

Access Gateway Function User Guide

Published
2024-06-11

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

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

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

Access Gateway Function User Guide
Copyright © 2024 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide | iv

1

Overview

Overview of 5G | 2

Access Gateway Function | 5

Authentication and Registration | 8

Routing Instances | 11

User Plane Function | 12

Quality of Service | 13

SCTP on the AGF | 14

AGF Using Junos Telemetry Interface | 15

Supported Standards | 16

2

Configure AGF

Overview of Configuring AGF | 18

Configure PPP Support for AGF | 18

Configure DHCP Support for AGF | 22

Configure AGF Services | 24

3

Migrate Subscribers from BNG to AGF

Migrate Subscribers from BNG to AGF | 29

4

Configuration Statements and Operational Commands

Junos CLI Reference Overview | 35

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.

1

CHAPTER

Overview

[Overview of 5G | 2](#)

[Access Gateway Function | 5](#)

[Authentication and Registration | 8](#)

[Routing Instances | 11](#)

[User Plane Function | 12](#)

[Quality of Service | 13](#)

[SCTP on the AGF | 14](#)

[AGF Using Junos Telemetry Interface | 15](#)

[Supported Standards | 16](#)

Overview of 5G

IN THIS SECTION

- [Components in a 5GC Network | 2](#)

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

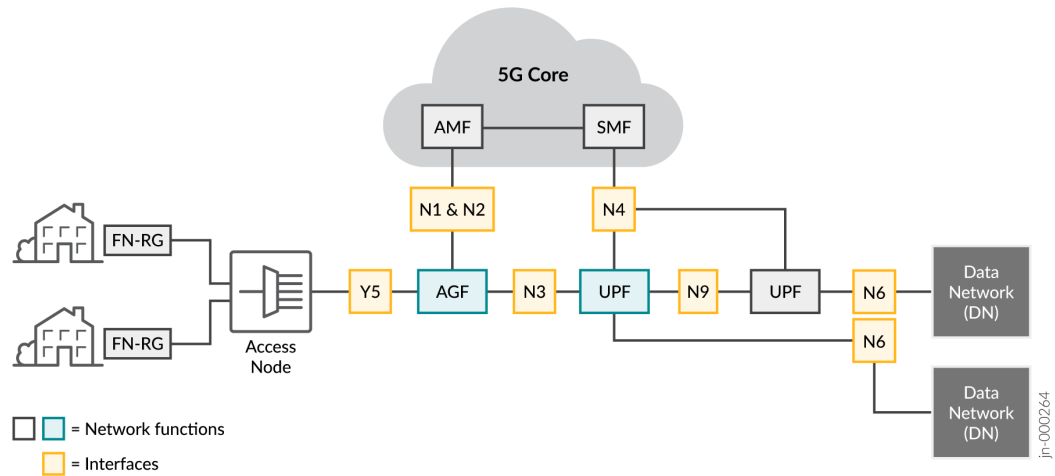


Table 1: Components of a 5G Network

Functions and Interfaces	Description
Access Gateway Function (AGF)	<p>Provides the access connection for residential gateways (RGs) to connect to the 5GC.</p> <p>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.</p>
Access and Mobility Management Function (AMF)	<p>Responsible for registration management, PDU session management, and forwarding of access facing traffic to and from the access network.</p>

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

Functions and Interfaces	Description
Fixed Network Residential Gateway (FN-RG)	<p>Connects the home network to the WAN.</p> <p>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.</p>
Session Management Function (SMF)	Establishes PDU sessions and interacts with the user plane function (UPF).
User plane function (UPF)	<p>Supports packet routing, forwarding, packet inspection, PDU session, and flow-level QoS.</p> <p>NOTE: An UPF can be external or colocated with the AGF.</p>
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 interface.
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 | 5](#)
- [Benefits of Access Gateway Function | 6](#)

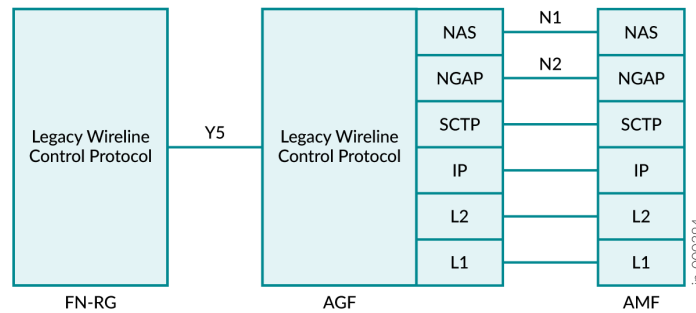
access Gateway Function

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

- 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:

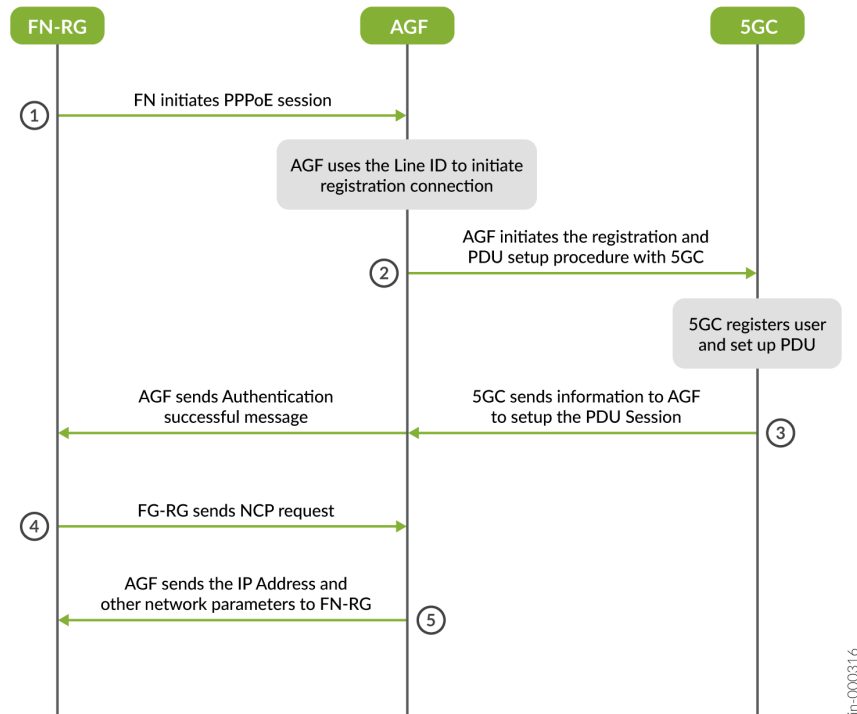
1. The FN-RG uses a unique global line identifier (GLI) to connect to the 5GC network. The GLI contains a circuit line ID and a remote line ID.
2. The Access Gateway Function (AGF) uses the circuit line ID and the remote line ID in the GLI to construct a unique Subscription Permanent Identifier (SUPI) 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.

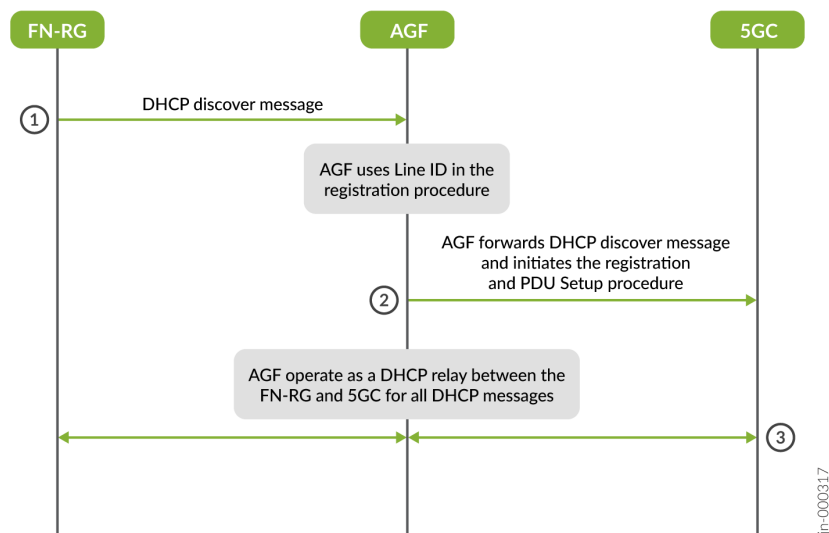
3. After a successful registration in the 5GC, the AGF responds with an authentication success message to the FN-RG.
4. The FN-RG initiates the Network Control Protocol (NCP) to establish different Network Layer protocols that are required to set up the PPP connections. The FN-RG uses Internet Protocol 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) which controls 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 on the AGF

Next Generation Application Protocol (NGAP) on the Access Gateway Function (AGF) uses the Stream Control Transmission Protocol (SCTP) to transport NGAP messages. NGAP messages provide control plane signaling between the AGF and the Access and Mobility Management Functions (AMFs). NGAP support TNLA usage type and weight factor. SCTP is a transport layer protocol that provides the mechanism for reliable, in-sequence transport of data between endpoints. The endpoints form a unique Transport Layer Network Association (TNLA), that enables seamless communication between nodes. For more information on SCTP, see *SCTP Overview*.

The AGF uses the configured values in the `services agf amf` hierarchy to initiate a static TNLA with the AMF.

The AMF can dynamically request TNLAs to be added or deleted between the AGF and AMF by sending an NGAP AMF configuration update message. The TNLA specifies whether the TNLA will be used for NGAP UE associated signaling, non-UE associated signaling, or both. The AMF specifies the TNLA's usage type and the weight factor when the TNLA is established. The AMF can dynamically modify the TNLAs usage type or weight factor as needed.

AGF supports the following :

- Multihoming support where one or both endpoints of a SCTP association can have more than one bound IP address.
- Separate routing instances for each AMF. SCTP communications occurs in the configured AMF routing instance. If a routing instance is not configured, AGF uses the default routing-instance.
- Up to 10 TNLAs with each AMF. The initial TNLA is a static TNLA. Subsequent TNLAs added by the AMF are dynamic TNLAs.
- Load balancing of user equipment (UE) across all TNLAs that support UE-associated signaling.

Figure 6: SCTP Multihoming

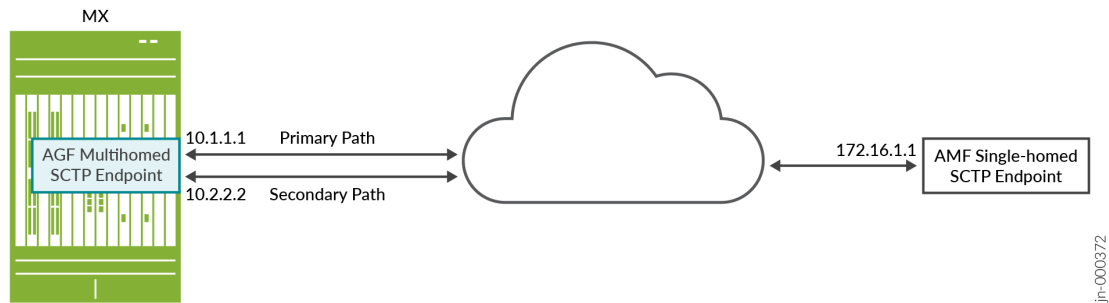


Figure 6 on page 15 shows a multihomed AGF SCTP endpoint and a single-homed AMF SCTP endpoint. SCTP maintains multiple packet paths between SCTP endpoints. One of the packet paths is designated as the primary path by the SCTP implementation. If the primary path fails, SCTP switches to the secondary path.

Configure the initial TNLA with the AMFs in the `[edit services agf amf]` hierarchy.

The following sample configuration shows AGF requesting a TNLA that supports both UE and non-UE associated signalling with a default weight factor of 128.

```
amf amf1 {
  node-id 0;
  ip-address 172.16.1.1; # AMF IP address
  port 38412;           # AMF port number (Defaults to 38412)
  local-endpoint {
    ip-address 10.1.1.1; # AGF IP address
    ip-address 10.2.2.2; # AGF IP address
    port 37100;          # AGF port number (Defaults to a Junos selected ephemeral port)
    initial-tnla-weight-factor 128;
  }
  default-amf;
}
```

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 | 18](#)

[Configure PPP Support for AGF | 18](#)

[Configure DHCP Support for AGF | 22](#)

[Configure AGF Services | 24](#)

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

- [Procedure | 19](#)

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 [PPP Subscriber Access Networks Overview](#)

Configure DHCP Support for AGF

IN THIS SECTION

- Procedure | 22

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 [DHCP Subscriber Access Networks Overview](#)

Configure AGF Services

IN THIS SECTION

- [Procedure | 25](#)

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

Migrate Subscribers from BNG to AGF

Migrate Subscribers from BNG to AGF | 29

Migrate Subscribers from BNG to AGF

IN THIS SECTION

- [Using an Interface Tag to Migrate DHCP Subscribers from the BNG to the AGF | 29](#)
- [Configure Access Support for BNG and AGF | 30](#)

Using an Interface Tag to Migrate DHCP Subscribers from the BNG to the AGF

Before Junos OS 23.2R1, you could only map one DHCP group to a physical interface (IFD) that is supporting dynamic VLANs. This limits the interface to supporting subscribers with the same DHCP requirements. Starting in Junos OS 23.2R1, you can use interface tags to map a single dynamic VLAN or a group of dynamic VLANs to different DHCP groups. Therefore, you can support subscribers with different DHCP requirements on one IFD. The device will use the interface tag to map the incoming subscriber VLAN ID in the profile to the DHCP group. This feature allows you to easily migrate users from the BNG to the AGF.

To support multiple DHCP groups on the same physical interface:

- Configure the `interface-tag` in the dynamic profile on a VLAN demux interface.
 - `set dynamic-profiles profile-name interfaces demux0 unit $junos-interface-unit interface-tag interface-tag-name`
- Configure the dynamic VLAN demux (auto-sensed) interface and corresponding dynamic profile. Specify the VLAN range subset that will map the dynamic profile to the DHCP group.
- Map the dynamic profile to the associated DHCP group by specifying the same `interface-tag` name. For more information on configuring DHCP Local Server and DHCP Relay Servers, see *Common DHCP Configuration for Interface Groups and Server Groups*.

DHCP Relay

- `set forwarding-options dhcp-relay group name interface-tag interface-tag-name`
- `set forwarding-options dhcp-relay dhcpv6 group name interface-tag interface-tag-name`

DHCP Local Server

- `set system services dhcp-local-server group sgroup interface-tag interface-tag-name`
- `set system services dhcp-local-server dhcpv6 group sgroup interface-tag interface-tag-name`

NOTE: Subscribers migrating from broadband to AGF will maintain their DHCP session until they terminate their session.

Subscribers who are eligible for migration remain connected in their DHCP session. Once the subscriber logs off and the DHCP session has been terminated, the router migrates the subscriber to AGF at the next successful login (DHCP renegotiation).

Use the following show DHCP binding command with the `detail` option to displays interface tag information:

- `show dhcp relay binding detail`
- `show dhcpv6 relay binding detail`
- `show dhcp server binding detail`
- `show dhcpv6 server binding detail`

Configure Access Support for BNG and AGF

The following example shows how to configure a physical interface (IFD) on a device to support both BNG and AGF subscribers. We configure two dynamic profiles on the demux interface (demux0—one profile for the BNG subscribers and one for AGF subscribers). The device uses the VLAN ID to map a subscriber to a dynamic profile. The device then uses the interface tag in the dynamic profile to map the subscriber to a DHCP group.

1. Configure dynamic profiles to support incoming subscribers on demux interface. Configure one dynamic profile for BNG subscribers and another profile for AGF subscribers. Use the same interface tag name in both the dynamic profile and the DHCP group. In this example, we use an interface tag that identifies the VLAN range.

BNG

```
set dynamic-profiles BNG_DPROFILE_1 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" actual-transit-statistics
set dynamic-profiles BNG_DPROFILE_1 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" interface-tag IFD_TAG_1_2000
```

```

set dynamic-profiles BNG_DPROFILE_1 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" proxy-arp
set dynamic-profiles BNG_DPROFILE_1 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" vlan-id "$junos-vlan-id"
set dynamic-profiles BNG_DPROFILE_1 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" family inet address 192.168.10.3/32
set dynamic-profiles BNG_DPROFILE_1 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" actual-transit-statistics
set dynamic-profiles BNG_DPROFILE_1 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" family inet6 address 2001:db8:1/128

```

AGF

```

set dynamic-profiles AGF_DPROFILE_2 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" interface-tag IFD_TAG_2001_4000
set dynamic-profiles AGF_DPROFILE_2 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" actual-transit-statistics
set dynamic-profiles AGF_DPROFILE_2 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" proxy-arp
set dynamic-profiles AGF_DPROFILE_2 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" vlan-id "$junos-vlan-id"
set dynamic-profiles AGF_DPROFILE_2 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" family inet address 192.168.10.3/32
set dynamic-profiles AGF_DPROFILE_2 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" actual-transit-statistics
set dynamic-profiles AGF_DPROFILE_2 interfaces "$junos-interface-ifd-name" unit "$junos-
interface-unit" family inet6 address 2001:db8:3/128

```

2. Configure the interface with two dynamic profiles (BNG_DPROFILE and AGF_DPROFILE). Specify the VLAN range in the dynamic profile that maps to the DHCP group.

```

set interfaces xe-1/1/0 description AGF_BNG
set interfaces xe-1/1/0 flexible-vlan-tagging
set interfaces xe-1/1/0 auto-configure remove-when-no-subscribers

```

BNG

```

set interfaces xe-1/1/0 auto-configure stacked-vlan-ranges dynamic-profile BNG_DPROFILE_1
accept inet
set interfaces xe-1/1/0 auto-configure stacked-vlan-ranges dynamic-profile BNG_DPROFILE_1

```

```
accept pppoe
set interfaces xe-1/1/0 auto-configure stacked-vlan-ranges dynamic-profile BNG_DPROFILE_1
ranges 1-2000
```

AGF

```
set interfaces xe-1/1/0 auto-configure stacked-vlan-ranges dynamic-profile AGF_DPROFILE_2
accept inet
set interfaces xe-1/1/0 auto-configure stacked-vlan-ranges dynamic-profile AGF_DPROFILE_2
accept pppoe
set interfaces xe-1/1/0 auto-configure stacked-vlan-ranges dynamic-profile AGF_DPROFILE_2
ranges 2001-4000
```

3. Configure the DHCP relay configuration for the access interface. Use the corresponding interface tag name from dynamic profile in the DHCP group. We configure the set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_2 interface xe-1/1/0.0 as a fallback when there are additional VLAN IDs. The router gives the interface tag precedence over the interface statement.

BNG

```
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_1 authentication password password
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_1 authentication username-include
user-prefix USER2
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_1 dynamic-profile dhcp-profile
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_1 access-profile legacy_access1
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_1 overrides trust-option-82
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_1 relay-option-82 remote-id keep-
incoming-remote-id
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_1 interface-tag IFD_TAG_1_2000
```

AGF

```
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_2 authentication password joshua
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_2 authentication username-include
user-prefix DEFAULT
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_2 dynamic-profile dhcp-profile
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_2 access-profile agf-access1
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_2 overrides trust-option-82
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_2 relay-option-82 remote-id keep-
incoming-remote-id
```

```
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_2 interface xe-1/1/0.0  
set forwarding-options dhcp-relay group DHCPv4_CLIENT_GROUP_2 interface-tag IFD_TAG_2001_4000
```

RELATED DOCUMENTATION

<https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/topic-map/dhcp-common-config-interface-group.html>

<https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-vlan/topics/task/subscriber-management-vlan-demux-dynamic.html>

<https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-vlan/topics/task/subscriber-management-ip-demux-dynamic.html>

4

CHAPTER

Configuration Statements and Operational Commands

[Junos CLI Reference Overview](#) | 35

Junos CLI Reference Overview

We've consolidated all Junos CLI commands and configuration statements in one place. Learn about the syntax and options that make up the statements and commands and understand the contexts in which you'll use these CLI elements in your network configurations and operations.

- [Junos CLI Reference](#)

Click the links to access Junos OS and Junos OS Evolved configuration statement and command summary topics.

- [Configuration Statements](#)
- [Operational Commands](#)