JUNIPER NETWORKS | Engineering Simplicity

Access Gateway Function User Guide

Published
2022-12-13

JUNOS

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

Access Gateway Function User Guide

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

The Access Gateway Function (AGF) provides subscribers with wireline access to the 5G core network and is an integral part of Junos Multi-Access User Plane solution. Use this document to learn more about Access Gateway Function on a MX Series router.

CHAPTER 1

Overview

Overview of 5G

IN THIS SECTION

5G is the fifth-generation technology standard for wireless networks. 5G delivers higher data speeds, lower latency, and supports more users, devices, and services while simultaneously improving network efficiency. As defined by the Third-Generation Partnership Project (3GPP), the 5G core (5GC) network is a cloud-aligned, service-based architecture (SBA) and covers all 5G functions and interactions. The converged 5GC lays the foundation for a single subscriber profile and policy management for both the existing wireline users with installed router gateway and the new 5G wireless users. The converged core offers the following benefits:

- Single control plane for wireline and wireless subscribers
- Ease of migration for existing subscribers to 5GC
- Access to a wireline fixed network router gateway (FN-RG)
- Hybrid access with a 5G residential gateway (5G-RG) for increased bandwidth and increased availability
- Single Operation Support System (OSS) and Business Support System (BSS) integration

Components in a 5GC Network

Figure 1 on page 3 shows the key components for the 5GC network to which the FN-RG has connected by using an Access Gateway Function (AGF). Table 1 on page 3 describes the key network functions and the logical interfaces between them. The interaction between the key network functions

and the logical interfaces is defined by the 3GPP. Other functions and interfaces defined for the 5G network are beyond the scope of this guide.

Figure 1: Components in a 5GC Network

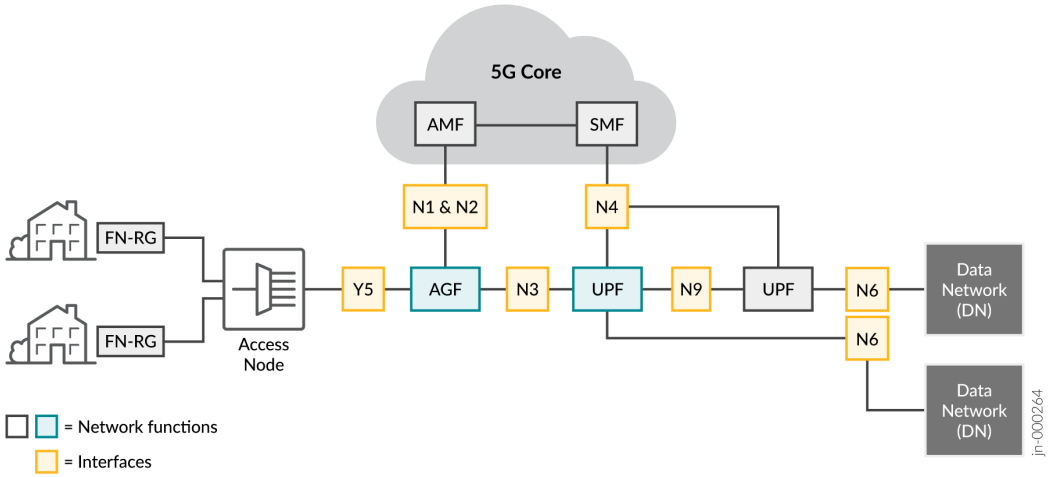


Table 1: Components of a 5G Network

Functions and Interfaces	Description
Access Gateway Function (AGF)	Provides the access connection for residential gateways (RGs) to connect to the 5GC. In adaptive mode, the AGF emulates N1 signaling for the FN-RG to connect to the 5GC. Additionally, the AGF sends messages to the AMF over the N2 interface and sends the protocol data unit (PDU) session traffic over the N3 interface to the UPF.
Access and Mobility Management Function (AMF)	Responsible for registration management, PDU session management, and forwarding of access facing traffic to and from the access network.

Table 1: Components of a 5G Network *(Continued)*

Functions and Interfaces	Description
Fixed Network Residential Gateway (FN-RG)	Connects the home network to the WAN. An FN-RG is a wireline device and works in a wireline network. It does not send signaling associated with RAN found in 5GC networks. For an FN-RG, N1 signaling originates on the AGF. The AGF acts as an endpoint on the 5GC and handles all N1 signaling on behalf of the FN-RG. You do not need new hardware or changes to the existing FN-RG hardware to work with AGF.
Session Management Function (SMF)	Establishes PDU sessions and interacts with the user plane function (UPF).
User plane function (UPF)	Supports packet routing, forwarding, packet inspection, PDU session, and flow-level QoS. **NOTE**: An UPF can be external or colocated with the AGF.
N1	Interface from the user equipment (UE) to the AMF. The N1 interface uses non-access stratum (NAS) layer signaling to exchange UE information that is related to connection and session that the UE establishes with the 5GC network.
N2	Control interface that connects the AGF to the AMF.
N3	The AGF connects to the UPF over the N3 interface using the general packet radio service (GPRS) tunneling protocol. The AGF and UPF exchange PDU session information over the N3 inteface.
N6	Interface that carries data between the UPF and the data network.
N9	Interface that connects one UPF to another.

Table 1: Components of a 5G Network *(Continued)*

Functions and Interfaces	Description
Y5	Interface that connects an FN-RG to the AGF over the wireline access network. The Y5 interface is the equivalent of the V interface in wireline broadband networks.

Access Gateway Function

IN THIS SECTION

Access Gateway Function

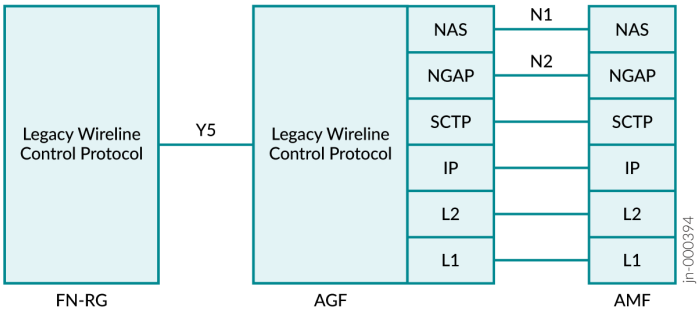
The Access Gateway Function (AGF) on Junos OS provides a solution that enables interworking of wireline-connected devices and the 5G core (5GC). In adaptive mode, the AGF manages the access connections between the residential gateway (RG) and the 5GC by providing the 5G signaling that is used in the 5GC network.

- IP connectivity
- AAA services
- QoS to subscribers on the RG
- Connection between the 5GC and the existing FN-RG, which uses Dynamic Host Configuration Protocol (DHCP), DHCPv6, or Point-to-Point Protocol over Ethernet (PPPoE)

Figure 2 on page 6 shows the legacy wireline control protocol stack used by the FN-RG, wireline AGF, and Access and Mobility Management Function (AMF). The wireline AGF acts as an N1 termination

point for the FN-RG. N1 signaling is defined in the Non-Access Stratum (NAS) protocol. N2 signaling is defined in the Next Generation Application Protocol (NGAP).

Figure 2: Control Protocol Stack Between FN-RG and 5GC

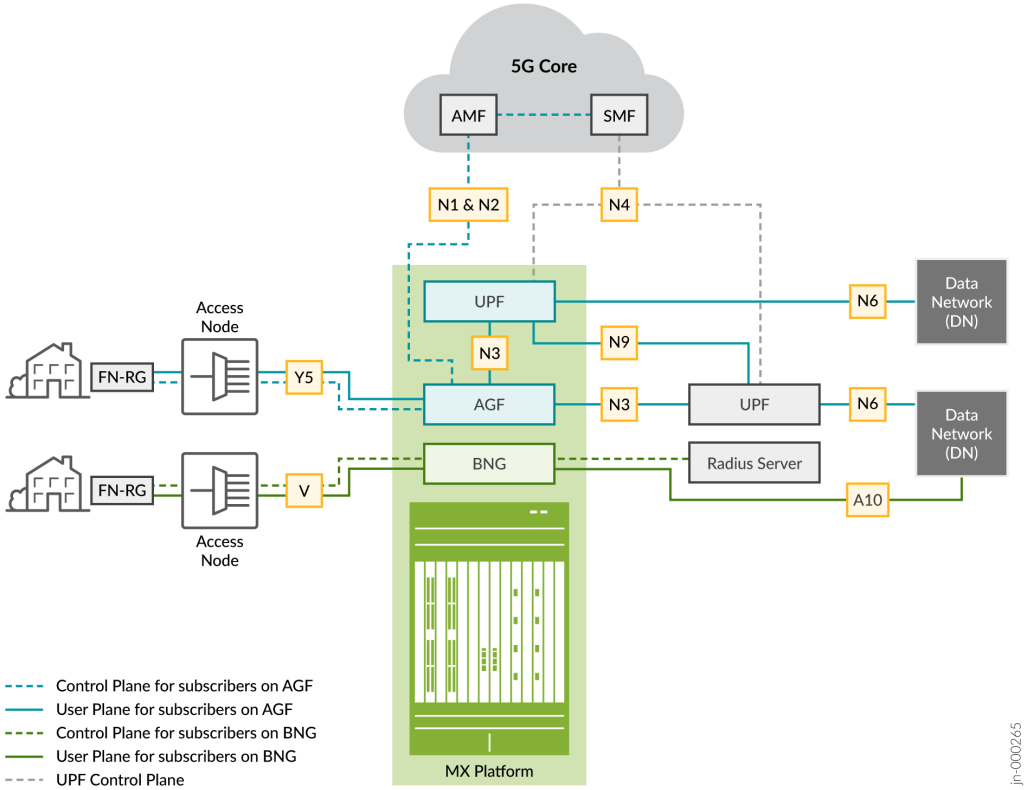


Benefits of Access Gateway Function

- Offers ease of migration for a subscriber with existing customer premise equipment (CPE), such as an FN-RG, to the 5G core (5GC)
- Provides a solution that enables interworking between wireline devices and the 5GC
- Supports existing FN-RG and existing hardware, such as the MX series routers.
- Optimizes data plane traffic with the User Plane Function (UPF), resulting in improved performance
- Eases deployment with by enabling the collocation of broadband network gateway (BNG), AGF, and UPF on the same platform

Figure 3 on page 6 shows the topology that subscribers use to access their broadband service provider. Subscribers can access services through the traditional broadband network gateway (BNG) or through the AGF.

Figure 3: Topology Enabling Subscriber Access to a Data Network



The BNG connects to the FN-RG through an access node that aggregates traffic for the service provider. The BNG routes the aggregated traffic to the service provider's network. The access node can be a DSL access multiplier (DSLAM) or an optical line termination (OLT). The BNG interacts with the FN-RG across the V interface and connects with the data network across the A10 interface.

The AGF connects to the FN-RG through the V interface. The AGF interacts with the wireline network to connect to the 5GC. From the 5GC point of view, the AGF is the equivalent of a 5G base station (gNodeB). In adaptive mode, the AGF provides the N1, N2, and N3 signaling on behalf of FN-RGs when the residential gateways (RGs) connect to the 5GC. The AGF provides the following services:

- Exchanges control plane data with the Access and Mobility Management functions and Session Management Functions (SMFs) through the N1 and N2 interfaces (The AGF uses N1 and N2 signaling to authenticate, authorize, and manage sessions).
- Registers the FN-RG as user equipment (UE) when the AGF establishes a connection with the AMF in the 5GC
- Passes the allocated IP address from the SMF to the FN-RG
- Passes the PDU session setup information (gateways, DNS, and so on) that is received from the 5GC for the FN-RG

- Enforces UE-level QoS and policy that it receives from the 5GC
- Sends and receives user plane data from the User Plane Function (UPF) through the N3 interface

The MX series routers support colocated BNG, AGF, and UPF services. AGF is an integral part of the Junos Multi-Access User Plane solution. See Junos Multi-Access User Plane.

Authentication and Registration

Authentication and registration of a subscriber's fixed-network residential gateway (FN-RG differs from authentication and registration of FN-RG on a wireline core network. The authentication and registration process comprises these steps:

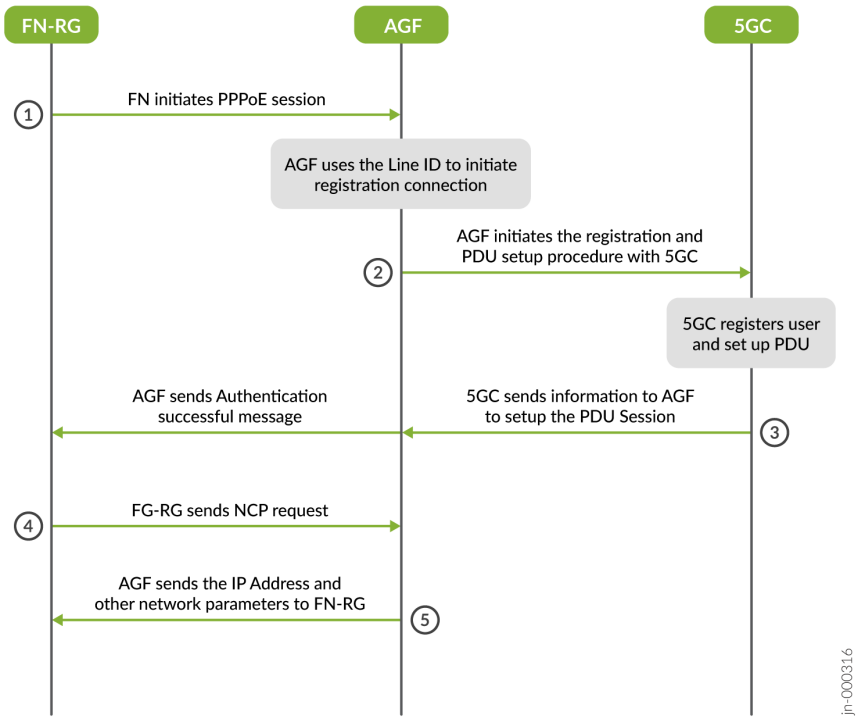
1. The FN-RG uses a unique global line identifier (GLI) to connect to the 5GC network. The GLI contains a circuit line ID and a remote line ID.
2. The Access Gateway Function (AGF) uses the circuit line ID and the remote line ID in the GLI to construct a unique Subscription Permanent Identifier (SUPI) for each FN-RG.
3. To preserve privacy, the AGF converts the SUPI to a Subscription Concealed Identifier (SUCI). The AGF then uses the SUCI to authenticate and to register a subscriber with the Access and Mobility Management Function (AMF) on the 5GC.

Upon successful authentication, the AMF allocates a Global Unique Temporary Identifier (GUTI) for the subscriber. The subscriber uses the GUTI during its registered session with the AMF. The GUTI contains information that identifies the user without revealing the user's permanent identity in the 5GC.

AGF supports the use of both Dynamic Host Configuration Protocol (DHCP) and Point-to-Point Protocol over Ethernet (PPPoE) in authenticating users, registering users, and in allocating an IP address to the FN-RG.

Figure 4 on page 9 shows a high-level view of the interaction between the FN-RG, AGF (in adaptive mode), and 5GC when you use PPPoE for authentication and registration. You can find detailed information on the registration process in 3GPP TS 23.316.

Figure 4: High-Level View of Authentication and Registration Using PPPoE



Authentication and registration of an FN-RG using PPPoE comprises the following steps;

1. Point-to-Point Protocol over Ethernet (PPPoE) begins when the FN-RG sends a PPPoE Active Discovery Initiation (PADI) message to the AGF.

   The PADI message contains PPPoE tags that include the PPPoE Circuit line ID and Remote line ID tags. .

2. The AGF uses the circuit line and remote line IDs to generate the subscriber's identity. The AGF then uses the subscriber's ID and the corresponding PPPoE tag to initiate a Point-to-Point (PPP) connection.

   Upon establishment of a PPPoE session, the FN-RG initiates the PPP authentication request. The AGF generates the SUPI and the SUCI from the Line ID. The AGF then completes the registration and protocol data unit (PDU) session setup with the 5GC over the N1 and N2 interfaces.

3. After a successful registration in the 5GC, the AGF responds with an authentication success message to the FN-RG.

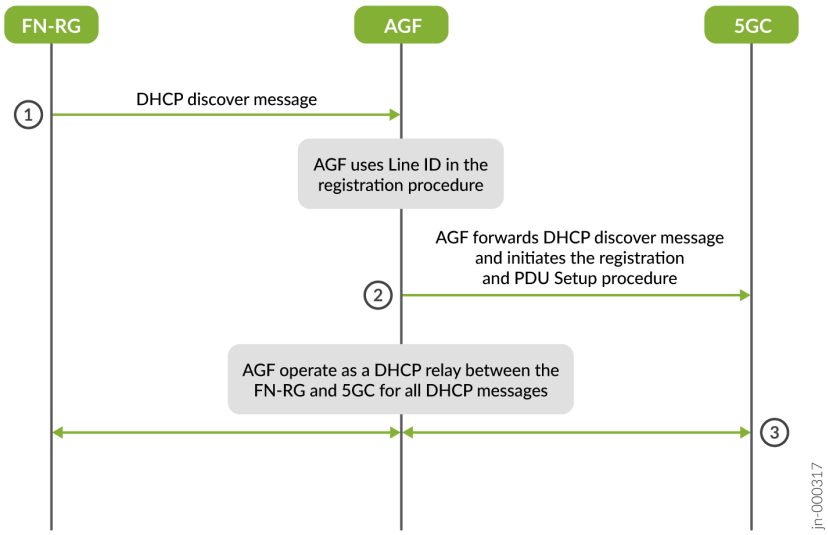
4. The FN-RG initiates the Network Control Protocol (NCP) to establish different Network Layer protocols that are required to set up the PPP connections. The FN-RG uses Internet Protocol Control Protocol (IPCP) to send either for an IPv4 or IPv6CP request to the AGF.

5. After the PPP connection is established, the AGF sends the IPv4 address that was received in the IPCP response during the protocol data unit (PDU) session setup with the FN-RG.

   On an IPv6CP request, AGF sends the Network ID that was part of the IPv6CP response. The AGF forwards the router advertisement containing the prefix that came from the 5GC.

Figure 5 on page 10 shows the DHCP interaction between the FN-RG, AGF (in adaptive mode), and 5GC is as follows:

Figure 5: High-Level View of Authentication and Registration Using DHCP



Authentication and registration of an FN-RG using DHCP comprises the following steps;

1. DHCP begins when the FN-RG sends a DHCPv4 discover message to the AGF.

   The DHCPv4 discover message contains the circuit line ID and remote line ID information in DHCP option 82.

2. Upon receiving the DHCP discover message from the FN-RG, the AGF generates the SUPI and SUCI from the Line ID. The AGF then initiates the deferred IP address allocation. It starts the registration and the PDU session setup on the 5GC over the N1 and N2 interfaces.

3. AGF operates as the DHCP relay and forwards all the DHCP messages between the FN-RG and the DHCP server on the 5GC.

IP Address Allocation

The current Broadband Edge architecture uses RADIUS servers to deploy IP addresses. In the 5G architecture, the session management function (SMF) is responsible for providing IP addresses. The Access Gateway Function (AGF) supports the following IP address allocation methods:

1. NAS signaling mode—For Point-to-Point Protocol over Ethernet (PPPoE) users, the AGF sends an IP address request to the Access and Mobility Management Function (AMF) on the 5GC. The AMF forwards the request to the SMF. The SMF allocates IP address and sends the IP address back as part of the N1 NAS signaling.

2. Deferred mode—For the Dynamic Host Configuration Protocol (DHCP) users, the AGF acts as a relay agent for the client (FN-RG). The AGF forwards the DHCP Discover, Offer, Request, Acknowledgment (DORA) messages to the SMF by way of the user plane function (UPF) on the N3 interface. The AGF forwards the DHCP messages by appending the GPRS tunneling protocol (GTP) headers provided by the AMF in the N1 message. The UPF forwards these DHCP messages to the SMF. The SMF acts as a DHCP relay agent and forwards the DHCP messages to the DHCP server. The DHCP server allocates the IP address and sends the IP address by way of the UPF to AGF. AGF then forwards the IP addresses to the DHCP client running the FN-RG.

> **NOTE**: The AGF supports the deferred IP address allocation when using IPv6.

Routing Instances

The Access Gateway Function (AGF) supports placing subscribers in different routing instances where each routing instance has its own routing table, routing policies, and interfaces. You can configure multiple routing instances to support the authentication and registration of subscribers to different Access and Mobility Management Functions (AMFs) and to support the routing of data packets to different user plane functions (UPFs).

To configure routing instances for the Point-to-Point Protocol over Ethernet (PPPoE) subscribers, set the `target-routing-instance` option at the `[edit access domain map]` hierarchy level or set the `subscriber-context` option under the `[edit access]` hierarchy. You will need to apply authentication attributes to subscribers. To apply attributes to the Point-to-Point Protocol (PPP) subscribers, use the `aaa-options` statement at the `[edit dynamic-profiles` *`profile-name`* `interfaces pp0 unit $junos-interface-unit ppp-options]` hierarchy level.

To configure routing instances for the Dynamic Host Configuration Protocol (DHCP) subscribers, set the `target-routing-instance` option at the `[edit access domain map]` hierarchy level. The AGF assigns the domain name to the subscriber using the DHCP group configuration.

You can also configure multiple routing instances to route the data packets to different UPFs. To configure the UPF routing instance and local tunnel endpoint for the GPRS tunneling protocol, user plane (GTP-U) tunnel to the UPF, set the `routing-instance` and `ip-address` options at the `[edit services agf user-planes]` hierarchy level.

User Plane Function

The user plane function (UPF) is the data plane in the 5G core (5GC). After the Access Gateway Function (AGF) authenticates the subscriber and establishes a protocol data unit (PDU) session, the session management function (SMF) selects the UPF for the subscriber. The UPF provides the following functionality:

- Subscriber tunnel encapsulations enabled by the GPRS tunneling protocol, user plane(GTP-U)
- Packet routing and forwarding
- Quality of service (QoS) and buffering
- Policy enforcement
- Statistics gathering and reporting
- Lawful intercept requests processing
- Optional advanced services

Juniper supports the UPF both on an MX platform, both when the platform is dedicated to the UPF and when the UPF is colocated with the Access Gateway Function (AGF) on the platform.You can configure the UPF as a target UPF or as an intermediate UPF. A target UPF communicates with the data network over the N6 interface. An intermediate UPF performs the role of an uplink classifier and communicates with other UPFs over the N9 interface.

AGF and UPF Colocation

Juniper supports the colocation of user plane functions (UPFs) on the same MX router. In the 5G architecture, the Access Gateway Function (AGF) forwards data packets to the UPF over the N3 interface. Conceptually, the colocated AGF and UPF send data packets internally over the N3 interface

to each other. When the UPF and the AGF are colocated, you can still configure the UPF to be both a target UPF and an intermediate UPF.

When you colocate the AGF with the UPF, the UPF operates on the edge of the network. Therefore, user application data can have lower latency and higher throughput.

To enable a colocated UPF, include `colocated-user-plane` at the `[edit services agf user-planes` *`user-plane-name`*`]` hierarchy.

For more information on configuring UPFs, see https://www.juniper.net/documentation/us/en/software/junos/multi-access-user-plane/topics/topic-map/cups-saegw-overview.html

Quality of Service

Quality of service in a 5G network is driven by QoS flows. A QoS flow represents the finest granularity of QoS differentiation in the protocol data unit (PDU) session. Each QoS flow is identified by a unique identifier called QoS Flow Identifier (QFI) and by QoS parameters that describe the characteristics of the packet flow. The session management function (SMF) whichcontrols the QoS and passes QoS characteristics to the user plane function (UPF) and the Access Gateway Function (AGF) when the PDU session is being established. The UPF enforces the QoS flows for a particular PDU session, and the AGF manages the aggregate of all the QoS flows going to the residential gateway (RG).

The 5G core (5GC) supports up to 64 QFIs for a single PDU session. The QoS flow parameters include the 5G QoS identifier (5QI). 5QI maps to the well-defined QoS characteristics, such as priority level, averaging window, maximum data burst volume, and so on. 3GPP Specification 23.501 defines how the standard 5QI values map to the QoS characteristics mappings.

The UPF identifies the QoS flows by sending a QFI, but the AGF does not use QFI to classify the packets. The AGF classifies the traffic by using the Differentiated Services code point (DSCP) in the GPRS tunneling protocol (GTP) header that the UPF sends over the N3 interface.. The SMF sends the Transport Level Marking (TLM) to the UPF. The UPF uses the TLM to mark up the GTP header in the outgoing N3 packets to the AGF. After classifying the packets (by using DSCP), the AGF uses the standard Junos class of service (CoS) classification configuration to classify and to shape the traffic.

The BBF standards specify that operators who use the per subscriber CoS parameters per household, should use Router Gateway Level Wireline Access Characteristics (RG-LWAC) to define the CoS limits and scope of service for the specified subscriber or a group of subscribers on a router. To configure the QoS characteristics of legacy access networks, the AGF uses the RG-LWAC information from the 5GC to set CoS queue shaping, firewall filters, and policers. The AGF leverages the existing shaping, policers, and firewall filters on Junos OS. The AGF uses the existing rewrite rules to set the PCP or DSCP value in the packet header sent to the access network.

For downstream traffic, the UPF sets the DSCP value based on the packet priority that was set by the 5GC and sends it to the AGF. The AGF uses hierarchical policers to shape downstream traffic. For this task, the AGF performs the following:

- Maps the outer DSCP value to a forwarding class.
- Assigns the forwarding class to an output queue.
- Assigns the forwarding class to the scheduler based on the forwarding class priority.
- Applies the RG-LWAC or the local configuration to classify the traffic and to rewrite the PCP or DSCP value when needed.

For more information on CoS, see CoS for Subscriber Access Overview.

SCTP

IN THIS SECTION

SCTP Overview

Stream Control Transmission Protocol (SCTP) is a transport layer protocol in the Internet protocol suite. SCTP exists at an equivalent level with UDP and TCP, which provides transport layer functions to many Internet applications. SCTP is a message stream-focused and reliable connection-oriented transport protocol with the following features:

- Multi-stream protocol—SCTP provides a mechanism to maintain multiple streams of messages for each SCTP endpoint.

  This protocol supports applications that perform the following tasks:

  - Deliver messages of different priorities
  - Deliver strict message order within stream
  - Bypass sequence delivery service within stream use multi-stream protocol

- User data fragmentation—To deliver a message of a size more than the path maximum transmission unit (MTU) limit, the SCTP fragments the message in data chunks and sends it in different SCTP packets. SCTP header has a flag to mark the last chunk of fragmented message. The receiver side reassembles all the fragmented chunks and passes it to the upper layer protocol.
- Chunk bundling—This feature enables the SCTP to bundle chunks from multiple messages in a single SCTP packet. The receiver side disassembles the chunks before delivering to the upper layer protocol.
- Packet validation—You can include a verification tag in the SCTP header to uniquely identify an SCTP association session. Use a new verification tag for the revival. of a session. This feature provides protection against masquerade attacks and stale SCTP packets from previous association.
- Multihoming support—The SCTP can specify the list of local transport addresses for the SCTP endpoint which the server and the client exchange during association startup. This list advertises at the other endpoint about the available destination address and source address in the SCTP packet that one endpoint receives after SCTP association setup. The other SCTP endpoint establishes the route for each of the received destination addresses and uses this route to ensure high availability for data transfer.

SCTP Connection to the AMF

The Access Gateway Function (AGF) uses the Stream Control Transmission Protocol (SCTP) to transport the Next Generation Application Protocol (NGAP) messages. These message provide control plane signaling with the Access and Mobility Management Functions (AMFs). The SCTP is a transport layer protocol which ensures reliable, in-sequence transport of data. SCTP provides multihoming support where one or both endpoints of a connection can consist of more than one IP address. This capability enables transparent failover between redundant network paths. The SCTP association is a connection

between two SCTP endpoints. The AGF creates a Transport Layer Network Association (TNLA) between endpoints on the AGF and the AMF.

Figure 6: SCTP Multihoming

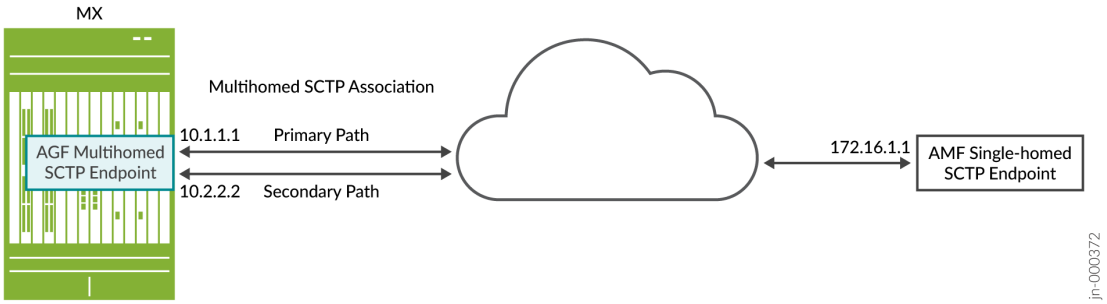


Figure 6 on page 16 shows a multihomed AGF SCTP endpoint and a single-homed AMF SCTP endpoint. With AGF SCTP endpoint multihoming, you can designate one of the AGF endpoints (IP address) as the primary path. If the primary path fails, the SCTP switches to the secondary path. The AGF supports the following capabilities:

- Multihomed local endpoint
- Routing instances to AMFs
- Up to 10 TNLAs for each AMF
- Load balancing of user equipment (UE) across all TNLAs that support UE-associated signaling.

You can configure the SCTP connections to AMFs in the `[edit services agf amf]` hierarchy.

AGF Using Junos Telemetry Interface

The Access Gateway Function (AGF) uses Junos telemetry interface (JTI) to export telemetry data from a device to a collector to help you monitor the health of your network and the traffic that it carries. JTI gathers telemetry data through a "push" model instead of the traditional "pull" models such as CLI or SNMP. Data delivery is automated and happens in real-time. You can use AGF-specific sensors to collect data on AGF interactions and use the data to:

- Improve your network design.
- Optimize traffic engineering.

- Gain early detection of problems on individual devices.

For information about AGF sensors, see Telemetry Sensor Explorer. For information about JTI, see Junos Telemetry Interface User Guide.

Supported Standards

- *Broadband Forum TR-456—5G Wireless Wireline Convergence Architecture*
- *Broadband Forum TR-470—5G FMC Architecture*
- *3GPP TS 23.316, Release 16—Wireless and wireline convergence access support for the 5G System (5GS)*
- *3GPP TS 23.501, Release 16—System Architecture for the 5G System*
- *3GPP TS 24.501, Release 16—NAS procedures in the 5G system*
- *3GPP TS 29.281, Release 16—GPRS Tunneling Protocol UP GTPv1-U*
- *3GPP TS 38.413, Release 16—NG Application Protocol*

2

CHAPTER

Configure AGF

Overview of Configuring AGF

The network functions in a 5G core (5GC) network interact with one another to support user connectivity. You can deploy the Access Gateway Function (AGF) between the residential gateway (RG) and the Access and Mobility Management Function (AMF) and user plane function (UPF). You can deploy the AGF by following these steps:

1. Configure either of the following protocols to provide subscribers access and authentication capability on the AMF:
   - Point-to-Point Protocol over Ethernet (PPPoE)
   - Dynamic Host Configuration Protocol (DHCP) Relay
2. Configure the AGF services.

Configure PPP Support for AGF

IN THIS SECTION

This example describes how to configure the Access Gateway Function (AGF) to support a subscriber using Point-to-Point Protocol over Ethernet (PPPoE) for authentication.

Procedure

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

```
set dynamic-profiles autoconf-vlan-demux routing-instances "$junos-routing-instance" interface
"$junos-interface-name" any
set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-unit" ppp-options
chap
set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-unit" ppp-options
pap
set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-unit" ppp-options
aaa-options nas-5g-access-options
set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-unit" pppoe-
options underlying-interface "$junos-underlying-interface"
set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-unit" pppoe-
options server
set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-unit" no-
keepalives
set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-unit" family inet
unnumbered-address "$junos-loopback-interface"
set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-unit" family
inet6 unnumbered-address "$junos-loopback-interface"
set access profile NAS-5G-AGF authentication-order nas-5g
set access nas-5g max-outstanding-requests 1000
set access nas-5g request-retry 3
set access nas-5g timeout 30
set access aaa-options NAS-5G-ACCESS-OPTIONS access-profile NAS-5G-AGF
set access aaa-options NAS-5G-ACCESS-OPTIONS aaa-context AMF-RI
set access aaa-options NAS-5G-ACCESS-OPTIONS subscriber-context UE-RI-1
set access domain map DOMAIN1.COM aaa-routing-instance AMF-RI
set access domain map DOMAIN1.COM access-profile nas-5g-agf
set access domain map DOMAIN1.COM target-routing-instance UE-RI-1
set routing-instances UE-RI-1 instance-type virtual-router
set routing-instances UE-RI-1 interface xe-2/0/1.3
set routing-instances UE-RI-1 interface lo0.1
```

Step-by-Step Procedure

1. Configure the dynamic profile for the Point-to-Point Protocol (PPP) subscriber.

```
[edit]
user@host# set dynamic-profiles autoconf-vlan-demux routing-instances "$junos-routing-
instance" interface "$junos-interface-name" any
user@host# set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-
unit" ppp-options chap
user@host# set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-
unit" ppp-options pap
user@host# set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-
unit" ppp-options aaa-options nas-5g-access-options
user@host# set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-
unit" pppoe-options underlying-interface "$junos-underlying-interface"
user@host# set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-
unit" pppoe-options server
user@host# set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-
unit" no-keepalives
user@host# set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-
unit" family inet unnumbered-address "$junos-loopback-interface"
user@host# set dynamic-profiles autoconf-vlan-demux interfaces pp0 unit "$junos-interface-
unit" family inet6 unnumbered-address "$junos-loopback-interface"
```

2. Set the access authentication method for the subscriber group to use Non-Access Stratum (NAS) signaling.

```
[edit]
user@host# set access profile NAS-5G-AGF authentication-order nas-5g
```

3. Configure the following options for NAS signaling between the AGF and the AMF.

   - Maximum number of outstanding request—The number of unanswered request messages from the AMF.
   - Number of retries—The number of attempts for a registration or deregistration request .
   - Timeout—The duration that the AGF waits for a response from the AMF.

```
[edit]
user@host# set access nas-5g max-outstanding-requests 1000
```

```
user@host# set access nas-5g request-retry 3
user@host# set access nas-5g timeout 30
```

4. Define the profile with a set of AAA options for the PPP subscriber by performing the following steps:

   - Create the access profile (`access-profile`) for the subscriber group.
   - Specify the logical-system:routing-instance (LS:RI) that the subscriber session uses for AAA (RADIUS) interactions.
   - Specify the LS:RI where the subscriber interface is placed. In this case, we are using the default routing instance.

```
[edit]
user@host# set access aaa-options NAS-5G-ACCESS-OPTIONS access-profile NAS-5G-AGF
user@host# set access aaa-options NAS-5G-ACCESS-OPTIONS aaa-context AMF-RI
user@host# set access aaa-options NAS-5G-ACCESS-OPTIONS subscriber-context UE-RI-1
```

   Alternatively, you can create a domain map and apply the domain map to the access profile.

```
[edit]
user@host# set access domain map DOMAIN1.COM aaa-routing-instance AMF-RI
user@host# set access domain map DOMAIN1.COM access-profile NAS-5G-AGF
user@host# set access domain map DOMAIN1.COM target-routing-instance UE-RI-1
```

5. Configure the routing instance.

```
[edit]
user@host# set routing-instances UE-RI-1 instance-type virtual-router
user@host# set routing-instances UE-RI-1 interface xe-2/0/1.3
user@host# set routing-instances UE-RI-1 interface lo0.1
```

For more information on PPP Subscribers, see https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-access/topics/topic-map/ppp-access-network-overview.html

Configure DHCP Support for AGF

IN THIS SECTION

This example describes how to configure the Access Gateway Function (AGF) to support the use of Dynamic Host Configuration Protocol (DHCP) for subscriber authentication. In this example, we configure DHCP relay to forward the DHCP request and reply packets between the subscriber (DHCP client) and the DHCP server on the 5G core (5GC).

Procedure

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

```
set group AGF_SUBSCRIBER_GROUP authentication password $abc123
set group AGF_SUBSCRIBER_GROUP authentication username-include user-prefix USER
set group AGF_SUBSCRIBER_GROUP access-profile NAS-5G-AGF
set group AGF_SUBSCRIBER_GROUP overrides trust-option-82
set group AGF_SUBSCRIBER_GROUP interface xe-1/0/0.0
set access profile NAS-5G-AGF authentication-order nas-5g
set access domain map DOMAIN1.COM aaa-routing-instance default
set access domain map DOMAIN1.COM access-profile NAS-5G-AGF
set access domain map DOMAIN1.COM target-routing-instance UE-RI-1
set access nas-5g max-outstanding-requests 1000
set access nas-5g request-retry 3
set access nas-5g timeout 30
set routing-instances UE-RI-1 instance-type virtual-router
```

```
set routing-instances UE-RI-1 interface xe-2/0/1.3
set routing-instances UE-RI-1 interface lo0.1
```

Step-by-Step Procedure

1. Create a subscriber group with the authentication fields that will be passed to the access interface.

```
[edit forwarding-options dhcp-relay]
user@host# set group AGF_SUBSCRIBER_GROUP authentication password $abc123
user@host# set group AGF_SUBSCRIBER_GROUP authentication username-include user-prefix USER
```

2. Create an access profile (`access-profile`) for the group subscribers that will be authenticating in the 5GC and attach the profile to the DHCP relay agent.

```
[edit forwarding-options dhcp-relay]
user@host# set group AGF_SUBSCRIBER_GROUP access-profile NAS-5G-AGF
```

3. Configure the router to always accept the DHCP client packets that contain option 82 information.

```
[edit forwarding-options dhcp-relay]
user@host# set group AGF_SUBSCRIBER_GROUP overrides trust-option-82
```

4. Specify the interface to which that the DHCP subscribers will connect.

```
[edit forwarding-options dhcp-relay]
user@host# set group AGF_SUBSCRIBER_GROUP interface xe-1/0/0.0
```

5. Set the access profile that the AGF will use to authenticate for the subscriber group to authenticate using Non-Access Stratum (NAS) signaling.

```
[edit]
user@host# set access profile NAS-5G-AGF authentication-order nas-5g
```

6. Create the domain map and apply the domain map to the access profile.

```
edit]
user@host# set access domain map DOMAIN1.COM aaa-routing-instance default
user@host# set access domain map DOMAIN1.COM access-profile NAS-5G-AGF
user@host# set access domain map DOMAIN1.COM target-routing-instance UE-RI-1
```

7. Configure the following options for NAS signaling between the AGF and the Access and Mobility Management Function (AMF).

   - Maximum number of outstanding request—The number of unanswered request messages from the AMF.
   - Number of retries—The number of attempts for a registration or deregistration request .
   - Timeout—The duration that the AGF waits for a response from the AMF.

```
[edit]
user@host# set access nas-5g max-outstanding-requests 1000
user@host# set access nas-5g request-retry 3
user@host# set access nas-5g timeout 30
```

8. Configure the routing instance.

```
[edit]
user@host# set routing-instances UE-RI-1 instance-type virtual-router
user@host# set routing-instances UE-RI-1 interface xe-2/0/1.3
user@host# set routing-instances UE-RI-1 interface lo0.1
```

For more information on DHCP subscribers, see https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-access/topics/topic-map/dhcp-subscriber-access-overview.html

Configure AGF Services

IN THIS SECTION

This example describes how to configure the Access Gateway Function (AGF) services to support residential gateways that connect to the 5G core (5GC).

Procedure

CLI Quick Configuration

To quickly configure this example:

1. Copy the following commands and paste them into a text file.
2. Remove any line breaks and change any details necessary to match your network configuration
3. Copy and paste the commands into the CLI at the `[edit]` hierarchy level

```
set services agf node-name AGF-NODE1
set services agf node-id 1
set services agf plmn te-plmn mcc 123
set services agf plmn te-plmn mnc 456
set services agf tracking-area 0 plmn te-plmn s-nssai 0 sst v2x sd 5
set services agf tracking-area 0 plmn te-plmn s-nssai 1 sst miot sd4
set services agf amf AMF1 node-id 1
set services agf amf AMF1 ip-address 10.1.1.7 port 38412
set services agf amf AMF1 local-endpoint ip-address 10.1.1.1 primary
set services agf amf AMF1 local-endpoint ip-address 10.20.1.1
set services agf amf AMF1 default-amf
set services agf user-planes UPF_DEFAULT ip-address 10.1.7.1
set services agf user-planes UPF_DEFAULT data-network-name DEFAULT-DN
set services agf user-planes UPF_COLOCATED 10.255.20.149
set services agf user-planes UPF_COLOCATED data-network-name COLOCATED-DN
```

```
set services agf user-planes UPF_COLOCATED colocated-user-plane ip-endpoint-address 10.255.20.149
set routing-instances AMF-RI instance-type virtual-router
set routing-instances AMF-RI interface xe-2/0/2.1
```

Step-by-Step Procedure

1. Configure the AGF node.

```
[edit services agf]
user@host# set node-name AGF-NODE1
user@host# set node-id 1
```

2. Configure the supported public land mobile network (PLMN) and tracking area.

```
[edit services agf]
user@host# set plmn te-plmn mcc 123
user@host# set plmn te-plmn mnc 456
user@host# set tracking-area 0 plmn te-plmn s-nssai 0 sst v2x sd 5
user@host# set tracking-area 0 plmn te-plmn s-nssai 1 sst miot sd4
```

3. Configure the connection to the Access Management and Mobility Function (AMF). The AMF IP address must be reachable in the configured AMF routing instance. Configure the Stream Control Transmission Protocol (SCTP) local endpoint on the AGF. If you are configuring a multihoming association, specify one local endpoint as a primary endpoint.

```
[edit services agf]
user@host# set services agf amf AMF1 node-id 1
user@host# set services agf amf AMF1 ip-address 10.1.1.7 port 38412
user@host# set services agf amf AMF1 local-endpoint ip-address 10.1.1.1 primary
user@host# set services agf amf AMF1 local-endpoint ip-address 10.20.1.1
user@host# set services agf amf AMF1 default-amf
user@host# set services agf amf AMF1 routing-instance AMF1-RI-1
```

4. Configure the user plane information. If you are configuring an user plane function (UPF) on the MX router, you must specify that the UPF is colocated and configure the `colocated-user-plane` information.

```
[edit services agf]
user@host# set services agf user-planes UPF_DEFAULT ip-address 10.1.7.1
```

```
user@host# set services agf user-planes UPF_DEFAULT data-network-name DEFAULT-DN
user@host# set services agf user-planes UPF_COLOCATED 10.255.20.149
user@host# set services agf user-planes UPF_COLOCATED data-network-name COLOCATED-DN
user@host# set services agf user-planes UPF_COLOCATED colocated-user-plane ip-endpoint-
address 10.255.20.149
```

5. Configure the routing instance to the AMF.

```
[edit]
user@host# set routing-instances AMF-RI instance-type virtual-router
user@host# set routing-instances AMF-RI interface xe-2/0/2.1
```

3

CHAPTER

Configuration Statements

agf

IN THIS SECTION

Syntax

```
agf {
 amfname {
 default-amf;
 ip-address ip-address;
 local-endpoint {
  initial-tnla-weight-factor initial-tnla-weight-factor;
  ip-address name {
   primary;
  }
 }
 node-id node-id;
 offline;
 port port;
 routing-instance routing-instance;
 tracking-area name;
}


node-id node-id;
node-name node-name;
plmn name {
```

```
 mcc mcc;
 mnc mnc;
}
tracking-area code {
 plmn name {
  s-nssai name {
   sd sd;
   sst(embb | miot | urllc | v2x);
  }
 }
}
user-planesname {
 colocated-user-plane {
  ip-endpoint-address ip-endpoint-address;
 }
 data-network-name data-network-name;
 ip-address ip-address;
 routing-instance routing-instance;
}
}
```

Hierarchy Level

```
[edit services]
```

Description

Configure the Access Gateway Function.

Options

node-id Specifies the AGF node identifier.

- **Range:** 0 through 255

`node-name`	AGF node name

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 22.3R1.

amf

IN THIS SECTION

Syntax

```
amf name {
<default-amf;
 ip-address ip-address;
 local-endpoint {
  initial-tnla-weight-factor initial-tnla-weight-factor;
  ip-address name {
   primary;
  }
 }
 node-id node-id;
 offline;
 port port;
 routing-instance routing-instance;
 tracking-area name;

}
```

Hierarchy Level

```
[edit services agf]
```

Description

Configure the connection to the Access and Mobility Management Function (AMF).

Options

`name`	Specifies the name of the Access and Mobility Management Function (AMF).
`default-amf`	Identifies the AMF as the default AMF.
`ip-address`	Specifies the IP address of the Stream Control Transmission Protocol (SCTP) endpoint on the AMF.
`node-id`	Specifies the AMF node identifier. • **Range:** 0 through 255
`offline`	Disable communication with this AMF.
`port` *`port number`*	Specifies the port number on the SCTP endpoint. You can specify a port from 0 through 65535. The default is 38412. • **Default:** 38412 • **Range:** 0 through 65535
`routing-instance` *`routing-instance-name`*	Binds the SCTP endpoint routing instance to the AMF connectivity.

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 22.3R1.

local-endpoint

IN THIS SECTION

Syntax

```
local-endpoint {
 initial-tnla-weight-factor initial-tnla-weight-factor;
 ip-address name {
  <primary>;
 }
}
```

Hierarchy Level

```
[edit services agf amf]
```

Description

AMF local endpoint

Options

initial-tnla-weight-factor The weight factor assigned to the Stream Control Transmission Protocol (SCTP) association. The weight factor is passed to the Access and Mobility Management Function (AMF) for load balancing. The AMF assigns the weight factor and is used in load balancing. The AGF recommends the initial TNLA weight factor as the SCTP tunnel is being established.

- **Default:** 128
- **Range:** 1 through 255

ip-address *ip-address* Specify the SCTP endpoint on the AGF.

primary (Optional) Identify the SCTP endpoint as a primary path.

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 22.3R1.

plmn

IN THIS SECTION

Syntax

```
plmn name {
 mcc mcc;
 mnc mnc;
}
```

Hierarchy Level

```
[edit services agf]
```

Description

Configure the public land mobile networks (PLMNs) that the Access Gateway Function (AGF) supports.

Options

name	Public land mobile network (PLMN) name
mcc *mcc*	Mobile country code
mnc *mnc*	Mobile network code

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 22.3R1.

s-nssai

IN THIS SECTION

Syntax

```
s-nssai name {
 sd sd;
 sst(embb | miot | urllc | v2x);
}
```

Hierarchy Level

```
[edit services agf tracking-area name plmn]
```

Description

Configure the single network slice selection assistance information (S-NSSAI). The S-NSSAI is used to uniquely identify a network slice. It consists of two components. For a fixed network residential gateway (FN-RG), the Access Gateway Function (AGF) sends a proxy S-NSSAI message to the Access and Mobility Management Function (AMF) during the initial setup.

- SST—Slice service type
- SD—Selection differentiator

Options

name Single network slice selection assistance information identifier

- **Range:**0 through 128

sd Selection differentiator

- **Default:** 0
- **Range:** 0 through 16777215

sst Slice service type

- embb—Enhanced mobile broadband slice
- miot—Massive Internet of Things (IoT)
- urllc—Ultra-reliable, low-latency communications
- v2x—V2X services

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 22.3R1.

tracking-area

IN THIS SECTION

Release Information | 42

Syntax

```
tracking-area code {
 plmn name {
  s-nssai name {
   sd sd;
   sst(embb | miot | urllc | v2x);
  }
 }
}
```

Hierarchy Level

```
[edit services agf]
```

Description

Tracking area for the AMF.

Options

name Tracking area code

- **Range:** 0 through 16777215

plmn Public land mobile network name

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 22.3R1.

user-planes

IN THIS SECTION

Syntax

```
user-planes name {
```

```
  colocated-user-plane {
   ip-endpoint-address ip-endpoint-address;
  }
  data-network-name data-network-name;
  ip-address ip-address;
  routing-instance routing-instance;
 }
```

Hierarchy Level

```
[edit services agf]
```

Description

Configure a tunnel to the User Plane Function (UPF).

Options

name	User plane name
colocated-user-plane	Specify there is a colocated UPF. The `ip-endpoint-address` *ip-endpoint-address* is the IP address of the UPF.
data-network-name	Data network name Name of the data network
ip-address *ip-endpoint-address*	User plane IP address
routing-instance	User plane routing instance

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 22.3R1.

4

CHAPTER

Operational Commands

clear network access nas-5g statistics

IN THIS SECTION

Syntax

```
clear network-access nas-5g statistics
```

Description

Clear the counter tracking network NAS 5G messages.

Options

none

Required Privilege Level

view

Release Information

Command introduced in Junos OS Release 22.3R1.

clear services agf nas statistics

IN THIS SECTION

Syntax

```
clear services agf nas statistics
```

Description

Clear Non-Access Stratum (NAS) messaging information that the Access Gateway Function (AGF) has collected.

Options

none

Required Privilege Level

view

Release Information

Command introduced in Junos OS Release 22.3R1.

clear services agf ngap amf

IN THIS SECTION

Syntax

```
clear services agf ngap amf
<amf-name>
statistics
```

Description

Clear N1 messages sent to the Access Gateway Function (AGF) from the Access and Mobility Management Functions (AMFs).

Options

amf-name	(Optional) Clear the statistics for a particular AMF.
statistics	Clear the statistics for all the AMFs.

Required Privilege Level

view

Release Information

Command introduced in Junos OS Release 22.3R1.

show network access nas-5g

IN THIS SECTION

Syntax

```
show network access nas-5g (state | statistics)
```

Description

Display statistics on the interactions between the Access Gateway Function (AGF) and other network functions during subscriber authentication.

Options

state Display the status of the 5G connections

statistics Display the statistics for the 5G core (5GC) connections.

Required Privilege Level

view

Output Fields

Table 2 on page 50 lists the output fields for the `show network access nas-5g` command.

Table 2: show network access nas-5g

Field Name	Field Description
Connection up transitions	Number of Non-Access Stratum (NAS) connections established.

Table 2: show network access nas-5g *(Continued)*

Field Name	Field Description
Connection down transitions	Number of NAS connections shut down.
Connection errors	Number of NAS connections that failed.
Total messages sent	Number of NAS signaling messages sent.
Total messages received	Number of NAS signaling messages received.
Total request retries	Number of retry attempts for NAS signaling messages.
Total request timeouts	Number of request messages that timed out.
Authentication request attempts	Number of attempted authentication request messages.
Authentication request messages sent	Number of authentication request messages sent successfully.
Authentication request messages authenticated	Number of authentication request messages authenticated.
Authentication request failures	Number of authentication request messages that failed.
Authentication response failures	Number of errors encountered during the processing of authentication response messages.

Table 2: show network access nas-5g *(Continued)*

Field Name	Field Description
Authentication request timeouts	Number of timed out authentication request messages.
Maximum number of outstanding requests exceeded failures	Number of times the outstanding requests exceeded the failure count.
Session terminate request messages sent	Number of session termination request messages sent.
Session terminate response messages received	Number of session termination response messages received
Session terminate request message failures	Number of session termination request messages that failed.
Session terminate request timeouts	Number of session termination request messages that timed out.
Session command logout received	Number of session log-out command messages received.
Session command logout receive failures	Number of session logout command messages that were received and failed.
Session disconnect request sent	Number of session disconnect request messages sent.
Session disconnect request send failures	Number of errors encountered while sending the session disconnect request messages.

Table 2: show network access nas-5g *(Continued)*

Field Name	Field Description
Session disconnect response received	Number of session disconnect response messages received.
Session disconnect response receive failures	Number of errors encountered during the processing of session disconnect response messages.
Number of outstanding requests	Number of pending sessions that have not been processed.
Total number of allocated messages	Total number of messages allocated in memory.

Sample Output

show network-access nas-5g state

```
user@host> show network-access nas-5g state
```

```
NAS-5G module state information
  Connection state: UP
  Total number of subscribers: 11
```

show network-access nas-5g statistics

```
user@host> show network-access nas-5g statistics
```

```
NAS-5G module
statistics
```

```
  Connection up transitions:
2
  Connection down transitions:
1
  Connection errors:
0

  Total messages sent:
11

  Total messages received:
11
  Total request retries:
0
  Total request timeouts:
0
  Authentication request attempts:
5
  Authentication request messages sent:
5
  Authentication request messages authenticated:
5
  Authentication request failures:
0
  Authentication response failures:
0
  Authentication request timeouts:
0
  Maximum number of outstanding requests exceeded failures:
0
  Session terminate request messages sent:
6
  Session terminate response messages received:
6
  Session terminate request message failures:
0
  Session terminate response failures:
0
  Session terminate request timeouts:
0
  Number of outstanding requests:
0
```

```
  Total number of allocated messages:
0
```

Release Information

Command introduced in Junos OS Release 22.3R1.

show services agf nas

IN THIS SECTION

Syntax

```
show services agf nas (statistics | user-equipment <ue-id>
<session-id session-id>
<brief | detail | extensive | summary > )
```

Description

Display information about the Non-Access Stratum (NAS) operation between the Access Gateway Function (AGF) and the user equipment (UE).

Options

statistics	(Optional) Display the statistics for different NAS messages that are sent and received on the AGF.
user-equipment *ue-id*	(Optional) Display NAS connection information on user equipment.
session-id *session-id*	Display information for a specified session ID.
brief | detail | extensive | summary	(Optional) Display the specified level of output.

Required Privilege Level

view

Output Fields

Table 3 on page 56 lists the output fields for the `show services agf nas` command.

Table 3: show-services-agf-nas

Field Name	Field Description
Message counts	Number of messages sent and received by the Access Gateway Function (AGF).
Messages received	Type and number of NAS signaling messages that has received sent by the AGF.

Table 3: show-services-agf-nas *(Continued)*

Field Name	Field Description
Messages sent	Type and number of NAS signaling messages that has been sent by the AGF.
PDU ID	PDU identifier
Session ID	Session identifier
Session State	Status of the session. The session can have one of the following states: • Inactive • Activating • Active • Deactivating • Deactivated
UE ID	User equipment (UE) identifier
UE State	Status of the UE. The UE can have one of the following states: • Initial • Registering • Registered • Deregistering • Deregistered • Releasing

Sample Output

show services agf nas statistics

```
user@host> show services agf nas user-equipment
```

```
UE id      UE State         PDU id   Session State  Session id
10076162   Registered       1        Active         4
```

show services agf nas statistics

```
user@host> show services agf nas statistics
```

```
Message counts:
    Sent                                13
    Sent discards                       0
    Received                            6
    Receive discards                    0

Messages sent:
    Registration Request                2
    Registration Complete               2
    Deregistration Request              1
    Deregistration Accept               0
    Identity Response                   0
    Authentication Response             0
    Authentication Failure              0
    Security Mode Complete              0
    Security Mode Reject                0
    Service Request                     0
    UL Nas Transport                    4
    5GMM Status                         0
    PDU Session Establishment Request   2
    PDU Session Modification Complete   0
    PDU Session Modification Reject     0
    PDU Session Release Request         1
```

```
    PDU Session Release Complete         1
    5GSM Status                          0

Messages received:
    Registration Accept                  2
    Registration Reject                  0
    Deregistration Accept                1
    Deregistration Request               0
    Identity Request                     0
    Authentication Request               0
    Authentication Result                0
    Authentication Reject                0
    Security Mode Command                0
    Service Accept                       0
    Service Reject                       0
    DL Nas Transport                     3
    5GMM Status                          0
    PDU Session Establishment Accept     2
    PDU Session Establishment Reject     0
    PDU Session Modification Command     0
    PDU Session Release Command          1
    PDU Session Release Reject           0
    5GSM Status                          0
```

Release Information

Command introduced in Junos OS Release 22.3R1.

show services agf ngap

IN THIS SECTION

Syntax

```
show services agf ngap (amf <amf-name>| user-equipment <ue-id>
<brief | detail | summary>)
```

Description

Display information about the Next Generation Application Protocol (NGAP) operations.

Options

amf *amf-name*	(Optional) Display the Next Generation Application Protocol (NGAP) information about the Access and Mobility Management Function (AMF).
user-equipment *ue-id*	(Optional) Display NGAP information about user equipment (UE).
brief | detail| summary	(Optional) Display the specified level of output.

Required Privilege Level

view

Output Fields

Table 4 on page 61 lists the Access and Mobility Management Function (AMF) output fields for the `show services agf ngap` command.

Table 4: show services agf ngap (AMF outputs)

Field Name	Field Description
AMF	AMF name in the configuration.
Backup AMF name	Fully qualified domain name (FQDN) of the backup AMF for the Globally Unique AMF ID (GUAMI). The GUAMI is provided by the AMF during the NG Setup Procedure. If the AMF does not provide a backup AMF name, then `None` is displayed.
Default	Identifies whether the AMF is configured as a default AMF. • Yes—This is configured as the default AMF. • No—This is not a default AMF.
IP address	IP address configured for the AMF.
MCC	Mobile Country Code
MNC	Mobile Network Code
Name	Globally unique, fully qualified domain name (FQDN) provided by the AMF during the NG Setup Procedure. This should be published in the Domain Name System (DNS).
Node id	Uniquely configured AMF node ID used internally by the AGF to identify the AMF.
Overload State	Current AMF overload state. When the AMF is in the overload state, the AGF does not select the AMF for any new user equipment (UE) setups
Port	Port number that is configured for the AMF. Defaults to port 38412 if it is not configured.

Table 4: show services agf ngap (AMF outputs) *(Continued)*

Field Name	Field Description
Routing Instance	Configured AMF routing instance. The IP address for the AMF must be reachable in the configured routing instance.
SD	Slice Differentiator
Served GUAMI	List of Global Unique AMF Identifier. The GUAMI consists of: • PLMN ID—Public land mobile network identifier which consists of an MCC and MNC. • Region ID—AMF region identifier. • AMF Set ID—AMF set identifier. The AMF set ID identifies the AMF set within the AMF region. • Pointer—AMF pointer. The AMF pointer identifies one or more AMFs within the AMF set.
SST	Service Slice Type • Embb—Enhanced mobile broadband • Miot— Massive IoT • Urllc—Ultra-reliable, low latency communications • V2x—Vehicle-to-everything

Table 4: show services agf ngap (AMF outputs) *(Continued)*

Field Name	Field Description
State	Status of the AMF. • Offline—The AGF is not connected to the AMF. • Offline (Admin) —The AGF is administratively disabled. The AMF configuration was not found. • Connecting—The AGF is in the process of connecting to the AMF. • Initializing—The AGF is in the initial NG Setup Procedure. • Online—The AGF has completed the NG Setup Procedure and is ready to service UE contexts.
Tracking areas	Configured AMF tracking areas.
UE count	Current number of UEs being serviced by the AMF.

Table 5 on page 63 lists the UE output fields for the `show services agf ngap` command.

Table 5: show services agf ngap Output Fields (UE outputs)

Field Name	Field Description
AMF	Name of the AMF servicing the UE.
AMF GUAMI	Globally Unique AMF Identifier assigned to service the UE context.
AMF UE ID	UE identifier allocated by the AMF.
RM State	Current registration management state. Registration management state is defined by the Third-Generation Partnership Project (3GPP). • RM_REGISTERED—The UE is registered with the 5GC. • RM_DEREGISTERED—The UE is not registered with the 5GC.

Table 5: show services agf ngap Output Fields (UE outputs) *(Continued)*

Field Name	Field Description
State	Current internal Next Generation Application Protocol (NGAP) UE state. • Establishing—The UE context is being set up in the AMF. • Established—The UE context setup is complete. • Releasing —The UE has requested the AMF to release the UE logical NG connection. • Released —The UE context has been released.
Type	UE Type. • Fixed Network Residential Gateway (FN-RG) • 5G Residential Gateway (5G-RG)
UE identifier	User equipment identifier. The identifier uniquely identifies the UE within the AGF.

Table 6 on page 64 lists the PDU session output fields for the `show services agf ngap` command.

Table 6: show services agf ngap Output Fields (PDU Session)

Field Name	Field Description
AGF IP address	Local AGF IP address.
Local GTP tunnel	The local GPRS tunneling protocol (GTP) tunnel attributes for the Protocol Data Unit (PDU) session allocated by the AGF.
PDU Session id	PDU session identifier allocated by the 5GC.
Remote GTP tunnel	The remote GTP tunnel attributes for the PDU session allocated by the user plane function (UPF).
SD	Slice Differentiator

Table 6: show services agf ngap Output Fields (PDU Session) ***(Continued)***

Field Name	Field Description
S-NSSAI	Single Network Service Slice Assistance Information. It consists of SST and SD values.
SST	Service Slice Type • Embb—Enhanced mobile broadband • Miot— Massive IoT • Urllc—Ultra-reliable, low latency communications • V2x—Vehicle-to-everything
State	Current state of the PDU session. • Activating—The PDU session resource setup is in progress. • Active—The PDU session has been set up and the session is active on the AGF. • Failed—The PDU session setup has failed on the AGF.
TEID	GTP tunnel endpoint identifier.
UPF IP address	Remote GTP tunnel endpoint IP address.

Sample Output

show services agf ngap amf

```
user@host> show services agf ngap amf
```

```
AMF              Routing instance     Default   State         Overload   UEs
amf1             default              Yes       Online        Off        1
```

show services agf ngap amf detail

```
user@host> show services agf ngap amf detail
```

```
AMF: amf.spirent.com
  Name:             amf.spirent.com
  Node id:          1
  Default:          Yes
  Ip address:       10.1.1.7
  Port:             38412
  Routing instance: default
  Tracking areas:   0
  State:            Online
  Overload state:   Off
  UE count:         1

  TNLA: 1
    Type:              Static
    Usage type:        UE and Non-UE associated signalling
    Weight factor:     128
    State:             Established
    Packets sent:      16
    Packets received:  10
    Local ip address   Port
    10.1.1.1           55465
    Peer ip address    Port      State
    10.1.1.7*          38412     Active

  Served GUAMI     PLMN id   Region id   Set id   Pointer   Backup AMF name
  0x123456090207   123456    9           8        7
None

  PLMN id: 123456 (MCC: 123, MNC: 456)
    SST: Embb, SD: 0
    SST: Miot, SD: 0
    SST: Urllc, SD: 0
```

show services agf ngap user-equipment detail

```
user@host> show services agf ngap user-equipment detail
```

```
UE identifier: 33
  State:          Established
  RM state:       RM-REGISTERED
  Type:           FN-RG
  AMF:            amf1
  AMF UE id:      3690987520
  AMF GUAMI:      0x123456090207
  PLMN id:        MCC: 123, MNC: 456
  AMF region id:  9
  AMF set id:     8
  AMF pointer:    7

  PDU session id: 1
    State: Active
    S-NSSAI: SST: Embb, SD: 0
    Remote GTP tunnel
      TEID: 0x001e8480
      UPF ip address: 10.250.1.62
      QoS flow identifier: 1
    Local GTP tunnel
      TEID: 0x000000e9
      AGF ip address: 10.1.1.51
```

Release Information

Command introduced in Junos OS Release 22.3R1.

show subscribers

IN THIS SECTION

Syntax

```
show subscribers
<detail | extensive | terse>
<aci-interface-set-name aci-interface-set-name>
<address address>
<agent-circuit-identifier agent-circuit-identifier>
<agent-remote-identifier agent-remote-identifier>
<aggregation-interface-set-name interface-set-name>
<client-type client-type>
<count>
<id session-id <accounting-statistics>>
<interface interface <accounting-statistics>>
<logical-system logical-system>
<mac-address mac-address>
<physical-interface physical-interface-name>
<profile-name profile-name>
<routing-instance routing-instance>
<stacked-vlan-id stacked-vlan-id>
<sub-system (agf | bng)>
<subscriber-state subscriber-state>
```

```
<user-name user-name>
<vci vci-identifier>
<vpi vpi-identifier>
<vlan-id vlan-id>
```

Description

Display information for active subscribers on both the broadband network gateway (BNG) and Access Gateway Function (AGF) subsystems. When you have subscribers logged in to both the BNG and the AGF, you can display the outputs specific to either subsytem with the `sub-system` option.

See "Sample Output for AGF" on page 118 for subscriber session information about the AGF subsystem.

Options

`detail | extensive | terse` (Optional) Display the specified level of output.

`aci-interface-set-name` (Optional) Display all the dynamic subscriber sessions that use the specified agent circuit identifier (ACI) interface set. You must use the ACI interface set name generated by the router, such as aci-1003-ge-1/0/0.4001, and not the actual ACI value found in the Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol over Ethernet (PPPoE) control packets.

address (Optional) Display subscribers whose IP address matches the specified address. You must specify the IPv4 or IPv6 address prefix without a netmask (for example, 192.0.2.0). If you specify the IP address as a prefix with a netmask (for example, 192.0.2.0/32), the router displays a message that the IP address is invalid and rejects the command.

agent-circuit-identifier (Optional) Display all the dynamic subscriber sessions whose ACI value matches the specified string. You can specify either the complete ACI string or a substring. To specify a substring, you must enter characters that form the beginning of the string, followed by an asterisk (*) as a wildcard to substitute for the remainder of the string. The wildcard can be used only at the end of the specified substring; for example:

```
user@host1> show subscribers agent-circuit-identifier substring*
```

Junos OS Release	Substring Support
Junos OS Release 13.3R1	You can specify a substring without a wildcard.
Starting in Junos OS Release 14.1R1	You must specify the complete ACI string; you cannot specify a wildcard.
Starting in Junos OS Releases 15.1R7, 16.1R7, 16.2R3, 17.1R3, 17.2R3, 17.3R3, 17.4R2, 18.1R2, 18.2R1	You can specify a substring, but you must include the wildcard character at the end of the substring.

agent-remote-identifier (Optional) Display all the dynamic subscriber sessions whose agent remote identifier (ARI) value matches the specified string. You must specify the complete ACI string; you cannot specify a wildcard.

aggregation-interface-set-name *interface-set-name* (Optional) Display summary information for the specified aggregation node interface set, including interface, VLAN ID, username, and logical system and routing instance (LS:RI).

client-type (Optional) Display subscribers whose client type matches one of the following client types:

- `dhcp`—Dynamic Host Configuration Protocol (DHCP) clients only.
- `dotlx`—802.1X clients only.
- `essm`—Extensible Subscribers Services Manager (ESSM) clients only.
- `fixed-wireless-access`—Fixed wireless access clients only.
- `fwauth`—FwAuth (authenticated across a firewall) clients only.
- `l2tp`—Layer 2 Tunneling Protocol (L2TP) clients only.
- `mlppp`—Multilink Point-to-Point Protocol (MLPPP) clients only.
- `ppp`—Point-to-Point Protocol (PPP) clients only.
- `pppoe`—Point-to-Point Protocol over Ethernet (PPPoE) clients only.
- `static`—Static clients only.

- `vlan`—VLAN clients only.
- `vlan-oob`—VLAN out-of-band (ANCP-triggered) clients only.
- `vpls-pw`—Virtual private LAN service (VPLS) pseudowire clients only.
- `xauth`—Xauth clients only.

count (Optional) Display the count of the total subscribers and active subscribers for any specified option. You can use the `count` option alone or with the `address`, `client-type`, `interface`, `logical-system`, `mac-address`, `profile-name`, `routing-instance`, `stacked-vlan-id`, `subscriber-state`, or `vlan-id` options.

id *session-id* (Optional) Display a specific subscriber session whose session ID matches the specified subscriber ID. You can display the subscriber IDs by using the `show subscribers extensive` command or the `show subscribers interface extensive` command.

id *session-id* accounting-statistics (Optional) Display accurate subscriber accounting statistics for a subscriber session with the specified ID. Requires the `actual-transmit-statistics` statement to be configured in the dynamic profile for the dynamic logical interface. If the statement is not configured, a value of 0 is displayed for accounting statistics.

interface (Optional) Display subscribers whose interface matches the specified interface.

***interface* accounting-statistics** (Optional) Display subscriber accounting statistics for the specified interface. Requires the `actual-transmit-statistics` statement to be configured in the dynamic profile for the dynamic logical interface.

logical-system (Optional) Display subscribers whose logical system matches the specified logical system.

mac-address (Optional) Display subscribers whose MAC address matches the specified MAC address.

physical-interface-name (M120, M320, and MX Series routers only) (Optional) Display subscribers whose physical interface matches the specified physical interface.

profile-name (Optional) Display subscribers whose dynamic profile matches the specified profile name.

routing-instance (Optional) Display subscribers whose routing instance matches the specified routing instance.

stacked-vlan-id (Optional) Display subscribers whose stacked VLAN ID matches the specified stacked VLAN ID.

subsystem (agf | bng) (Optional) Display subscriber information on the AGF or BNG subsystem.

> **NOTE**: The subsystem option is only available when both the AGF and BNG subscribers are logged into the router at the same time.

subscriber-state (Optional) Display subscribers whose subscriber state matches the specified subscriber state (ACTIVE, CONFIGURED, INIT, TERMINATED, or TERMINATING).

user-name (M120, M320, and MX Series routers only) (Optional) Display subscribers whose username matches the specified subscriber name.

vci-identifier (MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active Asynchronous Transfer Mode (ATM) subscribers whose ATM virtual circuit identifier (VCI) matches the specified VCI identifier. The range of values is 0 through 255.

vpi-identifier (MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual path identifier (VPI) matches the specified VPI identifier. The range of values is 0 through 65,535.

vlan-id (Optional) Display subscribers whose VLAN ID matches the specified VLAN ID, regardless of whether the subscriber uses a single-tagged or double-tagged VLAN. For subscribers using a double-tagged VLAN, this option displays subscribers where the inner VLAN tag matches the specified VLAN ID. To display only subscribers where the specified value matches only double-tagged VLANs, use the `stacked-vlan-id` *`stacked-vlan-id`* option to match the outer VLAN tag.

> **NOTE**: Because of display limitation, the logical system and routing instance output values are truncated when necessary.

Required Privilege Level

view

Output Fields

Table 7 on page 73 lists the output fields for the `show subscribers` command. Output fields are listed in the approximate order in which they appear.

Table 7: show subscribers Output Fields

Field Name	Field Description
`Interface`	Interface associated with the subscriber. The router or the switch displays the subscribers whose interface matches or begins with the specified interface. The asterisk (*) indicates a continuation of addresses for the same session.
`IP Address/VLAN ID`	Subscriber IP address or VLAN ID associated with the subscriber in the form *tpid.vlan-id* No IP address or VLAN ID is assigned to an L2TP tunnel-switched session. For these subscriber sessions, the value is `Tunnel-switched`.
`User Name`	Name of subscriber.
`LS:RI`	Logical system and routing instance associated with the subscriber.
`Type`	Subscriber client type (DHCP, FWA, GRE, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN).
`IP Address`	Subscriber IPv4 address.
`IP Netmask`	Subscriber IP netmask. (MX Series) This field displays 255.255.255.255 by default. For tunneled or terminated PPP subscribers only, this field displays the actual value of Framed-IP-Netmask when the SDB_FRAMED_PROTOCOL attribute in the session database is equal to AUTHD_FRAMED_PROTOCOL_PPP. This occurs in the use case where the L2TP network server (LNS) generates access-internal routes when it receives Framed-IP-Netmask from RADIUS during authorization. When it receives Framed-Pool from RADIUS, the pool mask is ignored and the default /32 mask is used.

Table 7: show subscribers Output Fields *(Continued)*

Field Name	Field Description
`Primary DNS Address`	IP address of the primary Domain Name System (DNS) server. This field is displayed with the `extensive` option only when the address is provided by RADIUS.
`Secondary DNS Address`	IP address of the secondary DNS server. This field is displayed with the `extensive` option only when the address is provided by RADIUS.
`IPv6 Primary DNS Address`	IPv6 address of the primary DNS server. This field is displayed with the `extensive` option only when the address is provided by RADIUS.
`IPv6 Secondary DNS Address`	IPv6 address of the secondary DNS server. This field is displayed with the `extensive` option only when the address is provided by RADIUS.
`Domain name server inet`	IP addresses for the DNS server, displayed in order of configuration. This field is displayed with the `extensive` option only when the addresses are derived from the access profile or the global access configuration.
`Domain name server inet6`	IPv6 addresses for the DNS server, displayed in order of configuration. This field is displayed with the `extensive` option only when the addresses are derived from the access profile or the global access configuration.
`Primary WINS Address`	IP address of the primary Windows Internet Name Service (WINS) server.
`Secondary WINS Address`	IP address of the secondary WINS server.
`IPv6 Address`	Subscriber IPv6 address, or multiple addresses.

Table 7: show subscribers Output Fields *(Continued)*

Field Name	Field Description
IPv6 Prefix	Subscriber IPv6 prefix. If you are using DHCPv6 prefix delegation, this is the delegated prefix.
IPv6 User Prefix	IPv6 prefix obtained through Neighbor Discovery Router Advertisement (NDRA).
IPv6 Address Pool	Subscriber IPv6 address pool. The IPv6 address pool is used to allocate IPv6 prefixes to the DHCPv6 clients.
IPv6 Network Prefix Length	Length of the network portion of the IPv6 address.
IPv6 Prefix Length	Length of the subscriber IPv6 prefix.
Logical System	Logical system associated with the subscriber.
Routing Instance	Routing instance associated with the subscriber.
Interface	(Enhanced subscriber management for the MX Series routers) Name of the enhanced subscriber management logical interface, in the form demux0.*nnnn* (for example, demux0.3221225472), to which access-internal and framed subscriber routes are mapped.
Interface Type	Whether the subscriber interface is Static or Dynamic.

Table 7: show subscribers Output Fields *(Continued)*

Field Name	Field Description
Interface Set	Internally generated name of the dynamic agent circuit identifier (ACI) or ATM line interface (ALI) interface set used by the subscriber session. The prefix of the name indicates the string received in DHCP or PPPoE control packets on which the interface set is based. For ALI interface sets, the prefix indicates that the value is configured as a trusted option to identify the subscriber line. The name of the interface set uses one of the following prefixes: • aci—ACI; for example, aci-1033-demux0.3221225524. This is the only prefix allowed for ACI interface sets. • ari—ARI or agent remote identifier; for example, ari-1033-demux0.3221225524. • aci+ari—Both the ACI and the ARI; for example, aci+ari-1033-demux0.3221225524. • noids—Neither the ACI nor the ARI were received; for example, noids-1033-demux0.3221225524. **NOTE**: ACI interface sets are configured with the agent-circuit-identifier autoconfiguration stanza. ALI interface sets are configured with the line-identity autoconfiguration stanza. Besides dynamic ACI and ALI interface sets, this field can be an interface set based on a substring of the ARI string. This occurs when the dynamic profile includes the predefined variable $junos-pon-id-interface-set-name, and the profile is applied for a passive optical network (PON). The ARI string is inserted by the optical line terminal (OLT). The final substring in the string, unique for the PON, identifies individual subscriber circuits, and is used as the name of the interface set.
Interface Set Type	Interface type of the ACI interface set: Dynamic. This is the only ACI interface set type currently supported.
Interface Set Session ID	Identifier of the dynamic ACI interface set entry in the session database.
Underlying Interface	Name of the underlying interface for the subscriber session.
Dynamic Profile Name	Dynamic profile used for the subscriber.

Table 7: show subscribers Output Fields *(Continued)*

Field Name	Field Description
Dynamic Profile Version	Version number of the dynamic profile used for the subscriber.
MAC Address	MAC address associated with the subscriber.
State	Current state of the subscriber session (Init, Configured, Active, Terminating, or Tunneled).
L2TP State	Current state of the L2TP session (Tunneled or Tunnel-switched). When the value is Tunnel-switched, two entries are displayed for the subscriber; the first entry is at the L2TP network server (LNS) interface on the L2TP tunnel switch (LTS) and the second entry is at the L2TP access concentrator (LAC) interface on the LTS.
Tunnel switch Profile Name	Name of the L2TP tunnel switch profile that initiates tunnel switching.
Local IP Address	IP address of the local gateway (LAC).
Remote IP Address	IP address of the remote peer (LNS).
PFE Flow ID	Forwarding flow identifier.
VLAN Id	VLAN ID associated with the subscriber in the form *tpid.vlan-id*.
Stacked VLAN Id	Stacked VLAN ID associated with the subscriber in the form *tpid.vlan-id*.
RADIUS Accounting ID	RADIUS accounting ID associated with the subscriber.

Table 7: show subscribers Output Fields *(Continued)*

Field Name	Field Description
Agent Circuit ID	For the dhcp client type, option 82 agent circuit ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in the hexadecimal format. For the vlan-oob client type, the agent circuit ID or access-loop circuit identifier that identifies the subscriber line based on the subscriber-facing DSL access multiplexer (DSLAM) interface on which the subscriber request originates.
Agent Remote ID	For the dhcp client type, option 82 agent remote ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format. For the vlan-oob client type, the agent remote ID or access-loop remote identifier that identifies the subscriber line based on the network access server (NAS)-facing DSLAM interface on which the subscriber request originates.
Aggregation Interface-set Name	Value of the $junos-aggregation-interface-set-name predefined variable; one of the following: • When the hierarchical-access-network-detection option is configured for the access lines and the value of the Access-Aggregation-Circuit-ID-ASCII attribute (TLV 0x0003) received either in the Access Node Control Protocol (ANCP) Port Up message or PPPoE Active Discover Request (PADR) IA tags begins with a # character, then the variable takes the value of the remainder of the string after the # character. • When the hierarchical-access-network-detection option is not configured, or if the sting does not begin with the # character, then the variable takes the value specified with the predefined-variable-defaults statement.
Accounting Statistics	Actual transmitted subscriber accounting statistics by the session ID or the interface. Service accounting statistics are not included. These statistics do not include overhead bytes or dropped packets; they are the accurate statistics used by RADIUS. The statistics are counted when the actual-transmit-statistics statement is included in the dynamic profile.
DHCP Relay IP Address	IP address used by the DHCP relay agent.

Table 7: show subscribers Output Fields *(Continued)*

Field Name	Field Description
ATM VPI	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual path identifier (VPI) on the subscriber's physical interface.
ATM VCI	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual circuit identifier (VCI) for each VPI configured on the subscriber interface.
Login Time	Date and time at which the subscriber logged in.
DHCPV6 Options	len = number of hex values in the message. The hex values specify the type, length, value (TLV) for the DHCPv6 options.
Server DHCP Options	len = number of hex values in the message. The hex values specify the type, length, value (TLV) for the DHCP options.
Server DHCPV6 Options	len = number of hex values in the message. The hex values specify the type, length, value (TLV) for the DHCPv6 options.
DHCPV6 Header	len = number of hex values in the message. The hex values specify the type, length, value (TLV) for the DHCPv6 options.
Effective shaping-rate	Actual downstream traffic shaping rate for the subscriber in kilobits per second.
IPv4 Input Service Set	Input service set in access dynamic profile.
IPv4 Output Service Set	Output service set in access dynamic profile.
PCEF Profile	Policy and charging enforcement function (PCEF) profile in access dynamic profile.
PCEF Rule/Rulebase	PCC rule or rulebase used in dynamic profile.

Table 7: show subscribers Output Fields *(Continued)*

Field Name	Field Description
Dynamic configuration	Values for variables that are passed into the dynamic profile from RADIUS.
Service activation time	Time at which the first family in this service became active.
IPv4 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to the IPv4 packets that fail the reverse-path-forwarding (RPF) check.
IPv6 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to the IPv6 packets that fail the RPF check.
DHCP Options	len = number of hex values in the message. The hex values specify the type, length, value (TLV) for the DHCP options, as defined in RFC 2132.
Session ID	ID number for a subscriber session.
Underlying Session ID	For DHCPv6 subscribers on a PPPoE network, displays the session ID of the underlying PPPoE interface.
Service Sessions	Number of service sessions (that is, a service activated using RADIUS Change of Authorization or CoA) associated with the subscribers.
Service Session ID	ID number for a subscriber service session.
Service Session Name	Service session profile name.
Session Timeout (seconds)	Number of seconds of access provided to the subscriber before the session is automatically terminated.
Idle Timeout (seconds)	Number of seconds for which the subscriber can be idle before the session is automatically terminated.

Table 7: show subscribers Output Fields *(Continued)*

Field Name	Field Description
IPv6 Delegated Address Pool	Name of the pool used for DHCPv6 prefix delegation.
IPv6 Delegated Network Prefix Length	Length of the prefix configured for the IPv6 delegated address pool.
IPv6 Interface Address	Address assigned by the Framed-Ipv6-Prefix AAA attribute. This field is displayed only when the predefined variable $junos-ipv6-address is used in the dynamic profile.
IPv6 Framed Interface Id	Interface ID assigned by the Framed-Interface-Id AAA attribute.
ADF IPv4 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv4 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
IPv4 Input Filter Name	Name assigned to the IPv4 input filter (client or service session).
IPv4 Output Filter Name	Name assigned to the IPv4 output filter (client or service session).

Table 7: show subscribers Output Fields *(Continued)*

Field Name	Field Description
IPv6 Input Filter Name	Name assigned to the IPv6 input filter (client or service session).
IPv6 Output Filter Name	Name assigned to the IPv6 output filter (client or service session).
IFL Input Filter Name	Name assigned to the logical interface input filter (client or service session).
IFL Output Filter Name	Name assigned to the logical interface output filter (client or service session).
DSL type	PPPoE subscriber's access line type reported by the PPPoE intermediate agent in a PADI or PADO packet in the Vendor-Specific-Tags TLV in subattribute DSL-Type (0x0091). The DSL type is one of the following types: ADSL, ADSL2, ADSL2+, OTHER, SDSL, VDSL, or VDSL2.
Frame/Cell Mode	Mode type of the PPPoE subscriber's access line determined by the PPPoE daemon based on the received subattribute DSL-Type (0x0091): • Cell—When the DSL line type is one of the following: asymmetric digital subscriber line (ADSL), asymmetric digital subscriber line 2 (ADSL2), or asymmetric digital subscriber line 2 plus (ADSL2+). • Frame—When the DSL line type is one of the following: OTHER, SDSL, VDSL, or VDSL2. The value is stored in the subscriber session database.
Overhead accounting bytes	Number of bytes added to or subtracted from the actual downstream cell or frame overhead to account for the technology overhead of the DSL line type. The value is determined by the PPPoE daemon based on the received subattribute DSL-Type (0x0091). The value is stored in the subscriber session database.
Actual upstream data rate	Unadjusted upstream data rate for the PPPoE subscriber's access line reported by the PPPoE intermediate agent in a PADI or PADO packet in the Vendor-Specific-Tags TLV in subattribute Actual-Net-Data-Rate-Upstream (0x0081).

Table 7: show subscribers Output Fields *(Continued)*

Field Name	Field Description
`Actual downstream data rate`	Unadjusted downstream data rate for the PPPoE subscriber's access line reported by the PPPoE intermediate agent in a PADI or PADO packet in the Vendor-Specific-Tags TLV in subattribute Actual-Net-Data-Rate-Downstream (0x0082).
`Adjusted downstream data rate`	Adjusted downstream data rate for the PPPoE subscriber's access line, calculated by the PPPoE daemon and stored in the subscriber session database.
`Adjusted upstream data rate`	Adjusted upstream data rate for the PPPoE subscriber's access line, calculated by the PPPoE daemon and stored in the subscriber session database. **NOTE**: This output field is only available on Junos Release 19.1R1 or earlier versions.
`AGF Mode`	Type of access. Adaptive mode indicates an FN-RG.
`Local TEID-U`	Tunnel endpoint identifier on the BNG for the GTP-U user plane tunnel to the eNodeB. The identifier is allocated by the BNG. A fully qualified local TEID-C consists of this identifier and the `GTPU Tunnel Local IP address` value.
`Local TEID-C`	Tunnel endpoint identifier on the BNG for the GTP-C control plane tunnel to the MME. The identifier is allocated by the BNG. A fully qualified local TEID-C consists of this identifier and the `GTPC Local IP address` value.
`Remote TEID-U`	Tunnel endpoint identifier on the eNodeB for the GTP-U user plane tunnel to the BNG. The identifier is allocated by the eNodeB. A fully qualified remote TEID-U consists of this identifier and the `GTPU Tunnel Remote IP address` value.

Table 7: show subscribers Output Fields *(Continued)*

Field Name	Field Description
Remote TEID-C	Tunnel endpoint identifier on the MME for the GPRS tunneling protocol, control (GTP-C) plane tunnel to the BNG. The identifier is allocated by the MME. A fully qualified remote TEID-C consists of this identifier and the GTPC Remote IP address value.
GTPU Tunnel Remote IP address	IP address of the S1-U interface on the eNodeB for the GPRS tunneling protocol, user plane (GTP-U) tunnel endpoint. A fully qualified remote TEID-U consists of this address and the Remote TEID-U value.
GTPU Tunnel Local IP address	IP address of the S1-U interface on the BNG for the GTP-U tunnel endpoint. A fully qualified local TEID-U consists of this address and the Local TEID-U value
GTPC Remote IP address	IP address of the S11 interface on the MME for the GTP-C tunnel endpoint. A fully qualified remote TEID-C consists of this address and the Remote TEID-C value.
GTPC Local IP address	IP address of the S11 interface on the BNG for the GTP-C tunnel endpoint. A fully qualified local TEID-C consists of this address and the Local TEID-C value.
Access Point Name	Access point name (APN) for the user equipment. The APN corresponds to the connection and service parameters that the subscriber's mobile device can use for connecting to the carrier's gateway to the Internet.
Tenant	Name of the tenant system. You can create multiple tenant system administrators for a tenant system with different permission levels based on your requirements.
Routing instance	Name of the routing instance. When a custom routing instance is created for a tenant system, all the interfaces defined in that tenant system are added to that routing instance.
Dynamic Profile Version Alias	Configured name for a specific variation of a base dynamic profile. IT's presence indicates that the profile configuration is different from that of the base profile. The value is conveyed to the RADIUS server during authentication in the Client-Profile-Name VSA (26–4874–174).

Sample Output

show subscribers (IPv4)

```
user@host> show subscribers
Interface               IP Address/VLAN ID   User Name         LS:RI
ge-1/3/0.1073741824     10                                     default:default
demux0.1073741824       203.0.113.10         WHOLESALER-CLIENT default:default
demux0.1073741825       203.0.113.3          RETAILER1-CLIENT  test1:retailer1
demux0.1073741826       203.0.113.3          RETAILER2-CLIENT  test1:retailer2
```

show subscribers (IPv6)

```
user@host> show subscribers
Interface          IP Address/VLAN ID   User Name           LS:RI
ge-1/0/0.0         2001:db8:c0:0:0:0/74    WHOLESALER-CLIENT   default:default
     *             2001:db8:1/128          subscriber-25       default:default
```

show subscribers (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers
Interface           IP Address/VLAN ID         User Name                      LS:RI
demux0.1073741834   0x8100.1002 0x8100.1                                  default:default
demux0.1073741835   0x8100.1001 0x8100.1                                  default:default
pp0.1073741836      203.0.113.13            dualstackuser1@example1.com     default:ASP-1
*                   2001:db8:1::/48
*                   2001:db8:1:1::/64
pp0.1073741837      203.0.113.33            dualstackuser2@example1.com     default:ASP-1
*                   2001:db8:1:2:5::/64
```

show subscribers (Single Session DHCP Dual Stack)

```
user@host> show subscribers

Interface           IP Address/VLAN ID        User Name               LS:RI
demux0.1073741364   192.168.10.10             dual-stack-retail35     default:default
```

```
                    2001:db8::100:0:0:0/74                          default:default
                    2001:db8:3ffe:0:4::/64
```

show subscribers (Single Session DHCP Dual Stack detail)

```
user@host> show subscribers id 27 detail
Type: DHCP
User Name: dual-stack-retail33
IP Address: 10.10.0.53
IPv6 Address: 2001:db8:3000:0:0:8003::2
IPv6 Prefix: 2001:db8:3ffe:0:4::/64
Logical System: default
Routing Instance: default
Interface: ae0.3221225472
Interface type: Static
Underlying Interface: ae0.3221225472
Dynamic Profile Name: dhcp-retail-18
MAC Address: 00:00:5E:00:53:02
State: Active
DHCP Relay IP Address: 10.10.0.1
Radius Accounting ID: 27
Session ID: 27
PFE Flow ID: 2
Stacked VLAN Id: 2000
VLAN Id: 1
Login Time: 2014-05-15 10:12:10 PDT
DHCP Options: len 60
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 00 64 01 01 02
00 06 00 04 00 03 00 19 00 03 00 0c 00 00 00 00 00 00 00 00
00 00 00 00 00 19 00 0c 00 00 00 00 00 00 00 00 00 00 00 00
```

show subscribers (LNS on MX Series Routers)

```
user@host> show subscribers
Interface          IP Address/VLAN ID   User Name         LS:RI
si-4/0/0.1         192.0.2.0          user@example.com   default:default
```

show subscribers (L2TP Switched Tunnels)

```
user@host> show subscribers
Interface           IP Address/VLAN ID    User Name              LS:RI
si-2/1/0.1073741842 Tunnel-switched       user@example.com        default:default
si-2/1/0.1073741843 Tunnel-switched       user@example.com        default:default
```

show subscribers aggregation-interface-set-name

```
user@host> show subscribers aggregation-interface-set-name FRA*

Interface              IP Address/VLAN ID              User Name                 LS:RI
ge-1/0/0.3221225472    50                                ancp                      default:isp1-
subscriber
```

show subscribers client-type dhcp detail

```
user@host> show subscribers client-type dhcp detail
Type: DHCP
IP Address: 203.0.113.29
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux
MAC Address: 00:00:5e:00:53:98
State: Active
Radius Accounting ID: user :2304
Login Time: 2009-08-25 14:43:52 PDT

Type: DHCP
IP Address: 203.0.113.27
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744383
Interface type: Dynamic
```

```
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:00:5e:00:53:f3
State: Active
Radius Accounting ID: 1234 :2560
Login Time: 2009-08-25 14:43:56 PDT
```

show subscribers client-type dhcp detail (DHCPv6)

```
user@host> show subscribers client-type dhcp detail
Type: DHCP
User Name: DEFAULTUSER
IPv6 Address: 2001:db8::2
IPv6 Prefix: 2001:db8:1::/64
Logical System: default
Routing Instance: default
Interface: demux0.3221225602
Interface type: Static
Underlying Interface: demux0.3221225602
Dynamic Profile Name: client-profile
MAC Address: 00:00:5E:00:53:01
State: Active
Radius Accounting ID: 142
Session ID: 142
PFE Flow ID: 148
Stacked VLAN Id: 1
VLAN Id: 1
Login Time: 2018-03-29 12:27:38 EDT
DHCP Options: len 56
00 08 00 02 00 00 00 01 00 0e 00 01 00 01 22 4f d0 33 00 11
01 00 00 01 00 03 00 0c 00 00 00 0a 00 04 9d 40 00 07 62 00
00 19 00 0c 00 00 00 0b 00 04 9d 40 00 07 62 00
Server DHCPV6 Options: len 94
00 0a 00 06 11 22 33 44 55 66 00 11 00 09 00 00 0c 4c 00 02
00 01 aa 00 11 00 20 00 00 0a 4c 00 02 00 02 32 33 00 03 00
03 34 35 36 00 05 00 06 31 32 33 34 35 36 00 06 00 01 31 00
11 00 09 00 00 0b 4c 00 02 00 01 bb 00 11 00 12 00 00 0d e9
00 01 00 03 aa bb cc 00 02 00 03 dd ee cc
DHCPV6 Header: len 4
01 fc e4 96
```

show subscribers client-type dhcp extensive

```
user@host> show subscribers client-type dhcp extensive
Type: DHCP
User Name: user
IP Address: 192.0.2.4
IP Netmask: 255.0.0.0
IPv6 Address: 2001:db8:3::103
IPv6 Prefix: 2001:db8::/68
Domain name server inet6: 2001:db8:1 abcd::2
Logical System: default
Routing Instance: default
Interface: ge-0/0/0.0
Interface type: Static
Underlying Interface: ge-0/0/0.0
MAC Address: 00:00:5e:00:53:01
State: Configured
Radius Accounting ID: 10
Session ID: 10
PFE Flow ID: 2
VLAN Id: 100
Agent Circuit ID: ge-0/0/0:100
Agent Remote ID: ge-0/0/0:100
Login Time: 2017-05-23 12:52:22 IST
DHCPV6 Options: len 69
00 01 00 0e 00 01 00 01 59 23 e3 31 00 10 94 00 00 01 00 08
00 02 00 00 00 19 00 29 00 00 00 00 00 04 9d 40 00 07 62 00
00 1a 00 19 00 09 3a 80 00 27 8d 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
Server DHCP Options: len 13
3a 04 00 00 00 ff 00 3b 04 00 00 0f 00
Server DHCPV6 Options: len 8
00 0a 00 04 ab cd ef ab
DHCPV6 Header: len 4
01 00 00 04
IP Address Pool: al_pool30
IPv6 Address Pool: ia_na_pool
IPv6 Delegated Address Pool: prefix_delegate_pool
```

show subscribers client-type fixed-wireless-access

```
user@host> show subscribers client-type fixed-wireless-access

Interface             IP Address/VLAN ID            User Name               LS:RI
ps1.3221225472        192.0.2.10                    505024101215074         default:default
ps1.3221225473        192.0.2.11                    505024101215075         default:default
```

show subscribers client-type fixed-wireless-access detail (Detail)

```
user@host> show subscribers client-type fixed-wireless-access detail
Type: FWA
User Name: 505024101215074
IP Address: 192.0.2.10
IP Netmask: 255.255.0.0
Interface: ps1.3221225472
Interface type: Dynamic
Dynamic Profile Name: fwa-profile
State: Active
Radius Accounting ID: 1
Session ID: 1
PFE Flow ID: 11
Login Time: 2019-04-10 14:10:12 PDT
Local TEID-U: 1
Local TEID-C: 1
Remote TEID-U: 2000000
Remote TEID-C: 1000000
GTPU Tunnel Remote IP Address: 203.0.113.1.3
GTPU Tunnel Local IP Address: 203.0.113.2.5
GTPC Remote IP Address: 203.0.113.1.2
GTPC Local IP Address: 203.0.113.1.1
Access Point Name: user21
```

show subscribers client-type vlan-oob detail

```
user@host> show subscribers client-type vlan-oob detail
Type: VLAN-OOB
User Name: L2WS.line-aci-1.line-ari-1
Logical System: default
```

```
Routing Instance: ISP1
Interface: demux0.1073744127
Interface type: Dynamic
Underlying Interface: ge-1/0/0
Dynamic Profile Name: Prof_L2WS
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 1234
Session ID: 77
VLAN Id: 126
Core-Facing Interface: ge-2/1/1
VLAN Map Id: 6
Inner VLAN Map Id: 2001
Agent Circuit ID: line-aci-1
Agent Remote ID: line-ari-1
Login Time: 2013-10-29 14:43:52 EDT
```

show subscribers count

```
user@host> show subscribers count
Total Subscribers: 188, Active Subscribers: 188
```

show subscribers address detail (IPv6)

```
user@host> show subscribers address 203.0.113.137 detail
Type: PPPoE
User Name: pppoeTerV6User1Svc
IP Address: 203.0.113.137
IP Netmask: 255.0.0.0
IPv6 User Prefix: 2001:db8:0:c88::/32
Logical System: default
Routing Instance: default
Interface: pp0.1073745151
Interface type: Dynamic
Underlying Interface: demux0.8201
Dynamic Profile Name: pppoe-client-profile
MAC Address: 00:00:5e:00:53:53
Session Timeout (seconds): 31622400
Idle Timeout (seconds): 86400
State: Active
```

```
Radius Accounting ID: example demux0.8201:6544
Session ID: 6544
Agent Circuit ID: ifl3720
Agent Remote ID: ifl3720
Login Time: 2012-05-21 13:37:27 PDT
Service Sessions: 1
```

show subscribers detail (IPv4)

```
user@host> show subscribers detail
Type: DHCP
IP Address: 203.0.113.29
IP Netmask: 255.255.0.0
Primary DNS Address: 192.0.2.0
Secondary DNS Address: 192.0.2.1
Primary WINS Address: 192.0.2.3
Secondary WINS Address: 192.0.2.4
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:00:5e:00:53:98
State: Active
Radius Accounting ID: example :2304
Idle Timeout (seconds): 600
Login Time: 2009-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 0f 21 2c
Service Sessions: 2
```

show subscribers detail (IPv6)

```
user@host> show subscribers detail
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2001:db8:ffff:1::/32
Logical System: default
```

```
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:00:5e:00:53:03
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

show subscribers detail (pseudowire Interface for GRE Tunnel)

```
user@host> show subscribers detail
Interface           IP Address/VLAN ID        User Name           LS:RI
ps0.3221225484      192.0.2.2
ps0.3221225485      192.0.2.3
demux0.3221225486    1                                          default:default
demux0.3221225487    1                                          default:default
demux0.3221225488   198.51.0.1                                  default:default
demux0.3221225489   198.51.0.2                                  default:default
```

show subscribers detail (IPv6 Static Demux Interface)

```
user@host> show subscribers detail
Type: STATIC-INTERFACE
User Name: user@example.com
IPv6 Prefix: 2001:db8:3:4:5:6:7:aa/32
Logical System: default
Routing Instance: default
Interface: demux0.1
Interface type: Static
Dynamic Profile Name: junos-default-profile
State: Active
Radius Accounting ID: 185
Login Time: 2010-05-18 14:33:56 EDT
```

show subscribers detail (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers detail
Type: L2TP
User Name: user@example.com
IP Address: 203.0.113.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
```

show subscribers detail (L2TP Switched Tunnels)

```
user@host> show subscribers detail
Type: L2TP
User Name: user@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741842
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 203.0.113.51
Remote IP Address: 192.0.2.0
Radius Accounting ID: 21
Session ID: 21
Login Time: 2013-01-18 03:01:11 PST

Type: L2TP
User Name: user@example.com
Logical System: default
```

```
Routing Instance: default
Interface: si-2/1/0.1073741843
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 203.0.113.31
Remote IP Address: 192.0.2.1
Session ID: 22
Login Time: 2013-01-18 03:01:14 PST
```

show subscribers detail (Tunneled Subscriber)

```
user@host> show subscribers detail
Type: PPPoE
User Name: user1@example.com
Logical System: default
Routing Instance: default
Interface: pp0.1
State: Active, Tunneled
Radius Accounting ID: 512
```

show subscribers detail (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@example1.com
```

```
IP Address: 203.0.113.13
IPv6 Prefix: 2001:db8:1::/32
IPv6 User Prefix: 2001:db8:1:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST

Type: DHCP
IPv6 Prefix: 2001:db8:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: test :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

show subscribers detail (ACI Interface Set Session)

```
user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0
Interface Set: aci-1001-ge-1/0/0.2800
Interface Set Session ID: 0
```

```
Underlying Interface: ge-1/0/0.2800
Dynamic Profile Name: aci-vlan-set-profile-2
Dynamic Profile Version: 1
State: Active
Session ID: 1
Agent Circuit ID: aci-ppp-dhcp-20
Login Time: 2012-05-26 01:54:08 PDT
```

show subscribers detail (PPPoE Subscriber Session with ACI Interface Set)

```
user@host> show subscribers detail
Type: PPPoE
User Name: ppphint2
IP Address: 203.0.113.15
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Interface Set: aci-1001-demux0.1073741824
Interface Set Type: Dynamic
Interface Set Session ID: 2
Underlying Interface: demux0.1073741824
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: 3
Session ID: 3
Agent Circuit ID: aci-ppp-dhcp-dvlan-50
Login Time: 2012-03-07 13:46:53 PST
```

show subscribers detail (Dynamic Profile Version Alias)

```
user@host> show subscribers detail

Type: PPPoE
User Name: DEFAULTUSER
IP Address: 192.0.2.21
IP Netmask: 255.255.255.255
IPv6 Address: 2001:db8::17
```

```
Logical System: default
Routing Instance: default
Interface: pp0.3221225720
Interface type: Dynamic
Underlying Interface: demux0.3221225719
Dynamic Profile Name: pppoe-client-profile
Dynamic Profile Version Alias: profile-version1a
MAC Address: 00:00:5E:00:53:38
State: Active
Radius Accounting ID: 288
Session ID: 288
PFE Flow ID: 344
VLAN Id: 1
Login Time: 2019-09-23 10:40:56 IST
```

show subscribers extensive

```
user@host> show subscribers extensive
Type: DHCP
User Name: uer@host
IP Address: 192.0.2.136
IP Netmask: 255.0.0.0
Logical System: default
Routing Instance: default
Interface: ge-0/0/0.0
Interface type: Static
Underlying Interface: ge-0/0/0.0
MAC Address: 00:10:94:00:00:01
State: Active
Radius Accounting ID: 15
Session ID: 15
PFE Flow ID: 2
VLAN Id: 100
Login Time: 2021-05-24 11:30:07 IST
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 01 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 31 2f
31 2d 30 2d 30 37 05 01 06 0f 21 2c
DHCP Header: len 44
01 01 06 00 00 00 00 1d 00 00 80 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 10 94 00 00 01 00 00 00 00 00 00
```

```
00 00 00 00
IP Address Pool: al_pool30
Access Line Attributes:
  Actual upstream data rate: 19998
  Actual downstream data rate: 79999
  Access loop encapsulation: 01 02 00
```

show subscribers extensive (Aggregation Node Interface Set and DSL Forum Attributes)

```
user@host> show subscribers extensive
Type: VLAN-OOB
User Name: ancp
Logical System: default
Routing Instance: isp1-subscriber
Interface: ge-1/0/0.3221225472
Interface type: Dynamic
Interface Set: FRA-DPU-C-100
Underlying Interface: ge-1/0/0
Core IFL Name: ge-1/0/4.0
Dynamic Profile Name: Prof_L2BSA
State: Active
Radius Accounting ID: 1
Session ID: 1
PFE Flow ID: 13
VLAN Id: 50
VLAN Map Id: 20
Inner VLAN Map Id: 1
Inner VLAN Tag Protocol Id: 0x88a8
Agent Circuit ID: circuit 201
Agent Remote ID: remote-id
Aggregation Interface-set Name: FRA-DPU-C-100
Login Time: 2018-05-29 08:43:42 EDT
Accounting interval: 72000
Dynamic configuration:
  junos-cos-scheduler-map: 100m
  junos-inner-vlan-tag-protocol-id: 0x88a8
  junos-vlan-map-id: 20

Type: PPPoE
IP Address: 192.85.128.1
IP Netmask: 255.255.255.255
```

```
Logical System: default
Routing Instance: default
Interface: pp0.3221225474
Interface type: Dynamic
Interface Set: ge-1/0/0
Underlying Interface: demux0.3221225473
Dynamic Profile Name: pppoe-client-profile-with-cos
MAC Address: 00:10:94:00:00:03
State: Active
Radius Accounting ID: 3
Session ID: 3
PFE Flow ID: 16
Stacked VLAN Id: 50
VLAN Id: 7
Agent Circuit ID: circuit 201
Agent Remote ID: remote-id
Aggregation Interface-set Name: FRA-DPU-C-100
Login Time: 2018-05-29 08:43:45 EDT
IP Address Pool: pool-1
Accounting interval: 72000
DSL type: G.fast
Frame/cell mode: Frame
Overhead accounting bytes: 10
Actual upstream data rate: 100000 kbps
Actual downstream data rate: 200000 kbps
Calculated downstream data rate: 180000 kbps
Calculated upstream data rate: 90000 kbps

Adjusted downstream data rate: 160000 kbps
DSL Line Attributes
  Agent Circuit ID: circuit 201
  Agent Remote ID: remote-id
  Actual upstream data rate: 100000
  Actual downstream data rate: 200000
  DSL type: G.fast
  Access Aggregation Circuit ID: #FRA-DPU-C-100
  Attribute type: 0xAA, Attribute length: 4
    198 51 100 78
```

show subscribers extensive (Passive Optical Network Circuit Interface Set)

```
user@host> show subscribers client-type dhcp extensive
Type: DHCP
IP Address: 192.0.2.136
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073741842
Interface type: Dynamic
Interface Set: otl01.xyz101-202
Underlying Interface: demux0.1073741841
Dynamic Profile Name: dhcp-profile
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: user :19
Session ID: 19
VLAN Id: 1100
Agent Remote ID: ABCD01234|100M|AAAA01234|otl01.xyz101-202

Login Time: 2017-03-29 10:30:46 PDT
DHCP Options: len 97
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 02 33 04 00 00
17 70 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 32 2f
32 2d 31 2d 31 37 05 01 06 0f 21 2c 52 2b 02 29 41 42 43 44
30 31 32 33 34 7c 31 30 30 4d 7c 41 41 41 41 30 31 32 33 34
7c 6f 74 6c 30 31 2e 78 79 7a 31 30 31 2d 32 30 32
IP Address Pool: POOL-V4
```

show subscribers extensive (DNS Addresses from Access Profile or Global Configuration)

```
user@host> show subscribers extensive
Type: DHCP
User Name: test-user@example-com
IP Address: 192.0.2.119
IP Netmask: 255.255.255.255
Domain name server inet: 198.51.100.1 198.51.100.2
IPv6 Address: 2001:db8::1:11
Domain name server inet6: 2001:db8:5001::12 2001:db8:3001::12
Logical System: default
```

```
Routing Instance: default
Interface: ge-2/0/3.0
Interface type: Static
Underlying Interface: ge-2/0/3.0
MAC Address: 00:00:5E:00:53:00
State: Active
Radius Accounting ID: 5
Session ID: 5
Login Time: 2017-01-31 11:16:21 IST
DHCP Options: len 53
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 03 33 04 00 00
00 3c 0c 16 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 35 2f
31 32 2d 30 2d 30 37 05 01 06 0f 21 2c
IP Address Pool: v4-pool
```

show subscribers extensive (DNS Addresses from RADIUS)

```
user@host> show subscribers extensive
Type: DHCP
User Name: test-user@example-com
IP Address: 192.0.2.119
IP Netmask: 255.255.255.255
Primary DNS Address: 198.51.100.1
Secondary DNS Address: 198.51.100.2
IPv6 Address: 2001:db8::1:11
IPv6 Primary DNS Address: 2001:db8:5001::12
IPv6 Secondary DNS Address: 2001:db8:3001::12
Logical System: default
Routing Instance: default
Interface: ge-2/0/3.0
Interface type: Static
Underlying Interface: ge-2/0/3.0
MAC Address: 00:00:5E:00:53:00
State: Active
Radius Accounting ID: 5
Session ID: 5
Login Time: 2017-01-31 11:16:21 IST
DHCP Options: len 53
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 03 33 04 00 00
00 3c 0c 16 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 35 2f
```

```
31 32 2d 30 2d 30 37 05 01 06 0f 21 2c
IP Address Pool: v4-pool
```

show subscribers extensive (IPv4 DNS Addresses from RADIUS, IPv6 from Access Profile or Global Configuration)

```
user@host> show subscribers extensive
Type: DHCP
User Name: test-user@example-com
IP Address: 192.0.2.119
IP Netmask: 255.255.255.255
Primary DNS Address: 198.51.100.1
Secondary DNS Address: 198.51.100.2
IPv6 Address: 2001:db8::1:11
Domain name server inet6: 2001:db8:5001::12 2001:db8:3001::12
Logical System: default
Routing Instance: default
Interface: ge-2/0/3.0
Interface type: Static
Underlying Interface: ge-2/0/3.0
MAC Address: 00:00:5E:00:53:00
State: Active
Radius Accounting ID: 5
Session ID: 5
Login Time: 2017-01-31 11:16:21 IST
DHCP Options: len 53
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 03 33 04 00 00
00 3c 0c 16 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 35 2f
31 32 2d 30 2d 30 37 05 01 06 0f 21 2c
IP Address Pool: v4-pool
```

show subscribers extensive (RPF Check Fail Filter)

```
user@host> show subscribers extensive
...
Type: VLAN
  Logical System: default
  Routing Instance: default
  Interface: ae0.1073741824
```

```
  Interface type: Dynamic
  Dynamic Profile Name: vlan-prof
  State: Active
  Session ID: 9
  VLAN Id: 100
  Login Time: 2011-08-26 08:17:00 PDT
  IPv4 rpf-check Fail Filter Name: rpf-allow-dhcp
  IPv6 rpf-check Fail Filter Name: rpf-allow-dhcpv6
...
```

show subscribers extensive (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers extensive
Type: L2TP
User Name: user@example.com
IP Address: 203.0.113.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
IPv4 Input Filter Name: classify-si-5/2/0.1073749824-in
IPv4 Output Filter Name: classify-si-5/2/0.1073749824-out
```

show subscribers extensive (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
```

```
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@example1.com
IP Address: 203.0.113.13
IPv6 Prefix: 2001:db8:1::/32
IPv6 User Prefix: 2001:db8:1:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST
IPv6 Delegated Network Prefix Length: 48
IPv6 Interface Address: 2001:db8:2016:1:1::1/64
IPv6 Framed Interface Id: 1:1:2:2
IPv4 Input Filter Name: FILTER-IN-pp0.1073741825-in
IPv4 Output Filter Name: FILTER-OUT-pp0.1073741825-out
IPv6 Input Filter Name: FILTER-IN6-pp0.1073741825-in
IPv6 Output Filter Name: FILTER-OUT6-pp0.1073741825-out

Type: DHCP
IPv6 Prefix: 2001:db8:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: test :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
```

```
00 00
IPv6 Delegated Network Prefix Length: 48
```

show subscribers extensive (ADF Rules)

```
user@host> show subscribers extensive
...
   Service Session ID: 12
   Service Session Name: SERVICE-PROFILE
   State: Active
   Family: inet
     ADF IPv4 Input Filter Name: __junos_adf_12-demux0.3221225474-inet-in
                       Rule 0: 010101000b0101020b020200201811
                               from {
                                   source-address 203.0.113.232;
                                   destination-address 198.51.100.0/24;
                                   protocol 17;
                               }
                               then {
                                   accept;
                               }
```

show subscribers extensive (Effective Shaping-Rate)

```
user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741837
Interface type: Dynamic
Interface Set: ifset-1
Underlying Interface: ae1
Dynamic Profile Name: svlan-dhcp-test
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.201
VLAN Id: 0x8100.201
Login Time: 2011-11-30 00:18:04 PST
```

```
Effective shaping-rate: 31000000k
...
```

show subscribers extensive (PPPoE Subscriber Access Line Rates)

```
user@host> show subscribers extensive
Type: PPPoE
 IP Address: 198.51.100.1
 IP Netmask: 255.255.255.255
 Logical System: default
 Routing Instance: default
 Interface: pp0.3221225475
 Interface type: Dynamic
 Underlying Interface: demux0.3221225474
 Dynamic Profile Name: pppoe-client-profile-with-cos
 MAC Address: 00:00:5e:00:53:02
 State: Active
 Radius Accounting ID: 4
 Session ID: 4
 PFE Flow ID: 14
 Stacked VLAN Id: 40
 VLAN Id: 1
 Agent Circuit ID: circuit0
 Agent Remote ID: remote0
 Login Time: 2017-04-06 15:52:32 PDT

 User Name: DAVE-L2BSA-SERVICE
 Logical System: default
 Routing Instance: isp-1-subscriber
 Interface: ge-1/2/4.3221225472
 Interface type: Dynamic
 Interface Set: ge-1/2/4
 Underlying Interface: ge-1/2/4
 Core IFL Name: ge-1/3/4.0
 Dynamic Profile Name: L2BSA-88a8-400LL1300VO
 State: Active
Radius Accounting ID: 1
 Session ID: 1
 PFE Flow ID: 14
 VLAN Id: 13
 VLAN Map Id: 102
```

```
 Inner VLAN Map Id: 1
 Agent Circuit ID: circuit-aci-3
 Agent Remote ID: remote49-3
 Login Time: 2017-04-05 16:59:29 EDT
 Service Sessions: 4
 IFL Input Filter Name: L2BSA-CP-400LL1300VO-ge-1/2/4.3221225472-in
 IFL Output Filter Name: L2BSA-CP-400LL1300VO-ge-1/2/4.3221225472-out
 Accounting interval: 900
 DSL type: VDSL
 Frame/Cell Mode: Frame
 Overhead accounting bytes: -10
 Actual upstream data rate: 1024 kbps
 Actual downstream data rate: 4096 kbps
 Adjusted downstream data rate: 3686 kbps
  Dynamic configuration:
   junos-vlan-map-id: 102
   Service Session ID: 5
   Service Session Name: SRL-L1
   State: Active
   Family: inet, inet6
   IFL Input Filter Name: L2BSA-FWF-in-10048-ge-1/2/4.3221225472-in
   IFL Output Filter Name: L2BSA-FWF-out-25088-ge-1/2/4.3221225472-out
   Service Activation time: 2017-04-05 16:59:30 EDT
   Dynamic configuration:
     l2bsa-fwf-in: L2BSA-FWF-in-10048
     l2bsa-fwf-out: L2BSA-FWF-out-25088
     rldown: 25088
     rlup: 10048
```

show subscribers extensive (Subscriber Session Using PCEF Profile)

```
user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225517
Interface type: Dynamic
Underlying Interface: ge-1/0/3
Dynamic Profile Name: svlan-dhcp
State: Active
Session ID: 59
```

```
PFE Flow ID: 71
Stacked VLAN Id: 0x8100.1
VLAN Id: 0x8100.2
Login Time: 2017-03-28 08:23:08 PDT

Type: DHCP
User Name: pcefuser
IP Address: 192.0.2.26
IP Netmask: 255.0.0.0
Logical System: default
Routing Instance: default
Interface: demux0.3221225518
Interface type: Dynamic
Underlying Interface: demux0.3221225517
Dynamic Profile Name: dhcp-client-prof
MAC Address: 00:00:5e:00:53:01
State: Active
Radius Accounting ID: 60
Session ID: 60
PFE Flow ID: 73
Stacked VLAN Id: 1
VLAN Id: 2
Login Time: 2017-03-28 08:23:08 PDT
Service Sessions: 1
DHCP Options: len 9
35 01 01 37 04 01 03 3a 3b
IP Address Pool: pool-ipv4
IPv4 Input Service Set: tdf-service-set
IPv4 Output Service Set: tdf-service-set
PCEF Profile: pcef-prof-1
PCEF Rule/Rulebase: default
Dynamic configuration:
  junos-input-service-filter: svc-filt-1
  junos-input-service-set: tdf-service-set
  junos-output-service-filter: svc-filt-1
  junos-output-service-set: tdf-service-set
  junos-pcef-profile: pcef-prof-1
  junos-pcef-rule: default

   Service Session ID: 61
   Service Session Name: pcef-serv-prof
   State: Active
   Family: inet
```

```
   IPv4 Input Service Set: tdf-service-set
   IPv4 Output Service Set: tdf-service-set
   PCEF Profile: pcef-prof-1
   PCEF Rule/Rulebase: limit-fb
   Service Activation time: 2017-03-28 08:31:19 PDT
   Dynamic configuration:
     pcef-prof: pcef-prof-1
     pcef-rule1: limit-fb
     svc-filt: svc-filt-1
     svc-set: tdf-service-set
```

show subscribers aci-interface-set-name detail (Subscriber Sessions Using Specified ACI Interface Set)

```
user@host> show subscribers aci-interface-set-name aci-1003-ge-1/0/0.4001 detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 203.0.113.17
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address:
```

```
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

show subscribers agent-circuit-identifier detail (Subscriber Sessions Using Specified ACI Substring)

```
user@host> show subscribers agent-circuit-identifier aci-ppp-vlan detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 203.0.113.17
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:5e:00:53:52
State: Active
Radius Accounting ID: 14
Session ID: 14
```

```
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

show subscribers id accounting-statistics

```
user@host> show subscribers id 601 accounting-statistics
Session ID: 601
Accounting Statistics:
Input bytes : 199994
Output bytes : 121034
Input packets: 5263
Output packets: 5263
IPv6:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
```

show subscribers interface accounting-statistics

```
user@host> show subscribers interface pp0.3221226949 accounting-statistics
Session ID: 501
Accounting Statistics:
Input bytes : 199994
Output bytes : 121034
Input packets: 5263
Output packets: 5263
IPv6:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Session ID: 502
Accounting Statistics:
Input bytes : 87654
Output bytes : 72108
Input packets: 3322
Output packets: 3322
IPv6:
```

```
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0

Session ID: 503
Accounting Statistics:
Input bytes : 156528
Output bytes : 123865
Input packets: 7448
Output packets: 7448
IPv6:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
```

show subscribers interface extensive

```
user@host> show subscribers interface demux0.1073741826 extensive
Type: VLAN
User Name: user@test.example.com
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Dynamic
Dynamic Profile Name: profile-vdemux-relay-23qos
MAC Address: 00:00:5e:00:53:04
State: Active
Radius Accounting ID: 12
Session ID: 12
Stacked VLAN Id: 0x8100.1500
VLAN Id: 0x8100.2902
Login Time: 2011-10-20 16:21:59 EST

Type: DHCP
User Name: user@test.example.com
IP Address: 192.0.2.0
IP Netmask: 255.255.255.0
Logical System: default
Routing Instance: testnet
```

```
Interface: demux0.1073741826
Interface type: Static
MAC Address: 00:00:5e:00:53:04
State: Active
Radius Accounting ID: 21
Session ID: 21
Login Time: 2011-10-20 16:24:33 EST
Service Sessions: 2

Service Session ID: 25
Service Session Name: SUB-QOS
State: Active

Service Session ID: 26
Service Session Name: service-cb-content
State: Active
IPv4 Input Filter Name: content-cb-in-demux0.1073741826-in
IPv4 Output Filter Name: content-cb-out-demux0.1073741826-out
```

show subscribers logical-system terse

```
user@host> show subscribers logical-system test1 terse
Interface                       IP Address/VLAN ID   User Name         LS:RI
demux0.1073741825           203.0.113.3         RETAILER1-CLIENT  test1:retailer1
demux0.1073741826           203.0.113.4         RETAILER2-CLIENT  test1:retailer2
```

show subscribers physical-interface count

```
user@host> show subscribers physical-interface ge-1/0/0 count
Total subscribers: 3998, Active Subscribers: 3998
```

show subscribers routing-instance inst1 count

```
user@host> show subscribers routing-instance inst1 count
Total Subscribers: 188, Active Subscribers: 183
```

show subscribers stacked-vlan-id detail

```
user@host> show subscribers stacked-vlan-id 101 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id detail (Combined Output)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 interface ge-1/2/0.* detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers user-name detail

```
user@host> show subscribers user-name larry1 detail
Type: DHCP
User Name: larry1
IP Address: 203.0.113.37
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.1
Interface type: Static
Dynamic Profile Name: foo
MAC Address: 00:00:5e:00:53:01
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-11-07 08:25:59 PST
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 01 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 32 2f
37 2d 30 2d 30 37 05 01 06 0f 21 2c
```

show subscribers vlan-id

```
user@host> show subscribers vlan-id 100
Interface           IP Address                              User Name
ge-1/0/0.1073741824
ge-1/2/0.1073741825
```

show subscribers vlan-id detail

```
user@host> show subscribers vlan-id 100 detail
Type: VLAN
Interface: ge-1/0/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT
```

```
Type: VLAN
Interface: ge-1/2/0.1073741825
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT
```

show subscribers vpi vci extensive (PPPoE-over-ATM Subscriber Session)

```
user@host> show subscribers vpi 40 vci 50 extensive
Type: PPPoE
User Name: testuser
IP Address: 203.0.113.2
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: pp0.0
Interface type: Static
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: 2
Session ID: 2
ATM VPI: 40
ATM VCI: 50
Login Time: 2012-12-03 07:49:26 PST
IP Address Pool: pool_1
IPv6 Framed Interface Id: 200:65ff:fe23:102
```

show subscribers address detail (Enhanced Subscriber Management)

```
user@host> show subscribers address 203.0.113.111 detail
Type: DHCP
User Name: simple_filters_service
IP Address: 203.0.113.111
IP Netmask: 255.0.0.0
Logical System: default
Routing Instance: default
Interface: demux0.3221225482
```

```
Interface type: Dynamic
Underlying Interface: demux0.3221225472
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:00:5e:00:53:0f
State: Active
Radius Accounting ID: 11
Session ID: 11
PFE Flow ID: 15
Stacked VLAN Id: 210
VLAN Id: 209
Login Time: 2014-03-24 12:53:48 PDT
Service Sessions: 1
DHCP Options: len 3
35 01 01
```

show subscribers extensive (Tenant Systems)

```
user@host:TSYS1> show subscribers extensive
Type: XAUTH
User Name: userX
+    Tenant: TSYS1
    Routing Instance: TSYS1-ri
IP Address: 192.0.2.0
IP Netmask: 203.0.113.0
Primary DNS Address: 198.51.100.0
Secondary DNS Address: 198.51.100.1
Dynamic Profile Name: radius
State: Active
Session ID: 1
Login Time: 2018-09-18 13:49:00 PDT
```

Sample Output for AGF

The following sample output shows subscribers connected to the AGF:

show subscribers extensive (DHCP on an FN-RG)

```
user@host> show subscribers extensive
Type: DHCP
User Name: USER2
IP Address: 172.16.0.227
Logical System: default
Routing Instance: default
Interface: demux0.3221230587
Interface type: Dynamic
Underlying Interface: demux0.3221230586
Dynamic Profile Name: dhcp-profile
MAC Address: 00:44:46:44:44:44
State: Active
DHCP Relay IP Address: 10.1.0.1
Radius Accounting ID: 5128
Session ID: 5128
PFE Flow ID: 5185
Stacked VLAN Id: 1
VLAN Id: 1
Agent Circuit ID: aci1
Agent Remote ID: ari1
Login Time: 2022-04-26 09:24:56 PDT
Service Sessions: 1
DHCP Options: len 9
35 01 01 37 04 01 03 3a 3b
DHCP Header: len 44
01 01 06 00 10 bd b4 93 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 44 46 44 44 44 00 00 00 00 00 00
00 00 00 00
AGF Mode: Adaptive
Local TEID-U: 10183810
Remote TEID-U: 6354992
GTPU Tunnel Remote IP Address: 10.0.0.1
GTPU Tunnel Local IP Address: 10.0.0.1
5G-QFI: 1
IPv6 Framed Interface Id: 0:7fff:ffff:eaa0
IPv4 Input Filter Name: RG-LWAC-V4-INPUT-FILTER-01-demux0.3221230587-in
IPv4 Output Filter Name: RG-LWAC-V4-OUTPUT-FILTER-01-demux0.3221230587-out
Access Line Attributes:
  Agent Circuit ID: aci1
  Agent Remote ID: ari1
```

```
Dynamic configuration:
  junos-cos-guaranteed-rate: 1000000
  junos-cos-guaranteed-rate-burst: 250000
      junos-cos-scheduler: GOLD
          junos-cos-scheduler-shaping-rate: 200000000
          junos-cos-scheduler-tx: 200000000
  junos-cos-scheduler-map: DATA_VOICE_VIDEO_SMAP_UID1468
  junos-cos-shaping-rate: 200000000
  junos-cos-shaping-rate-burst: 50000
  junos-cos-traffic-control-profile: TRAFFIC_CONTROL_PROFILE
  junos-input-filter: RG-LWAC-V4-INPUT-FILTER-01
  junos-input-ipv6-filter: RG-LWAC-V6-INPUT-FILTER-01
  junos-output-filter: RG-LWAC-V4-OUTPUT-FILTER-01
  junos-output-ipv6-filter: RG-LWAC-V6-OUTPUT-FILTER-01

   Service Session ID: 5129
   Service Session Name: SERVICE-PROFILE-BASIC-POLICER
   State: Active
   Family: inet
   Service session type: Service-Profile
   IPv4 Input Filter Name: CAP-POLICER-demux0.3221230587-in
   IPv4 Output Filter Name: CAP-POLICER-demux0.3221230587-out
   Service Activation time: 2022-04-26 09:24:57 PDT
   Dynamic configuration:
     bandwidth-limit: 200k
     burst-size-limit: 75k
```

Release Information

Command introduced in Junos OS Release 9.3.

`client-type`, `mac-address`, `subscriber-state`, and `extensive` options introduced in Junos OS Release 10.2.

`count` option usage with other options introduced in Junos OS Release 10.2.

Options `aci-interface-set-name` and `agent-circuit-identifier` introduced in Junos OS Release 12.2.

The `physical-interface` and `user-name` options introduced in Junos OS Release 12.3.

Options `vci` and `vpi` introduced in Junos OS Release 12.3R3 and supported in later 12.3R*x* releases.

Options `vci` and `vpi` supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Enhanced subscriber management supported in Junos OS Release 15.1R3 on MX Series routers.

`accounting-statistics` option added in Junos OS Release 15.1R3 and 17.4R1 on MX Series routers.

`aggregation-interface-set-name` option added in Junos OS Release 18.4R1 on MX Series routers.

`sub-system` added in Junos OS Release 22.3R1.

RELATED DOCUMENTATION

> *Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration*
>
> *Verifying and Managing Configurations for Dynamic VLANs Based on Access-Line Identifiers*
>
> *Verifying and Managing Junos OS Enhanced Subscriber Management*

show subscribers summary

IN THIS SECTION

Syntax

```
show subscribers summary
<all>
```

```
<detail | extensive | terse>
<count>
<physical-interface physical-interface-name>
<logical-system logical-system pic | port | routing-instance routing-instance | slot>
<sub-system (agf | bng)>
```

Description

Display summary information for subscribers.

Options

none	Display summary information by state and client type for all subscribers.
all	(Optional) Display summary information by state, client type, and logical system and routing instance (LS:RI).
detail | extensive | terse	(Not supported on MX Series routers) (Optional) Display the specified level of output.
count	(Not supported on MX Series routers) (Optional) Display the count of total subscribers and active subscribers for any specified option.
logical-system *logical-system*	(Optional) Display subscribers whose logical system matches the specified logical system.
physical-interface *physical-interface-name*	(M120, M320, and MX Series routers only) (Optional) Display the count of subscribers whose physical interface matches the specified physical interface, by subscriber state, client type, and LS:RI.
pic	(M120, M320, and MX Series routers only) (Optional) Display the count of subscribers by PIC number and the total number of subscribers.
port	(M120, M320, and MX Series routers only) (Optional) Display the count of subscribers by port number and the total number of subscribers.
routing-instance *routing-instance*	(Optional) Display subscribers whose routing instance matches the specified routing instance.

slot	(M120, M320, and MX Series routers only) (Optional) Display the count of subscribers by Flexible PIC Concentrator (FPC) slot number and the total number of subscribers.
sub-system (agf | bng)	(Optional) Display a count of subscribers using either the Access Gateway Function (AGF) or broadband network gateway (BNG) services.

> **NOTE**: The subsystem option is only available when both the AGF and BNG subscribers are logged into the router at the same time.

> **NOTE**: Because of display limitation, the logical system and routing instance output values are truncated when necessary.

Starting from Junos OS 20.4R1 release, you need a license to use the Extensible Subscribers Services Manager (ESSM) feature.

Required Privilege Level

view

Output Fields

Table 8 on page 124 lists the output fields for the `show subscribers summary` command. Output fields are listed in the approximate order in which they appear.

Table 8: show subscribers summary Output Fields

Field Name	Field Description	Level of Output
Subscribers by State	Number of subscribers summarized by state. The summary includes the following information: • Init—Number of subscribers currently in the initialization state. • Configured—Number of configured subscribers. • Active—Number of active subscribers. • Terminating—Number of subscribers currently terminating. • Terminated—Number of terminated subscribers. • Total—Total number of subscribers for all states.	detail none
Subscribers by Client Type	Number of subscribers summarized by client type. Client types can include DHCP, GRE, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN, and VLAN-OOB. This field also displays the total number of subscribers for all client types (Total).	detailextensive none
Subscribers by LS:RI	Number of subscribers summarized by logical system:routing instance (LS:RI) combination. This field also displays the total number of subscribers for all the LS:RI combinations (Total).	detail none
Subscribers by Connection Type	Number of subscribers summarized by connection type, Cross-connected or Terminated.	extensive
Subscribers by Sub-System	Number of subscribers on the subsystem—AGF or BNG as well as the total number of subscriber.	All levels

Table 8: show subscribers summary Output Fields *(Continued)*

Field Name	Field Description	Level of Output

`Interface`	Interface associated with the subscriber. The router or the switch displays subscribers whose interface matches or begins with the specified interface.
	
	The asterisk (*) indicates a continuation of addresses for the same session.
	
	For aggregated Ethernet interfaces, the output of the `summary (pic | port | slot)` options prefixes the interface name with ae0:.
	
	For pseudowire IFDs, this field displays both the pseudowire and the associated logical tunnel (LT) and the redundant logical tunnel (RLT) anchor interface. For example:
	
	`ps0: lt-2/1/0`
	`ps1: rlt0: lt-4/0/0`
		All levels

`Count`	Count of subscribers displayed for each PIC, port, or slot when those options are specified with the `summary` option. For an aggregated Ethernet configuration, the total subscriber count does not equal the sum of the individual PIC, port, or slot counts, because each subscriber can be in more than one aggregated Ethernet link. Multiple pseudowire interfaces can share a given logical tunnel or redundant logical tunnel anchor interface. Starting in Junos OS Release 18.1R1, the field displays subscribers per individual pseudowire interface. In earlier releases, the field displays the same number of subscribers for all the pseudowire interfaces that share the same tunnel interface as their anchor point.	`detailextensive` none
`Total Subscribers`	Total number of subscribers for all physical interfaces, all PICs, all ports, or all LS:RI slots.	`detailextensive` none
`IP Address/VLAN ID`	Subscriber IP address or VLAN ID associated with the subscriber in the form *tpid.vlan-id*	`terse`

Table 8: show subscribers summary Output Fields *(Continued)*

Field Name	Field Description	Level of Output
User Name	Name of the subscriber.	terse
LS:RI	Logical system and routing instance associated with the subscriber.	terse

Sample Output

show subscribers summary

```
user@host> show subscribers summary

Subscribers by State
   Active: 52194
   Total: 52194

Subscribers by Client Type
   DHCP: 10000
   VLAN: 15997
   VLAN-OOB: 3600
   PPPoE: 15998
   ESSM: 6599
   Total: 52194
```

show subscribers summary all

```
user@host> show subscribers summary all
Subscribers by State
    Init                    3
    Configured             2
    Active                  183
    Terminating             2
    Terminated             1
```

```
    TOTAL                   191

Subscribers by Client Type
    DHCP                    107
    PPP                     76
    VLAN                     8

    TOTAL               191

Subscribers by LS:RI
    default:default      1
    default:ri1              28
    default:ri2              16
    ls1:default             22
    ls1:riA                 38
    ls1:riB                 44
    logsysX:routinstY     42

    TOTAL                    191
```

show subscribers summary physical-interface

```
user@host> show subscribers summary physical-interface ge-1/0/0
Subscribers by State
   Active: 3998
   Total: 3998

Subscribers by Client Type
   DHCP: 3998
   Total: 3998

Subscribers by LS:RI
   default:default: 3998
   Total: 3998
```

show subscribers summary physical-interface pic

```
user@host> show subscribers summary physical-interface ge-0/2/0 pic
Subscribers by State
   Active: 4825
```

```
   Total: 4825

Subscribers by Client Type
   DHCP: 4825
   Total: 4825

Subscribers by LS:RI
   default:default: 4825
   Total: 4825
```

show subscribers summary physical-interface port

```
user@host> show subscribers summary physical-interface ge-0/3/0 port
Subscribers by State
   Active: 4825
   Total: 4825

Subscribers by Client Type
   DHCP: 4825
   Total: 4825

Subscribers by LS:RI
   default:default: 4825
   Total: 4825
```

show subscribers summary physical-interface slot

```
user@host> show subscribers summary physical-interface ge-2/0/0 slot
Subscribers by State
   Active: 4825
   Total: 4825

Subscribers by Client Type
   DHCP: 4825
   Total: 4825

Subscribers by LS:RI
   default:default: 4825
   Total: 4825
```

show subscribers summary pic

```
user@host> show subscribers summary pic
Interface           Count
ge-1/0              1000
ge-1/3              1000

Total Subscribers: 2000
```

show subscribers summary pic (Aggregated Ethernet Interfaces)

```
user@host> show subscribers summary pic
Interface           Count
ae0: ge-1/0         801
ae0: ge-1/3         801

Total Subscribers: 801
```

show subscribers summary port

```
user@host> show subscribers summary port
Interface           Count
ge-5/0/1              201
ge-5/0/2              301

Total Subscribers: 502
```

show subscribers summary port (Pseudowire Interfaces)

```
user@host> show subscribers summary port
ps0: lt-2/1/0 10
ps1: lt-2/1/0 20

Total Subscribers: 30
```

show subscribers summary port extensive

```
user@host>show subscribers summary port extensive
Interface: xe-3/0/3
Port Count: 100
Detail:
Subscribers by Client Type
   PPPoE: 1
   ESSM: 99
Subscribers by Connection Type
   Terminated: 1

Interface: xe-3/1/3
Port Count: 3100
Detail:
Subscribers by Client Type
   PPPoE: 1600
   ESSM: 1100
   VLAN-OOB: 400
Subscribers by Connection Type
   Tunneled: 500
   Terminated: 1100
   Cross-connected: 400

Total Subscribers: 26197
```

show subscribers summary slot

```
user@host> show subscribers summary slot
Interface           Count
ge-1                2000

Total Subscribers: 2000
```

show subscribers summary terse

```
user@host> show subscribers summary terse
Interface                       IP Address/VLAN ID   User Name         LS:RI
ge-1/3/0.1073741824         100                                    default:default
```

```
demux0.1073741824           203.0.113.10         WHOLESALER-CLIENT default:default
demux0.1073741825           203.0.113.13         RETAILER1-CLIENT  test1:retailer1
demux0.1073741826           203.0.113.213        RETAILER2-CLIENT  test1:retailer2
```

show subscribers summary (agf)

```
user@host> show subscribers summary
Subscribers by Sub-System
   AGF: 3000
   BNG: 0
   Total: 3000

Subscribers by State
   Active: 4000
   Total: 4000

Subscribers by Client Type
   VLAN: 1000
   PPPoE: 3000
   Total: 4000
```

show subscribers summary sub-system agf

```
user@host> show subscribers summary sub-system agf
AGF Subscribers by State
    Init:     3
    Active:  12
    Total:   15

AGF Subscribers by Client Type
     DHCP:           2
     PPPOE:          5
     PPPOE-5G        5
     TOTAL          12
```

Release Information

Command introduced in Junos OS Release 10.2.

`sub-system` added in Junos OS Release 22.3R1.

RELATED DOCUMENTATION

show subscribers | 68