Credit Control Answer Received :         0

  Name:   ocs-dne
     Packets Received :                       3
     Packets Transmitted :                    4
     Request Timeouts :                       1
     Credit Control Request Transmitted :     4
     Credit Control Answer Received :         3
```

show unified-edge tdf diameter network-element statistics detail

```
user@host> show unified-edge tdf diameter network-element statistics detail

  Name :                                  pcrf-dne
  FPC/PIC :                               0/0
  Packets Received :                      0
  Packets Transmitted :                   0
  Request Timeouts :                      0
  Credit Control Request Transmitted :    0
  Credit Control Answer Received :        0

  FPC/PIC :                               0/1
  Packets Received :                      0
  Packets Transmitted :                   0
  Request Timeouts :                      0
  Credit Control Request Transmitted :    0
  Credit Control Answer Received :        0

  Name :                                  ocs-dne
```

```
FPC/PIC :                              0/0
Packets Received :                     0
Packets Transmitted :                  0
Request Timeouts :                     0
Credit Control Request Transmitted :   0
Credit Control Answer Received :       0

FPC/PIC :                              0/1
Packets Received :                     3
Packets Transmitted :                  4
Request Timeouts :                     1
Credit Control Request Transmitted :   4
Credit Control Answer Received :       3
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf diameter network-element statistics | 791

show unified-edge tdf diameter network-element status | 981

show unified-edge tdf diameter network-element status

IN THIS SECTION

- Syntax | 982
- Description | 982
- Options | 982
- Required Privilege Level | 982
- Output Fields | 982
- Sample Output | 983
- Release Information | 984

Syntax

```
show unified-edge tdf diameter network-element status
<fpc-slot fpc-slot>
<gateway gateway-name>
<network-element-name network-element-name>
<pic-slot pic-slot>
```

Description

Display the status for one or more Diameter network elements. If a network element is not specified, then status for all network elements is displayed. If a TDF gateway is not specified, then status for all TDF gateways is displayed.

Options

none	Display status for all network elements for all TDF gateways.
fpc-slot ***fpc-slot***	(Optional) Display the status for the specified Flexible PIC Concentrator (FPC).
gateway ***gateway-name***	(Optional) Display the status for the specified TDF gateway.
network-element-name ***network-element-name***	(Optional) Display the status for the specified network element.
pic-slot ***pic-slot***	(Optional) Display the status for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

view

Output Fields

Table 48 on page 983 lists the output fields for the **show unified-edge tdf diameter network-element status** command. Output fields are listed in the approximate order in which they appear.

Table 48: show unified-edge tdf diameter network-element status Output Fields

Field Name	Field Description
DNE	Name of the network element.
PEER	Name of the peer.
FPC/PIC	FPC and PIC slot numbers through which the network element was reached.
PEER STATE	Current state of the peer. Possible states are: **Closed**, **Closing**, **I-Open**, **R-Open**, **Wait-Conn-Ack**, **Wait-Conn-Ack/Elect**, **Wait-I-CEA**, and **Wait-Returns**.
WATCHDOG STATE	Peer watchdog status. • **closed**—Connection between Diameter peers is terminated. • **initial**—Connection between Diameter peers is being initialized. • **okay**—Connection between Diameter peers is established and active.

Sample Output

show unified-edge tdf diameter network-element status

```
user@host> show unified-edge tdf diameter network-element status
DNE : pcrf-dne
    PEER : pcrf
       FPC/PIC          PEER STATE            WATCHDOG STATE
         0/0            Closed                initial
         0/1            Closed                initial
DNE : ocs-dne
    PEER : ocs
       FPC/PIC          PEER STATE            WATCHDOG STATE
         0/0            I-Open                okay
         0/1            I-Open                okay
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf diameter network-element statistics | 978

show unified-edge tdf diameter pcc-gx statistics

IN THIS SECTION

- Syntax | 984
- Description | 984
- Options | 985
- Required Privilege Level | 985
- Output Fields | 985
- Sample Output | 990
- Release Information | 991

Syntax

```
show unified-edge tdf diameter pcc-gx statistics
<brief | detail>
<fpc-slot fpc-slot>
<gateway gateway-name>
<pic-slot pic-slot>
```

Description

Display statistics for the Gx application for one or more TDF gateways. If a TDF gateway is not specified, then statistics for all TDF gateways are displayed.

Options

none	Display statistics for the Gx application for all TDF gateways.
brief | detail	(Optional) Display the specified level of output. The **brief** output is displayed by default.
fpc-slot *fpc-slot*	(Optional) Display statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway-name*	(Optional) Display statistics for the specified TDF gateway.
pic-slot *pic-slot*	(Optional) Display statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

view

Output Fields

Table 49 on page 985 lists the output fields for the **show unified-edge tdf diameter pcc-gx statistics** command. Output fields are listed in the approximate order in which they appear.

Table 49: show unified-edge tdf diameter pcc-gx statistics Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the TDF gateway.	All levels
FPC/PIC	FPC and PIC slots for which the statistics are displayed.	**detail**
Total Sessions Established	Total number of active sessions.	All levels
Total Sessions Terminated	Total number of terminated sessions.	All levels

Table 49: show unified-edge tdf diameter pcc-gx statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Internal Errors	Number of internal errors.	**detail**
Total	• **Requests**—Total number of request messages. • **Answers**—Total number of answer messages.	none **brief**
Credit Control Initial	• **Requests**—Number of initial transfer type Credit-Control-Request (CCR) messages. • **Answers**—Number of initial transfer type Credit-Control-Answer (CCA) messages.	none **brief**
Credit Control Update	• **Requests**—Number of update transfer type CCR messages. • **Answers**—Number of update transfer type CCA messages.	none **brief**
Credit Control Terminate	• **Requests**—Number of terminate transfer type CCR messages. • **Answers**—Number of terminate transfer type CCA messages.	none **brief**
Re-Auth	• **Requests**—Number of Re-Auth-Request (RAR) messages. • **Answers**—Number of Re-Auth-Answer (RAA) messages.	none **brief**
Dropped	• **Requests**—Number of dropped request messages. • **Answers**—Number of dropped answer messages.	none **brief**

Table 49: show unified-edge tdf diameter pcc-gx statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Requests Transmitted	• **Initial**—Number of initial transfer type CCR messages sent. • **Update**—Number of update transfer type CCR messages sent. • **Terminate**—Number of terminate transfer type CCR messages sent. • **Total**—Number of CCR messages sent.	**detail**
Request Timeouts	• **Initial**—Number of initial transfer type CCR messages that timed out. • **Update**—Number of update transfer type CCR messages that timed out. • **Terminate**—Number of terminate transfer type CCR messages that timed out. • **Total**—Number of CCR messages that timed out.	**detail**
Request Tx Timeouts	• **Initial**—Number of initial transfer type CCR messages sent that timed out. • **Update**—Number of update transfer type CCR messages sent that timed out. • **Terminate**—Number of terminate transfer type CCR messages sent that timed out. • **Total**—Number of CCR messages sent that timed out.	**detail**

Table 49: show unified-edge tdf diameter pcc-gx statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Request Discarded	• **Initial**—Number of initial transfer type CCR messages sent that were discarded. • **Update**—Number of update transfer type CCR messages sent that were discarded. • **Terminate**—Number of terminate transfer type CCR messages sent that were discarded. • **Total**—Number of CCR messages sent that were discarded.	**detail**
Answers Received	• **Initial**—Number of initial transfer type CCA messages received. • **Update**—Number of update transfer type CCA messages received. • **Terminate**—Number of terminate transfer type CCA messages received. • **Total**—Number of CCA messages received.	**detail**
Answers Dropped	• **Initial**—Number of initial transfer type CCA messages dropped. • **Update**—Number of update transfer type CCA messages dropped. • **Terminate**—Number of terminate transfer type CCA messages dropped. • **Total**—Number of CCA messages dropped.	**detail**

Table 49: show unified-edge tdf diameter pcc-gx statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Answers Parse Errors	• **Initial**—Number of initial transfer type CCA messages with parse errors. • **Update**—Number of update transfer type CCA messages with parse errors. • **Terminate**—Number of terminate transfer type CCA messages with parse errors. • **Total**—Number of CCA messages with parse errors.	**detail**
Answers with Invalid AVP(s)	• **Initial**—Number of initial transfer type CCA messages with invalid AVPs. • **Update**—Number of update transfer type CCA messages with invalid AVPs. • **Terminate**—Number of terminate transfer type CCA messages with invalid AVPs. • **Total**—Number of CCA messages with invalid AVPs.	**detail**
Requests Received	Number of RAR messages received.	**detail**
Requests Dropped	Number of RAR messages dropped.	**detail**
Requests Parse Errors	Number of RAR messages with parse errors.	**detail**
Requests with Invalid AVP(s)	Number of RAR messages with invalid AVPs.	**detail**
Answers Transmitted	Number of RAA messages sent.	**detail**

Sample Output

show unified-edge tdf diameter pcc-gx statistics

```
user@host> show unified-edge tdf diameter pcc-gx statistics
  Gateway: TDF
    Total Sessions Established:             0
    Total Sessions Terminated:                      0
                               Requests             Answers
    ------------------------------------------------------
    Total                      0                    0
    Credit Control Initial     0                    0
    Credit Control Update      0                    0
    Credit Control Terminate   0                    0
    Re-Auth                    0                    0
    Dropped                    0                    0
```

show unified-edge tdf diameter pcc-gx statistics detail

```
user@host> show unified-edge tdf diameter pcc-gx statistics detail
  Gateway: TDF
  FPC/PIC: 0/0
    Total Sessions Established:             0
    Total Sessions Terminated:  0
    Internal Errors:            0

    Credit Control                  Initial     Update      Terminate       Total
    ------------------------------------------------------------------------------
    Requests Transmitted            0           0           0               0
    Request Timeouts                0           0           0               0
    Request Tx Timeouts             0           0           0               0
    Request Discarded               0           0           0               0
    Answers Received                0           0           0               0
    Answers Dropped                 0           0           0               0
    Answers Parse Errors            0           0           0               0
    Answers with Invalid AVP(s)     0           0           0               0

    Server Requests                 Re-Auth
    ---------------------------------------
    Requests Received               0
```

```
    Requests Dropped                0
    Requests Parse Errors           0
    Requests with Invalid AVP(s)    0
    Answers Transmitted             0

  Gateway: TDF
  FPC/PIC: 0/1
    Total Sessions:             0
    Total Sessions Terminated:  0
    Internal Errors:            0

    Credit Control                  Initial     Update      Terminate       Total
    ------------------------------------------------------------------------------
    Requests Transmitted            0           0           0               0
    Request Timeouts                0           0           0               0
    Request Tx Timeouts             0           0           0               0
    Request Discarded               0           0           0               0
    Answers Received                0           0           0               0
    Answers Dropped                 0           0           0               0
    Answers Parse Errors            0           0           0               0
    Answers with Invalid AVP(s)     0           0           0               0

    Server Requests                 Re-Auth
    ---------------------------------------
    Requests Received               0
    Requests Dropped                0
    Requests Parse Errors           0
    Requests with Invalid AVP(s)    0
    Answers Transmitted             0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf diameter pcc-gx statistics | 793

show unified-edge tdf diameter peer statistics

IN THIS SECTION

- Syntax | 992
- Description | 992
- Options | 992
- Required Privilege Level | 993
- Output Fields | 993
- Sample Output | 996
- Release Information | 998

Syntax

```
show unified-edge tdf diameter peer statistics
<brief | detail>
<fpc-slot fpc-slot>
<gateway gateway-name>
<peer-name peer-name>
<pic-slot pic-slot>
```

Description

Display statistics for Diameter peers for one or more TDF gateways. If a peer is not specified, then statistics for all Diameter peers are displayed. If a TDF gateway is not specified, then statistics for all TDF gateways are displayed.

Options

none	(Same as brief) Display statistics for Diameter peers for all TDF gateways in brief.
brief | detail	(Optional) Display the specified level of output. The **brief** output is displayed by default.

fpc-slot *fpc-slot*	(Optional) Display statistics for the specified Flexible PIC Concentrator (FPC).
gateway *gateway-name*	(Optional) Display statistics for the specified TDF gateway.
peer-name *peer-name*	(Optional) Display statistics for the specified peer.
pic-slot *pic-slot*	(Optional) Display statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

view

Output Fields

Table 50 on page 993 lists the output fields for the **show unified-edge tdf diameter peer statistics** command. Output fields are listed in the approximate order in which they appear.

Table 50: show unified-edge tdf diameter peer statistics Output Fields

Field Name	Field Description	Level of Output
Peer	Name of the peer.	All levels
FPC/PIC	FPC and PIC slot numbers through which the peer was reached.	**detail**
Request Timeouts	Number of request timeouts.	All levels
Request Retransmissions	Number of request retransmissions.	All levels
Connect Failures	Number of connection failures.	**detail**
Duplicate Requests	Number of duplicate requests.	**detail**
Malformed Messages	Number of malformed requests.	**detail**

Table 50: show unified-edge tdf diameter peer statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Dropped Responses	Number of dropped responses.	**detail**
Dropped Requests	Number of dropped requests.	**detail**
Last Disconnect Cause	Number of last disconnect cause messages.	**detail**
Transport Failures	Number of transport failures.	**detail**
Unknown Messages	Number of unknown type errors.	**detail**
High Watermark Hits	Number of times the high watermark is reached.	**detail**
Low Watermark Hits	Number of times the low watermark is reached.	**detail**
Device Watchdog Failured	Number of device watchdog failures.	**detail**
Capabilities Exchange Failures	Number of capabilities exchange failures.	**detail**
Total Messages	Total number of messages transmitted and received.	All levels
Credit Control Requests	Number of Credit-Control-Request messages transmitted and received.	All levels
Credit Control Answers	Number of Credit-Control-Answer messages transmitted and received.	All levels
Re-Auth Requests	Number of Re-Auth-Request messages transmitted and received.	All levels

Table 50: show unified-edge tdf diameter peer statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Re-Auth Answers	Number of Re-Auth-Answer messages transmitted and received.	All levels
Abort Session Requests	Number of Abort-Session-Request messages transmitted and received.	All levels
Abort Session Answers	Number of Abort-Session-Answer messages transmitted and received.	All levels
Capability Exchange Requests	Number of Capabilities-Exchange-Request messages transmitted and received.	All levels
Capability Exchange Answers	Number of Capabilities-Exchange-Answer messages transmitted and received.	All levels
Device Watchdog Requests	Number of Device-Watchdog-Request messages transmitted and received.	All levels
Device Watchdog Answers	Number of Device-Watchdog-Answer messages transmitted and received.	All levels
Disconnect Peer Requests	Number of Disconnect-Peer-Request messages transmitted and received.	All levels
Disconnect Peer Answers	Number of Disconnect-Peer-Answer messages transmitted and received.	All levels
Permanent Failures	Number of permanent failure result codes transmitted and received.	**detail**

Table 50: show unified-edge tdf diameter peer statistics Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Protocol Errors	Number of protocol error result codes transmitted and received.	**detail**
Transient Failures	Number of transient failure result codes transmitted and received.	**detail**

Sample Output

show unified-edge tdf diameter peer statistics

```
user@host> show unified-edge tdf diameter peer statistics
Peer: ocs
    Request Timeouts:                   1
    Request Retransmissions:            0
    Messages                            Transmitted       Received
    ------------------------------------------------------------
    Total Messages                      6                 5
    Credit Control Requests             4                 0
    Credit Control Answers              0                 3
    Re-Auth Requests                    0                 0
    Re-Auth Answers                     0                 0
    Abort Session Requests              0                 0
    Abort Session Answers               0                 0
    Capability Exchange Requests        2                 0
    Capability Exchange Answers         0                 2
    Device Watchdog Requests            0                 0
    Device Watchdog Answers             0                 0
    Disconnect Peer Requests            0                 0
    Disconnect Peer Answers             0                 0
```

show unified-edge tdf diameter peer statistics detail

```
user@host> show unified-edge tdf diameter peer statistics detail
Peer: ocs
    FPC/PIC: 0/0
    Request Timeouts:                   0
    Request Retransmissions:            0
    Connect Failures:                   0
    Duplicate Requests:                 0
    Malformed Messages:                 0
    Dropped Responses:                  0
    Dropped Requests:                   0
    Last Disconnect Cause:              0
    Transport Failures:                 0
    Unknown Messages:                   0
    High Watermark Hits:                0
    Low Watermark Hits:                 0
    Device Watchdog Failured:           0
    Capabilities Exchange Failures:     0

    Messages                            Transmitted       Received
    ------------------------------------------------------------
    Total Messages                      1                 1
    Credit Control Requests             0                 0
    Credit Control Answers              0                 0
    Re-Auth Requests                    0                 0
    Re-Auth Answers                     0                 0
    Abort Session Requests              0                 0
    Abort Session Answers               0                 0
    Capability Exchange Requests        1                 0
    Capability Exchange Answers         0                 1
    Device Watchdog Requests            0                 0
    Device Watchdog Answers             0                 0
    Disconnect Peer Requests            0                 0
    Disconnect Peer Answers             0                 0

    Result-Code                         Transmitted       Received
    ------------------------------------------------------------
    Permanent Failures                  0                 0
    Protocol Errors                     0                 0
    Transient Failures                  0                 0
```

```
FPC/PIC: 0/1
Request Timeouts:                   1
Request Retransmissions:            0
Connect Failures:                   0
Duplicate Requests:                 0
Malformed Messages:                 0
Dropped Responses:                  0
Dropped Requests:                   0
Last Disconnect Cause:              0
Transport Failures:                 0
Unknown Messages:                   0
High Watermark Hits:                0
Low Watermark Hits:                 0
Device Watchdog Failured:           0
Capabilities Exchange Failures:     0

Messages                            Transmitted       Received
-------------------------------------------------------------
Total Messages                      5                 4
Credit Control Requests             4                 0
Credit Control Answers              0                 3
Re-Auth Requests                    0                 0
Re-Auth Answers                     0                 0
Abort Session Requests              0                 0
Abort Session Answers               0                 0
Capability Exchange Requests        1                 0
Capability Exchange Answers         0                 1
Device Watchdog Requests            0                 0
Device Watchdog Answers             0                 0
Disconnect Peer Requests            0                 0
Disconnect Peer Answers             0                 0

Result-Code                         Transmitted       Received
-------------------------------------------------------------
Permanent Failures                  0                 0
Protocol Errors                     0                 0
Transient Failures                  0                 0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf diameter peer statistics | 795

show unified-edge tdf diameter peer status | 999

show unified-edge tdf diameter peer status

IN THIS SECTION

- Syntax | 999
- Description | 999
- Options | 1000
- Required Privilege Level | 1000
- Output Fields | 1000
- Sample Output | 1002
- Release Information | 1003

Syntax

```
show unified-edge tdf diameter peer status
<brief | detail>
<fpc-slot fpc-slot>
<gateway gateway-name>
<peer-name peer-name>
<pic-slot pic-slot>
```

Description

Display the status for one or more Diameter peers. If a peer is not specified, then status for all Diameter peers is displayed. If a TDF gateway is not specified, then status for all TDF gateways is displayed.

Options

none	(Same as brief) Display the status for Diameter peers for all TDF gateways in brief.
brief | detail	(Optional) Display the specified level of output. The **brief** output is displayed by default.
fpc-slot *fpc-slot*	(Optional) Display the status for the specified Flexible PIC Concentrator (FPC).
gateway *gateway-name*	(Optional) Display the status for the specified TDF gateway.
peer-name *peer-name*	(Optional) Display the status for the specified peer.
pic-slot *pic-slot*	(Optional) Display the status for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level

view

Output Fields

Table 51 on page 1000 lists the output fields for the **show unified-edge tdf diameter peer status** command. Output fields are listed in the approximate order in which they appear.

Table 51: show unified-edge tdf diameter peer status Output Fields

Field Name	Field Description	Level of Output
Name	Name of the peer. For the **brief** output, the name is truncated if it exceeds 11 characters.	All levels
FPC/PIC	FPC and PIC slot numbers through which the peer was reached.	All levels
Address	IP address of the Diameter peer.	**brief** none

Table 51: show unified-edge tdf diameter peer status Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Port	Port number of the Diameter peer.	**brief** none
State	Current state of the Diameter peer. Possible states are: **Closed**, **Closing**, **I-Open**, **R-Open**, **Wait-Conn-Ack**, **Wait-Conn-Ack/Elect**, **Wait-I-CEA**, and **Wait-Returns**. For the **brief** and none output, the state is truncated if it exceeds 11 characters.	All levels
Duration	Duration for which the Diameter peer has been in the current state in Coordinated Universal Time (UTC) format (HH:MM:SS).	none **brief**
State Duration	Duration for which the Diameter peer has been in the current state in Coordinated Universal Time (UTC) format (HH:MM:SS).	**detail**
Watchdog	Peer watchdog status. • **closed**—Connection between Diameter peers is terminated. • **initial**—Connection between Diameter peers is being initialized. • **okay**—Connection between Diameter peers is established and active.	none **brief**
Watchdog State	Peer watchdog status. • **closed**—Connection between Diameter peers is terminated. • **initial**—Connection between Diameter peers is being initialized. • **okay**—Connection between Diameter peers is established and active.	**detail**

Table 51: show unified-edge tdf diameter peer status Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Origin Host	Diameter Origin-Host.	**detail**
Origin Realm	Diameter Origin-Realm.	**detail**
Peer Address	IP address of the Diameter peer.	**detail**
Peer port	Port number of the Diameter peer.	**detail**
Source Address	Local source IP address used to connect to the peer.	**detail**
Source Port	Local source port number used to connect to the peer.	**detail**

Sample Output

show unified-edge tdf diameter peer status

```
user@host> show unified-edge tdf diameter peer status
Name          FPC/PIC  Address          Port    State        Duration  Watchdog
p_jpkt1       4/0      192.0.2.2        3868    Closed       00:00:00  initial
p_jpkt1       4/1      192.0.2.2        3868    Closed       00:00:00  initial
p_jpkt1       5/0      192.0.2.2        3868    Wait-Conn-A  00:00:00  initial
abcabcabcab   4/0      192.0.2.2        3868    Closed       00:00:00  initial
abcabcabcab   4/1      192.0.2.2        3868    Closed       00:00:00  initial
abcabcabcab   5/0      192.0.2.2        3868    Wait-Conn-A  00:00:00  initial
```

show unified-edge tdf diameter peer status detail

```
user@host> show unified-edge tdf diameter peer status detail
Diameter Peer Status
  Name : ocs
     FPC/PIC               :          0/0
```

```
    State                 :          I-Open
    State Duration        :          00:00:00
    Watchdog State        :          okay
    Origin Host           :          host5
    Origin Realm          :          example.com
    Peer Address          :          198.51.100.2
    Peer port             :          3868
    Source Address        :          203.0.113.1
    Source Port           :          30965
Name : ocs
    FPC/PIC               :          0/1
    State                 :          I-Open
    State Duration        :          00:00:00
    Watchdog State        :          okay
    Origin Host           :          host5
    Origin Realm          :          example.com
    Peer Address          :          198.51.100.2
    Peer port             :          3868
    Source Address        :          203.0.113.1
    Source Port           :          30709
Name : pcrf
    FPC/PIC               :          0/0
    State                 :          Closed
    State Duration        :          00:00:00
    Watchdog State        :          initial
    Peer Address          :          192.168.1.2
    Peer port             :          3868
    Source Address        :          203.0.113.1
    Source Port           :          0
Name : pcrf
    FPC/PIC               :          0/1
    State                 :          Closed
    State Duration        :          00:00:00
    Watchdog State        :          initial
    Peer Address          :          192.168.1.2
    Peer port             :          3868
    Source Address        :          203.0.113.1
    Source Port           :          0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf diameter peer statistics | 992

show unified-edge tdf domain service-mode

IN THIS SECTION

- Syntax | 1004
- Description | 1004
- Options | 1004
- Required Privilege Level | 1005
- Output Fields | 1005
- Sample Output | 1006
- Release Information | 1007

Syntax

```
show unified-edge tdf domain service-mode
<domain-name tdf-domain-name>
<brief | detail>
<gateway gateway>
```

Description

Display service mode information for a TDF domain for one or more TDF gateways. If a TDF domain is not specified, then the information for all domains for one or more TDF gateways is displayed.

Options

none (Same as brief) Display the TDF domain service mode information in brief for all TDF gateways.

brief | detail	(Optional) Display the specified level of output.
domain-name *tdf-domain-name*	(Optional) Display service mode information for the specified TDF domain.
gateway *gateway*	(Optional) Display service mode information for the specified TDF gateway.

Required Privilege Level

view

Output Fields

Table 52 on page 1005 lists the output fields for the **show unified-edge tdf domain service-mode** command. Output fields are listed in the approximate order in which they appear.

Table 52: show unified-edge tdf domain service-mode Output Fields

Field Name	Field Description	Level of Output
Maintenance Mode	Phases applicable when the address pool is in maintenance mode. • **MM - Active Phase**—All the attributes of the address pool can be modified. • **MM - In/Out Phase**—Only the non-maintenance mode attributes of the address pool can be modified.	None specified
Gateway Name	Name of the TDF gateway.	None specified
Gateway	Name of the TDF gateway.	**detail**
TDF domain Name	Name of the TDF domain.	All levels

Table 52: show unified-edge tdf domain service-mode Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Service Mode	Service mode for the TDF gateway: • **Operational**—Gateway is in operational mode. • **Maintenance**—Gateway is in maintenance mode.	All levels

Sample Output

show unified-edge tdf domain service-mode brief

```
user@host> show unified-edge tdf domain service-mode brief
Maintenance Mode
    MM Active Phase - System is ready to accept configuration changes for all
                      attributes of this object and its sub-hierarchies.
    MM In/Out Phase - System is ready to accept configuration changes only for
                      non-maintenance mode attributes of this object and
                      its sub-hierarchies.

TDF domain Name               Gateway Name                    Service Mode

jnpr-sunnyvale                  TDF                             Operational
jnpr-toxin                      TDF                             Operational
zoo                             TDF1                            Maintenance -
Active Phase
```

show unified-edge tdf domain service-mode detail

```
user@host> show unified-edge tdf domain service-mode detail
Gateway: TDF
TDF domain Name        : jnpr-sunnyvale
Service Mode    : Operational

TDF domain Name        : jnpr-toxin
```

```
Service Mode     : Operational
Gateway: TDF1

TDF domain Name         : zoo
Service Mode     : Maintenance - Active Phase
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf service-mode | 1017

show unified-edge tdf domain statistics

IN THIS SECTION

- Syntax | 1007
- Description | 1008
- Options | 1008
- Required Privilege Level | 1008
- Output Fields | 1008
- Sample Output | 1012
- Release Information | 1014

Syntax

```
show unified-edge tdf domain statistics
<domain-name domain-name>
<gateway gateway>
```

Description

Display statistics for one or more domains in a TDF gateway. If a TDF gateway is not specified, then statistics for all TDF gateways are displayed.

Options

none	Display statistics for all domains for all TDF gateways.
domain-name *domain-name*	(Optional) Display the statistics for the specified TDF domain. The output of the **show unified-edge tdf domain statistics** command is the same as the output of the **show unified-edge tdf statistics** command with the **tdf-domain** option.
gateway *gateway*	(Optional) Display the statistics for the specified TDF gateway.

Required Privilege Level

view

Output Fields

Table 53 on page 1008 lists the output fields for the **show unified-edge tdf domain statistics** command. Output fields are listed in the approximate order in which they appear.

Table 53: show unified-edge tdf domain statistics Output Fields

Field Name	Field Description
Gateway	Name of the TDF gateway.
Control Plane Statistics	
Subscriber attach attempts	Number of attempted session establishments and number of successful session establishments (**Success**).

Table 53: show unified-edge tdf domain statistics Output Fields *(Continued)*

Field Name	Field Description
TDF Time of day initiated update attempts	Number of attempted activations of rules based on time of day settings and number of successful activations (**Success**).
TDF initiated subscriber detach attempts	Number of attempted subscriber session detachments initiated by the TDF.
PCRF initiated subscriber detach attempts	Number of attempted subscriber session detachments initiated by the PCRF.
Peer initiated subscriber detach attempts	Number of attempted subscriber session detachments initiated by the peer.
Subscriber attach failures by cause	Number of session establishments that failed: • **System failure** • **No resources** • **Policy denied** • **Service denied** • **Others**
Rejects due to early CAC	Number of subscriber sessions rejected due to early call admission control (CAC) for the TDF gateway.
Policy statistics	

Table 53: show unified-edge tdf domain statistics Output Fields *(Continued)*

Field Name	Field Description
Subscriber session activation attempts	Number of subscriber session activations attempted. In addition, the number of successful subscriber session establishments (**Success**) is displayed.
TDF initiated modification attempts	Number of session modifications initiated by TDF gateway. In addition, the number session modifications that were successful (**Success**) is displayed.
PCRF initiated modification attempts	Number of session modifications initiated by the policy and charging rules function (PCRF). In addition, the number of modifications that were successful (**Success**) is displayed.
TDF initiated session deactivations	Number of subscriber session deactivations initiated by the TDF gateway.
PCRF initiated session deactivations	Number of subscriber session deactivations initiated by the PCRF.
Modification event reason	The number of Gx modifications for each event reason: • **Application Start** • **Application Stop**

Table 53: show unified-edge tdf domain statistics Output Fields *(Continued)*

Field Name	Field Description
Failure Statistics	• **Session terminations due to unreachable PCRF**—Number of sessions terminated because the PCRF was unreachable. • **Session terminations due to PCRF restart**—Number of sessions terminated because the PCRF was restarted. • **Rule Validation Failures**—Number of sessions terminated because the validation of rules failed.
PCC Rule Statistics	• **Dynamic rule activations**—Number of dynamic rule activations and deactivations (**Deactivations**). • **Static rule activations**—Number of static rule activations and deactivations (**Deactivations**). • **Dynamic rule modifications**—Number of dynamic rule modifications.
PCC Rule Failure Statistics	• **Rule update failure**—Number of rules that cannot be updated.
ePCC/ADC Rule Statistics	• **Dynamic rule activations**—Number of dynamic rule activations and deactivations (**Deactivations**). • **Static rule activations**—Number of static rule activations and deactivations (**Deactivations**). • **Dynamic rule modifications**—Number of dynamic rule modifications.
ePCC/ADC Rule Failure Statistics	• **Rule update failure**—Number of rules that cannot be updated.

Sample Output

show unified-edge tdf domain statistics gateway

```
user@host> show unified-edge tdf domain statistics gateway tdf
Gateway: TDF
Control Plane Statistics:
    Subscriber attach attempts:                 0     Success: 0
    TDF Time of day initiated update attempts:  0     Success: 0
    TDF initiated subscriber detach attempts:   0
    PCRF initiated subscriber detach attempts:  0
    Peer initiated subscriber detach attempts:  0
    Subscriber attach failures by cause:
       System failure:      0
       No resources:        0
       Service denied:      0
       Policy denied:       0
       Others:              0
    Rejects due to early CAC: 0
Policy Statistics:
    Subscriber session activation attempts:     0     Success: 0
    TDF initiated modification attempts:        0     Success: 0
    PCRF initiated modification attempts:       0     Success: 0
    TDF initiated session deactivations:        0
    PCRF initiated session deactivations:       0
  Modification Event Reason:
       Application Start:   0
       Application Stop:    0
  Failure Statistics:
       Session terminations due to unreachable PCRF:  0
       Session terminations due to PCRF restart:      0
       Rule validation failures:                      0
  PCC Rule Statistics:
       Dynamic rule activations:     0      Deactivations:   0
       Static rules activations:     0      Deactivations:   0
       Dynamic rule modifications:   0
  PCC Rule Failure Statistics:
       Rule update failure:                 0
  ePCC/ADC Rule Statistics:
       Dynamic rule activations:     0      Deactivations:   0
       Static rules activations:     0      Deactivations:   0
       Dynamic rule modifications:   0
```

```
  ePCC/ADC Rule Failure Statistics:
       Rule update failure:                  0
```

show unified-edge tdf domain statistics domain-name

```
user@host> show unified-edge tdf domain statistics domain-name domain1
domain-name domain1
Gateway: TDF
Control Plane Statistics:
    Subscriber attach attempts:                 0     Success: 0
    TDF Time of day initiated update attempts:  0     Success: 0
    TDF initiated subscriber detach attempts:   0
    PCRF initiated subscriber detach attempts:  0
    Peer initiated subscriber detach attempts:  0
    Subscriber attach failures by cause:
       System failure:      0
       No resources:        0
       Service denied:      0
       Policy denied:       0
       Others:              0
Policy Statistics:
    Subscriber session activation attempts:     0     Success: 0
    TDF initiated modification attempts:        0     Success: 0
    PCRF initiated modification attempts:       0     Success: 0
    TDF initiated session deactivations:        0
    PCRF initiated session deactivations:       0
  Modification Event Reason:
       Application Start:   0
       Application Stop:    0
  Failure Statistics:
       Session terminations due to unreachable PCRF:  0
       Session terminations due to PCRF restart:      0
       Rule validation failures:                      0
  PCC Rule Statistics:
       Dynamic rule activations:     0      Deactivations:   0
       Static rules activations:     0      Deactivations:   0
       Dynamic rule modifications:   0
  PCC Rule Failure Statistics:
       Rule update failure:                  0
  ePCC/ADC Rule Statistics:
```

```
        Dynamic rule activations:     0      Deactivations:   0
        Static rules activations:     0      Deactivations:   0
        Dynamic rule modifications:   0
  ePCC/ADC Rule Failure Statistics:
        Rule update failure:                  0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

clear unified-edge tdf statistics | **797**

show unified-edge tdf resource-manager clients

IN THIS SECTION

- Syntax | **1014**
- Description | **1015**
- Options | **1015**
- Required Privilege Level | **1015**
- Output Fields | **1015**
- Sample Output | **1016**
- Release Information | **1017**

Syntax

show unified-edge tdf resource-manager clients

<gateway *gateway*>

Description

Display information about the resource management clients (the session Dense Port Concentrators [DPCs] and interface DPCs and Modular Port Concentrators [MPCs]) on one or more TDF gateways. If a TDF gateway is not specified, then information for all TDF gateways is displayed.

Options

none	Display information for all TDF gateways.
gateway *gateway-name*	(Optional) Display information for the specified TDF gateway.

Required Privilege Level

view

Output Fields

Table 54 on page 1015 lists the output fields for the **show unified-edge gateways tdf resource-manager clients** command. Output fields are listed in the approximate order in which they appear.

Table 54: show unified-edge tdf resource-manager clients Output Fields

Field Name	Field Description
Client	Name of the resource manager client slot identified by the FPC and PIC slot numbers; for example, pfe-1/2/0 or ms-/7/0/0.
State	Resource manager client state. **In-Service** means that the client can handle session creation requests.
Role	Role of the resource manager client slot: • **Primary**—The resource manager client is a primary member. • **Secondary**—The resource manager client is a secondary or backup member.

Table 54: show unified-edge tdf resource-manager clients Output Fields *(Continued)*

Field Name	Field Description
Client type	Type of resource manager client: • **Session PIC**—Session PIC client used for the mobile control plane in the TDF gateway. • **Service PIC**—services PIC used for anchoring services-related subscriber sessions in the TDF gateway.
Gateway	Name of the TDF gateway to which the resource manager client belongs.

Sample Output

show unified-edge tdf resource-manager clients

```
user@host> show unified-edge tdf resource-manager clients
Client      State          Redundancy role Client type Gateway
ms-2/0/0    In-Service     Primary         Service-PIC TDF
ms-2/1/0    In-Service     Secondary       Service-PIC TDF
ms-3/0/0    In-Service     Primary         Service-PIC TDF
ms-3/1/0    In-Service     Primary         Service-PIC TDF
ms-5/0/0    In-Service     Primary         Session-PIC TDF
ms-5/1/0    In-Service     Secondary       Session-PIC TDF
```

show unified-edge tdf resource-manager clients gateway

```
user@host> show unified-edge tdf resource-manager clients gateway TDF
Client      State          Redundancy role Client type Gateway
ms-3/0/0    In-Service     Secondary       Session-PIC TDF
ms-3/1/0    In-Service     Primary         Session-PIC TDF
ms-3/2/0    In-Service     Secondary       Service-PIC TDF
ms-3/3/0    In-Service     Primary         Service-PIC TDF
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf subscribers | 1038

show unified-edge tdf system interfaces | 1059

show unified-edge tdf service-mode

IN THIS SECTION

- Syntax | 1017
- Description | 1017
- Options | 1018
- Required Privilege Level | 1018
- Output Fields | 1018
- Sample Output | 1019
- Release Information | 1020

Syntax

show unified-edge tdf service-mode
<brief | detail>
<**domain-name** *tdf-domain-name*>
<gateway *gateway-name***>**

Description

Display service mode information for one or more TDF gateways. If a TDF gateway is not specified, then service mode information for all the TDF gateways is displayed.

Options

none	(Same as brief) Display service mode information in brief for all TDF gateways.
brief | detail	(Optional) Display the specified level of output.
tdf-domain *domain-name*	(Optional) Display service mode information for the specified TDF domain. The output of the **show unified-edge tdf service-mode** command with the **tdf-domain** option is the same as the output of the **show unified-edge tdf domain service-mode** command.
gateway *gateway-name*	(Optional) Display service mode information for the specified TDF gateway.

Required Privilege Level

view

Output Fields

Table 55 on page 1018 lists the output fields for the **show unified-edge tdf service-mode** command. Output fields are listed in the approximate order in which they appear.

Table 55: show unified-edge tdf service-mode Output Fields

Field Name	Field Description	Level of Output
Maintenance Mode	Phases applicable when the TDF domain is in maintenance mode. • **MM - Active Phase**—All the attributes of the address pool can be modified. • **MM - In/Out Phase**—Only the non-maintenance mode attributes of the address pool can be modified.	none
Gateway Name	Name of the TDF gateway.	none

Table 55: show unified-edge tdf service-mode Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Service Mode	Service mode for the TDF gateway: • **Operational**—Gateway is in operational mode. • **Maintenance**—Gateway is in maintenance mode.	All levels

Sample Output

show unified-edge tdf service-mode brief

```
user@host> show unified-edge tdf service-mode brief
Maintenance Mode
    MM Active Phase - System is ready to accept configuration changes for all
                      attributes of this object and its sub-hierarchies.
    MM In/Out Phase - System is ready to accept configuration changes only for
                      non-maintenance mode attributes of this object and
                      its sub-hierarchies.

Gateway Name                    Service Mode

TDF                             Operational
TDF2                            Operational
```

show unified-edge tdf service-mode detail

```
user@host> show unified-edge tdf service-mode detail
Service Mode Status
Gateway Name    : PGW
Service Mode    : Operational
Service Mode Status
Gateway Name    : PGW2
Service Mode    : Operational
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf domain service-mode | 1004

show unified-edge tdf statistics

IN THIS SECTION

- Syntax | 1020
- Description | 1020
- Options | 1021
- Required Privilege Level | 1021
- Output Fields | 1021
- Sample Output | 1029
- Release Information | 1031

Syntax

```
show unified-edge tdf statistics
<domain domain-name>
<gateway gateway>
```

Description

Display statistics for one or more TDF gateways. If a TDF gateway is not specified, then statistics for all TDF gateways are displayed.

Options

none	Display statistics for all TDF gateways.
domain *domain-name*	(Optional) Display statistics for the specified TDF domain. The output of the **show unified-edge tdf statistics** command with the **domain** *domain-name* option is the same as the output of the **show unified-edge tdf domain statistics** command.
gateway *gateway*	(Optional) Display statistics for the specified TDF gateway.

Required Privilege Level

view

Output Fields

Table 56 on page 1021 lists the output fields for the **show unified-edge tdf statistics** command. Output fields are listed in the approximate order in which they appear.

Table 56: show unified-edge tdf statistics Output Fields

Field Name	Field Description
Gateway	Name of the TDF gateway.
Control Plane Statistics	
Subscriber attach attempts	Number of attempted session establishments and number of successful session establishments for IP-based subscribers (**Success**).
Peer initiated subscriber update attempts	Number of RADIUS client attempts to update the subscriber context of an IP-based subscriber.

Table 56: show unified-edge tdf statistics Output Fields *(Continued)*

Field Name	Field Description
TDF Time of day initiated update attempts	Number of attempted activations, deactivations, and revalidations of PCC rules and revalidations of the PCEF session for the time-of-day feature, and number of successful attempts (**Success**).
TDF initiated update attempts	Number of TDF gateway attempts to update an IFL-based subscriber context as a result of access interfaces going up or down, or as a result of access interfaces being added to or deleted from the subscriber configuration.
TDF initiated subscriber detach attempts	Number of attempted subscriber session detachments initiated by the TDF gateway.
Policy Server initiated subscriber detach attempts	Number of attempted subscriber session detachments initiated by the policy server.
Peer initiated subscriber detach attempts	Number of attempted IP-based subscriber session detachments initiated by the RADIUS client. For IFL-based subscribers, 0 is displayed.

Table 56: show unified-edge tdf statistics Output Fields *(Continued)*

Field Name	Field Description
Subscriber attach failures by cause	Number of session establishments that failed: • **System failure** • **No resources** • **Service denied** • **Policy denied** • **Service PIC NACK** • **Others**
Rejects due to early CAC	Number of rejects on the TDF gateway caused by early CAC.
Subscriber detach by cause	Number of subscriber detachments for the following cause: • **service PIC NACK**
Policy statistics	
Subscriber session activation attempts	Number of subscriber session activations attempted. In addition, the number of successful subscriber session establishments (**Success**) is displayed.
TDF initiated modification attempts	Number of session modifications initiated by TDF gateway. In addition, the number of session modifications that were successful (**Success**) is displayed.

Table 56: show unified-edge tdf statistics Output Fields *(Continued)*

Field Name	Field Description
Policy Server initiated modification attempts	Number of session modifications initiated by the policy server. In addition, the number of modifications that were successful (**Success**) is displayed.
TDF initiated session deactivations	Number of subscriber session deactivations initiated by the TDF gateway.
Policy Server initiated session deactivations	Number of subscriber session deactivations initiated by the policy server.
Modification event reason	Number of Gx modifications for each event reason: • **Application Start** • **Application Stop** • **Revalidation**—PCEF re-requested PCC rules from the PCRF.
Failure Statistics	• **Session terminations due to unreachable policy server**—Number of sessions terminated because the policy server was unreachable. • **Session terminations due to PCRF restart**—Number of sessions terminated because the PCRF was restarted. • **Rule Validation Failures**—Number of sessions terminated because the validation of rules failed.

Table 56: show unified-edge tdf statistics Output Fields *(Continued)*

Field Name	Field Description
PCC Rule Statistics	• **Dynamic rule activations**—Number of dynamic rule activations and deactivations (**Deactivations**). • **Static rules activations**—Number of static rule activations and deactivations (**Deactivations**). • **Dynamic rule modifications**—Number of dynamic rule modifications.
PCC Rule Failure Statistics	• **Rule update failure**—Number of rules that cannot be updated.
ePCC/ADC Rule Statistics	• **Dynamic rule activations**—Number of dynamic rule activations and deactivations (**Deactivations**). • **Static rules activations**—Number of static rule activations and deactivations (**Deactivations**). • **Dynamic rule modifications**—Number of dynamic rule modifications.
ePCC/ADC Rule Failure Statistics	• **Rule update failure**—Number of rules that cannot be updated.
Usage Monitoring Statistics	
UMI AVP validation failures	Number of times that decoding fails for any of the grouped AVPs that belong to the Usage Monitoring Information, such as the Monitoring key, Monitoring Level, and Granted Service Unit AVPs.

Table 56: show unified-edge tdf statistics Output Fields *(Continued)*

Field Name	Field Description
Session Level	The following information about usage monitoring at the session level is displayed: • **UM activations**—Number of session-level monitoring keys that the TDF gateway has activated. • **UM update quota attempts**—Number of times the PCRF has attempted to update the quota for a session-level monitoring key. The number of reports that the TDF gateway sent as a result of the update quota attempts is shown in **Stats report sent**. • **UM implicit deactivations**—Number of times that a session-level monitoring key has been implicitly deactivated by the TDF gateway. For example, this happens if a monitoring key does not receive additional quota after a threshold has been reached. • **UM explicit deactivations**—Number of session-level monitoring key deactivations that the TDF gateway has received from the PCRF. The number of reports that the TDF gateway sent as a result of the deactivations is shown in **Stats report sent**. • **Usage report request received**—Number of requests for session-level usage reports that the TDF gateway has received from the PCRF. The number of reports that the TDF gateway sent as a result of the requests is shown in **Stats report sent**. • **UM threshold hit**—Number of times that a threshold for a session-level monitoring key has been reached. The number of reports that the TDF gateway sent as a result of the threshold being reached is shown in **Stats report sent**.

Table 56: show unified-edge tdf statistics Output Fields *(Continued)*

Field Name	Field Description
Rule Level	The following information about usage monitoring at the rule level is displayed: • **UM activations**—Number of rule-level monitoring keys that the TDF gateway has activated. • **UM update quota attempts**—Number of times the PCRF has attempted to update the quota for a rule-level monitoring key. The number of reports that the TDF gateway sent as a result of the update quota attempts is shown in **Stats report sent**. • **UM implicit deactivations**—Number of times that a rule-level monitoring key has been implicitly deactivated by the TDF gateway. For example, this happens if a monitoring key does not receive additional quota after a threshold has been reached. • **UM explicit deactivations**—Number of rule-level monitoring key deactivations that the TDF gateway has received from the PCRF. The number of reports that the TDF gateway sent as a result of the deactivations is shown in **Stats report sent**. • **Usage report request received**—Number of requests for rule-level usage reports that the TDF gateway has received from the PCRF. The number of reports that the TDF gateway sent as a result of the requests is shown in **Stats report sent**. • **UM threshold hit**—Number of times that a threshold for a rule-level monitoring key has been reached. The number of reports that the TDF gateway sent as a result of the threshold being reached is shown in **Stats report sent**. • **UM with no rule reference**—Number of rule-level monitoring keys received by the TDF gateway that had no rule referring to it. These keys are not activated.
Service plane statistics	

Table 56: show unified-edge tdf statistics Output Fields *(Continued)*

Field Name	Field Description
Subscriber detach attempts (NACK) by cause	Number of service PIC messages to session PIC indicating that subscriber creation or modification failed for the following causes: • **Memory watermark high threshold hit** • **Memory watermark critical threshold hit** • **Memory alloc failure** • **Subscriber lookup failure** • **Others**
Data plane statistics	
Subscriber Stats	The following information about packets processed by the data plane for subscribers connected to the TDF domains in the TDF gateway is displayed: • **Uplink**—Statistics for traffic in the uplink direction from the TDF gateway to the PDN (Internet). • **Downlink**—Statistics for traffic in the downlink direction from the PDN (Internet) to the TDF gateway. • **Packets**—Number of packets forwarded in the uplink direction and in the downlink direction. • **Bytes**—Number of bytes forwarded in the uplink direction and in the downlink direction. • **Dropped Packets**—Number of packets dropped in the uplink direction and in the downlink direction. • **Dropped Bytes**—Number of bytes dropped in the uplink direction and in the downlink direction.

Table 56: show unified-edge tdf statistics Output Fields *(Continued)*

Field Name	Field Description
Non Subscriber Stats	The following information about packets processed by the data plane for traffic that does not belong to subscribers connected to the TDF domains in the TDF gateway is displayed: • **Uplink**—Statistics for traffic in the uplink direction from the TDF gateway to the PDN (Internet). • **Downlink**—Statistics for traffic in the downlink direction from the PDN (Internet) to the TDF gateway. • **Packets**—Number of packets sent in the uplink direction and in the downlink direction. • **Bytes**—Number of bytes sent in the uplink direction and in the downlink direction. • **Dropped Packets**—Number of packets dropped in the uplink direction and in the downlink direction. • **Dropped Bytes**—Number of bytes dropped in the uplink direction and in the downlink direction.

Sample Output

show unified-edge tdf statistics

```
user@host> show unified-edge tdf statistics
Gateway: TDF
Control Plane Statistics:
    Subscriber attach attempts:                 0     Success: 0
    Peer initiated subscriber update attempts:  0     Success: 0
    TDF Time of day initiated update attempts:  0     Success: 0
    TDF initiated update attempts:              0     Success: 0
    TDF initiated subscriber detach attempts:   0
    Policy Server initiated subscriber detach attempts:  0
    Peer initiated subscriber detach attempts:  0
    Subscriber attach failures by cause:
       System failure:      0
```

```
      No resources:        0
      Service denied:      0
      Policy denied:       0
      Service PIC NACK:    0
      Others:              0
  Rejects due to early CAC:   0
  Subscriber detach by cause:
     service PIC NACK: 0
Policy Statistics:
  Subscriber session activation attempts:     0     Success: 0
  TDF initiated modification attempts:        0     Success: 0
  Policy Server initiated modification attempts:       0     Success: 0
  TDF initiated session deactivations:        0
  Policy Server initiated session deactivations:       0
Modification Event Reason:
     Application Start:               0
     Application Stop:                0
     Revalidation:                    0
Failure Statistics:
     Session terminations due to unreachable policy server: 0
     Session terminations due to PCRF restart:              0
     Rule validation failures:                              0
PCC Rule Statistics:
     Dynamic rule activations:     0      Deactivations:   0
     Static rules activations:     0      Deactivations:   0
     Dynamic rule modifications:   0
PCC Rule Failure Statistics:
     Rule update failure:                0
ePCC/ADC Rule Statistics:
     Dynamic rule activations:     0      Deactivations:   0
     Static rules activations:     0      Deactivations:   0
     Dynamic rule modifications:   0
ePCC/ADC Rule Failure Statistics:
     Rule update failure:                0
Usage Monitoring Statistics:
     UMI AVP validation failures:   0
  Session Level:
       UM activations:               0
       UM update quota attempts:     0      Stats report sent: 0
       UM implicit deactivations:    0
       UM explicit deactivations:    0      Stats report sent: 0
       Usage report request received: 0     Stats report sent: 0
       UM threshold hit:             0      Stats report sent: 0
```

```
    Rule Level:
         UM activations:                0
         UM update quota attempts:      0      Stats report sent: 0
         UM implicit deactivations:     0
         UM explicit deactivations:     0      Stats report sent: 0
         Usage report request received: 0      Stats report sent: 0
         UM threshold hit:              0      Stats report sent: 0
         UM with no rule reference: 0

Service plane statistics:
   Subscriber detach attempts (NACK) by cause:
     Memory watermark high threshold hit:      0
     Memory watermark critical threshold hit:  0
     Memory alloc failure:                     0
     Subscriber lookup failure:                0
     Others:                                   0

Data plane statistics:

Subscriber Stats:
                      Uplink                Downlink
-----------------------------------------------------------------
    Packets          :0                    :0
    Bytes            :0                    :0
    Dropped Packets  :0                    :0
    Dropped Bytes    :0                    :0

Non Subscriber Stats:
                      Uplink                Downlink
-----------------------------------------------------------------
    Packets          :0                    :0
    Bytes            :0                    :0
    Dropped Packets  :0                    :0
    Dropped Bytes    :0                    :0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- clear unified-edge tdf statistics | 797
- show unified-edge tdf domain statistics | 1007
- IP-Based and IFL-Based TDF Subscribers Overview | 107

show unified-edge tdf status

IN THIS SECTION

- Syntax | 1032
- Description | 1032
- Options | 1033
- Required Privilege Level | 1033
- Output Fields | 1033
- Sample Output | 1036
- Release Information | 1038

Syntax

```
show unified-edge tdf status
<brief | detail | extensive>
<domain domain-name>
<fpc-slot fpc-slot>
<gateway gateway>
<pic-slot pic-slot>
<subscriber-state>
```

Description

Display status information, such as the number of subscribers, active sessions, and so on, for one or more TDF gateways. If a TDF gateway name is not specified, then the status information for all the TDF gateways is displayed.

Options

none	(Same as brief) Display the TDF gateway status information in brief for all TDF gateways.
brief | detail | extensive	(Optional) Display the specified level of output.
domain *domain-name*	(Optional) Display the status information for the specified TDF domain.
fpc-slot *fpc-slot*	(Optional) Display the status information for the specified FPC slot number.
gateway *gateway*	(Optional) Display the status information for the specified TDF gateway name.
pic-slot *pic-slot*	(Optional) Display the status information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.
subscriber-state	(Optional) Display the status of the subscribers.

Required Privilege Level

view

Output Fields

Table 57 on page 1033 lists the output fields for the **show unified-edge tdf status** command. Output fields are listed in the approximate order in which they appear.

Table 57: show unified-edge tdf status Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the TDF gateway.	All levels
Established	Number of established subscribers.	none with the **subscriber-state** option
Deleting	Number of subscribers that are being deleted.	none with the **subscriber-state** option

Table 57: show unified-edge tdf status Output Fields *(Continued)*

Field Name	Field Description	Level of Output

Control Plane	The following is displayed for the control plane:
	• **Active Subscribers**—Number of subscribers that are active in each of the following categories:
	  • **IP Subscribers**
	  • **IFL Subscribers**
		none
		brief

Service Plane	The following is displayed for the service plane:
	• **Active Subscribers**—Number of subscribers that are actively using services in each of the following categories:
	  • **IP Subscribers**
	  • **IFL Subscribers**
	• **Active Sessions**—Number of active subscriber sessions.
		none
		brief

CPU Load (%)	Percentage of the CPU load.	All levels
Memory Load (%)	Percentage of the memory load.	All levels
FPC SLOT	FPC slot number of the interface for which the status information is displayed.	**detail** **extensive**

Table 57: show unified-edge tdf status Output Fields *(Continued)*

Field Name	Field Description	Level of Output
PIC SLOT	PIC slot number of the FPC for which the status information is displayed.	**detail** **extensive**
Role	Role of the Packet Forwarding Engine, services PIC, or session PIC on the TDF gateway: • **Standalone** • **Primary**—Primary member. • **Secondary**—Secondary member.	**detail** **extensive**
Type	Indicates whether the PIC is a Packet Forwarding Engine, a session PIC, or a services PIC.	**detail** **extensive**
Active Subscribers	Number of logged-in subscribers on the TDF gateway in each of the following categories: • **IP Subscribers** • **IFL Subscribers**	**brief** **detail** **extensive**
Delete Pending Subscribers	Number of pending subscribers that are being deleted on the TDF gateway in each of the following categories: • **IP Subscribers** • **IFL Subscribers**	**detail** **extensive**

Table 57: show unified-edge tdf status Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Active Sessions	Number of logged-in sessions on the TDF gateway. **NOTE**: Active Sessions count may not match the output of the **show services session count** command. This is due to internal asynchronous message queues.	**detail** **extensive**

Sample Output

show unified-edge tdf status brief

```
user@host> show unified-edge tdf status brief
Gateway: TDF
    TDF gateway status:
    Control Plane:
        Active Subscribers                          :         0
            IP Subscribers                          :         0
            IFL Subscribers                         :         0
    Service Plane:
        Active Subscribers                          :         0
            IP Subscribers                          :         0
            IFL Subscribers                         :         0
        Active Sessions                             :         0
    CPU Load (%)                                    :         0
    Memory Load (%)                                 :         26
```

show unified-edge tdf status detail

```
user@host> show unified-edge tdf status detail
Gateway: TDF

    FPC SLOT: 0   PIC SLOT: 2
```

```
    Role                                        :       Primary
    Type                                        :       Session-PIC
    Active Subscribers                          :       0
        IP Subscribers                          :       0
        IFL Subscribers                         :       0
    CPU Load (%)                                :       0
    Memory Load (%)                             :       26

    FPC SLOT: 0   PIC SLOT: 3
    Role                                        :       Primary
    Type                                        :       Service-PIC
    Active Subscribers                          :       0
        IP Subscribers                          :       0
        IFL Subscribers                         :       0
    Delete Pending Subscribers                  :       0
        IP Subscribers                          :       0
        IFL Subscribers                         :       0
    Active Sessions                             :       0
    CPU Load (%)                                :       1
    Memory Load (%)                             :       12

    FPC SLOT: 1   PIC SLOT: 1
    Role                                        :       Secondary
    Type                                        :       Session-PIC
    Active Subscribers                          :       0
        IP Subscribers                          :       0
        IFL Subscribers                         :       0
    CPU Load (%)                                :       0
    Memory Load (%)                             :       26
```

show unified-edge tdf status subscriber-state

```
user@host> show unified-edge tdf status subscriber-state
show unified-edge tdf status subscriber-state
Gateway: TDF
    Established          :              1
    Deleting             :              0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf aaa statistics | 945

IP-Based and IFL-Based TDF Subscribers Overview | 107

show unified-edge tdf subscribers

IN THIS SECTION

- Syntax | 1038
- Description | 1039
- Options | 1039
- Required Privilege Level | 1040
- Output Fields | 1040
- Sample Output | 1053
- Release Information | 1058

Syntax

```
show unified-edge tdf subscribers
<brief | detail | extensive>
<business-subscribers>
<data-plane>
<domain domain-name>
<fpc-slot fpc-slot>
<gateway gateway>
<pdn-type (ipv4 | ipv4-v6 | ipv6)>
<pic-slot pic-slot>
<routing-instance routing-instance>
```

```
<stuck>
<subscriber-name subscriber-name>
<v4-addr v4-addr>
<v6-addr v6-addr>
```

Description

Display the subscriber information for one or more TDF gateways. If a TDF gateway is not specified, then subscriber information for all TDF gateways is displayed.

Options

none	(Same as brief) Display subscriber information in brief for all TDF gateways.
brief | detail | extensive	(Optional) Display the specified level of output.
business-subscribers	(Optional) Display subscriber information for only enterprise business subscribers (subscribers whose IPv4 prefix length is less than 32).
data-plane	(Optional) Display subscriber information for the data plane.
domain *domain-name*	(Optional) Display subscriber information for the specified TDF domain.
fpc-slot *fpc-slot*	(Optional) Display subscriber information for the specified FPC slot number.
gateway *gateway*	(Optional) Display subscriber information for the specified TDF gateway.
pdn-type (ipv4 | ipv4-v6 | ipv6)	(Optional) Display subscriber information according to the type of Packet Data Network (PDN): IPv4, IPv6, and both IPv4 and IPv6.
pic-slot *pic-slot*	(Optional) Display subscriber information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.
routing-instance *routing-instance*	(Optional) Display subscriber information for the specified routing instance.
stuck	(Optional) Display subscribers for the TDF gateway that are not logged in successfully and are in a blocked state.
subscriber-name *subscriber-name*	(Optional) Display subscriber information for the specified IFL-based subscriber.

v4-addr *v4-addr* (Optional) Display subscriber information for the specified IPv4 address of the subscriber's user equipment.

v6-addr *v6-addr* (Optional) Display subscriber information for the specified IPv6 address of the subscriber's user equipment.

Required Privilege Level

view

Output Fields

Table 58 on page 1040 lists the output fields for the **show unified-edge tdf subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 58: show unified-edge tdf subscribers Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the TDF gateway.	All levels none
MSISDN/ Name	MSISDN number of the IP-based subscriber's user equipment.	**brief** none
V4 Address	IPv4 address of the IP-based subscriber.	**brief** none
V6 Address	IPv6 address, if any, of the IP-based subscriber. Otherwise, **None** is displayed.	**brief** none
NAS-IP-Address	IP address to be used for the NAS IP address attribute of the IP-based subscriber when sending the requests to the RADIUS server.	**brief** none

Table 58: show unified-edge tdf subscribers Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Domain	TDF domain, on the TDF gateway, to which the subscriber is attached.	**brief** none
IFL-Subscriber-Name	Name of the IFL-based subscriber.	**brief** none
Subscriber Information		
Subscriber Type	Type of subscriber: • **IFL**—Interface-based subscriber. • **IP**—IP-based subscriber.	**detail** **extensive**
IMSI	IMSI of the IP-based subscriber's user equipment.	**detail** **extensive** none
IMEI	International Mobile Station Equipment Identity (IMEI) of the IP-based subscriber's user equipment.	**detail** **extensive**
MSISDN/ Username	MSISDN number of the IP-based subscriber's user equipment.	**detail** **extensive**
Subscriber Name	Name of the IFL-based subscriber.	**detail** **extensive**

Table 58: show unified-edge tdf subscribers Output Fields *(Continued)*

Field Name	Field Description	Level of Output
State	State of the subscriber session on the signaling plane.	**detail** **extensive**
Session Duration	Duration of the PDP session.	**detail** **extensive**
Domain	Name of the TDF domain that is used to establish the session on the TDF gateway for the subscriber.	**detail** **extensive**
Data VRF	Name of the data plane VRF.	**detail** **extensive**
TDF domain Name	Unique identifier that denotes the TDF domain to be used for the subscriber's session. This setting is applicable only when the domain specified in the Create Session Request message from the subscriber is virtual.	**detail** **extensive**
NAS-IP-Addr	IP address to be used for the NAS IP address attribute of the IP-based subscriber when sending the requests to the RADIUS server.	**detail** **extensive**
APN name	Name of the APN for the IP-based subscriber that is denoted by a unique identifier.	**detail** **extensive**
V4 Address	IPv4 address of the IP-based subscriber.	**detail** **extensive**

Table 58: show unified-edge tdf subscribers Output Fields *(Continued)*

Field Name	Field Description	Level of Output
V4 Prefix Length	IPv4 prefix length of the IP-based subscriber's IPv4 address. This is displayed only if the length is less than 32.	**detail** **extensive** **data-plane**
V6 Address	IPv6 address of the IP-based subscriber, if any. Otherwise, **None** is displayed.	**detail** **extensive**
V6 Prefix Length	IPv6 prefix length of the IP-based subscriber's IPv6 address.	**detail**
Session PIC	FPC and PIC slots for the session PIC on which the subscriber control session is present.	**detail** **extensive**
Service PIC	FPC and PIC slots for the service PIC on which the subscriber control session is present.	**detail** **extensive**

Table 58: show unified-edge tdf subscribers Output Fields *(Continued)*

Field Name	Field Description	Level of Output
PCRF Event Triggers	Policy and charging rules function (PCRF) event triggers, if any. If no trigger is configured, **None** is displayed. The notation used for the event triggers displayed in the output and the corresponding event triggers as per the 3GPP specifications are as follows: • **SGSN**—SGSN CHANGE (0) • **QoS**—QOS CHANGE (1) • **RAT**—RAT CHANGE (2) • **TFT**—TFT CHANGE (3) • **PLMN**—PLMN CHANGE (4) • **BL**—subscriber LOSS (5) • **BR**—subscriber RECOVERY (6) • **IPCAN**—IPCAN CHANGE (7) • **EAUTH**—EXCEEDING AUTH (11) • **RAI**—RAI CHANGE (12) • **ULI**—ULI CHANGE (13) • **NET**—NO EVENT TRIGGERS (14) • **OOC**—OUT OF CREDIT (15) • **ROC**—REALLOCATION OF CREDIT (16) • **REVALIDATION_TIMEOUT**—REVALIDATION TIMEOUT (17) • **IP ALLOC**—UE_IP_ADDRESS_ALLOCATE (18) • **IP RELEASE**—UE_IP_ADDRESS_RELEASE (19) • **DEFAULT QoS**—DEFAULT QoS (20) • **GW**—AN GW CHANGE (21)	**detail** **extensive**

Table 58: show unified-edge tdf subscribers Output Fields *(Continued)*

Field Name	Field Description	Level of Output
	• **RA**—RESOURCE_ALLOCATION (22) • **RM**—RESOURCE_MODIFICATION (23) • **TRACE**—PGW TRACE CONTROL (24) • **TZ** —UE_TZ_CHANGE (25) • **TAI**—TAI CHANGE (26) • **ECGI**—ECGI CHANGE (27) • **CCE**—CHARGING CORRELATION EXCHANGE (28) • **AMBR**—AMBR CHANGE (29) • **UCIC**—USR CSG INFO CHANGE (30) • **QMF**—QoS MODIFICATION FAILURE (31) • **UR**—USAGE REPORT (33)	
Revalidation due in	Time remaining in days, hours, minutes, and seconds until PCEF session revalidation takes place if the **REVALIDATION_TIMEOUT** event trigger is armed. Otherwise **N/A** is displayed.	**detail** **extensive**
Idle Timeout	Idle timeout for the session, in minutes.	**detail** **extensive**
Subscriber MBR	TDF subscriber maximum bit rate (MBR) for uplink and downlink traffic. Uplink traffic originates from the subscriber towards the public data network (PDN), and downlink traffic comes from the PDN and is destined for the subscriber.	**detail** **extensive**

Table 58: show unified-edge tdf subscribers Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Subscriber burst	TDF subscriber burst size configured for uplink and downlink traffic. Uplink traffic originates from the subscriber towards the PDN, and downlink traffic comes from the PDN and is destined for the subscriber.	**detail** **extensive**
Access IFL List	The following is displayed for each interface assigned to an IFL-based subscriber: • **Name**—Name of the interface. • **Index**—Index number of the interface. • **State**—Operational state of the interface: **Active** or **Inactive**.	
PCC Profile Name	Name of the PCEF profile that is assigned to the subscriber.	**detail** **extensive**

Table 58: show unified-edge tdf subscribers Output Fields *(Continued)*

Field Name	Field Description	Level of Output

Usage Monitoring Information	The following is displayed for each monitoring key, which corresponds to a data set that is being monitored for the subscriber:
	• **Monitoring Key**—Identifier for the monitoring key.
	• **Level**—Indication of whether the monitoring key applies to particular PCC rules (Rule) or to the entire TDF subscriber session (Session).
	• **Status**—Indication of whether monitoring with the key is active or inactive.
	• **Total Available Quota**—Volume and time quota sent from the PCRF to indicate when a report should be sent to the PCRF. A value of zero indicates that the field is not applicable to the key.
	  • **Input**—Uplink traffic volume quota.
	  • **Output**—Downlink traffic volume quota.
	  • **Total**—Uplink and downlink traffic volume quota.
	  • **Time**—Time quota, in seconds.
		detail
		extensive

Table 58: show unified-edge tdf subscribers Output Fields *(Continued)*

Field Name	Field Description	Level of Output

PCC Rule Information	**NOTE**: Both ePCC rules and PCC rules appear under **PCC Rule Information**. Fields that apply only to ePCC rules are identified in the description.
	
	The following information for each PCC or ePCC rule is displayed per subscriber:
	
	• **Rule Name**—Name of the rule. In addition, the following is displayed:
	  • **Type**—Rrule type: **Static** or **Dynamic**.
	  • **Associated Rule Base**—Rule set with which the rule is associated, if any.
	  • **Precedence**—Rule precedence, which defines the order in which the policy is applied for incoming or outgoing packets; the lower the number, the higher its precedence.
	  • **Activation due in**—Day, time, or both at which the rule is scheduled for activation for the subscriber. If activation/deactivation settings have not been applied to the rule, then **N/A** appears.
	  • **Deactivation due in**—Day, time, or both at which the rule is scheduled for deactivation for the subscriber. If activation/deactivation settings have not been applied to the rule, then **N/A** appears.
	  • **Status**—Rule status: **Initialized**, **Active**, **Inactive**, or **Removal Pending**.
	  • **Application Id**—(ePCC rules only) Name of the application identification parameter associated with the rule.
	  • **Application Id Base**–(ePCC rules only) Name of the base application that serves as the primary application identification service if a group or cluster are configured.
		detail
		
		extensive

Table 58: show unified-edge tdf subscribers Output Fields *(Continued)*

Field Name	Field Description	Level of Output

	• **Mute Notification**—(ePCC rules only) Whether the Mute-Notification AVP is included in the rule.
	• **QoS Parameters**—The following QoS attributes are displayed for each rule per subscriber:
	  • **MBR Uplink (kbps)**—Maximum bit rate (MBR) in the uplink direction, in kbps. Identifier.
	  • **MBR Downlink (kbps)**—MBR in the downlink direction, in kbps.
	  • **Burst size Uplink (bytes)**—TDF domain's default TDF subscriber burst size configured for uplink traffic, in bytes.
	  • **Burst size Downlink (bytes)**—TDF domain's default TDF subscriber burst size configured for downlink traffic, in bytes. Uplink traffic originates from the subscriber towards the public data network (PDN), and downlink traffic comes from the PDN and is destined for the subscriber.
	• **Charging Attributes**—The following charging attributes are displayed for each rule per subscriber:
	  • **Rating Group**—Rating group for the rule.
	  • **Service Id**—Service ID for the rule.
	  • **Gating Status**—Whether the flow is enabled or not. One of the following:
	  • **enable-uplink**
	  • **enable-downlink**
	  • **enable-both**
	  • **disable-both**
	  • **AF Charging Id**—Application function record information, which contains an octet string and the charging ID.	

Table 58: show unified-edge tdf subscribers Output Fields *(Continued)*

Field Name	Field Description	Level of Output

	• **Charging Method**—Charging method for the rule (**none**, **offline**, **offline-online**, or **online**).
	• **Metering Method**—Charging metering method for the rule:
	  • **Time**—Time based.
	  • **Volume**—Volume based.
	  • **Volume-Time**—Both volume and time based.
	  • **None**—No metering.
	• **Usage Monitoring Key**—Monitoring key that is associated with the rule.
	• **Services Attributes**—The following information about resource management and steering is displayed for the subscribers connected to the TDF gateway or the TDF domain:
	  • **Steering IP**—IPv4 or IPv6 address for HTTP steering of the packets.
	  • **Keep existing steering**—Whether existing steering is enabled or disabled.
	  • **Service Chain VRF**—Routing instance for steering of packets. Use this to steer traffic to either a local service chain or external service chain.
	  • **Forwarding Class**—Forwarding class that needs to be assigned to the packet.
	  • **HCM ID**—Profile that identifies the HTTP header enrichment rules to apply. This action is restricted to PCC rules that are only matching HTTP-based applications.
	  • **LRF ID**—Unique ID of the Location Retrieval Function
	• **Filter Attributes**—The following filter attributes are displayed per filter in each rule:	

Table 58: show unified-edge tdf subscribers Output Fields *(Continued)*

Field Name	Field Description	Level of Output
	• **Remote IP/Mask**—Remote IP address and subnet mask of the filter. • **Protocol**—Protocol configured for the filter. If all protocols are supported for the filter, **Any** is displayed. For the explanation of what the numbers represent, refer to the 3GPP specifications. • **Direction**—Direction in which the filter is applicable (**Downlink**, **Uplink**, or **Both**). • **Local Ports**—Local ports or port range for the filter. **Any** indicates that the filter does not restrict the local ports. • **Remote Ports**—Remote ports or port range for the filter. **Any** indicates that the filter does not restrict the remote ports. • **Application Name**—(ePCC rules only) Name of the predefined or custom application signature.	

Table 58: show unified-edge tdf subscribers Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Data Plane statistics	The following information about packets processed by the data plane for subscribers connected to the TDF domains in the TDF gateway: • **Subscriber-Name**—Name of the IFL-based subscriber. • **V4 Address**—IPv4 address of the IP-based subscriber. • **V6 Address**—IPv6 address of the IP-based subscriber. • **V6 Prefix Length**—IPv6 prefix length of the IP-based subscriber's IPv6 address. • **Vrf Id**—Name of the data plane VRF. • **Subscriber Stats**—Total statistics for the subscriber. • **Rule**—Statistics for traffic that was handled by the specified PCC rule. • **Uplink**—Statistics for traffic in the uplink direction from the TDF gateway to the PDN (Internet). • **Downlink**—Statistics for traffic in the downlink direction from the PDN (Internet) to the TDF gateway. • **Sessions**—Number of sessions in the uplink and downlink direction. • **Packets**—Number of packets forwarded in the uplink direction and in the downlink direction. • **Bytes**—Number of bytes forwarded in the uplink direction and in the downlink direction. • **Dropped Packets**—Number of packets dropped in the uplink direction and in the downlink direction. • **Dropped Bytes**—Number of bytes dropped in the uplink direction and in the downlink direction.	**data-plane** option

Sample Output

show unified-edge tdf subscribers (IP-Based Subscriber)

```
user@host> show unified-edge tdf subscribers
Gateway: TDF
   MSISDN/name       V4 Address      V6 Address          NAS-IP-Address  Domain
   att               192.0.2.11     None               198.51.100.123 domain1
```

show unified-edge tdf subscribers (IFL-Based Subscriber)

```
user@host> show unified-edge tdf subscribers
IFL-Subscriber-Name                                 Domain
   ifl-sub-radius-001                               domain-ifl-radius
   ifl-sub-static-001                               domain-ifl-static
```

show unified-edge tdf subscribers extensive

```
user@host> show unified-edge tdf subscribers extensive
Gateway: TDF

Subscriber Information:
     Subscriber Type : IFL
     Subscriber Name : IFL1
     State      : Established                    Session Duration: 000065 hrs
50 mins 15 secs
     Domain     : domain1
     Data VRF   : default
     Session PIC: 3 /0  (FPC/PIC)
     Service PIC: 3 /1  (FPC/PIC)
     PCRF Event Triggers : None
     Revalidation due in : N/A
     Subscriber MBR:   Uplink (kbps):  0            Downlink (kbps):  0
     Subscriber burst: Uplink (bytes): 0            Downlink (bytes): 0
     Access IFL List:          Name      (Index)      State
                         ge-1/1/8.0      (362  )      Active
                         ge-1/1/1.0      (361  )      Active
```

```
                        ge-1/0/9.0      (360  )      Active
    PCC Profile Name : pcef-prof-static
    PCC Rule Information:
    Rule Name: google-traffic
       Type      : Static             Associated Rule Base: None
       Precedence: 20                 Status: Active
       Activation due in  : N/A
       Deactivation due in: N/A
     QoS Parameters:
       MBR Uplink (kbps):         0           MBR Downlink (kbps):         0
       Burst size Uplink (bytes): 0           Burst size Downlink (bytes): 0
     Charging Attributes:
       Rating Group: 0          Service ID: 0               Gating Status:
enable-both
       AF Charging Id: None     Charging Method: None       Metering Method: None
       Usage Monitoring Key :  NULL
     Logging Rule Name :  r1
     Services Attributes:
       Forwarding Class: best-effort
     Filter Attributes:
       Remote IP/Mask: any/any            Protocol: any Direction: Both
       Local Ports:  any
       Remote Ports: any
       Application Name   : junos:google
       Application Name   : junos:udp
       Application Name   : junos:http
    Rule Name: http-traffic
       Type      : Static             Associated Rule Base: None
       Precedence: 30                 Status: Active
       Activation due in  : N/A
       Deactivation due in: N/A
     QoS Parameters:
       MBR Uplink (kbps):         0           MBR Downlink (kbps):         0
       Burst size Uplink (bytes): 0           Burst size Downlink (bytes): 0
     Charging Attributes:
       Rating Group: 0          Service ID: 0               Gating Status:
enable-both
       AF Charging Id: None     Charging Method: None       Metering Method: None
       Usage Monitoring Key :  NULL
     Logging Rule Name :  r1
     Services Attributes:
       Forwarding Class: best-effort
     Filter Attributes:
```

```
       Remote IP/Mask: any/any            Protocol: any Direction: Both
       Local Ports:  any
       Remote Ports: any
       Application Name   : junos:http
    Rule Name: all-traffic
       Type      : Static             Associated Rule Base: None
       Precedence: 40                 Status: Active
       Activation due in  : N/A
       Deactivation due in: N/A
     QoS Parameters:
       MBR Uplink (kbps):         0           MBR Downlink (kbps):         0
       Burst size Uplink (bytes): 0           Burst size Downlink (bytes): 0
     Charging Attributes:
       Rating Group: 0          Service ID: 0               Gating Status:
enable-both
       AF Charging Id: None     Charging Method: None       Metering Method: None
       Usage Monitoring Key :  NULL
     Logging Rule Name :  r1
     Services Attributes:
       Forwarding Class: best-effort
     Filter Attributes:
       Remote IP/Mask: any/any            Protocol: any Direction: Both
       Local Ports:  any
       Remote Ports: any
```

show unified-edge tdf subscribers detail

```
user@host> show unified-edge tdf subscribers detail
Gateway: TDF

Subscriber Information:
     Subscriber Type : IP

     IMSI       : 988888888888899               MSISDN/Username : 9741488201
     IMEI       : None
     State      : Established                    Session Duration: 000000 hrs
41 mins 04 secs
     Domain     : aaa
     Data VRF   : bng_vrf
     NAS-IP-Addr: 198.51.100.123
     NAS-ID     : dfssw
```

```
 APN name   : 3242
 V4 Address : 192.0.2.11
 V6 Address : 2001:db8::                          V6 Prefix Length: 64
 Session PIC: 3 /3  (FPC/PIC)
 Service PIC: 3 /0  (FPC/PIC)
 PCRF Event Triggers : UR
 Revalidation due in : N/A
 Idle Timeout: 0   min
 Subscriber MBR:   Uplink (kbps):  0             Downlink (kbps):  0
 Subscriber burst: Uplink (bytes): 0             Downlink (bytes): 0
PCC Profile Name : pcef-jpkt-prof-dyn
Usage Monitoring Information:
  Monitoring Key: 302
   Level: Session Status: Active
     Total Available Quota:
       Input: 0       Output: 0
       Total: 20000   Time  : 100
  Monitoring Key: 301
    Level: PCC-Rule Status: Active
      Total Available Quota:
        Input: 0       Output: 0
        Total: 20000   Time  : 0
PCC Rule Information:
Rule Name: Dyn_Rule_1
   Type : Dynamic Associated Rule Base: None
   Precedence: 1 Status: Active
   Activation due in : N/A
   Deactivation due in: N/A
 QoS Parameters:
   MBR Uplink (kbps): 2000 MBR Downlink (kbps): 3000
   Burst size Uplink (bytes): 0 Burst size Downlink (bytes): 0
 Charging Attributes:
   Rating Group: 0 Service ID: 0 Gating Status: enable-uplink
   AF Charging Id: None Charging Method: None Metering Method: None
   Usage Monitoring Key : 301
 Services Attributes:
   Steering VRF Uplink: changed_vrf     Downlink: new_vrf
   HCM ID: hcmtag1
 Filter Attributes:
   Remote IP/Mask: 203.0.113/32 Protocol: 1 Direction: Both
   Local Ports: any
   Remote Ports: any
   Application Id : None
```

```
       Application Id Base: None
```

show unified-edge tdf subscribers data-plane

```
user@host> show unified-edge tdf subscribers data-plane
Gateway: TDF
Data plane statistics :

V4 Address:192.0.2.11
V6 Address:2001:db8::                          V6 Prefix Length: 64
Subscriber-Type:IP
Vrf Id: 11
Subscriber Stats:
                      Uplink                 Downlink
-------------------------------------------------------------------
    Packets          :0                     :0
    Bytes            :0                     :0
    Dropped Packets  :0                     :0
    Dropped Bytes    :0                     :0


Rule: rule_zynga
                      Uplink                 Downlink
-------------------------------------------------------------------
    Sessions         :0                     :0
    Packets          :0                     :0
    Bytes            :0                     :0
    Dropped Packets  :0                     :0
    Dropped Bytes    :0                     :0


Rule: rule_youtube
                      Uplink                 Downlink
-------------------------------------------------------------------
    Sessions         :0                     :0
    Packets          :0                     :0
    Bytes            :0                     :0
    Dropped Packets  :0                     :0
    Dropped Bytes    :0                     :0
```

```
Rule: rule_amazon
                      Uplink                Downlink
-------------------------------------------------------------------
    Sessions          :0                    :0
    Packets           :0                    :0
    Bytes             :0                    :0
    Dropped Packets   :0                    :0
    Dropped Bytes     :0                    :0


Rule: rule_monster
                      Uplink                Downlink
-------------------------------------------------------------------
    Sessions          :0                    :0
    Packets           :0                    :0
    Bytes             :0                    :0
    Dropped Packets   :0                    :0
    Dropped Bytes     :0                    :0


Rule: all-traffic-s
                      Uplink                Downlink
-------------------------------------------------------------------
    Sessions          :0                    :0
    Packets           :0                    :0
    Bytes             :0                    :0
    Dropped Packets   :0                    :0
    Dropped Bytes     :0                    :0
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- show unified-edge tdf statistics | **1020**
- clear unified-edge tdf subscribers | **798**
- IP-Based and IFL-Based TDF Subscribers Overview | **107**

show unified-edge tdf system interfaces

IN THIS SECTION

- Syntax | 1059
- Description | 1059
- Options | 1059
- Required Privilege Level | 1059
- Output Fields | 1060
- Sample Output | 1061
- Release Information | 1061

Syntax

show unified-edge tdf system interfaces
<gateway *gateway-name*>

Description

Display information about the aggregated Packet Forwarding Engine and the aggregated multiservices (AMS) interfaces and their states on one or more TDF gateways. If a TDF gateway is not specified, then information for all TDF gateways is displayed.

Options

none	Display information for all TDF gateways.
gateway *gateway-name*	(Optional) Display information for the specified TDF gateway.

Required Privilege Level

view

Output Fields

Table 59 on page 1060 lists the output fields for the **show unified-edge tdf system interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 59: show unified-edge tdf system interfaces Output Fields

Field Name	Field Description
Gateway	Name of the TDF gateway.
Interfaces	Name of the interface: • Aggregated multiservices; for example, ams0 • Aggregated Packet Forwarding Engine; for example, apfe1 • Member of aggregated multiservices; for example, mams-1/0/0 • Multiservices; for example, ms-1/0/0 • Packet Forwarding Engine; for example, pfe-0/1/0
Members	For ams and apfe interfaces, the member interfaces that are part of the aggregated interfaces are displayed.
Operational State	Whether the interface is operational (**Active**) or not (**Inactive**).
Redundancy Role	Redundancy state in which the interface is configured: • **Primary**—Interface is a primary member. • **Secondary**—Interface is a backup to all the primary members. • **Standalone**—Interface has not been configured for redundancy.

Sample Output

show unified-edge tdf system interfaces

```
user@host> show unified-edge tdf system interfaces
Gateway: TDF
    Interfaces          Members         Operational     Redundancy
                                           State           Role
    ms-1/0/0                            Active          Standalone
    ms-1/1/0                            Active          Standalone
    ms-2/0/0                            Active          Standalone
    ms-2/1/0                            Active          Standalone
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

- show interfaces anchor-group (Aggregated Packet Forwarding Engine) | 831
- show interfaces load-balancing (Aggregated Multiservices) | 836
- show unified-edge tdf resource-manager clients | 1014
- show unified-edge tdf system interfaces service-mode | 1061

show unified-edge tdf system interfaces service-mode

IN THIS SECTION

- Syntax | 1062
- Description | 1062
- Options | 1062
- Required Privilege Level | 1062

Output Fields | 1062
Sample Output | 1064
Release Information | 1064

Syntax

```
show unified-edge tdf system interfaces service-mode
<brief | detail>
<gateway gateway-name>
```

Description

Display the service mode information for the interfaces on one or more TDF gateways. If a TDF gateway is not specified, then information for all TDF gateways is displayed.

Options

none	(Same as brief) Display service mode information for all TDF gateways.
brief | detail	(Optional) Display the specified level of output.
gateway-name *gateway-name*	(Optional) Display service mode information for the specified TDF gateway.

Required Privilege Level

view

Output Fields

Table 60 on page 1063 lists the output fields for the **show unified-edge tdf system interfaces service-mode** command. Output fields are listed in the approximate order in which they appear.

Table 60: show unified-edge tdf system interfaces service-mode Output Fields

Field Name	Field Description	Level of Output
Maintenance Mode	Phases applicable when the TDF interface is in maintenance mode. • **MM - Active Phase**—All the attributes of the address pool can be modified. • **MM - In/Out Phase**—Only the non-maintenance mode attributes of the address pool can be modified.	None **brief**
Interface Name	Name of the interface for which the service mode information is displayed: • Aggregated multiservices; for example, ams0 • Aggregated Packet Forwarding Engine; for example, apfe1 • Multiservices; for example, ms-1/0/0	All levels
Gateway	Name of the TDF gateway.	None **brief**
Gateway Name	Name of the TDF gateway.	**detail**
Service Mode Status	Status of service mode for the TDF gateway.	**detail**
Service Mode	Service mode for the TDF gateway. The following service modes are possible: • **Operational**—Gateway is in operational mode. • **Maintenance**—Gateway is in maintenance mode.	All levels

Sample Output

show unified-edge tdf system interfaces service-mode brief

```
user@host> show unified-edge tdf system interfaces service-mode brief
Maintenance Mode
    MM Active Phase - System is ready to accept configuration changes for all
                      attributes of this object and its sub-hierarchies.
    MM In/Out Phase - System is ready to accept configuration changes only for
                      non-maintenance mode attributes of this object and
                      its sub-hierarchies.

Interface Name     Gateway                            Service Mode

ms-2/1/0          TDF                               Operational
ams1               TDF                               Operational
```

show unified-edge tdf system interfaces service-mode detail

```
user@host> show unified-edge tdf system interfaces service-mode detail
Service Mode Status
Interface Name  : ms-2/1/0
Gateway Name    : TDF
Service Mode    : Operational
Service Mode Status
Interface Name  : ams1
Gateway Name    : TDF
Service Mode    : Operational
```

Release Information

Statement introduced in Junos OS Release 17.1.

RELATED DOCUMENTATION

show unified-edge tdf system interfaces | 1059