NOKIA

7750 SERVICE ROUTER

VIRTUALIZED SERVICE ROUTER

BNG CUPS USER PLANE FUNCTION GUIDE

RELEASE 22.10.R1

3HE 18377 AAAD TQZZA 01
Issue 01

October 2022

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Table of contents

1 Getting started

1.1 About this guide

This guide describes the Nokia SR OS User Plane Function (UPF) in a Broadband Network Gateway (BNG) Control and User Plane Separation (CUPS) system. The BNG CUPS UPF is based on the fundamentals of the BNG and reuses fundamental QoS and forwarding concepts, while moving the control plane handling to the BNG CUPS Control Plane Function (CPF).

See the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide* for more information about BNG.

See the *CMG BNG CUPS Control Plane Function Guide* for an overview of the BNG CUPS solution and the BNG CUPS CPF.

This guide is organized into functional chapters that provide concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.

Note: This guide provides configuration examples based on MD-CLI syntax.

The topics and commands described in this document apply to the following SR OS products:

- 7750 SR
- Virtualized Service Router

See the *SR OS R22.x.Rx Software Release Notes*, part number 3HE 18412 000 *x* TQZZA, for a list of unsupported features by platform and chassis.

Command outputs shown in this guide are examples only; actual displays may differ depending on supported functionality and user configuration.

Note: The BNG CUPS UPF supports configuration using classic CLI and MD-CLI. This guide provides configuration examples based on MD-CLI syntax only.
The SR OS CLI trees and command descriptions can be found in the following guides:

- *7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide*
- *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Command Reference Guide*
- *7450 ESS, 7750 SR, 7950 XRS, and VSR Clear, Monitor, Show, and Tools Command Reference Guide* (for both MD-CLI and Classic CLI)

Note: This guide generically covers Release 22.*x*.R*x* content and may contain some content that is released in later maintenance loads. See the *SR OS R22.x.Rx Software Release Notes*, part number 3HE 18412 000 *x* TQZZA, for information about features supported in each load of the Release 22.*x*.R*x* software.

1.2 Conventions

This section describes the general conventions used in this guide.

1.2.1 Precautionary and information messages

The following are information symbols used in the documentation.

DANGER: Danger warns that the described activity or situation may result in serious personal injury or death. An electric shock hazard could exist. Before you begin work on this equipment, be aware of hazards involving electrical circuitry, be familiar with networking environments, and implement accident prevention procedures.

WARNING: Warning indicates that the described activity or situation may, or will, cause equipment damage, serious performance problems, or loss of data.

Caution: Caution indicates that the described activity or situation may reduce your component or system performance.

Note: Note provides additional operational information.

Tip: Tip provides suggestions for use or best practices.

1.2.2 Options or substeps in procedures and sequential workflows

Options in a procedure or a sequential workflow are indicated by a bulleted list. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform one of the listed options to complete the step.

Example: Options in a procedure

1. User must perform this step.
2. This step offers three options. User must perform one option to complete this step.
   - This is one option.
   - This is another option.
   - This is yet another option.

Substeps in a procedure or a sequential workflow are indicated by letters. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform two substeps (a. and b.) to complete the step.

Example: Substeps in a procedure

1. User must perform this step.
2. User must perform all substeps to complete this action.
   a. This is one substep.
   b. This is another substep.

2 PFCP association

This chapter provides an overview of the BNG CUPS UPF Packet Forwarding Control Protocol (PFCP) association configuration, heartbeat and headless mode operation, and operational management and debugging options.

2.1 UPF PFCP association

A BNG CUPS UPF requires an active PFCP association with the BNG CUPS CPF. Through the PFCP association, the BNG CPF installs the rules that determine how the BNG UPF forwards subscriber traffic.

The BNG UPF requires the PFCP association to be preconfigured using the **configure subscriber-mgmt pfcp association** command.

Each PFCP association is linked to a specific peer, interface, and router instance. The loopback interface is the recommended interface because it allows resiliency over multiple physical interfaces.

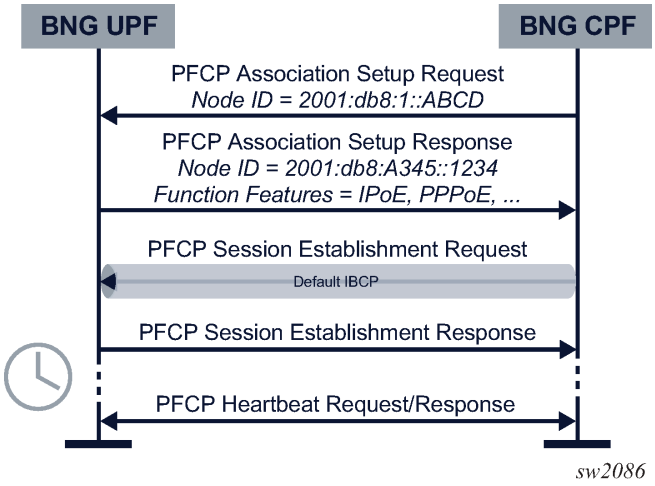
As soon as the PFCP association is configured and administratively enabled, the UPF connects to the BNG CPF by sending PFCP Association Setup Request messages. The UPF sends the messages periodically, until the association is either set up or administratively disabled.

To configure the retry interval for the PFCP association setup, the **association-setup-retry** command is used.

The UPF can also set up the PFCP association when it receives a PFCP Association Setup Request from the configured peer. However, the UPF does not accept an association setup from a non-configured peer.

Figure 1: BNG UPF PFCP association setup flow shows the PFCP association setup flow for the BNG UPF.

Figure 1: BNG UPF PFCP association setup flow



The PFCP protocol supports node identification using node IDs. The node ID can be either an IP address or a FQDN. By default, the IP address of the linked interface is chosen; however, this can be overridden using the **node-id** command. All the UPFs in a deployment require different node IDs.

PFCP messages sent for an active association use the following configuration under the PFCP association **tx** command:

- The **ttl** command defines the outgoing TTL.
- The **timeout** command defines the request message timeout (T1).
- The **retries** command defines the number of times a request message is retried (N1).

Note: For heartbeat messages, N1 and T1 are configured separately. For correct operation, N1 and T1 must be configured identically on both the BNG CPF and UPF. See the *CMG BNG CUPS Control Plane Function Guide* and the *7750 SR MG and CMG CLI Reference Guide* for more information about the BNG CUPS CPF configuration.

The QoS of the outgoing PFCP messages is managed through **sgt-qos** command configuration in the routing instance used by the PFCP. In the **application** list command, a **pfcp** keyword can be mapped to its own DSCP value (default NC2), after which that DSCP value can be mapped to a specific Forwarding Class (FC).

See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide*, section "QoS for Self-Generated (CPU) Traffic on Network Interfaces" for more information about QoS configuration.

When a PFCP association is administratively disabled, it is not immediately brought down. The BNG UPF requests a graceful CPF release and keeps the PFCP association up until the BNG CPF removes it, or the association release timeout expires.

To configure the PFCP association release timeout, use the **association-release-timeout** command.

To force an immediate PFCP association removal, configure the **association-release-timeout** to **none**.

The following example shows a BNG UPF PFCP association configuration.

```
[gl:configure subscriber-mgmt pfcp association "BNG-CPF"]
A:admin@DUT-B# info detail
    admin-state enable
 ## description
    association-setup-retry 1
    association-release-timeout 3600
    path-restoration-time 180
    node-id {
     ## fqdn
     ## use-ip-address
    }
    interface {
        router-instance "to_cp"
        name "endpoint"
    }
    peer {
        ip-address 17.17.17.10
    }
    heartbeat {
        interval 60
        timeout 5
        retries 4
    }
    tx {
        timeout 5
        retries 3
```

```
        ttl 255
    }
```

2.2 PFCP heartbeats and headless mode

The following concepts define the connectivity between the BNG UPF and the BNG CPF:

- **PFCP association**
  One PFCP association is allowed per BNG UPF and BNG CPF. The identifiers of the association are the BNG UPF and BNG CPF node IDs.
- **PFCP path**
  Multiple PFCP paths are possible per association. The identifier of a PFCP path is the pair of IP addresses that are used to communicate between the BNG UPF and the BNG CPF. Paths are not negotiated but are learned while using PFCP signaling.

  See UPF PFCP association for information about how PFCP associations are negotiated.

Note: The terms PFCP path and PFCP association are often used interchangeably because there is typically only one PFCP path per PFCP association.

The BNG UPF only uses one IP address, but starts heartbeats for each PFCP path it learns. The frequency, timeout, and retry values of the heartbeats are configured for the PFCP association using the **interval**, **retries**, and **timeout** commands in the **configure subscriber-mgmt pfcp association heartbeat** context.

If a heartbeat fails, the BNG UPF starts a timer based on the **path-restoration-time** command configuration under the PFCP association. If the timer expires or is not configured, all sessions associated with that path are removed. If the path recovers before the timer expires, the timer is canceled, and no sessions are removed.

Note: For correct operation, the heartbeat configuration must be identical on both the BNG UPF and BNG CPF. Nokia strongly recommends configuring the **path-restoration-time** to at least twice the sum of the **heartbeat interval** plus the total timeout (**heartbeat retries** x **heartbeat timeout** = N1 x T1).

To expedite the detection of path failures, enable BFD using the **bfd-expedited-path-down** command in the **configure subscriber-mgmt pfcp association** context. When enabled, the system starts a BFD session for each known PFCP path on the BNG UPF. If the system detects a BFD failure, it immediately brings down the associated path. BFD does not affect the path recovery detection, which requires the configuration of PFCP heartbeats. BFD-based path down detection requires the configuration of the **path-restoration-time** command under the PFCP association.

2.3 Default IBCP session

The BNG UPF always enables the IPoE and PPPoE BBF function features. A compatible BNG CPF uses this as an indication to set up a default IBCP tunnel to send control plane packets, such as DHCP discover or PADI, that do not match an existing session. The default tunnel is signaled as a special PFCP session without a PDN type. The special PFCP session can apply traffic-matching rules the same as any other PFCP session for which the BNG UPF applies rules.

Packets sent over the default In-band Control Plane (IBCP) tunnel include local BNG UPF parameters that are inserted in a network service header. The network service header is inserted between the GTP-U header and the encapsulated control packet. These parameters include the following:

- **MAC address**

  This is the MAC address that is associated with the capture SAP on which the IBCP packet was received. The BNG CPF uses the MAC address as a source MAC address when sending control packet responses. In case of inter-UPF resiliency, the BNG CPF can ignore this MAC address and use the FSG MAC address instead. For more information about inter-UPF resiliency, see BNG UPF resiliency.

- **Layer 2 access ID**

  The Layer 2 access ID (also known as the logical port) identifies the local port, the LAG, or the pw-port that is used by the capture SAP. The BNG CPF reflects this parameter as is when setting up a session so the BNG UPF installs the session in this context. To simplify provisioning on the BNG CPF, you can provide an alias for the L2 access ID. The alias must be unique within the BNG UPF and cannot overlap with any identifier such as a port or a LAG name.

  To configure the L2 access ID alias, use the **configure service vpls capture-sap pfcp l2-access-id-alias** command.

See IBCP for more information about IBCP.

2.4 Operational commands and debugging

This section describes commands that can be used for operational and debugging purposes.

To display the number of PFCP associations and sessions, use the **show subscriber-mgmt pfcp summary** command.

To display PFCP message statistics, including information about packets that are received and transmitted and any transmission errors, use the **show subscriber-mgmt pfcp statistics** command.

To reset the PFCP association statistics to zero, use the **clear subscriber-mgmt pfcp-association statistics** command.

To display information including association-level parameters such as function features and node IDs, use the **show subscriber-mgmt pfcp association** command.

To display path state information, use the **show subscriber-mgmt pfcp peer** command.

See PFCP heartbeats and headless mode for information about the distinction between PFCP association and path.

To display default IBCP tunnel information, use the **show subscriber-mgmt pfcp session default-tunnel** command.

To display details about a specific PFCP session, use the **show subscriber-mgmt pfcp session detail** command. This command provides an overview for the PFCP parameters of the session. Various filters can be applied to narrow a specific session or set of sessions.

See Operational commands for more information about basic operational commands.

To forcefully remove a PFCP session, use the **clear subscriber-mgmt pfcp-session** command.

Caution: Although it is possible to forcefully remove a PFCP session, Nokia does not recommend invoking this command in a live network because this may cause the BNG CPF to be

out of sync with the UPF. If the UPF contains a session that is not on the CPF, it is preferable to first run a manual PFCP audit.

To perform basic PFCP debugging, use the **debug subscriber-mgmt pfcp** command. The output of this command allows inspection of PFCP packets received and transmitted. As well, any session-specific failure is reported in the PFCP response to the BNG CPF, which can display the specific error as part of session debugging.

3 Session management

This chapter provides an overview of the common and fixed access session functionality.

3.1 Subscribers, QoS, and filters

The BNG CUPS automatically links sessions together into subscribers, based on the QoS Enforcement Rule (QER) Correlation ID it receives in the PFCP session. If the BNG CUPS UPF does not receive a QER Correlation ID, it assumes there is only one session per subscriber.

The usual subscriber-management processing applies, as described in the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide*, sections "QoS for subscribers and hosts" through "Configuring IP and IPv6 filter policies for subscriber hosts".

The PFCP may pass the following parameters:

- subscriber and SLA profile names; if these are not provided the name "default" is used

  Note: You must always configure the SLA and subscriber profiles for use with BNG CUPS; for example, **configure subscriber-mgmt sla-profile control cups** or **configure subscriber-mgmt sub-profile control cups**. This disables any feature that is not supported within BNG CUPS.

- direct QoS overrides of QoS objects such as aggregate-rate, schedulers, arbiters, queues, and policers
- SLA filter overrides, either by name or ID
- intermediate destination ID

PFCP can also signal GBR and MBR values directly in the QER, which is not linked directly to a specific QoS object. If the QER applies to the entire session, you can map the MBR and GBR to a direct QoS object PIR or CIR override using the **configure subscriber-mgmt sla-profile** *name* **pfcp-mappings session-qer** command. The BNG CUPS CPF signals the QER rate, for example, to install a session-AMBR (5G) or APN-AMBR (4G) for FWA sessions.

3.2 IBCP

Most BNG session types have one or more control plane messages that are sent in-band and therefore arrive directly on the UPF. Because the BNG UPF cannot handle these messages, they are forwarded to the BNG CPF. To accomplish this, the BNG CPF installs specific Ethernet or IP filter rules that match these packets; for example, by matching UDP destination port 67 to extract DHCP. These packets are encapsulated in GTP-U and sent to the CPF. Similarly, the BNG CPF sends downstream In-Band Control Plane (IBCP) packets over GTP-U toward the BNG UPF.

For upstream traffic, the BNG UPF sends any control plane messages that do not match a session over a default tunnel. See Default IBCP session for information about how this tunnel is signaled. If the control plane messages do not match the default tunnel rules, the messages are dropped.

When a session is created, either out-of-band or via a trigger over the default tunnel, the BNG CPF installs per-session control plane rules for both upstream and downstream. Packets that match the upstream rules are forwarded to the BNG CPF using the signaled GTP-U parameters. For downstream rules, the BNG UPF allocates a TEID that the BNG CPF can use to send packets. The BNG UPF does not support a default downstream IBCP tunnel.

The upstream IBCP (including default) follows the **sgt-qos dscp application** configuration, using the **ibcp** keyword on the router or VPRN. A specific DSCP value (default NC2) can be provisioned and mapped to a specific FC, as usual.

See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Quality of Service Guide*, section "QoS for Self-Generated (CPU) Traffic on Network Interfaces" for more information.

Downstream IBCP packets are handled directly in the data path. Ingress QoS is applied based on the provisioning. Egress QoS depends on the session type. The session types are as follows:

- **fixed access sessions**

  Egress QoS packets bypass per-session processing, including egress QoS and filters. Egress QoS is instead based on the QoS configuration of the capture SAP that is linked to the session.

- **FWA sessions**

  Egress QoS packets go through regular per-session processing and are subject to the QoS and filters provisioned in the SLA profile.

3.3 IP gateway, services, and routing

In many deployments, a BNG UPF acts as a direct IP gateway for sessions. The BNG CPF provides all the IP addresses and framed routes using the PFCP protocol. To assist with forwarding, the BNG CPF also signals the following information using the PFCP protocol:

- name of the preprovisioned IES or VPRN service in which forwarding must occur
- aggregate routes that the BNG UPF announces in routing protocols to attract traffic

  Note: The BNG CPF guarantees that no addresses from the aggregate routes are assigned to sessions on another BNG UPF. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide* for more information about route policies.

- IPv4 gateway address, which is typically a dedicated address within the aggregate route
- IPv6 gateway link-local address, only one of which is supported per VPRN or IES

The BNG UPF runs the appropriate routing protocols and responds to ARP/ND for the gateway addresses. For the purpose of exporting routes, the operator can distinguish all CUPS routes using the **pfcp** option for the **configure policy-options policy-statement entry from origin** command. Additionally, the operator can further distinguish routes using the following options for the **protocol** command in the same context:

- **sub-mgmt** option for session IP addresses and prefixes, as signaled in the UE IP Address IE in PFCP
- **managed** option for framed routes, as signaled in the Framed-Route IE in PFCP

  Note: When using the **pd-as-framed-route** option on the BNG CPF, an IPv6 PD prefix uses the **managed** option (instead of the **sub-mgmt** option) because the BNG UPF cannot distinguish the PD framed route from a regular framed route.

- **direct** option for all other routes, such as aggregate routes and gateway addresses

3.4 Statistics reporting

Statistics reporting uses the PFCP Usage Reporting Rule (URR) mechanism. The BNG UPF supports a single URR to count all statistics that are related to a session. The BNG UPF supports sending the following statistics for the URR:

- Aggregate octet counters are always signaled.
- Aggregate packet counters are signaled, if enabled by the CPF.
- Per-queue and per-policer statistics are signaled, if enabled by the CPF. The specific counters depend on the statistics mode (**stat-mode**) configured in either the QoS policy or SLA profile.

All counters, including aggregates, are based on QoS counters and are therefore affected by QoS modifiers, such as the **packet-byte-offset** command.

The BNG UPF sends reports for a URR in the following cases:

- The BNG CPF explicitly queries the UPF via a PFCP Session Modification Request.
- The periodic URR reporting is enabled and the BNG UPF sends unsolicited PFCP Session Report Request messages.

PFCP statistics are reported in an incremental manner. This means that only new statistics after the last report are signaled. To achieve this, the BNG UPF baselines the counters on every report. Consequently, it is not possible to manually clear statistics on the BNG UPF using the **clear service statistics subscriber** command. Other operational commands (for example, **show service active-subscribers detail**) only show the accumulated statistics on the BNG UPF.

Because statistics are based on QoS counters, sessions sharing the same SLA Profile Instance (SPI) also share statistics, and a report for one session baselines the counters for the entire SPI. As a result, per-session statistics on the BNG CPF are not correct when sharing an SPI; however, their aggregate counts are correct. The BNG CPF must provide the appropriate aggregate level (for example, subscriber-level accounting). When an SPI changes, the BNG UPF reports the final SPI statistics in PFCP if instructed to do so by the BNG CPF.

Hardware failures are automatically taken into account for statistics reporting. Statistics generated after the last report are irretrievably lost. However, as a result of the incremental reporting, the BNG CPF does not lose any older counters and does not see a sudden reset. That is, aggregate counters on the BNG CPF never decrease as a result of a hardware failure. However, the BNG UPF local statistics as seen in **show** commands reset upon a hardware failure, and therefore a mismatch of BNG CPF counters may result.

3.5 Operational commands

Most of the traditional BNG operational commands, as described in the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide*, apply to the CUPS BNG UPF. The significant exceptions to this rule are operational commands related to specific protocols (such as DHCP, DHCPv6, RADIUS, and PPPoE), because a BNG CUPS UPF is not aware of these states.

The primary BNG CUPS UPF operational commands are as follows:

- **show service active-subscribers**

This command contains several sub-commands that provide details about a specific subscriber or session within a subscriber. These commands incorporate information about CUPS subscribers. Information that is only available on the BNG CPF is not shown on the BNG UPF (for example, details on RADIUS and metadata such as **remote-id** and **circuit-id**).

- **show subscriber-mgmt statistics**

  This command contains several sub-commands that provide a wide variety of statistics on various granularity levels. These commands are extended to incorporate BNG CUPS statistics.

IBCP statistics can be displayed via the PFCP statistics using the **show subscriber-mgmt pfcp statistics** command.

Operational commands that are specific to PFCP associations are described in Operational commands and debugging.

3.6 SAP and group interface templates

The system auto-provisions any required objects, which means that subscriber interfaces, group interfaces, and SAPs do not need to be provisioned. These objects are hidden from configuration and are not modifiable. Aside from the capture SAP, the only required configuration is the VPRN or IES where IP forwarding occurs.

You can manage SAP creation by configuring a SAP template under the **configure subscriber-mgmt sap-template** command. The SAP template supports the configuration of the following:

- The **hold-time** command delays the deletion of the SAP after the last PFCP session is removed. The **infinite** option can be configured for the **hold-time** but it is not recommended. Idle SAPs can be cleared using the **idle-saps** option under **clear subscriber-mgmt sap-template**.
- The **cpu-protection** and **dist-cpu-protection** commands configure CPU protection; see the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*, section "Centralized CPU protection and distributed CPU protection" for more information about CPU protection.

Note: On platforms where CPU protection and distributed CPU protection are not supported, these commands are ignored.

Similarly, group-interface creation can be manipulated by configuring a group interface template under the **configure subscriber-mgmt group-interface-template** command. When setting up a PFCP session, a template name is passed using PFCP. If the template name is absent, the system falls back to the name "default".

A group interface template allows the configuration of the following:

- **ip-mtu**; is applied to outgoing packets
- **urpf-check**; see *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide,* section "Unicast reverse path forwarding check"
- **icmp**
- **remote-proxy-arp**; see *7450 ESS, 7750 SR, 7950 XRS, and VSR Router Configuration Guide*, section "Proxy ARP"

Note: The SAP and group interface templates must be configured on the BNG UPF (as well as the name "default") to ensure that the session setup does not fail.
Changing the configuration of a template does not automatically change all created SAPs or group interfaces.

3.6.1 Mixing different encapsulation sessions on the same port

The BNG UPF supports the following mix of encapsulation sessions:

- on a :*.* capture SAP: dot1q and null encapsulation sessions

  Note: To support this, the user must set the **configure service system extended-default-qinq-sap-lookup** command to **true** on the systems where this is not the default.

- on a :* capture SAP: null encapsulation sessions

The system internally creates SAPs with :N.0, :0.0, and :0 encapsulation to support the mix. The user can apply the SAP templates to these SAPs similarly to any other SAPs.

Traffic as seen on the wire typically does not include an S-tag or C-tag with a tag value explicitly set to zero because the absence of a tag is equal to a zero tag. Occasionally, an explicit zero tag is included; for example, when a dot1p or DEI bit needs to be set in the tag header. The internally created SAPs interact with such traffic as follows:

- Because generated traffic never includes an explicit zero tag, it is not possible to set a dot1p or DEI bit in the tag header.
- Traffic with a C-tag value explicitly set to zero is always dropped, even if it matches an internally created :N.0 or :0.0 SAP.
- Traffic with only the S-tag value explicitly set to zero is handled if it matches either a :0 or a :0.0 SAP. This kind of traffic matches the same session as if it was received without any S-tag.

3.7 Fixed access sessions

To enable fixed access sessions, you must provision a capture SAP under the VPLS service with appropriate values for trigger-packet and a link to the PFCP association. The triggers are mandatory and are not automatically derived from the default IBCP tunnel.

Sessions without any encapsulation are supported on a dot1q capture SAP. The system creates internal constructs to correctly handle sessions without encapsulation. These sessions can be combined with dot1q encapsulated sessions on the same capture SAP.

The following example shows trigger-packet provisioning in a PFCP association configuration.

```
A:admin@DUT-B# info
    pfcp {
        association "BNG-CPF"
    }
    trigger-packet {
        pppoe true
    }
```

To identify sessions in the data plane, the BNG CPF must provide the following parameters:

- The logical port (also known as the Layer 2 access ID) identifies the port, the LAG, or the pw-port where the session is terminated. The BNG CPF knows the correct logical port because the BNG UPF includes this logical port in the IBCP packets sent over the default IBCP tunnel. See Default IBCP session.
- The VLAN tags, along with the logical port, identify a SAP where the session is terminated, also known as a Layer 2 circuit (l2-circuit). The BNG CPF must signal all the VLAN tags to match the encapsulation type provisioned for the port; for example, only signaling an s-tag for a q-in-q port is not allowed. As an exception, the BNG CPF can install sessions without any VLAN tags on a dot1q capture SAP, as described at the beginning of this section.
- The source MAC address is required.
- The PPPoE session ID is used for PPPoE only.
- The IP anti-spoofing IP address is optionally used to enable IP anti-spoofing. While this can be signaled per session, the BNG UPF only supports a single anti-spoof type per SAP. When a second session on the same SAP has a conflicting anti-spoof indication, the setup fails. IP anti-spoofing is not supported for framed routes.

For PPPoE, the BNG UPF can perform LCP keep-alive offload, if supported and signaled by the BNG CPF. The BNG UPF automatically signals support for this feature when the PFCP association is created.

3.8 Fixed wireless access sessions

To configure Fixed Wireless Access (FWA) sessions, the operator must provision a GTP UPF data endpoint using the **gtp upf-data-endpoint** command in the **service vprn**or **router** context. The endpoint must reference an interface in the routing instance where GTP-U tunnels to the RAN are set up. Additionally, an FPE construct is required to enable datapath functions in the router. The FPE must be configured as type **multi-path**. See the 7450 ESS, 7750 SR, 7950 XRS, and VSR Interface Configuration Guide for more information.

The system automatically creates all the required constructs to correctly handle FWA sessions. Additionally, the system load-balances sessions over each FPE path, using the path that is the least loaded when the session is set up.

The following example shows provisioning of a UPF data endpoint and multipath FPE.

```
[gl:/configure service vprn "to_ran" gtp upf-data-endpoint]
A:admin@BNG-UPF# info
    interface "gtp_u_endpoint"
    fpe 1
[gl:/configure fwd-path-ext fpe 1]
A:admin@BNG-UPF# info
    multi-path {
        path 1 {
            pxc 1
        }
    }
    application {
        sub-mgmt-extension true
    }
```

Unlike in fixed access sessions, a default IBCP tunnel is not used for FWA sessions because the initial session setup is out-of-band and does not involve the BNG UPF. Per-session IBCP is supported to forward DHCP (Deferred Allocation), ICMPv6 RS/RA, and DHCPv6 packets.

3.9 Routed subscriber sessions

Enterprise IP VPNs often use BGP to exchange routing information, for example, between headquarters and branch offices. Providing BGP connectivity to an enterprise router via a residential access connection requires BGP peering over a BNG CUPS subscriber session. To configure this on the BNG CUPS UPF, use a static BGP neighbor that has as its neighbor address the fixed IPv4 or IPv6 WAN address of the subscriber session.

Example configuration

```
# configure service vprn 1000
    --- snip ---
    subscriber-interface "_tmnx_cups_1131076" fwd-service 2148278386
    /fwd-subscriber-interface "_tmnx_cups_1131075" wan-mode mode128
        description "default subscriber interface template"
        private-retail-subnets
        address 10.0.240.254/20
        ipv6
        exit
    exit
    bgp
        group "enterprise-1"
            neighbor 10.0.0.1
                family ipv4
                local-address 10.0.240.254
                type external
                local-as 65536
                peer-as 65501
            exit
        exit
        no shutdown
    exit
    no shutdown
```

BNG CUPS subscriber sessions support static BGP neighbors for the following:

- BGPv4 neighbors with IPv4 and IPv6 address families
- BGPv6 neighbors with IPv4 and IPv6 address families
- IPoE and PPPoE sessions
- numbered and unnumbered interfaces
- single-hop and multi-hop BGP neighbors

4 Network Address Translation

This chapter provides an overview of Network Address Translation (NAT) functionality for BNG CUPS.

4.1 Residential NAT for BNG CUPS

For BNG CUPS, NAT responsibilities are divided between the BNG CPF and BNG UPF.

The role of the BNG CPF is to associate the subscriber session with NAT during the session authentication phase. This process consists mainly of allocating the outside IP address and port-block to the NAT subscriber session. These parameters are submitted to the BNG UPF through the PFCP association.

The BNG UPF performs NAT on the data traffic. On the BNG UPF, NAT runs on MS-ISA service adapters, including the Integrated Service Adapter (ISA), Virtual ISA (vISA), and Extended Service Adapter (ESA). For the inside IP addresses, the incoming data traffic is sprayed across ISAs. This traffic spraying is based on the subscriber context, which typically represents a residence. For the outside IP addresses, the NAT prefix that is received from the BNG CPF is segmented into smaller subnets and equally distributed across ISAs. This approach requires fair load distribution of traffic across service adapters in the upstream and downstream directions.

Note: In this document, all service adapter types are referred to as ISAs, except when it is necessary to identify a specific type. See the *7450 ESS, 7750 SR, and VSR Multiservice Integrated Service Adapter and Extended Services Appliance Guide* for more information about MS-ISA service adapters.
See the *CMG BNG CUPS Control Plane Function Guide* for more information about NAT terminology and an overview of Residential NAT that describes the division of NAT responsibilities between the BNG CPF and BNG UPF.

4.2 UP NAT policy template

A UP NAT policy template contains parameters that define NAT behavior for a group of subscribers within a NAT pool. This NAT behavior includes support for ALGs, setting limits for the number of NAT flows per subscriber, protocol timer definitions, flow-based logging, watermarks, and so on. The UP NAT policy configuration allows the NAT behavior to be customized for different groups of subscribers within the same NAT pool.

Although the UP NAT policy template is configured on the BNG UPF, its assignment to the NAT-enabled session is performed on the BNG CPF during the authentication phase, using a reference in the CP NAT profile configuration.

The roles of the CP NAT profile and UP NAT policy can be summarized as follows:

- The CP NAT profile is configured on the BNG CPF and identifies NAT subscribers during the authentication phase. Parameters defined in the CP NAT profile affect the selection of the NAT pool within a specific outside routing context. This includes the allocation of the outside IP addresses, port-blocks, and NAT mode of operation (NAPT or 1:1). These resources are managed by the BNG CPF.

- The UP NAT policy template is configured on the BNG UPF and is used to define NAT behavior for a group of subscribers within a NAT pool. This behavior is closer to the NAT translation in the forwarding plane (for example, ALGs and protocol timers).

4.3 Guidelines for configuring NAT subscribers in the sub-profile

Many NAT configuration parameters are defined in the UP NAT policy template (**up-nat-policy**) or the CP NAT profile (see UP NAT policy template). There are also some parameters that may be used for NAT configuration that require further granularity of definition, such as the UPNP policy that enables the dynamic port forward allocation. If a UPNP policy is used for NAT, it must be defined in the **configure subscriber-management sub-profile** context, as shown in the following example.

```
configure {
   subscriber-management {
       sub-profile name {
           upnp-policy policy-name
       }
   }
}
```

4.4 Guidelines for configuring NAT groups

A NAT group represents a collection of ISAs that are used to process NAT traffic for subscribers. NAT traffic is distributed over multiple ISAs in a NAT group to achieve better performance and scale. BNG CUPS supports a single NAT group per BNG UPF, however, other NAT groups can be configured in the system outside CUPS.

A NAT group is a mandatory configuration. After the NAT group is defined, it must be referenced by a PFCP association. A NAT group is configured using commands in the **configure isa nat-group** context.

See Provisioning residential NAT for BNG CUPS for a configuration example.

4.5 Guidelines for configuring accounting and logging

Aggregated NAT logging based on port blocks is performed on the BNG CPF, and flow-based logging can be enabled on the BNG UPF. Because a number of logs are produced in flow logging, flow logs are exported directly from the ISA, bypassing the BNG CPF and the CPM on the BNG UPF. The BNG UPF supports flow logging in IPFIX format.

An IPFIX export policy must be configured in the **configure service ipfix export-policy** context, as shown in the following example.

```
configure {
   service {
      ipfix {
         export-policy policy1
       }
   }
}
```

After the export policy is configured, it must be associated with a UP NAT policy, as shown in the following example.

```
configure {
   service {
      nat {
         up-nat-policy natpolicy1 {
             flow-log-policy {
                 ipfix exportpolicy1
             }
         }
      }
   }
}
```

4.6 Guidelines for configuring watermarks

The following watermarks are supported on the BNG UPF:

- The session-level watermarks on the member ISA level monitor the NAT flow usage against the configured limit per member ISA. They are configured using the NAT group, as shown in the following example.

```
configure {
   isa {
      nat-group id {
         session-limits {
             watermarks {
                 high number
                 low number
             }
         }
      }
   }
}
```

- The session-level watermarks on the subscriber level monitor the NAT flows usage against the configured limit per subscriber. They are configured using the UP NAT policy, as shown in the following example.

```
configure {
   service {
      nat id {
         up-nat-policy name {
             session-limits {
                 watermarks {
                    high number
                    low number
                 }
             }
         }
      }
   }
}
```

- The port usage watermarks on the subscriber level are used to monitor port usage against the configured limit per subscriber. They are configured using the UP NAT policy, as shown in the following example.

```
configure {
   service {
      nat id {
         up-nat-policy name {
             port-limits {
                 watermarks {
                    high number
                    low number
                }
             }
         }
      }
   }
}
```

- On the BNG CPF, a watermark threshold can be configured in either absolute value or percentages to monitor micronet usage within a NAT outside pool. See the *CMG BNG CUPS Control Plane Function Guide* for more information.

4.7 Guidelines for configuring intra-chassis redundancy

ISA redundancy on the BNG UPF level supports the following modes of operation:

- **N:M active/standby mode**

  M number of standby ISAs protect *N* number of active ISAs.

- **all active mode**

  This mode supports failure of up to two ISAs simultaneously. During an ISA failure, the configuration from the failed ISA is distributed over the remaining operational ISAs.

Both modes are stateless which means that NAT binding must be re-established after the switchover.

ISA redundancy is configured in the **configure isa nat-group** context and active/standby mode is enabled using the following commands.

```
configure {
   isa {
      nat-group id {
         mda mda-id
             redundancy {
                 active-mda-limit number
                 intra-chassis {
                     active-standby
                }
             }
         }
      }
   }
```

These commands associate MDAs with the NAT group, set the mode of operation to active/standby, and configure the number of active ISAs in the NAT group. Any ISAs within the NAT group that are in excess of the configured number are automatically considered standby.

All active mode is enabled using the following commands.

```
configure {
   isa {
      nat-group id {
         mda mda-id
             redundancy {
                 active-mda-limit number
                 intra-chassis {
                     active-active {
                        failed-mda-limit number
                     }
                  }
              }
           }
        }
```

4.8 Provisioning residential NAT for BNG CUPS

Prerequisites

Review the residential NAT for BNG CUPS overview information; see Network Address Translation.

A UP NAT policy is required; it can be created (exist) for the UPF or it is sufficient to use the default parameters. See Guidelines for configuring NAT groups.

To configure residential NAT on BNG CUPS, perform the following minimum configuration steps:

Procedure

Step 1. Configure the CPF as described in the *CMG BNG CUPS Control Plane Function Guide*.

Step 2. Configure the UPF.

a. Configure the NAT policy template.

```
configure {
   service {
      nat {
         up-nat-policy “pol-1” {

         }
      }
   }
```

b. Configure the NAT group, including the ISA redundancy mode.

```
configure {
   isa {
      nat-group 1 {
         mda 1/2
         mda 3/1
         mda 2/2
         redundancy {
             active-mda-limit 2
             intra-chassis {
                active-standby
             }
         }
```

```
      }
   }
}
```

c. Associate the NAT group created in step 2.b with the PFCP interface.

```
configure {
    subscriber-mgmt {
       pfcp {
           association "profile-1" {
               nat {
                  nat-group 1
               }
       }
   }
}
```

5 BNG UPF resiliency

Resiliency based on Fate Sharing Group

The BNG CPF groups the sessions in Fate Sharing Groups (FSGs). All sessions in an FSG share their fate, that is, they become active or standby together. The BNG CPF provides the following parameters to the BNG UPF per FSG:

- FSG ID
- status (active or standby)
- unique FSG MAC address also known as a virtual MAC
- list of associated sessions and one or more aggregate routes associated with these sessions. For more information, see IP gateway, services, and routing.
- FSG template

When the BNG CPF does not provide an FSG template, the template with the name default is used. If there is no default template, the setup of the FSG and any associated session fails.

To configure FSG templates, use the **configure subscriber-mgmt up-resiliency fate-sharing-group-template** command.

After this, the active BNG UPF and standby BNG UPF are used in the context of a single FSG. Each BNG UPF can have multiple FSGs and can have a different status for each FSG.

To attract traffic from the access network, an active BNG UPF replies to ARP requests or ND messages for any IP gateway associated with the FSG. A standby BNG UPF never replies to those ARP or ND messages. To expedite convergence upon switching from standby to active, the new active BNG UPF sends Gratuitous ARP (GARP) messages using one of the IP gateway addresses for the FSG, or the system IP address if no IP gateway is known.

To configure the granularity of GARP messages for q-in-q SAPs, use the **configure subscriber-mgmt up-resiliency fate-sharing-group-template gratuitous-arp** command. You can configure the BNG UPF to send a single GARP message per SAP or per outer tag.

To correctly draw traffic to the active BNG UPF, the **fsg-active** and **fsg-standby** options are added to the **state** command in the **configure policy-options policy-statement entry from** context. All routes received from PFCP, including per-session framed routes, have one of these values as parameter. You can use this parameter to adjust values in routing export policies; for example, adjust a metric or a preference to the needs of the used routing protocol.

The following reduced configuration example shows a simplified policy that sets a metric of 100 for active routes and a metric of 200 for standby routes.

```
[gl:/configure policy-options policy-statement "upf_resiliency_aware_export"]
A:admin@BNG-UPF# info
    entry 20 {
        from {
            origin pfcp
            state fsg-active
        }
        action {
            action-type accept
```

```
            metric {
                set 100
            }
        }
    }
    entry 30 {
        from {
            origin pfcp
            state fsg-standby
        }
        action {
            action-type accept
            metric {
                set 200
            }
        }
    }
```

An active BNG UPF always forwards traffic in both directions. It uses the FSG MAC as source MAC for downlink unicast traffic. A standby BNG UPF by default forwards downlink traffic using its local port MAC as source MAC and drops all received uplink traffic. You can modify the default behavior in the following ways:

- To shunt downlink traffic from the standby to the active BNG UPF and have the active BNG UPF forward that downlink traffic, do the following:
  - Configure a redundant interface using the **configure subscriber-mgmt up-resiliency fate-sharing-group-template redundant-interface** command.
  - Configure the same shunt ID on the active and the standby BNG UPF using the **configure service ies subscriber-mgmt multi-chassis-shunt-id** or **configure service vprn subscriber-mgmt multi-chassis-shunt-id** command depending on the service (IES or VPRN).
- To enable forwarding of uplink traffic by the standby BNG UPF, use the **configure subscriber-mgmt up-resiliency fate-sharing-group-template uplink-forwarding-while-standby** command.

Caution: Enabling the **uplink-forwarding-while-standby** command can lead to packet replication toward the core network. To prevent the possibility of packet replication toward the core network, provision the access network not to replicate unicast packets to the BNG UPF.

When the standby BNG UPF forwards uplink traffic, it can significantly lower packet loss during transition scenarios. The following examples illustrate this benefit:

- If the current active BNG UPF fails and an access node detects this faster than the BNG CPF (for example, using BFD), the access node can start sending packets to the standby BNG UPF before that BNG UPF has become active. When the **uplink-forwarding-while-standby** command is enabled, the uplink packets are not lost because the standby BNG UPF forwards them.
- During scheduled maintenance, the BNG CPF can switch the roles of the active and standby BNG UPF while both are healthy. For some time, the access node continues to send packets to the previously active BNG UPF that has become the standby BNG UPF. When the **uplink-forwarding-while-standby** command is enabled, the uplink packets are not lost because the previously active BNG UPF still forwards them. When the **uplink-forwarding-while-standby** command is disabled, the previously active BNG UPF drops the packets until the access node learns the path to the new active BNG UPF (using GARP).

The resiliency based on FSG does not use the SRRP protocol, but the system internally consumes an SRRP instance for each unique combination of FSG, port, and group interface template. To avoid potential

conflicts with pre-configured SRRP instance IDs, define a range of SRRP instance IDs for the inter-UPF resiliency functionality using the **configure redundancy srrp auto-srrp-id-range** command.

BNG UPF health reporting

The BNG UPF can send health reports to the BNG CPF using PFCP Node Report messages. The BNG CPF uses the health reports to determine the need for a BNG UPF status change (active or standby). Per FSG, the BNG CPF selects the active and the standby BNG UPF. For example, the BNG CPF can base its decision on link failures in the access network.

The BNG UPF supports health reports for the following contexts:

- **per network instance**
  Configure the health monitoring using the commands in the **configure service ies subscriber-mgmt up-resiliency** or **configure service vprn subscriber-mgmt up-resiliency** context, depending on the service. The health reports per network instance can, for example, be used to indicate the status of the network where the subscriber is serviced.
- **per Layer 2 access ID**
  Configure the health monitoring using the commands in the **configure service vpls capture-sap pfcp up-resiliency** context. The health reports per Layer 2 access ID can, for example, be used to indicate the status of the access links.

Each health report generates a single byte health value between 0 (unhealthy) and 255 (healthy). The base health value is 255 and decreases with the number of failed members in the operation group x the configured health drop number for the operational group.

Whenever a member of the operational group changes its state (fails or recovers), the BNG UPF calculates the health value and sends an updated report to the BNG CPF.

To configure the operational group and the health drop number, use the **monitor-oper-group** and the **monitor-oper-group health-drop** commands in the above mentioned contexts.

For more information about operational groups, see 7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN, sections *Object grouping and state monitoring*.

With the following example configuration, the BNG UPF sends health reports for Layer 2 access ID (port) lag-access. The operational group has five members (port 1/1/20 to port 1/1/24) and the health value decreases with 51 per failed member, that is, with 20% of the base health value.

```
[gl:/configure port 1/1/20]
A:admin@BNG-UPF# info
    oper-group "lag_access_health"
[gl:/configure port 1/1/21]
A:admin@BNG-UPF# info
    oper-group "lag_access_health"
[gl:/configure port 1/1/22]
A:admin@BNG-UPF# info
    oper-group "lag_access_health"
[gl:/configure port 1/1/23]
A:admin@BNG-UPF# info
    oper-group "lag_access_health"
[gl:/configure port 1/1/24]
A:admin@BNG-UPF# info
    oper-group "lag_access_health"
[gl:/configure service vpls "access" capture-sap lag-access:*.* pfcp up-resiliency]
A:admin@BNG-UPF# info
    monitor-oper-group "lag_access_health" {
        health-drop 51
    }
```

With the following example configuration, the BNG UPF sends health reports for network instance HSI. The health drop number is not configured, that is, the default value of 255 is used. The health is based on a BFD session that is used to check if the BNG UPF is isolated from the rest of the network. When the BFD session is up, the health value equals 255, otherwise, the health value equals 0.

```
[gl:/configure service oper-group "hsi-bfd"]
A:admin@BNG-UPF# info
    bfd-liveness {
        router-instance "to_uplink_router"
        interface-name "endpoint"
        dest-ip 203.0.113.10
    }
[gl:/configure service vprn "hsi" subscriber-mgmt up-resiliency]
A:admin@BNG-UPF# info
    monitor-oper-group "hsi-bfd" {
    }
```

The BNG UPF sends a health report for every status change in the operational group. Additionally, it sends all health reports periodically (every 60 seconds) and when a PFCP audit is requested.

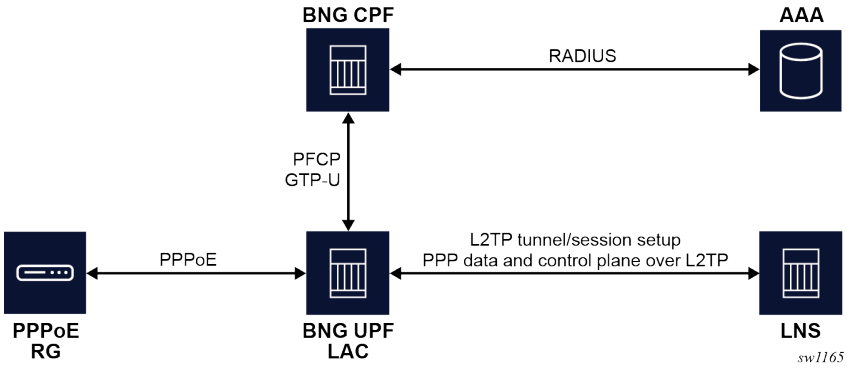
6 Layer 2 Tunneling Protocol

The BNG CUPS environment supports L2TP functionality.

6.1 UPF-triggered L2TP access concentrator

The BNG CUPS UPF supports PPPoE LAC sessions with L2TP control plane signaling running on the BNG CUPS UPF. This relies on the SR L2TP functionality described in the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide*, section *Layer 2 Tunneling Protocol (L2TP)*.

Figure 2: L2TP LAC network components



To run a PPPoE LAC session with L2TP control plane signaling on the BNG UPF, the BNG CPF provides the following parameters during the PFCP session data plane setup:

- list of potential L2TP Network Server (LNS) tunnel endpoints
- common or per-LNS parameters such as retry timers, preferences, and authorization IDs; see the *CMG BNG CUPS Control Plane Function Guide* for more information about how to configure these parameters
- per-session PPP LCP and PPP authentication attributes to be sent by proxy to the chosen LNS, so the LNS can avoid renegotiating LCP and authentication with the PPPoE session
- unique name to identify the tunnel group over shared sessions

The BNG UPF performs normal L2TP tunnel management over the group of tunnels, including deny list management, as described in the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide*, section *Traffic Steering on L2TP LAC*. To accomplish this, the BNG UPF creates an internal L2TP group in the VPRN service or base router provided by the PFCP. This internal group is not configurable, but common parameters configured under **configure router l2tp** or **configure vprn** *service-name* **l2tp** are applied to the setup of the tunnels. If a parameter is configured locally and also in PFCP, the PFCP parameter takes precedence. To set up tunnels, the **l2tp** context must also be administratively enabled in the router or VPRN.

Based on the tunnel management, the BNG UPF selects a tunnel for the session, or creates the tunnel if it does not exist, and an L2TP session is created for that specific PPPoE session. After the tunnel and

session setup are complete, a response including the following parameters is sent to the triggering PFCP message for operational management on the BNG CPF:

- L2TP tunnel and session IDs of both the LAC and the LNS
- LNS and LAC hostnames, also known as auth IDs
- L2TP tunnel and session IDs for both LNS and LAC
- Call Serial Number (CSN)

After the connection is established, the PPP data packets are forwarded to the LNS. The PFCP message instructs the BNG UPF to stop sending PPP control plane messages to the BNG CPF, and to send them to the LNS instead. Only the PPPoE discovery packets are forwarded to the BNG CPF. For example, a PADT packet is handled by the BNG CPF, while an LCP terminate packet is handled by the LNS.

If L2TP session or tunnel setup fails, the normal L2TP backoff and deny list behavior applies. If the setup fails for all provided tunnels, an explicit PFCP error message is sent to the BNG CPF. However, the BNG UPF does not time out the PFCP message if the setup takes too long, for example, because multiple LNSs are unreachable. The BNG triggers an explicit delete after the PFCP message times out, using its local PFCP N1 or T1 configuration. If a delete is received for an in-progress setup, the setup is aborted.

Note: An aborted setup does not count as a tunnel timeout and the tunnel is not placed in automatic deny lists for timeout hold-off purposes. You must configure the **max-retries-not-estab** command to ensure that the total timeout does not exceed the PFCP session timeout on the BNG CPF. See the *CMG BNG CUPS Control Plane Function Guide* for more information about how to correctly align the timeouts.

7 Lawful intercept

This chapter provides an overview of the Lawful Intercept (LI) functionality for BNG CUPS.

7.1 Overview of the LI implementation on the BNG UPF

To perform LI for BNG CUPS, configurations are required on both the BNG CUPS CPF and UPF:

- The CPF supports reporting of subscriber and LI events; see the *CMG BNG CUPS Control Plane Function Guide* and the *7750 SR MG and CMG CLI Reference Guide* for more information about BNG CUPS CPF configuration.
- The UPF supports the provisioning of LI targets and mirroring of LI packets.

After the LI mediation gateway identifies an LI subscriber through the CPF-reported events, the provisioning of the LI subscriber can be performed directly on the UPF, using the **configure li li-source** commands as described in the *7450 ESS, 7750 SR, 7950 XRS, and VSR OAM and Diagnostics Guide*. Provisioning can be performed using CLI or SNMPv3, however, SNMPv3 is the preferred platform.

Note: In CUPS architecture, the UPF creates a new subscriber ID every time the subscriber or LI subscriber logs in. For this reason, it is highly recommended to use a mediation device to automate the LI configuration. It is not recommended to perform LI configuration through CLI on the UPF.

When the BNG CUPS CPF is configured, it notifies the LI mediation device about the UP subscriber IDs and IP addresses. The LI mediation device sends an SNMPv3 command directly to the UPF IP address to set up an LI target. Li targets typically include the following parameters:

- mirror destination service; can be a layer 3 encapsulation or a SAP
- subscriber ID; for example, " _cups_549"

  Note: The UPF automatically appends " _cups_" to the auto-generated subscriber ID.

- ingress and egress direction
- session ID and intercept ID, which allow the LI mediation device to correlate subscriber events and mirrored packets (optional); see the *7450 ESS, 7750 SR, 7950 XRS, and VSR OAM and Diagnostics Guide*, section "Lawful Intercept" for information about additional parameters

When the subscriber logs out, the LI mediation device removes the subscriber from the LI source through SNMPv3. When the same subscriber logs in again, the system auto-generates a new UPF subscriber ID.

For the procedure to configure SNMPv3 and BNG CUPS, see Provisioning SNMPv3 and LI subscribers for the BNG CUPS UPF.

7.2 Provisioning SNMPv3 and LI subscribers for the BNG CUPS UPF

Prerequisites

Before you begin, review Overview of the LI implementation on the BNG UPF.

To provision SNMPv3 and LI subscribers for the BNG CUPS UPF, perform the following steps:

Procedure

Step 1. Create the SNMPv3 group for LI.

Step 2. Provision an LI administrator for the UPF with both LI access and SNMP access.

Step 3. Associate the SNMPv3 group created in step 1 with the LI administrator.

See the *7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide*, for more information about LI users and SNMPv3 setup.

Step 4. Provision the LI subscriber directly on the UPF, using the **configure li li-source** commands.

See the *7450 ESS, 7750 SR, 7950 XRS, and VSR OAM and Diagnostics Guide* for information about user plane LI management and procedures.

See the *CMG BNG CUPS Control Plane Function Guide* and the *7750 SR MG and CMG CLI Reference Guide* for information about the related BNG CUPS CPF configuration.

8 Standards and protocol support

Note:
The information provided in this chapter is subject to change without notice and may not apply to all platforms.

Nokia assumes no responsibility for inaccuracies.

8.1 Access Node Control Protocol (ANCP)

draft-ietf-ancp-protocol-02, *Protocol for Access Node Control Mechanism in Broadband Networks*

RFC 5851, *Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks*

8.2 Application Assurance (AA)

3GPP Release 12, *ADC rules over Gx interfaces*

RFC 3507, *Internet Content Adaptation Protocol (ICAP)*

8.3 Bidirectional Forwarding Detection (BFD)

draft-ietf-idr-bgp-ls-sbfd-extensions-01, *BGP Link-State Extensions for Seamless BFD*

RFC 5880, *Bidirectional Forwarding Detection (BFD)*

RFC 5881, *Bidirectional Forwarding Detection (BFD) IPv4 and IPv6 (Single Hop)*

RFC 5882, *Generic Application of Bidirectional Forwarding Detection (BFD)*

RFC 5883, *Bidirectional Forwarding Detection (BFD) for Multihop Paths*

RFC 7130, *Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces*

RFC 7880, *Seamless Bidirectional Forwarding Detection (S-BFD)*

RFC 7881, *Seamless Bidirectional Forwarding Detection (S-BFD) for IPv4, IPv6, and MPLS*

RFC 7883, *Advertising Seamless Bidirectional Forwarding Detection (S-BFD) Discriminators in IS-IS*

RFC 7884, *OSPF Extensions to Advertise Seamless Bidirectional Forwarding Detection (S-BFD) Target Discriminators*

8.4 Border Gateway Protocol (BGP)

draft-gredler-idr-bgplu-epe-14, *Egress Peer Engineering using BGP-LU*

draft-hares-idr-update-attrib-low-bits-fix-01, *Update Attribute Flag Low Bits Clarification*

draft-ietf-idr-add-paths-guidelines-08, *Best Practices for Advertisement of Multiple Paths in IBGP*

draft-ietf-idr-best-external-03, *Advertisement of the best external route in BGP*

draft-ietf-idr-bgp-flowspec-oid-03, *Revised Validation Procedure for BGP Flow Specifications*

draft-ietf-idr-bgp-gr-notification-01, *Notification Message support for BGP Graceful Restart*

draft-ietf-idr-bgp-ls-app-specific-attr-16, *Application-Specific Attributes Advertisement with BGP Link-State*

draft-ietf-idr-bgp-ls-flex-algo-06, *Flexible Algorithm Definition Advertisement with BGP Link-State*

draft-ietf-idr-bgp-optimal-route-reflection-10, *BGP Optimal Route Reflection (BGP-ORR)*

draft-ietf-idr-error-handling-03, *Revised Error Handling for BGP UPDATE Messages*

draft-ietf-idr-flowspec-interfaceset-03, *Applying BGP flowspec rules on a specific interface set*

draft-ietf-idr-flowspec-path-redirect-05, *Flowspec Indirection-id Redirect* – localised ID

draft-ietf-idr-flowspec-redirect-ip-02, *BGP Flow-Spec Redirect to IP Action*

draft-ietf-idr-link-bandwidth-03, *BGP Link Bandwidth Extended Community*

draft-ietf-idr-long-lived-gr-00, *Support for Long-lived BGP Graceful Restart*

RFC 1772, *Application of the Border Gateway Protocol in the Internet*

RFC 1997, *BGP Communities Attribute*

RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*

RFC 2439, *BGP Route Flap Damping*

RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*

RFC 2858, *Multiprotocol Extensions for BGP-4*

RFC 2918, *Route Refresh Capability for BGP-4*

RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*

RFC 4360, *BGP Extended Communities Attribute*

RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 4456, *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*

RFC 4486, *Subcodes for BGP Cease Notification Message*

RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*

RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*

RFC 4724, *Graceful Restart Mechanism for BGP* – helper mode

RFC 4760, *Multiprotocol Extensions for BGP-4*

RFC 4798, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*

RFC 5004, *Avoid BGP Best Path Transitions from One External to Another*

RFC 5065, *Autonomous System Confederations for BGP*

RFC 5291, *Outbound Route Filtering Capability for BGP-4*

RFC 5396, *Textual Representation of Autonomous System (AS) Numbers* – asplain

RFC 5492, *Capabilities Advertisement with BGP-4*

RFC 5668, *4-Octet AS Specific BGP Extended Community*

RFC 6286, *Autonomous-System-Wide Unique BGP Identifier for BGP-4*

RFC 6793, *BGP Support for Four-Octet Autonomous System (AS) Number Space*

RFC 6810, *The Resource Public Key Infrastructure (RPKI) to Router Protocol*

RFC 6811, *Prefix Origin Validation*

RFC 6996, *Autonomous System (AS) Reservation for Private Use*

RFC 7311, *The Accumulated IGP Metric Attribute for BGP*

RFC 7606, *Revised Error Handling for BGP UPDATE Messages*

RFC 7607, *Codification of AS 0 Processing*

RFC 7674, *Clarification of the Flowspec Redirect Extended Community*

RFC 7752, *North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP*

RFC 7854, *BGP Monitoring Protocol (BMP)*

RFC 7911, *Advertisement of Multiple Paths in BGP*

RFC 7999, *BLACKHOLE Community*

RFC 8092, *BGP Large Communities Attribute*

RFC 8097, *BGP Prefix Origin Validation State Extended Community*

RFC 8212, *Default External BGP (EBGP) Route Propagation Behavior without Policies*

RFC 8277, *Using BGP to Bind MPLS Labels to Address Prefixes*

RFC 8571, *BGP - Link State (BGP-LS) Advertisement of IGP Traffic Engineering Performance Metric Extensions*

RFC 8950, *Advertising IPv4 Network Layer Reachability Information (NLRI) with an IPv6 Next Hop*

RFC 8955, *Dissemination of Flow Specification Rules*

RFC 8956, *Dissemination of Flow Specification Rules for IPv6*

RFC 9086, *Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing BGP Egress Peer Engineering*

8.5 Broadband Network Gateway (BNG) Control and User Plane Separation (CUPS)

3GPP 23.007, *Restoration procedures*

3GPP 29.244, *Interface between the Control Plane and the User Plane nodes*

3GPP 29.281, *General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)*

BBF TR-459, *Control and User Plane Separation for a Disaggregated BNG*

RFC 8300, *Network Service Header (NSH)*

8.6 Certificate management

RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*

RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 6712, *Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)*

RFC 7030, *Enrollment over Secure Transport*

RFC 7468, *Textual Encodings of PKIX, PKCS, and CMS Structures*

8.7 Circuit emulation

RFC 4553, *Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)*

RFC 5086, *Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)*

RFC 5287, *Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks*

8.8 Ethernet

IEEE 802.1AB, *Station and Media Access Control Connectivity Discovery*

IEEE 802.1ad, *Provider Bridges*

IEEE 802.1ag, *Connectivity Fault Management*

IEEE 802.1ah, *Provider Backbone Bridges*

IEEE 802.1ak, *Multiple Registration Protocol*

IEEE 802.1aq, *Shortest Path Bridging*

IEEE 802.1ax, *Link Aggregation*

IEEE 802.1D, *MAC Bridges*

IEEE 802.1p, *Traffic Class Expediting*

IEEE 802.1Q, *Virtual LANs*

IEEE 802.1s, *Multiple Spanning Trees*

IEEE 802.1w, *Rapid Reconfiguration of Spanning Tree*

IEEE 802.1X, *Port Based Network Access Control*

IEEE 802.3ac, *VLAN Tag*

IEEE 802.3ad, *Link Aggregation*

IEEE 802.3ah, *Ethernet in the First Mile*

IEEE 802.3x, *Ethernet Flow Control*

ITU-T G.8031/Y.1342, *Ethernet Linear Protection Switching*

ITU-T G.8032/Y.1344, *Ethernet Ring Protection Switching*

ITU-T Y.1731, *OAM functions and mechanisms for Ethernet based networks*

8.9 Ethernet VPN (EVPN)

draft-ietf-bess-evpn-ipvpn-interworking-06, *EVPN Interworking with IPVPN*

draft-ietf-bess-evpn-irb-mcast-04, *EVPN Optimized Inter-Subnet Multicast (OISM) Forwarding* – ingress replication

draft-ietf-bess-evpn-pref-df-06, *Preference-based EVPN DF Election*

draft-ietf-bess-evpn-unequal-lb-16, *Weighted Multi-Path Procedures for EVPN Multi-Homing* – section 9

draft-ietf-bess-evpn-virtual-eth-segment-06, *EVPN Virtual Ethernet Segment*

draft-ietf-bess-pbb-evpn-isid-cmacflush-00, *PBB-EVPN ISID-based CMAC-Flush*

draft-sajassi-bess-evpn-ip-aliasing-05, *EVPN Support for L3 Fast Convergence and Aliasing/Backup Path* – IP Prefix routes

RFC 7432, *BGP MPLS-Based Ethernet VPN*

RFC 7623, *Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)*

RFC 8214, *Virtual Private Wire Service Support in Ethernet VPN*

RFC 8317, *Ethernet-Tree (E-Tree) Support in Ethernet VPN (EVPN) an Provider Backbone Bridging EVPN (PBB-EVPN)*

RFC 8365, *A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)*

RFC 8560, *Seamless Integration of Ethernet VPN (EVPN) with Virtual Private LAN Service (VPLS) and Their Provider Backbone Bridge (PBB) Equivalents*

RFC 8584, *DF Election and AC-influenced DF Election*

RFC 9136, *IP Prefix Advertisement in Ethernet VPN (EVPN)*

RFC 9161, *Operational Aspects of Proxy ARP/ND in Ethernet Virtual Private Networks*

RFC 9251, *Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Proxies for Ethernet VPN (EVPN)*

8.10 gRPC Remote Procedure Calls (gRPC)

cert.proto version 0.1.0, *gRPC Network Operations Interface (gNOI) Certificate Management Service*

file.proto version 0.1.0, *gRPC Network Operations Interface (gNOI) File Service*

gnmi.proto version 0.7.0, *gRPC Network Management Interface (gNMI) Service Specification*

PROTOCOL-HTTP2, *gRPC over HTTP2*

system.proto Version 1.0.0, *gRPC Network Operations Interface (gNOI) System Service*

8.11 Intermediate System to Intermediate System (IS-IS)

draft-ietf-isis-mi-02, *IS-IS Multi-Instance*

draft-kaplan-isis-ext-eth-02, *Extended Ethernet Frame Size Support*

ISO/IEC 10589:2002 Second Edition, *Intermediate system to Intermediate system intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)*

RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*

RFC 2973, *IS-IS Mesh Groups*

RFC 3359, *Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System*

RFC 3719, *Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)*

RFC 3787, *Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)*

RFC 4971, *Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information*

RFC 5120, *M-ISIS: Multi Topology (MT) Routing in IS-IS*

RFC 5130, *A Policy Control Mechanism in IS-IS Using Administrative Tags*

RFC 5301, *Dynamic Hostname Exchange Mechanism for IS-IS*

RFC 5302, *Domain-wide Prefix Distribution with Two-Level IS-IS*

RFC 5303, *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*

RFC 5304, *IS-IS Cryptographic Authentication*

RFC 5305, *IS-IS Extensions for Traffic Engineering TE*

RFC 5306, *Restart Signaling for IS-IS* – helper mode

RFC 5307, *IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

RFC 5308, *Routing IPv6 with IS-IS*

RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*

RFC 5310, *IS-IS Generic Cryptographic Authentication*

RFC 6119, *IPv6 Traffic Engineering in IS-IS*

RFC 6213, *IS-IS BFD-Enabled TLV*

RFC 6232, *Purge Originator Identification TLV for IS-IS*

RFC 6233, *IS-IS Registry Extension for Purges*

RFC 6329, *IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging*

RFC 7775, *IS-IS Route Preference for Extended IP and IPv6 Reachability*

RFC 7794, *IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability*

RFC 7987, *IS-IS Minimum Remaining Lifetime*

RFC 8202, *IS-IS Multi-Instance* – single topology

RFC 8570, *IS-IS Traffic Engineering (TE) Metric Extensions* – Min/Max Unidirectional Link Delay metric for flex-algo, RSVP, SR-TE

RFC 8919, *IS-IS Application-Specific Link Attributes*

8.12 Internet Protocol (IP) Fast Reroute (FRR)

draft-ietf-rtgwg-lfa-manageability-08, *Operational management of Loop Free Alternates*

RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*

RFC 7431, *Multicast-Only Fast Reroute*

RFC 7490, *Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)*

RFC 8518, *Selection of Loop-Free Alternates for Multi-Homed Prefixes*

8.13 Internet Protocol (IP) general

draft-grant-tacacs-02, *The TACACS+ Protocol*

RFC 768, *User Datagram Protocol*

RFC 793, *Transmission Control Protocol*

RFC 854, *Telnet Protocol Specifications*

RFC 1350, *The TFTP Protocol (revision 2)*

RFC 2347, *TFTP Option Extension*

RFC 2348, *TFTP Blocksize Option*

RFC 2349, *TFTP Timeout Interval and Transfer Size Options*

RFC 2428, *FTP Extensions for IPv6 and NATs*

RFC 2617, *HTTP Authentication: Basic and Digest Access Authentication*

RFC 2784, *Generic Routing Encapsulation (GRE)*

RFC 2818, *HTTP Over TLS*

RFC 2890, *Key and Sequence Number Extensions to GRE*

RFC 3164, *The BSD syslog Protocol*

RFC 4250, *The Secure Shell (SSH) Protocol Assigned Numbers*

RFC 4251, *The Secure Shell (SSH) Protocol Architecture*

RFC 4252, *The Secure Shell (SSH) Authentication Protocol* – publickey, password

RFC 4253, *The Secure Shell (SSH) Transport Layer Protocol*

RFC 4254, *The Secure Shell (SSH) Connection Protocol*

RFC 4511, *Lightweight Directory Access Protocol (LDAP): The Protocol*

RFC 4513, *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms* – TLS

RFC 4632, *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*

RFC 5082, *The Generalized TTL Security Mechanism (GTSM)*

RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2* – TLS client, RSA public key

RFC 5425, *Transport Layer Security (TLS) Transport Mapping for Syslog* – RFC 3164 with TLS

RFC 5656, *Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer* – ECDSA

RFC 5925, *The TCP Authentication Option*

RFC 5926, *Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)*

RFC 6398, *IP Router Alert Considerations and Usage* – MLD

RFC 6528, *Defending against Sequence Number Attacks*

RFC 7011, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*

RFC 7012, *Information Model for IP Flow Information Export*

RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*

RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*

RFC 7232, *Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests*

RFC 7301, *Transport Layer Security (TLS) Application Layer Protocol Negotiation Extension*

RFC 7616, *HTTP Digest Access Authentication*

RFC 8446, *The Transport Layer Security (TLS) Protocol Version 1.3*

8.14 Internet Protocol (IP) multicast

cisco-ipmulticast/pim-autorp-spec01, *Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast* – version 1

draft-ietf-bier-pim-signaling-08, *PIM Signaling Through BIER Core*

draft-ietf-idmr-traceroute-ipm-07, *A "traceroute" facility for IP Multicast*

draft-ietf-l2vpn-vpls-pim-snooping-07, *Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)*

RFC 1112, *Host Extensions for IP Multicasting*

RFC 2236, *Internet Group Management Protocol, Version 2*

RFC 2365, *Administratively Scoped IP Multicast*

RFC 2375, *IPv6 Multicast Address Assignments*

RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*

RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses*

RFC 3376, *Internet Group Management Protocol, Version 3*

RFC 3446, *Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*

RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*

RFC 3618, *Multicast Source Discovery Protocol (MSDP)*

RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*

RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*

RFC 3973, *Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)* – auto-RP groups

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*

RFC 4607, *Source-Specific Multicast for IP*

RFC 4608, *Source-Specific Protocol Independent Multicast in 232/8*

RFC 4610, *Anycast-RP Using Protocol Independent Multicast (PIM)*

RFC 4611, *Multicast Source Discovery Protocol (MSDP) Deployment Scenarios*

RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*

RFC 5186, *Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction*

RFC 5384, *The Protocol Independent Multicast (PIM) Join Attribute Format*

RFC 5496, *The Reverse Path Forwarding (RPF) Vector TLV*

RFC 6037, *Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs*

RFC 6512, *Using Multipoint LDP When the Backbone Has No Route to the Root*

RFC 6513, *Multicast in MPLS/BGP IP VPNs*

RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/IP VPNs*

RFC 6515, *IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPNs*

RFC 6516, *IPv6 Multicast VPN (MVPN) Support Using PIM Control Plane and Selective Provider Multicast Service Interface (S-PMSI) Join Messages*

RFC 6625, *Wildcards in Multicast VPN Auto-Discover Routes*

RFC 6826, *Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Path*

RFC 7246, *Multipoint Label Distribution Protocol In-Band Signaling in a Virtual Routing and Forwarding (VRF) Table Context*

RFC 7385, *IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points*

RFC 7716, *Global Table Multicast with BGP Multicast VPN (BGP-MVPN) Procedures*

RFC 7761, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*

RFC 8279, *Multicast Using Bit Index Explicit Replication (BIER)*

RFC 8296, *Encapsulation for Bit Index Explicit Replication (BIER) in MPLS and Non-MPLS Networks* – MPLS encapsulation

RFC 8401, *Bit Index Explicit Replication (BIER) Support via IS-IS*

RFC 8444, *OSPFv2 Extensions for Bit Index Explicit Replication (BIER)*

RFC 8487, *Mtrace Version 2: Traceroute Facility for IP Multicast*

RFC 8534, *Explicit Tracking with Wildcard Routes in Multicast VPN* – (C-*,C-*) wildcard

RFC 8556, *Multicast VPN Using Bit Index Explicit Replication (BIER)*

8.15 Internet Protocol (IP) version 4

RFC 791, *Internet Protocol*

RFC 792, *Internet Control Message Protocol*

RFC 826, *An Ethernet Address Resolution Protocol*

RFC 951, *Bootstrap Protocol (BOOTP)* – relay

RFC 1034, *Domain Names - Concepts and Facilities*

RFC 1035, *Domain Names - Implementation and Specification*

RFC 1191, *Path MTU Discovery* – router specification

RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*

RFC 1534, *Interoperation between DHCP and BOOTP*

RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*

RFC 1812, *Requirements for IPv4 Routers*

RFC 1918, *Address Allocation for Private Internets*

RFC 2003, *IP Encapsulation within IP*

RFC 2131, *Dynamic Host Configuration Protocol*

RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

RFC 2401, *Security Architecture for Internet Protocol*

RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*

RFC 3046, *DHCP Relay Agent Information Option (Option 82)*

RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*

RFC 4884, *Extended ICMP to Support Multi-Part Messages* – ICMPv4 and ICMPv6 Time Exceeded

8.16 Internet Protocol (IP) version 6

RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*

RFC 2529, *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*

RFC 3122, *Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification*

RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

RFC 3587, *IPv6 Global Unicast Address Format*

RFC 3596, *DNS Extensions to Support IP version 6*

RFC 3633, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*

RFC 3646, *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*

RFC 3971, *SEcure Neighbor Discovery (SEND)*

RFC 3972, *Cryptographically Generated Addresses (CGA)*

RFC 4007, *IPv6 Scoped Address Architecture*

RFC 4193, *Unique Local IPv6 Unicast Addresses*

RFC 4291, *Internet Protocol Version 6 (IPv6) Addressing Architecture*

RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*

RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*

RFC 4862, *IPv6 Stateless Address Autoconfiguration* – router functions

RFC 4890, *Recommendations for Filtering ICMPv6 Messages in Firewalls*

RFC 4941, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*

RFC 5007, *DHCPv6 Leasequery*

RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*

RFC 5722, *Handling of Overlapping IPv6 Fragments*

RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6* – IPv6

RFC 5952, *A Recommendation for IPv6 Address Text Representation*

RFC 6092, *Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service* – Internet Control and Management, Upper-Layer Transport Protocols, UDP Filters, IPsec and Internet Key Exchange (IKE), TCP Filters

RFC 6106, *IPv6 Router Advertisement Options for DNS Configuration*

RFC 6164, *Using 127-Bit IPv6 Prefixes on Inter-Router Links*

RFC 6437, *IPv6 Flow Label Specification*

RFC 6603, *Prefix Exclude Option for DHCPv6-based Prefix Delegation*

RFC 8021, *Generation of IPv6 Atomic Fragments Considered Harmful*

RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*

RFC 8201, *Path MTU Discovery for IP version 6*

8.17 Internet Protocol Security (IPsec)

draft-ietf-ipsec-isakmp-mode-cfg-05, *The ISAKMP Configuration Method*

draft-ietf-ipsec-isakmp-xauth-06, *Extended Authentication within ISAKMP/Oakley (XAUTH)*

RFC 2401, *Security Architecture for the Internet Protocol*

RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*

RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*

RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*

RFC 2406, *IP Encapsulating Security Payload (ESP)*

RFC 2407, *IPsec Domain of Interpretation for ISAKMP (IPsec DoI)*

RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*

RFC 2409, *The Internet Key Exchange (IKE)*

RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*

RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*

RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman group for Internet Key Exchange (IKE)*

RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*

RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*

RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*

RFC 3947, *Negotiation of NAT-Traversal in the IKE*

RFC 3948, *UDP Encapsulation of IPsec ESP Packets*

RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec ESP*

RFC 4109, *Algorithms for Internet Key Exchange version 1 (IKEv1)*

RFC 4301, *Security Architecture for the Internet Protocol*

RFC 4303, *IP Encapsulating Security Payload*

RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*

RFC 4308, *Cryptographic Suites for IPsec*

RFC 4434, *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*

RFC 4543, *The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH*

RFC 4754, *IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*

RFC 4835, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*

RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*

RFC 4945, *The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2 and PKIX*

RFC 5019, *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*

RFC 5282, *Using Authenticated Encryption Algorithms with the Encrypted Payload of the IKEv2 Protocol*

RFC 5903, *ECP Groups for IKE and IKEv2*

RFC 5996, *Internet Key Exchange Protocol Version 2 (IKEv2)*

RFC 5998, *An Extension for EAP-Only Authentication in IKEv2*

RFC 6379, *Suite B Cryptographic Suites for IPsec*

RFC 6380, *Suite B Profile for Internet Protocol Security (IPsec)*

RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*

RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2)*

RFC 7321, *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*

RFC 7383, *Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation*

RFC 7427, *Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)*

8.18 Label Distribution Protocol (LDP)

draft-pdutta-mpls-ldp-adj-capability-00, *LDP Adjacency Capabilities*

draft-pdutta-mpls-ldp-v2-00, *LDP Version 2*

draft-pdutta-mpls-mldp-up-redundancy-00, *Upstream LSR Redundancy for Multi-point LDP Tunnels*

draft-pdutta-mpls-multi-ldp-instance-00, *Multiple LDP Instances*

draft-pdutta-mpls-tldp-hello-reduce-04, *Targeted LDP Hello Reduction*

RFC 3037, *LDP Applicability*

RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol* – helper mode

RFC 5036, *LDP Specification*

RFC 5283, *LDP Extension for Inter-Area Label Switched Paths (LSPs)*

RFC 5443, *LDP IGP Synchronization*

RFC 5561, *LDP Capabilities*

RFC 5919, *Signaling LDP Label Advertisement Completion*

RFC 6388, *Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

RFC 6512, *Using Multipoint LDP When the Backbone Has No Route to the Root*

RFC 6826, *Multipoint LDP in-band signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

RFC 7032, *LDP Downstream-on-Demand in Seamless MPLS*

RFC 7473, *Controlling State Advertisements of Non-negotiated LDP Applications*

RFC 7552, *Updates to LDP for IPv6*

8.19 Layer Two Tunneling Protocol (L2TP) Network Server (LNS)

draft-mammoliti-l2tp-accessline-avp-04, *Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions*

RFC 2661, *Layer Two Tunneling Protocol "L2TP"*

RFC 2809, *Implementation of L2TP Compulsory Tunneling via RADIUS*

RFC 3438, *Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers: Internet Assigned Numbers Authority (IANA) Considerations Update*

RFC 3931, *Layer Two Tunneling Protocol - Version 3 (L2TPv3)*

RFC 4719, *Transport of Ethernet Frames over Layer 2 Tunneling Protocol Version 3 (L2TPv3)*

RFC 4951, *Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover"*

8.20 Multiprotocol Label Switching (MPLS)

draft-ietf-mpls-lsp-ping-ospfv3-codepoint-02, *OSPFv3 CodePoint for MPLS LSP Ping*

RFC 3031, *Multiprotocol Label Switching Architecture*

RFC 3032, *MPLS Label Stack Encoding*

RFC 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services* – E-LSP

RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*

RFC 4023, *Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)*

RFC 4182, *Removing a Restriction on the use of MPLS Explicit NULL*

RFC 5332, *MPLS Multicast Encapsulations*

RFC 5884, *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*

RFC 6374, *Packet Loss and Delay Measurement for MPLS Networks* – Delay Measurement, Channel Type 0x000C

RFC 6424, *Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels*

RFC 6425, *Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping*

RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

RFC 7510, *Encapsulating MPLS in UDP*

RFC 7746, *Label Switched Path (LSP) Self-Ping*

RFC 7876, *UDP Return Path for Packet Loss and Delay Measurement for MPLS Networks* – Delay Measurement

RFC 8029, *Detecting Multiprotocol Label Switched (MPLS) Data-Plane Failures*

8.21 Multiprotocol Label Switching - Transport Profile (MPLS-TP)

RFC 5586, *MPLS Generic Associated Channel*

RFC 5921, *A Framework for MPLS in Transport Networks*

RFC 5960, *MPLS Transport Profile Data Plane Architecture*

RFC 6370, *MPLS Transport Profile (MPLS-TP) Identifiers*

RFC 6378, *MPLS Transport Profile (MPLS-TP) Linear Protection*

RFC 6426, *MPLS On-Demand Connectivity and Route Tracing*

RFC 6427, *MPLS Fault Management Operations, Administration, and Maintenance (OAM)*

RFC 6428, *Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile*

RFC 6478, *Pseudowire Status for Static Pseudowires*

RFC 7213, *MPLS Transport Profile (MPLS-TP) Next-Hop Ethernet Addressing*

8.22 Network Address Translation (NAT)

draft-ietf-behave-address-format-10, *IPv6 Addressing of IPv4/IPv6 Translators*

draft-ietf-behave-v6v4-xlate-23, *IP/ICMP Translation Algorithm*

draft-miles-behave-l2nat-00, *Layer2-Aware NAT*

draft-nishitani-cgn-02, *Common Functions of Large Scale NAT (LSN)*

RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*

RFC 5382, *NAT Behavioral Requirements for TCP*

RFC 5508, *NAT Behavioral Requirements for ICMP*

RFC 6146, *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*

RFC 6333, *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*

RFC 6334, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite*

RFC 6887, *Port Control Protocol (PCP)*

RFC 6888, *Common Requirements For Carrier-Grade NATs (CGNs)*

RFC 7753, *Port Control Protocol (PCP) Extension for Port-Set Allocation*

RFC 7915, *IP/ICMP Translation Algorithm*

8.23 Network Configuration Protocol (NETCONF)

RFC 5277, *NETCONF Event Notifications*

RFC 6020, *YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)*

RFC 6022, *YANG Module for NETCONF Monitoring*

RFC 6241, *Network Configuration Protocol (NETCONF)*

RFC 6242, *Using the NETCONF Protocol over Secure Shell (SSH)*

RFC 6243, *With-defaults Capability for NETCONF*

RFC 8342, *Network Management Datastore Architecture (NMDA)* – Startup, Candidate, Running and Intended datastores

RFC 8525, *YANG Library*

RFC 8526, *NETCONF Extensions to Support the Network Management Datastore Architecture* – <get-data> operation

8.24 Open Shortest Path First (OSPF)

RFC 1765, *OSPF Database Overflow*

RFC 2328, *OSPF Version 2*

RFC 3101, *The OSPF Not-So-Stubby Area (NSSA) Option*

RFC 3509, *Alternative Implementations of OSPF Area Border Routers*

RFC 3623, *Graceful OSPF Restart Graceful OSPF Restart* – helper mode

RFC 3630, *Traffic Engineering (TE) Extensions to OSPF Version 2*

RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

RFC 4222, *Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance*

RFC 4552, *Authentication/Confidentiality for OSPFv3*

RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 5185, *OSPF Multi-Area Adjacency*

RFC 5187, *OSPFv3 Graceful Restart* – helper mode

RFC 5243, *OSPF Database Exchange Summary List Optimization*

RFC 5250, *The OSPF Opaque LSA Option*

RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*

RFC 5340, *OSPF for IPv6*

RFC 5642, *Dynamic Hostname Exchange Mechanism for OSPF*

RFC 5709, *OSPFv2 HMAC-SHA Cryptographic Authentication*

RFC 5838, *Support of Address Families in OSPFv3*

RFC 6549, *OSPFv2 Multi-Instance Extensions*

RFC 6987, *OSPF Stub Router Advertisement*

RFC 7471, *OSPF Traffic Engineering (TE) Metric Extensions* – Min/Max Unidirectional Link Delay metric for flex-algo, RSVP, SR-TE

RFC 7684, *OSPFv2 Prefix/Link Attribute Advertisement*

RFC 7770, *Extensions to OSPF for Advertising Optional Router Capabilities*

RFC 8362, *OSPFv3 Link State Advertisement (LSA) Extensibility*

RFC 8920, *OSPF Application-Specific Link Attributes*

8.25 OpenFlow

TS-007 Version 1.3.1, *OpenFlow Switch Specification* – OpenFlow-hybrid switches

8.26 Path Computation Element Protocol (PCEP)

draft-ietf-pce-binding-label-sid-15, *Carrying Binding Label/Segment Identifier (SID) in PCE-based Networks.* – MPLS binding SIDs

draft-alvarez-pce-path-profiles-04, *PCE Path Profiles*

draft-dhs-spring-pce-sr-p2mp-policy-00, *PCEP extensions for p2mp sr policy*

RFC 5440, *Path Computation Element (PCE) Communication Protocol (PCEP)*

RFC 8231, *Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE*

RFC 8281, *PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model*

RFC 8408, *Conveying Path Setup Type in PCE Communication Protocol (PCEP) Messages*

RFC 8664, *Path Computation Element Communication Protocol (PCEP) Extensions for Segment Routing*

8.27 Point-to-Point Protocol (PPP)

RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*

RFC 1377, *The PPP OSI Network Layer Control Protocol (OSINLCP)*

RFC 1661, *The Point-to-Point Protocol (PPP)*

RFC 1662, *PPP in HDLC-like Framing*

RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*

RFC 1989, *PPP Link Quality Monitoring*

RFC 1990, *The PPP Multilink Protocol (MP)*

RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*

RFC 2153, *PPP Vendor Extensions*

RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*

RFC 2615, *PPP over SONET/SDH*

RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

RFC 2878, *PPP Bridging Control Protocol (BCP)*

RFC 4638, *Accommodating a Maximum Transit Unit/Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)*

RFC 5072, *IP Version 6 over PPP*

8.28 Policy management and credit control

3GPP TS 29.212 Release 11, *Policy and Charging Control (PCC); Reference points* – Gx support as it applies to wireline environment (BNG)

RFC 4006, *Diameter Credit-Control Application*

RFC 6733, *Diameter Base Protocol*

8.29 Pseudowire (PW)

draft-ietf-l2vpn-vpws-iw-oam-04, *OAM Procedures for VPWS Interworking*

MFA Forum 12.0.0, *Multiservice Interworking - Ethernet over MPLS*

MFA Forum 13.0.0, *Fault Management for Multiservice Interworking v1.0*

MFA Forum 16.0.0, *Multiservice Interworking - IP over MPLS*

RFC 3916, *Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)*

RFC 3985, *Pseudo Wire Emulation Edge-to-Edge (PWE3)*

RFC 4385, *Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*

RFC 4446, *IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)*

RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*

RFC 5085, *Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires*

RFC 5659, *An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge*

RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*

RFC 6073, *Segmented Pseudowire*

RFC 6310, *Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping*

RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*

RFC 6575, *Address Resolution Protocol (ARP) Mediation for IP Interworking of Layer 2 VPNs*

RFC 6718, *Pseudowire Redundancy*

RFC 6829, *Label Switched Path (LSP) Ping for Pseudowire Forwarding Equivalence Classes (FECs) Advertised over IPv6*

RFC 6870, *Pseudowire Preferential Forwarding Status bit*

RFC 7023, *MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking*

RFC 7267, *Dynamic Placement of Multi-Segment Pseudowires*

RFC 7392, *Explicit Path Routing for Dynamic Multi-Segment Pseudowires* – ER-TLV and ER-HOP IPv4 Prefix

RFC 8395, *Extensions to BGP-Signaled Pseudowires to Support Flow-Aware Transport Labels*

8.30 Quality of Service (QoS)

RFC 2430, *A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)*

RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*

RFC 2597, *Assured Forwarding PHB Group*

RFC 3140, *Per Hop Behavior Identification Codes*

RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*

8.31 Remote Authentication Dial In User Service (RADIUS)

draft-oscca-cfrg-sm3-02, *The SM3 Cryptographic Hash Function*

RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*

RFC 2866, *RADIUS Accounting*

RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*

RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

RFC 2869, *RADIUS Extensions*

RFC 3162, *RADIUS and IPv6*

RFC 4818, *RADIUS Delegated-IPv6-Prefix Attribute*

RFC 5176, *Dynamic Authorization Extensions to RADIUS*

RFC 6613, *RADIUS over TCP* – with TLS

RFC 6614, *Transport Layer Security (TLS) Encryption for RADIUS*

RFC 6929, *Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions*

RFC 6911, *RADIUS attributes for IPv6 Access Networks*

8.32 Resource Reservation Protocol - Traffic Engineering (RSVP-TE)

draft-newton-mpls-te-dynamic-overbooking-00, *A Diffserv-TE Implementation Model to dynamically change booking factors during failure events*

RFC 2702, *Requirements for Traffic Engineering over MPLS*

RFC 2747, *RSVP Cryptographic Authentication*

RFC 2961, *RSVP Refresh Overhead Reduction Extensions*

RFC 3097, *RSVP Cryptographic Authentication -- Updated Message Type Value*

RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*

RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions* – IF_ID RSVP_HOP object with unnumbered interfaces and RSVP-TE graceful restart helper procedures

RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*

RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*

RFC 3906, *Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels*

RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*

RFC 4124, *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering*

RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*

RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*

RFC 4561, *Definition of a Record Route Object (RRO) Node-Id Sub-Object*

RFC 4875, *Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)*

RFC 4950, *ICMP Extensions for Multiprotocol Label Switching*

RFC 5151, *Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*

RFC 5712, *MPLS Traffic Engineering Soft Preemption*

RFC 5817, *Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks*

8.33 Routing Information Protocol (RIP)

RFC 1058, *Routing Information Protocol*

RFC 2080, *RIPng for IPv6*

RFC 2082, *RIP-2 MD5 Authentication*

RFC 2453, *RIP Version 2*

8.34 Segment Routing (SR)

draft-bashandy-rtgwg-segment-routing-uloop-06, *Loop avoidance using Segment Routing*

draft-filsfils-spring-net-pgm-extension-srv6-usid-13, *Network Programming extension: SRv6 uSID instruction*

draft-filsfils-spring-srv6-net-pgm-insertion-04, *SRv6 NET-PGM extension: Insertion*

draft-ietf-6man-spring-srv6-oam-10, *Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Data plane (SRv6)*

draft-ietf-idr-bgp-ls-segment-routing-ext-16, *BGP Link-State extensions for Segment Routing*

draft-ietf-idr-segment-routing-te-policy-11, *Advertising Segment Routing Policies in BGP*

draft-ietf-isis-mpls-elc-10, *Signaling Entropy Label Capability and Entropy Readable Label Depth Using IS-IS* – advertising ELC

draft-ietf-lsr-flex-algo-16, *IGP Flexible Algorithm*

draft-ietf-lsr-isis-srv6-extensions-14, *IS-IS Extension to Support Segment Routing over IPv6 Dataplane*

draft-ietf-ospf-mpls-elc-12, *Signaling Entropy Label Capability and Entropy Readable Label-stack Depth Using OSPF* – advertising ELC

draft-ietf-rtgwg-segment-routing-ti-lfa-01, *Topology Independent Fast Reroute using Segment Routing*

draft-ietf-spring-conflict-resolution-05, *Segment Routing MPLS Conflict Resolution*

draft-ietf-spring-segment-routing-policy-08, *Segment Routing Policy Architecture*

draft-ietf-teas-sr-rsvp-coexistence-rec-02, *Recommendations for RSVP-TE and Segment Routing LSP co-existence*

draft-voyer-6man-extension-header-insertion-10, *Deployments With Insertion of IPv6 Segment Routing Headers*

draft-voyer-pim-sr-p2mp-policy-02, *Segment Routing Point-to-Multipoint Policy*

draft-voyer-spring-sr-p2mp-policy-03, *SR Replication Policy for P2MP Service Delivery*

RFC 8287, *Label Switched Path (LSP) Ping/Traceroute for Segment Routing (SR) IGP-Prefix and IGP-Adjacency Segment Identifiers (SIDs) with MPLS Data Planes*

RFC 8476, *Signaling Maximum SID Depth (MSD) Using OSPF* – node MSD

RFC 8491, *Signaling Maximum SID Depth (MSD) Using IS-IS* – node MSD

RFC 8660, *Segment Routing with the MPLS Data Plane*

RFC 8661, *Segment Routing MPLS Interworking with LDP*

RFC 8663, *MPLS Segment Routing over IP* – BGP SR with SR-MPLS-over-UDP/IP

RFC 8665, *OSPF Extensions for Segment Routing*

RFC 8666, *OSPFv3 Extensions for Segment Routing*

RFC 8667, *IS-IS Extensions for Segment Routing*

RFC 8669, *Segment Routing Prefix Segment Identifier Extensions for BGP*

RFC 8754, *IPv6 Segment Routing Header (SRH)*

RFC 8814, *Signaling Maximum SID Depth (MSD) Using the Border Gateway Protocol - Link State*

RFC 8986, *Segment Routing over IPv6 (SRv6) Network Programming*

RFC 9252, *BGP Overlay Services Based on Segment Routing over IPv6 (SRv6)*

8.35 Simple Network Management Protocol (SNMP)

draft-blumenthal-aes-usm-04, *The AES Cipher Algorithm in the SNMP's User-based Security Model* – CFB128-AES-192 and CFB128-AES-256

draft-ietf-isis-wg-mib-06, *Management Information Base for Intermediate System to Intermediate System (IS-IS)*

draft-ietf-mboned-msdp-mib-01, *Multicast Source Discovery protocol MIB*

draft-ietf-mpls-ldp-mib-07, *Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP)*

draft-ietf-mpls-lsr-mib-06, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base Using SMIv2*

draft-ietf-mpls-te-mib-04, *Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base*

draft-ietf-ospf-mib-update-08, *OSPF Version 2 Management Information Base*

draft-ietf-vrrp-unified-mib-06, *Definitions of Managed Objects for the VRRP over IPv4 and IPv6* – IPv6

ESO-CONSORTIUM-MIB revision 200406230000Z, *esoConsortiumMIB*

IANA-ADDRESS-FAMILY-NUMBERS-MIB revision 200203140000Z, *ianaAddressFamilyNumbers*

IANAifType-MIB revision 200505270000Z, *ianaifType*

IANA-RTPROTO-MIB revision 200009260000Z, *ianaRtProtoMIB*

IEEE8021-CFM-MIB revision 200706100000Z, *ieee8021CfmMib*

IEEE8021-PAE-MIB revision 200101160000Z, *ieee8021paeMIB*

IEEE8023-LAG-MIB revision 200006270000Z, *lagMIB*

LLDP-MIB revision 200505060000Z, *lldpMIB*

RFC 1157, *A Simple Network Management Protocol (SNMP)*

RFC 1212, *Concise MIB Definitions*

RFC 1215, *A Convention for Defining Traps for use with the SNMP*

RFC 1724, *RIP Version 2 MIB Extension*

RFC 1901, *Introduction to Community-based SNMPv2*

RFC 2021, *Remote Network Monitoring Management Information Base Version 2 using SMIv2*

RFC 2206, *RSVP Management Information Base using SMIv2*

RFC 2213, *Integrated Services Management Information Base using SMIv2*

RFC 2494, *Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type*

RFC 2578, *Structure of Management Information Version 2 (SMIv2)*

RFC 2579, *Textual Conventions for SMIv2*

RFC 2580, *Conformance Statements for SMIv2*

RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*

RFC 2819, *Remote Network Monitoring Management Information Base*

RFC 2856, *Textual Conventions for Additional High Capacity Data Types*

RFC 2863, *The Interfaces Group MIB*

RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*

RFC 2933, *Internet Group Management Protocol MIB*

RFC 3014, *Notification Log MIB*

RFC 3165, *Definitions of Managed Objects for the Delegation of Management Scripts*

RFC 3231, *Definitions of Managed Objects for Scheduling Management Operations*

RFC 3273, *Remote Network Monitoring Management Information Base for High Capacity Networks*

RFC 3410, *Introduction and Applicability Statements for Internet Standard Management Framework*

RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*

RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*

RFC 3413, *Simple Network Management Protocol (SNMP) Applications*

RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*

RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)* – SNMP over UDP over IPv4

RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

RFC 3419, *Textual Conventions for Transport Addresses*

RFC 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures*

RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

RFC 3592, *Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type*

RFC 3593, *Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals*

RFC 3635, *Definitions of Managed Objects for the Ethernet-like Interface Types*

RFC 3637, *Definitions of Managed Objects for the Ethernet WAN Interface Sublayer*

RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

RFC 3877, *Alarm Management Information Base (MIB)*

RFC 3895, *Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types*

RFC 3896, *Definitions of Managed Objects for the DS3/E3 Interface Type*

RFC 4001, *Textual Conventions for Internet Network Addresses*

RFC 4022, *Management Information Base for the Transmission Control Protocol (TCP)*

RFC 4113, *Management Information Base for the User Datagram Protocol (UDP)*

RFC 4220, *Traffic Engineering Link Management Information Base*

RFC 4273, *Definitions of Managed Objects for BGP-4*

RFC 4292, *IP Forwarding Table MIB*

RFC 4293, *Management Information Base for the Internet Protocol (IP)*

RFC 4631, *Link Management Protocol (LMP) Management Information Base (MIB)*

RFC 4878, *Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on Ethernet-Like Interfaces*

RFC 7420, *Path Computation Element Communication Protocol (PCEP) Management Information Base (MIB) Module*

RFC 7630, *HMAC-SHA-2 Authentication Protocols in the User-based Security Model (USM) for SNMPv3*

SFLOW-MIB revision 200309240000Z, *sFlowMIB*

8.36 Timing

GR-1244-CORE Issue 3, *Clocks for the Synchronized Network: Common Generic Criteria*

GR-253-CORE Issue 3, *SONET Transport Systems: Common Generic Criteria*

IEEE 1588-2008, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*

ITU-T G.781, *Synchronization layer functions*

ITU-T G.813, *Timing characteristics of SDH equipment slave clocks (SEC)*

ITU-T G.8261, *Timing and synchronization aspects in packet networks*

ITU-T G.8262, *Timing characteristics of synchronous Ethernet equipment slave clock (EEC)*

ITU-T G.8262.1, *Timing characteristics of an enhanced synchronous Ethernet equipment slave clock (eEEC)*

ITU-T G.8264, *Distribution of timing information through packet networks*

ITU-T G.8265.1, *Precision time protocol telecom profile for frequency synchronization*

ITU-T G.8275.1, *Precision time protocol telecom profile for phase/time synchronization with full timing support from the network*

RFC 3339, *Date and Time on the Internet: Timestamps*

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*

8.37 Two-Way Active Measurement Protocol (TWAMP)

RFC 5357, *A Two-Way Active Measurement Protocol (TWAMP)* – server, unauthenticated mode

RFC 5938, *Individual Session Control Feature for the Two-Way Active Measurement Protocol (TWAMP)*

RFC 6038, *Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features*

RFC 8545, *Well-Known Port Assignments for the One-Way Active Measurement Protocol (OWAMP) and the Two-Way Active Measurement Protocol (TWAMP)* – TWAMP

RFC 8762, *Simple Two-Way Active Measurement Protocol* – unauthenticated

RFC 8972, *Simple Two-Way Active Measurement Protocol Optional Extensions* – unauthenticated

8.38 Virtual Private LAN Service (VPLS)

RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*

RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*

RFC 5501, *Requirements for Multicast Support in Virtual Private LAN Services*

RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*

RFC 7041, *Extensions to the Virtual Private LAN Service (VPLS) Provider Edge (PE) Model for Provider Backbone Bridging*

RFC 7117, *Multicast in Virtual Private LAN Service (VPLS)*

8.39 Voice and video

DVB BlueBook A86, *Transport of MPEG-2 TS Based DVB Services over IP Based Networks*

ETSI TS 101 329-5 Annex E, *QoS Measurement for VoIP - Method for determining an Equipment Impairment Factor using Passive Monitoring*

ITU-T G.1020 Appendix I, *Performance Parameter Definitions for Quality of Speech and other Voiceband Applications Utilizing IP Networks - Mean Absolute Packet Delay Variation & Markov Models*

ITU-T G.107, *The E Model - A computational model for use in planning*

ITU-T P.564, *Conformance testing for voice over IP transmission quality assessment models*

RFC 3550, *RTP: A Transport Protocol for Real-Time Applications* – Appendix A.8

RFC 4585, *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*

RFC 4588, *RTP Retransmission Payload Format*

8.40 Wireless Local Area Network (WLAN) gateway

3GPP TS 23.402, *Architecture enhancements for non-3GPP accesses* – S2a roaming based on GPRS

8.41 Yet Another Next Generation (YANG)

RFC 6991, *Common YANG Data Types*

RFC 7950, *The YANG 1.1 Data Modeling Language*

RFC 7951, *JSON Encoding of Data Modeled with YANG*

8.42 Yet Another Next Generation (YANG) OpenConfig Modules

openconfig-aaa.yang version 0.4.0, *OpenConfig AAA Module*

openconfig-aaa-radius.yang version 0.3.0, *OpenConfig AAA RADIUS Module*

openconfig-aaa-tacacs.yang version 0.3.0, *OpenConfig AAA TACACS+ Module*

openconfig-acl.yang version 1.0.0, *OpenConfig ACL Module*

openconfig-bfd.yang version 0.1.0, *OpenConfig BFD Module*

openconfig-bgp.yang version 3.0.1, *OpenConfig BGP Module*

openconfig-bgp-common.yang version 3.0.1, *OpenConfig BGP Common Module*

openconfig-bgp-common-multiprotocol.yang version 3.0.1, *OpenConfig BGP Common Multiprotocol Module*

openconfig-bgp-common-structure.yang version 3.0.1, *OpenConfig BGP Common Structure Module*

openconfig-bgp-global.yang version 3.0.1, *OpenConfig BGP Global Module*

openconfig-bgp-neighbor.yang version 3.0.1, *OpenConfig BGP Neighbor Module*

openconfig-bgp-peer-group.yang version 3.0.1, *OpenConfig BGP Peer Group Module*

openconfig-bgp-policy.yang version 4.0.1, *OpenConfig BGP Policy Module*

openconfig-if-aggregate.yang version 2.0.0, *OpenConfig Interfaces Aggregated Module*

openconfig-if-ethernet.yang version 2.0.0, *OpenConfig Interfaces Ethernet Module*

openconfig-if-ip.yang version 2.0.0, *OpenConfig Interfaces IP Module*

openconfig-if-ip-ext.yang version 2.0.0, *OpenConfig Interfaces IP Extensions Module*

openconfig-igmp.yang version 0.2.0, *OpenConfig IGMP Module*

openconfig-interfaces.yang version 2.0.0, *OpenConfig Interfaces Module*

openconfig-isis.yang version 0.3.2, *OpenConfig IS-IS Module*

openconfig-isis-policy.yang version 0.3.2, *OpenConfig IS-IS Policy Module*

openconfig-isis-routing.yang version 0.3.2, *OpenConfig IS-IS Routing Module*

openconfig-lacp.yang version 1.1.0, *OpenConfig LACP Module*

openconfig-lldp.yang version 0.1.0, *OpenConfig LLDP Module*

openconfig-local-routing.yang version 1.0.1, *OpenConfig Local Routing Module*

openconfig-mpls.yang version 2.3.0, *OpenConfig MPLS Module*

openconfig-mpls-ldp.yang version 3.0.2, *OpenConfig MPLS LDP Module*

openconfig-mpls-rsvp.yang version 2.3.0, *OpenConfig MPLS RSVP Module*

openconfig-mpls-te.yang version 2.3.0, *OpenConfig MPLS TE Module*

openconfig-network-instance.yang version 1.1.0, *OpenConfig Network Instance Module*

openconfig-network-instance-l3.yang version 0.11.1, *OpenConfig L3 Network Instance Module* – static routes

openconfig-packet-match.yang version 1.0.0, *OpenConfig Packet Match Module*

openconfig-pim.yang version 0.2.0 *OpenConfig PIM Module*

openconfig-platform.yang version 0.12.2, *OpenConfig Platform Module*

openconfig-platform-fan.yang version 0.1.1, *OpenConfig Platform Fan Module*

openconfig-platform-linecard.yang version 0.1.2, *OpenConfig Platform Linecard Module*

openconfig-platform-port.yang version 0.3.3, *OpenConfig Port Module*

openconfig-platform-transceiver.yang version 0.7.1, *OpenConfig Transceiver Module*

openconfig-procmon.yang version 0.4.0, *OpenConfig Process Monitoring Module*

openconfig-relay-agent.yang version 0.1.0, *OpenConfig Relay Agent Module*

openconfig-routing-policy.yang version 3.0.0, *OpenConfig Routing Policy Module*

openconfig-rsvp-sr-ext.yang version 0.1.0, *OpenConfig RSVP-TE and SR Extensions Module*

openconfig-system.yang version 0.9.1, *OpenConfig System Module*

openconfig-system-logging.yang version 0.3.1, *OpenConfig System Logging Module*

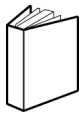
openconfig-system-terminal.yang version 0.3.0, *OpenConfig System Terminal Module*

openconfig-telemetry.yang version 0.5.0, *OpenConfig Telemetry Module*

openconfig-terminal-device.yang version 1.7.3, *OpenConfig Terminal Optics Device Module*

openconfig-vlan.yang version 2.0.0, *OpenConfig VLAN Module*

Customer document and product support



Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback