



7750 Service Router Virtualized Service Router

Release 23.3.R1

Gy AVPs Reference Guide

3HE 19219 AAAA TQZZA 01
Edition 01
March 2023

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.

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

© 2023 Nokia.

Table of contents

| | | |
|----------|---|----------|
| 1 | Getting started..... | 6 |
| 1.1 | About this guide..... | 6 |
| 1.1.1 | Audience..... | 6 |
| 1.1.2 | References..... | 6 |
| 2 | Diameter Gy interface specification..... | 7 |
| 2.1 | Diameter Gy – Credit-Control-Request (CCR) command..... | 7 |
| 2.1.1 | Diameter Gy – CCR message top level AVPs..... | 8 |
| 2.1.2 | Diameter Gy – CCR message grouped AVPs..... | 25 |
| 2.1.2.1 | Diameter Gy CCR – Subscription-Id grouped AVP..... | 25 |
| 2.1.2.2 | Diameter Gy CCR – Multiple-Services-Credit-Control grouped AVP..... | 27 |
| 2.1.2.3 | Diameter Gy CCR – Requested-Service-Unit grouped AVP..... | 28 |
| 2.1.2.4 | Diameter Gy CCR – Used-Service-Unit grouped AVP..... | 28 |
| 2.1.2.5 | DIAMETER Gy CCR - User-Equipment-Info grouped AVP..... | 30 |
| 2.1.2.6 | Diameter Gy CCR – Service-Information grouped AVP..... | 31 |
| 2.1.2.7 | Diameter Gy CCR – PS-Information grouped AVP..... | 32 |
| 2.2 | Diameter Gy – Credit-Control-Answer (CCA) command..... | 33 |
| 2.2.1 | Diameter Gy – CCA message top level AVPs..... | 33 |
| 2.2.2 | Diameter Gy – CCA message grouped AVPs..... | 37 |
| 2.2.2.1 | Diameter Gy CCA – Failed-AVP grouped AVP..... | 37 |
| 2.2.2.2 | Diameter Gy CCA – Multiple-Services-Credit-Control grouped AVP..... | 37 |
| 2.2.2.3 | Diameter Gy CCA – Final-Unit-Indication grouped AVP..... | 39 |
| 2.2.2.4 | DIAMETER Gy CCA - Redirect-Server grouped AVP..... | 41 |
| 2.2.2.5 | Diameter Gy CCA – Granted-Service-Unit grouped AVP..... | 42 |
| 2.3 | Diameter Gy – Re-Auth-Request (RAR) command..... | 43 |
| 2.3.1 | Diameter Gy – RAR message format..... | 43 |
| 2.3.2 | Diameter Gy – RAR message top level AVPs..... | 44 |
| 2.4 | Diameter Gy – Re-Auth-Answer (RAA) command..... | 45 |
| 2.4.1 | Diameter Gy – RAA message format..... | 45 |
| 2.4.2 | Diameter Gy – RAA message top level AVPs..... | 45 |
| 2.5 | Diameter Gy – Abort-Session-Request (ASR) command..... | 47 |
| 2.5.1 | Diameter Gy – ASR message format..... | 47 |
| 2.5.2 | Diameter Gy – ASR message top level AVPs..... | 47 |

| | | |
|----------|---|-----------|
| 2.6 | Diameter Gy – Abort-Session-Answer (ASA) command..... | 48 |
| 2.6.1 | Diameter Gy – ASA message format..... | 48 |
| 2.6.2 | Diameter Gy – ASA message top level AVPs..... | 49 |
| 3 | Standards and protocol support..... | 51 |
| 3.1 | Access Node Control Protocol (ANCP)..... | 51 |
| 3.2 | Bidirectional Forwarding Detection (BFD)..... | 51 |
| 3.3 | Border Gateway Protocol (BGP)..... | 51 |
| 3.4 | Broadband Network Gateway (BNG) Control and User Plane Separation (CUPS)..... | 53 |
| 3.5 | Certificate management..... | 53 |
| 3.6 | Circuit emulation..... | 54 |
| 3.7 | Ethernet..... | 54 |
| 3.8 | Ethernet VPN (EVPN)..... | 54 |
| 3.9 | gRPC Remote Procedure Calls (gRPC)..... | 55 |
| 3.10 | Intermediate System to Intermediate System (IS-IS)..... | 55 |
| 3.11 | Internet Protocol (IP) Fast Reroute (FRR)..... | 57 |
| 3.12 | Internet Protocol (IP) general..... | 57 |
| 3.13 | Internet Protocol (IP) multicast..... | 58 |
| 3.14 | Internet Protocol (IP) version 4..... | 60 |
| 3.15 | Internet Protocol (IP) version 6..... | 60 |
| 3.16 | Internet Protocol Security (IPsec)..... | 61 |
| 3.17 | Label Distribution Protocol (LDP)..... | 62 |
| 3.18 | Layer Two Tunneling Protocol (L2TP) Network Server (LNS)..... | 63 |
| 3.19 | Multiprotocol Label Switching (MPLS)..... | 63 |
| 3.20 | Multiprotocol Label Switching - Transport Profile (MPLS-TP)..... | 64 |
| 3.21 | Network Address Translation (NAT)..... | 64 |
| 3.22 | Network Configuration Protocol (NETCONF)..... | 65 |
| 3.23 | Open Shortest Path First (OSPF)..... | 65 |
| 3.24 | OpenFlow..... | 66 |
| 3.25 | Path Computation Element Protocol (PCEP)..... | 66 |
| 3.26 | Point-to-Point Protocol (PPP)..... | 67 |
| 3.27 | Policy management and credit control..... | 67 |
| 3.28 | Pseudowire (PW)..... | 67 |
| 3.29 | Quality of Service (QoS)..... | 68 |
| 3.30 | Remote Authentication Dial In User Service (RADIUS)..... | 68 |
| 3.31 | Resource Reservation Protocol - Traffic Engineering (RSVP-TE)..... | 69 |

| | | |
|------|--|----|
| 3.32 | Routing Information Protocol (RIP)..... | 69 |
| 3.33 | Segment Routing (SR)..... | 69 |
| 3.34 | Simple Network Management Protocol (SNMP)..... | 71 |
| 3.35 | Timing..... | 73 |
| 3.36 | Two-Way Active Measurement Protocol (TWAMP)..... | 73 |
| 3.37 | Virtual Private LAN Service (VPLS)..... | 74 |
| 3.38 | Voice and video..... | 74 |
| 3.39 | Wireless Local Area Network (WLAN) gateway..... | 74 |
| 3.40 | Yet Another Next Generation (YANG)..... | 74 |
| 3.41 | Yet Another Next Generation (YANG) OpenConfig Modules..... | 75 |

1 Getting started

1.1 About this guide

This document details the Diameter Gy interface specification. The Diameter Gy application is also referred to as Diameter Credit Control Application (DCCA).

The tables in this document provide Attribute Value Pair (AVP) details organized per message type.

The SR OS also provides a Diameter Python interface that enables flexible insertion, deletion, and formatting of AVPs received from and sent to a Diameter application server. For more information about the Diameter Python API, see the *7450 ESS, 7750 SR, and VSR Triple Play Service Delivery Architecture Guide*.

**Note:**

Unless otherwise indicated, CLI commands, contexts, and configuration examples in this guide apply for both the classic CLI and the MD-CLI.

1.1.1 Audience

This document is intended for network administrators who are responsible for configuring and operating 7750 SR and VSR service routers and using Diameter applications. It is assumed that the network administrators have an understanding of networking principles and configurations, routing processes, protocols, and standards.

1.1.2 References

RFC 2865, "Remote Authentication Dial In User Service (RADIUS)", June 2000

RFC 4006, "Diameter Credit-Control Application", August 2005

RFC 6733, "Diameter Base Protocol", October 2012

3GPP TS 32.299 v9.4.0, "Diameter charging applications", June 2010

7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide

2 Diameter Gy interface specification

[Table 1: Diameter Gy application messages](#) provides a summary of the Diameter Gy application messages.

Table 1: Diameter Gy application messages

| Diameter message | | Code | RFC |
|------------------|------------------------|------|----------|
| CCR | Credit-Control-Request | 272 | RFC 4006 |
| CCA | Credit-Control-Answer | 272 | RFC 4006 |
| RAR | Re-Auth-Request | 258 | RFC 6733 |
| RAA | Re-Auth-Answer | 258 | RFC 6733 |
| ASR | Abort-Session-Request | 274 | RFC 6733 |
| ASA | Abort-Session-Answer | 274 | RFC 6733 |

2.1 Diameter Gy – Credit-Control-Request (CCR) command

This section describes the Diameter Gy CCR message format as defined in RFC 4006, *Diameter Credit-Control Application*. Strikethrough formatted AVPs are not included in CCR. AVPs listed in *italics* appearing after [AVP] and are not defined in RFC 4006.

```

<Credit-Control-Request> ::= < Diameter Header: 272, REQ, PXY >
    < Session-Id >
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Application-Id }
    { Service-Context-Id }
    { CC-Request-Type }
    { CC-Request-Number }
    [ Destination-Host ]
    [ User-Name ]
    [CC-Sub-Session-Id]
    [Acct-Multi-Session-Id]
    [ Origin-State-Id ]
    [ Event-Timestamp ]
    *[ Subscription-Id ]
    [Service-Identifier]
    [ Termination-Cause ]
    [Requested-Service-Unit]
    [Requested-Action]
    *[ Used-Service-Unit ]
    [ Multiple-Services-Indicator ]
    *[ Multiple-Services-Credit-Control ]
    *[ Service-Parameter-Info ]
    [CC-Correlation-Id]

```

```

*[ Route-Record ]
    [ User-Equipment-Info ]
    *[ Proxy-Info ]
    *[ AVP ]
    [ Framed-IP-Address ]
    [ Called-Station-Id ]
    [ Framed-IPv6-Prefix ]
    [ Delegated-IPv6-Prefix ]
    [ Alc-IPv6-Address ]
    [ 3GPP-IMSI ]
    [ 3GPP-Charging-Id ]
    [ 3GPP-GPRS-QoS-Negotiated-Profile ]
    [ 3GPP-GGSN-Address ]
    [ 3GPP-NSAPI ]
    [ 3GPP-Session-Stop-Indicator ]
    [ 3GPP-Selection-Mode ]
    [ 3GPP-Charging-Characteristics ]
    [ 3GPP-GGSN-v6-Address ]
    [ 3GPP-RAT-Type ]
    [ 3GPP-User-Location-Info ]
    [ GGSN-Address ]
    [ Service-Information ]
    [ Charging-Rule-Base-Name ]
    [ PDP-Context-Type ]

```

2.1.1 Diameter Gy – CCR message top level AVPs

[Table 2: Diameter Gy CCR: top level AVP description](#) provides a detailed description of each top-level AVP present in a Diameter Gy CCR message. Unless mentioned in the description, the AVP is present in Initial, Update, and Terminate messages. Grouped AVPs are marked with "↳ (grouped AVP)". The grouped AVP format and embedded AVP description and format are described in [Diameter Gy – CCR message grouped AVPs](#).

Table 2: Diameter Gy CCR: top level AVP description

| AVP code | AVP name | Description |
|----------|-------------------|--|
| 1 | User-Name | <p>RADIUS username</p> <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy aaa-user-name</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp radius-user-name</pre> <p>default: not included</p> |
| 8 | Framed-IP-Address | <p>The IP address of the IPv4 subscriber host that triggered the creation of the Diameter Gy session.</p> |

| AVP code | AVP name | Description |
|----------|-------------------|--|
| | | <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp address-avp</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp address-avp</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured with the following commands:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>default: included</p> |
| 30 | Called-Station-Id | <p>The AVP is included if configured in the diameter application policy command:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp called-station-id</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp called-station-id</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs using the following commands:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> |

| AVP code | AVP name | Description |
|----------|-----------------------|---|
| | | value: string up to 64 characters default: no called-station-id |
| 55 | Event-Timestamp | Timestamp when the request was generated. |
| 97 | Framed-IPv6-Prefix | <p>The IPv6 prefix of the SLAAC subscriber host that triggered the creation of the Diameter Gy session.</p> <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp address-avp</pre> <ul style="list-style-type: none"> • classic CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp address-avp</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> <ul style="list-style-type: none"> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>default: included</p> |
| 123 | Delegated-IPv6-Prefix | <p>The IPv6 prefix of the DHCPv6 IA-PD subscriber host that triggered the creation of the Diameter Gy session.</p> <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp address-avp</pre> <ul style="list-style-type: none"> • classic CLI <pre>configure subscriber-mgmt diameter-applicaton-policy gy include-avp address-avp</pre> |

| AVP code | AVP name | Description |
|----------|---------------------|---|
| | | <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured using the following command:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>default: included</p> |
| 258 | Auth-Application-Id | Fixed value: 4 = Diameter Credit Control Application |
| 263 | Session-Id | <p>A session is a logical concept at the application layer that exists between the Diameter client and the Diameter server; it is identified via the Session-Id AVP.</p> <p>Format:</p> <p><DiameterIdentity>; <high 32 bits>; <low 32 bits></p> <ul style="list-style-type: none"> <DiameterIdentity> is the configured origin host <high 32 bits> are encoded as the Diameter initialization time (number of seconds because 1 January, 1970) <low 32 bits> are encoded as a sequentially increasing number starting at 1 <p>Example: bng.nokia.com;1326398325;1</p> |
| 264 | Origin-Host | <p>Diameter Identity. As configured in the corresponding diameter-peer-policy.</p> <p>Example: bng.nokia.com</p> |
| 278 | Origin-State-Id | <p>Initialized to the Diameter process startup time. Encoded as number of seconds since 1 January, 1970.</p> |
| 283 | Destination-Realm | <p>Diameter Identity. As configured in the corresponding diameter-peer-policy or learned from CCA/RAR.</p> <p>Example: nokia.com</p> |
| 293 | Destination-Host | <p>Diameter Identity. As configured in the corresponding diameter-peer-policy or learned from CCA/RAR. Omitted in CCR-I if not configured.</p> <p>Example: server.nokia.com</p> |
| 295 | Termination-Cause | (CCR-T only) |

| AVP code | AVP name | Description |
|----------|---|---|
| | | Indicates the reason that the credit control session was terminated. Values: 1 = Diameter Logout 4 = Diameter Administrative - a diameter session could not be created because of category mismatch or system resources |
| 296 | Origin-Realm | Diameter Identity. As configured in the corresponding diameter-peer-policy. Example: nokia.com |
| 415 | CC-Request-Number | Initial Request: 0 Update and Termination Request: sequence number |
| 416 | CC-Request-Type | 1 = Initial Request 2 = Update Request 3 = Termination Request |
| 443 | Subscription-Id ↳ (grouped AVP) | Identifies the subscriber host or session. The value is as configured in the diameter application policy: <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy avp-subscription-id origin</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy avp-subscription-id origin</pre> If no data is available for the specified origin, then the subscriber-id is used instead. default: avp-subscription-id subscriber-id type private For GTP access, the configured value is ignored and two Subscription-Id AVPs are included: IMSI (type imsi) and MSISDN (type e164) with the corresponding values learned from the GTP Create Session Request message. |
| 455 | Multiple-Services-Indicator | (CCR-I only) Fixed value: 1 = MULTIPLE_SERVICES_SUPPORTED |
| 456 | Multiple-Services-Credit-Control ↳ (grouped AVP) | Up to 16 Multiple-Services-Credit-Control AVPs, each corresponding with a single rating group. A rating group maps |

| AVP code | AVP name | Description |
|------------|--|--|
| | | <p>to a category configured in a category-map using the following commands.</p> <pre>configure subscriber-mgmt category-map category rating-group</pre> |
| 458 | User-Equipment-Info ↳ (grouped AVP) | <p>(GTP access only)</p> <p>The AVP is included if configured in the diameter application policy:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp user-equipment-info-type type imeisv</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp user-equipment-info type imeisv</pre> <p>value: IMEI as signaled in the GTP Create Session Request message.</p> <p>default: not included</p> |
| 461 | Service-Context-Id | <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp service-context-id</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp service-context-id</pre> <p>value: string of up to 32 characters</p> <p>default: no service-context-id</p> |
| NOKIA – 99 | Alc-IPv6-Address | <p>The IPv6 address of the DHCPv6 IA-NA subscriber host that triggered the creation of the Diameter Gy session.</p> <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp address-avp</pre> |

| AVP code | AVP name | Description |
|----------|-----------|---|
| | | <ul style="list-style-type: none"> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp address-avp</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured using the following command:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>default: included</p> |
| 3GPP – 1 | 3GPP-IMSI | <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-imsi</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-imsi</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured using the following command:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>values:</p> <ul style="list-style-type: none"> circuit-id imsi subscriber-id <p>default: included with value subscriber-id</p> |

| AVP code | AVP name | Description |
|----------|----------------------------------|--|
| 3GPP – 2 | 3GPP-Charging-Id | <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-charging-id</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-charging-id</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>values:</p> <ul style="list-style-type: none"> • auto: defaults to esm-info for vendor-support three-gpp • esm-info: <subscriber-id>;<sap-id>;<sla-profile>[<SPI sharing id>] • id: a unique 32 bit integer value per session <p>default: included with esm-info value (auto)</p> |
| 3GPP – 5 | 3GPP-GPRS-QoS-Negotiated-Profile | <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-gprs-negotiated-qos-profile</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-gprs-negotiated-qos-profile</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured using the following command:</p> |

| AVP code | AVP name | Description |
|----------|-------------------|--|
| | | <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>value: the active SLA profile name default: included</p> |
| 3GPP – 7 | 3GPP-GGSN-Address | <p>The local IPv4 address used to setup the diameter peer. The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-ggsn-ipv4-address</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-ggsn-address</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>.</p> <p>value:</p> <ol style="list-style-type: none"> 1. Use the configured IPv4 source address: <ul style="list-style-type: none"> • MD-CLI <pre>configure aaa diameter-peer-policy ipv4-source- address</pre> • classic CLI <pre>configure aaa diameter-peer-policy source-address</pre> |

| AVP code | AVP name | Description |
|-----------|-----------------------------|---|
| | | <p>2. If the router equals base or vprn service id, use the system interface IPv4 address</p> <p>else if the router equals management, use the active management port IP address configured in the BOF</p> <p>default: included</p> |
| 3GPP – 10 | 3GPP-NSAPI | <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-nsapi</pre> <ul style="list-style-type: none"> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-nsapi</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> <ul style="list-style-type: none"> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>value: <system name>;<service-id>;<sap-id></p> <p>default: included</p> |
| 3GPP – 11 | 3GPP-Session-Stop-Indicator | <p>(CCR-T only)</p> <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-session-stop-indicator</pre> <ul style="list-style-type: none"> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-session-stop-indicator</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured using the following command:</p> |

| AVP code | AVP name | Description |
|-----------|-------------------------------|---|
| | | <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>Fixed value: 0x FF default: included</p> |
| 3GPP – 12 | 3GPP-Selection-Mode | <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-selection-mode</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-selection-mode</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>Fixed value: 0x 00 00 00 00 (MS or network provided APN, subscribed verified) default: included</p> |
| 3GPP – 13 | 3GPP-Charging-Characteristics | <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-charging-characteristics</pre> |

| AVP code | AVP name | Description |
|-----------|----------------------|--|
| | | <ul style="list-style-type: none"> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-charging-characteristics</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured using the following command:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>Fixed value: "0000" default: included</p> |
| 3GPP – 16 | 3GPP-GGSN-v6-Address | <p>The local IPv6 address used to setup the diameter peer. The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-ggsn-ipv6-address</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured using the following command:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ps-information</pre> <p>value:</p> <ol style="list-style-type: none"> Use the configured IPv6 source address: <pre>configure aaa diameter peer-policy ipv6-source-address</pre> |

| AVP code | AVP name | Description |
|-----------|-------------------------|---|
| | | <p>2. If router = base or vprn service id: use the system interface IPv6 address</p> <p>else if router = management: use the active management port IP address configured in the BOF</p> <p>default: not included</p> |
| 3GPP – 21 | 3GPP-RAT-Type | <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-rat-type</pre> <ul style="list-style-type: none"> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-rat-type</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured with the following command options:</p> <pre>gy include-avp ps-information</pre> <p>value: [1 to 255]</p> <p>default: not included</p> <p>For GTP access, the RAT-Type value is learned from the GTP Create Session Request message. The configured value is used when the GTP learned value is unknown or invalid.</p> |
| 3GPP - 22 | 3GPP-User-Location-Info | <p>(GTP access only)</p> <p>Provides UE location details</p> <p>The AVP is included if configured in the diameter application policy:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp 3gpp-user-location-info</pre> <ul style="list-style-type: none"> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp three-gpp-user-location-info</pre> <p>value: ULI learned from the GTP Create Session Request message.</p> <p>default: not included</p> |

| AVP code | AVP name | Description |
|------------|--|---|
| 3GPP – 847 | GGSN-Address | <p>The local address used to setup the diameter peer.</p> <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ggsn-address type (ipv4 ipv6)</pre> • classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy include-avp ggsn-address {ipv4 ipv6}</pre> <p>Either IPv4 or IPv6 address can be included.</p> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured with the following command options:</p> <pre>gy include-avp ps-information</pre> <p>value:</p> <ol style="list-style-type: none"> 1. Use the configured IP source address: <ul style="list-style-type: none"> • MD-CLI <pre>configure aaa diameter peer-policy ipv6-source-address</pre> <pre>configure aaa diameter peer-policy ipv4-source-address</pre> • classic CLI <pre>configure aaa diameter-peer-policy ipv6-source-address</pre> <pre>configure aaa diameter-peer-policy ipv4-source-address</pre> 2. If router = base or vprn service id: use the system interface IP address else if router = management: use the active management port IP address configured in the BOF <p>default: not included</p> |
| 3GPP – 873 | Service-Information ↳ (grouped AVP) | <p>Grouped AVP containing the [3GPP – 874] PS-Information grouped AVP and embedding following AVPs:</p> <ul style="list-style-type: none"> • [8] Framed-IP-Address |

| AVP code | AVP name | Description |
|-------------|-------------------------|---|
| | | <ul style="list-style-type: none"> • [30] Called-Station-Id • [97] Framed-IPv6-Prefix • [123] Delegated-IPv6-Prefix • [NOKIA – 99] Alc-IPv6-Address • [3GPP – 1] 3GPP-IMSI • [3GPP – 2] 3GPP-Charging-Id • [3GPP – 5] 3GPP-GPRS-Negotiated-QoS-profile • [3GPP – 7] 3GPP-GGSN-Address • [3GPP – 10] GGSN-NSAPI • [3GPP – 11] 3GPP-Session-Stop-Indicator • [3GPP – 12] 3GPP-Selection-Mode • [3GPP – 13] 3GPP-Charging-Characteristics • [3GPP – 16] 3GPP-GGSN-IPv6-Address • [3GPP – 21] 3GPP-RAT-Type • [3GPP – 847] GGSN-Address • [3GPP – 1004] Charging-Rule-Base-Name • [3GPP – 1247] PDP-Context-Type <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> <ul style="list-style-type: none"> • classic CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information</pre> <p>When not configured the above listed AVPs are included at command level.</p> <p>default: no ps-information</p> |
| 3GPP – 1004 | Charging-Rule-Base-Name | <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> • MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp charging-rule-base-name category-map</pre> |

| AVP code | AVP name | Description |
|-------------|------------------|--|
| | | <ul style="list-style-type: none"> classic CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp charging-rule-base-name category-map-name</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured with the following command options:</p> <pre>gy include-avp ps-information</pre> <p>value:</p> <ul style="list-style-type: none"> category-map-name: the name of the category-map in use for this session string: a string of max. 64 characters. <p>default: charging-rule-base-name category-map-name</p> |
| 3GPP – 1247 | PDP-Context-Type | <p>(CCR-I only)</p> <p>The AVP is included if configured in the diameter application policy using the following command:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp pdp-context-type</pre> <ul style="list-style-type: none"> classic CLI <pre>configure subscriber-mgmt diameter-gy-policy gy include-avp pdp-context-type</pre> <p>Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs when configured with the following command options:</p> <pre>gy include-avp ps-information</pre> <p>Fixed value: 0 (primary) default: included</p> |

Table 3: Diameter Gy CCR: top level AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|----------|-------------------|-------------------|--------------|-------|
| 1 | User-Name | RFC 2865/RFC 6733 | UTF8 String | M |
| 8 | Framed-IP-Address | RFC 2865 | Octet String | M |
| 30 | Called-Station-Id | RFC 2865 | UTF8 String | M |

| AVP code | AVP name | Standard | Data format | Flags |
|------------|---|----------------------|-------------------|-------|
| 55 | Event-Timestamp | RFC 6733/RFC 4006 | Time | M |
| 97 | Framed-IPv6-Prefix | RFC 3162 | Octet String | M |
| 123 | Delegated-IPv6-Prefix | RFC 4818 | Octet String | M |
| 258 | Auth-Application-Id | RFC 6733/RFC 4006 | Unsigned 32 | M |
| 263 | Session-Id | RFC 6733 | UTF8 String | M |
| 264 | Origin-Host | RFC 6733 | Diameter Identity | M |
| 278 | Origin-State-Id | RFC 6733 | Unsigned 32 | M |
| 283 | Destination-Realm | RFC 6733 | Diameter Identity | M |
| 293 | Destination-Host | RFC 6733 | Diameter Identity | M |
| 295 | Termination-Cause | RFC 6733 | Enumerated | M |
| 296 | Origin-Realm | RFC 6733 | Diameter Identity | M |
| 415 | CC-Request-Number | RFC 4006 | Unsigned 32 | M |
| 416 | CC-Request-Type | RFC 4006 | Enumerated | M |
| 443 | Subscription-Id ↳ (grouped AVP) | RFC 4006 | Grouped | M |
| 455 | Multiple-Services-Indicator | RFC 4006 | Enumerated | M |
| 456 | Multiple-Services-Credit-Control ↳ (grouped AVP) | RFC 4006 | Grouped | M |
| 458 | User-Equipment-Info ↳ (grouped AVP) | RFC 4006 | Grouped | M |
| 461 | Service-Context-Id | RFC 4006 | UTF8 String | M |
| NOKIA – 99 | Alc-IPv6-Address | - | Octet String | V |
| 3GPP – 1 | 3GPP-IMSI | TS 29.061/ TS 32.299 | UTF8 String | V |
| 3GPP – 2 | 3GPP-Charging-Id | TS 29.061/ TS 32.299 | UTF8 String | V |
| 3GPP – 5 | 3GPP-GPRS-QoS-Negotiated-Profile | TS 29.061 | UTF8 String | V |
| 3GPP – 7 | 3GPP-GGSN-Address | TS 29.061 | Octet String | V |
| 3GPP – 10 | 3GPP-NSAPI | TS 29.061 | UTF8 String | V |
| 3GPP – 11 | 3GPP-Session-Stop-Indicator | TS 29.061 | UTF8 String | V |

| AVP code | AVP name | Standard | Data format | Flags |
|-------------|--|-----------|--------------|-------|
| 3GPP – 12 | 3GPP-Selection-Mode | TS 29.061 | UTF8 String | V |
| 3GPP – 13 | 3GPP-Charging-Characteristics | TS 29.061 | UTF8 String | V |
| 3GPP – 16 | 3GPP-GGSN-v6-Address | TS 29.061 | Octet String | V |
| 3GPP – 21 | 3GPP-RAT-Type | TS 29.061 | Octet String | V |
| 3GPP – 22 | 3GPP-User-Location-Info | TS 29.061 | Octet String | V |
| 3GPP – 847 | GGSN-Address | TS 32.299 | Address | V |
| 3GPP – 873 | Service-Information ↳ (grouped AVP) | TS 32.299 | Grouped | V |
| 3GPP – 1004 | Charging-Rule-Base-Name | TS 29.212 | Octet String | V, M |
| 3GPP – 1247 | PDP-Context-Type | TS 32.299 | Enumerated | V, M |

2.1.2 Diameter Gy – CCR message grouped AVPs

This section provides an overview of CCR message grouped AVPs.

2.1.2.1 Diameter Gy CCR – Subscription-Id grouped AVP

Grouped AVP format as defined in RFC 4006:

```
Subscription-Id ::= < AVP Header: 443 >
                { Subscription-Id-Type }
                { Subscription-Id-Data }
```

Table 4: Diameter Gy CCR: Subscription-Id grouped AVP description

| AVP code | AVP name | Description |
|----------|----------------------|--|
| 450 | Subscription-Id-Type | <p>Value as configured in the diameter application policy:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy avp- subscription-id origin configure subscriber-mgmt diameter-gy-policy gy avp- subscription-id type</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy avp-subscription-id <i>origin</i> (circuit-id dual-stack- remote-id imei imsi mac msisdn nas-port-id subscriber- id username) [type (e164 imsi nai private)]</pre> |

| AVP code | AVP name | Description |
|----------|----------------------|---|
| | | <p>values:</p> <ul style="list-style-type: none"> e164: identifier in international E.164 format (ITU-T E.164) imsi: identifier in international IMSI format (ITU-T E.212) nai: identifier in the form of a Network Access Identifier (RFC 2486) private: a credit control server private identifier <p>default: type private</p> <p>For GTP access, the configured value is ignored and the type is set to imsi and msisdn respectively for each of the two included Subscription-Id AVPs.</p> |
| 444 | Subscription-Id-Data | <p>The value as configured in the diameter application policy:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy avp-subscription-id origin configure subscriber-mgmt diameter-gy-policy gy avp-subscription-id type</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy gy avp-subscription-id origin [type]</pre> <p>Note that there is no check if the provided data is in the format of the following configured type.</p> <p>values:</p> <ul style="list-style-type: none"> circuit-id subscriber-id imsi msisdn imei <p>default: avp-subscription-id subscriber-id</p> <p>For GTP access, the Subscription ID data is learned from GTP and contains the IMSI and MSISDN.</p> |

Table 5: Diameter Gy CCR: Subscription-Id grouped AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|----------|----------------------|----------|-------------|-------|
| 450 | Subscription-Id-Type | RFC 4006 | Enumerated | M |
| 444 | Subscription-Id-Data | RFC 4006 | UTF8 String | M |

2.1.2.2 Diameter Gy CCR – Multiple-Services-Credit-Control grouped AVP

Grouped AVP format as defined in RFC 4006. Strikethrough formatted AVPs are not included in CCR. *Italic* formatted AVPs listed after [AVP] are not defined in RFC 4006.

```
Multiple-Services-Credit-Control ::= < AVP Header: 456 >
    [Granted-Service-Unit]
    [ Requested-Service-Unit ]
    *[ Used-Service-Unit ]
    [Tariff-Change-Usage]
    *[ Service-Identifier ]
    [ Rating-Group ]
    *[ G-S-U-Pool-Reference ]

[ Validity-Time ]
[ Result-Code ]
[ Final-Unit-Indication ]

    *[ AVP ]
    [Reporting-Reason ]
```

Table 6: Diameter Gy CCR: Multiple-Services-Credit-Control Grouped AVP description

| AVP code | AVP name | Description |
|------------|---|---|
| 432 | Rating-Group | Rating group for which the quota is requested or reported. Corresponds with a category within a category-map defining the queues and policers and direction to monitor. configure subscriber-mgmt category-map category rating-group |
| 437 | Requested-Service-Unit ↳ (grouped AVP) | (CCR-I and CCR-U only) When included, the Requested-Service-Unit AVP has an empty data field in all CCR Initial/Update messages. |
| 446 | Used-Service-Unit ↳ (grouped AVP) | (CCR-U and CCR-T only) Amount of used service units measured for a specified category or rating group to a specified quota type. The Used-Service-Unit AVP is not present in CCR-U when all contained AVP values are zero and the Reporting-Reason = Validity Time (4) or Forced Reauthorization (7). |
| 3GPP – 872 | Reporting-Reason | Specifies the reason for which the Used-Service-Units are reported. CCR-U and CCR-T only. Values <ul style="list-style-type: none"> 0 (Threshold): used quota reached time or volume threshold value (threshold value different from zero) |

| AVP code | AVP name | Description |
|----------|----------|--|
| | | <ul style="list-style-type: none"> • 1 (Quota Holding Time): expiration of the Quota Holding Time • 2 (Final): Diameter session termination; can be client or server initiated. • 3 (Quota Exhausted): no threshold or threshold is zero and quota exhausted. • 4 (Validity Time): expiration of the Validity Time • 5 (Other Quota Type): not supported • 6 (Rating Condition Change): not supported • 7 (Forced Reauthorisation): reception of a RAR message • 8 (Pool Exhausted): not supported |

Table 7: Diameter Gy CCR: Multiple-Services-Credit-Control grouped AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|------------|---|-----------|-------------|-------|
| 432 | Rating-Group | RFC 4006 | Unsigned 32 | M |
| 437 | Requested-Service-Unit ↳ (grouped AVP) | RFC 4006 | Grouped | M |
| 446 | Used-Service-Unit ↳ (grouped AVP) | RFC 4006 | Grouped | M |
| 3GPP – 872 | Reporting-Reason | TS 32.299 | Enumerated | V, M |

2.1.2.3 Diameter Gy CCR – Requested-Service-Unit grouped AVP

Grouped AVP format as defined in RFC 4006. Strikethrough formatted AVPs are not included in CCR.

```
Requested-Service-Unit ::= < AVP Header: 437 >
                        { CC-Time }
                        { CC-Money }
                        { CC-Total-Octets }
                        { CC-Input-Octets }
                        { CC-Output-Octets }
                        { CC-Service-Specific-Units }
                        *{ AVP }
```

The Requested-Service-Unit AVP has an empty data field in all CCR Initial/Update messages and is not present in a CCR Terminate message.

2.1.2.4 Diameter Gy CCR – Used-Service-Unit grouped AVP

Grouped AVP format as defined in RFC 4006. Strikethrough formatted AVPs are not included in CCR.

```
Used-Service-Unit ::= < AVP Header: 446 >
    [Tariff-Change-Usage]
    [ CC-Time ]
    [CC-Money]
    [ CC-Total-Octets ]
    [ CC-Input-Octets ]
    [ CC-Output-Octets ]
    [CC-Service-Specific-Units]
    *[ AVP ]
```

Table 8: Diameter Gy CCR: Used-Service-Unit grouped AVP description

| AVP code | AVP name | Description |
|----------|------------------|---|
| 412 | CC-Input-Octets | <p>Number of ingress bytes forwarded via queues or policers that are monitored in the ingress direction for this rating group.</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt category-map category ingress policer value configure subscriber-mgmt category-map category ingress queue value</pre> classic CLI <pre>configure subscriber-mgmt category-map category queue queue-id {ingress-only} configure subscriber-mgmt category-map category policer policer-id {ingress-only}</pre> <p>Value equals zero when credit type is time or when no queues/policers are monitored in ingress direction.</p> |
| 414 | CC-Output-Octets | <p>Number of egress bytes forwarded via queues or policers that are monitored in egress direction for this rating group.</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt category-map category egress policer value configure subscriber-mgmt category-map category egress queue value</pre> classic CLI <pre>configure subscriber-mgmt category-map category queue queue-id {egress-only} configure subscriber-mgmt category-map category policer policer-id {egress-only}</pre> |

| AVP code | AVP name | Description |
|----------|-----------------|---|
| | | Value equals zero when credit type is time. Or when no queues/policers are monitored in egress direction. |
| 420 | CC-Time | <p>Total number of seconds during which activity is detected for queues or policers that are monitored for this rating group.</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt category-map category ingress policer <i>value</i> configure subscriber-mgmt category-map category ingress queue <i>value</i></pre> classic CLI <pre>configure subscriber-mgmt category-map category queue <i>queue-id</i> {ingress-only egress-only ingress-egress} configure subscriber-mgmt category-map category policer <i>policer-id</i> {ingress-only egress-only ingress-egress}</pre> <p>Only sampling periods exceeding the configured activity-threshold are counted:</p> <pre>configure subscriber-mgmt category-map activity-threshold</pre> <p>Value equals zero when credit type is volume.</p> |
| 421 | CC-Total-Octets | <p>Total number of bytes used for this rating-group. Corresponds with the sum of CC-Input-Octets and CC-Output-Octets.</p> <p>Value equals zero when credit type is time.</p> |

Table 9: Diameter Gy CCR: Used-Service-Unit grouped AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|----------|------------------|----------|-------------|-------|
| 412 | CC-Input-Octets | RFC 4006 | Unsigned 64 | M |
| 414 | CC-Output-Octets | RFC 4006 | Unsigned 64 | M |
| 420 | CC-Time | RFC 4006 | Unsigned 32 | M |
| 421 | CC-Total-Octets | RFC 4006 | Unsigned 64 | M |

2.1.2.5 DIAMETER Gy CCR - User-Equipment-Info grouped AVP

Grouped AVP format as defined in RFC 4006.

```
User-Equipment-Info ::= < AVP Header: 458 >
    { User-Equipment-Info-Type }
    { User-Equipment-Info-Value }
```

Table 10: Diameter Gy CCR: User-Equipment-Info grouped AVP description

| AVP code | AVP name | Description |
|----------|---------------------------|---|
| 459 | User-Equipment-Info-Type | (GTP access only) fixed value: IMEISV (0) |
| 460 | User-Equipment-Info-Value | (GTP access only) The Internet Mobile Equipment Identifier (IMEI) as signaled in the GTP Create Session Request message. |

Table 11: Diameter Gy CCR: User-Equipment-Info grouped AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|----------|---------------------------|----------|-------------|-------|
| 459 | User-Equipment-Info-Type | RFC 4006 | Enumerated | |
| 460 | User-Equipment-Info-Value | RFC 4006 | UTF8 String | |

2.1.2.6 Diameter Gy CCR – Service-Information grouped AVP

Grouped AVP format as defined in TS 32.29. ~~Strikethrough~~ formatted AVPs are not included in CCR.

```
Service-Information ::= < AVP Header: 873>
    * { Subscription-Id }
    { AoC-Information }
    [ PS-Information ]
    { WLAN-Information }
    { IMS-Information }
    { LCS-Information }
    { PoC-Information }
    { MBMS-Information }
    { SMS-Information }
    { MMTel-Information }
    { Service-Generic-Information }
    { IM-Information }
    { DCD-Information }
```

Table 12: Diameter Gy CCR: Service-Information grouped AVP description

| AVP code | AVP name | Description |
|------------|-----------------------------------|--|
| 3GPP – 874 | PS-Information ↳ (grouped AVP) | Allows the transmission of additional Packet Switched service-specific information elements. |

Table 13: Diameter Gy CCR: Service-Information grouped AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|------------|-----------------------------------|-----------|-------------|-------|
| 3GPP – 874 | PS-Information ↳ (grouped AVP) | TS 32.299 | Grouped | V |

2.1.2.7 Diameter Gy CCR – PS-Information grouped AVP

Grouped AVP format as defined in TS 32.299:

Strikethrough formatted AVPs are not included in CCR. *Italic* formatted AVPs listed at the end are not defined in TS 32.299.

For a description and format of the AVPs embedded in the grouped PS-Information AVP, see [Table 2: Diameter Gy CCR: top level AVP description](#) and [Table 3: Diameter Gy CCR: top level AVP format](#).

```

PS-Information ::= < AVP Header: 874>
    [ 3GPP-Charging-Id ]
    { PDN-Connection-ID }
    { Node-Id }
    { 3GPP-PDP-Type }
    { PDP-Address }
    { Dynamic-Address-Flag }
    { QoS-Information }
    { SGSN-Address }
    [ GGSN-Address ]
    { CG-Address }
    { Serving-Node-Type }
    { SGW-Change }
    { 3GPP-IMSI-MCC-MNC }
    { IMSI-Unauthenticated-Flag }
    { 3GPP-GGSN-MCC-MNC }
    [ 3GPP-NSAPI ]
    [ Called-Station-Id ]
    [ 3GPP-Session-Stop-Indicator ]
    [ 3GPP-Selection-Mode ]
    [ 3GPP-Charging-Characteristics ]
    { Charging-Characteristics-Selection-Mode }
    { 3GPP-SGSN-MCC-MNC }
    { 3GPP-MS-TimeZone }
    * [ Charging-Rule-Base-Name ]
    { 3GPP-User-Location-Info }
    { User-CSG-Information }
    { 3GPP2-BSID }
    [ 3GPP-RAT-Type ]
    { PS-Furnish-Charging-Information }
    [ PDP-Context-Type ]
    { Offline-Charging }

```



```

        * { Traffic-Data-Volumes }
        * { Service-Data-Container }
{ User-Equipment-Info }
{ Terminal-Information }
{ Start-Time }
{ Stop-Time }
{ Change-Condition }
{ Diagnostics }
[ Framed-IP-Address ]
[ Framed-IPv6-Prefix ]
[ Delegated-IPv6-Prefix ]
[ Alc-IPv6-Address ]
[ 3GPP-IMSI ]
[ 3GPP-GPRS-Negotiated-QoS-profile ]
[ 3GPP-GGSN-Address ]
[ 3GPP-GGSN-IPv6-Address ]

```

2.2 Diameter Gy – Credit-Control-Answer (CCA) command

This section describes the Diameter Gy CCA message format as defined in RFC 4006. ~~Strikethrough~~ formatted AVPs should not appear or are ignored in CCA. *Italic* formatted AVPs listed after [AVP] are not defined in RFC 4006.

```

<Credit-Control-Answer> ::= < Diameter Header: 272, PXY >
    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    { Auth-Application-Id }
    { CC-Request-Type }
    { CC-Request-Number }
{ User-Name }
[ CC-Session-Failover ]
{ CC-Sub-Session-Id }

{ Acct-Multi-Session-Id }
{ Origin-State-Id }
{ Event-Timestamp }
{ Granted-Service-Unit }

    *[ Multiple-Services-Credit-Control ]
    { Cost-Information }

{ Final-Unit-Indication }
{ Check-Balance-Result }

    [ Credit-Control-Failure-Handling ]
{ Direct-Debiting-Failure-Handling }

{ Validity-Time }

    *{ Redirect-Host }

{ Redirect-Host-Usage }
{ Redirect-Max-Cache-Time }

    *{ Proxy-Info }
    *{ Route-Record }
    *[ Failed-AVP ]
    *[ AVP ]
    [ Charging-Rule-Base-Name ]

```

2.2.1 Diameter Gy – CCA message top level AVPs

Table 14: Diameter Gy CCA: top level AVP description provides a detailed description for each top level AVP present in a Diameter Gy CCA message. Unless mentioned different in the description, the AVP is present in Initial, Update and Terminate messages. Grouped AVPs are marked with “↳ (grouped AVP)”. The grouped AVP format and embedded AVP description and format are described in section Diameter Gy – CCR message grouped AVPs .

Table 14: Diameter Gy CCA: top level AVP description

| AVP code | AVP name | Description |
|----------|---------------------|--|
| 258 | Auth-Application-Id | Fixed value: 4 = Diameter Credit Control Application |
| 263 | Session-id | <p>A session is a logical concept at the application layer that exists between the Diameter client and the Diameter server; it is identified via the Session-Id AVP.</p> <p>Format:</p> <p><DiameterIdentity>;<high 32 bits>;<low 32 bits></p> <ul style="list-style-type: none"> • <DiameterIdentity> is the configured origin host • <high 32 bits> are encoded as the Diameter initialization time (the number of seconds since 1 Jan 1970) • <low 32 bits> are encoded as a sequentially increasing number starting at 1 <p>Example: bng.nokia.com;1326398325;1</p> |
| 264 | Origin-Host | <p>Diameter Identity. Used as destination host in the next Diameter message.</p> <p>Example: server.nokia.com</p> |
| 268 | Result-Code | <p>Values:</p> <p>2001 = Diameter Success</p> <p>3xxx = Protocol Errors</p> <p>4001 = Diameter Authentication Rejected</p> <p>4010 = Diameter End User Service Denied (CCA-U only)</p> <p>4011 = Diameter Credit Control Not Applicable</p> <p>4012 = Diameter Credit Limit Reached (CCA-U only)</p> <p>5003 = Diameter Authorization Rejected</p> <p>5030 = Diameter User Unknown</p> <p>5031 = Diameter Rating Failed (CCA-U only)</p> <p>Values not listed result in a Diameter Session Failure and the Credit Control Failure Handling action is executed.</p> |

| AVP code | AVP name | Description |
|----------|---------------------------------|---|
| 278 | Failed-AVP ↳ (grouped AVP) | Provides debugging information when CCR is rejected or not fully processed because of unsupported AVP or AVP value. |
| 296 | Origin-Realm | Diameter Identity. Used as destination host in the next Diameter message. Example: nokia.com |
| 415 | CC-Request-Number | Values: CCA-Initial: 0 CCA-Update and CCA-Termination: sequence number |
| 416 | CC-Request-Type | Values: 1 = Initial Answer 2 = Update Answer 3 = Termination Answer |
| 418 | CC-Session-Failover | Specifies if a secondary peer should be attempted in case of Credit Control Failure Handling. Use the commands in the following context to override the configured failover value: <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy on-failure failover [true false] handling [terminate continue retry-and-terminate]</pre> classic CLI <pre>configure subscriber-mgmt diameter- application-policy on-failure [failover {enabled disabled}] [handling {continue retry-and-terminate terminate}]</pre> Values: 0 = Failover Not Supported 1 = Failover Supported |
| 427 | Credit-Control-Failure-Handling | Action to take when the Credit Control client does not receive a valid CCA message within the interval specified with tx-timer (default 10s). Use the following commands to override the configured failure handling: |

| AVP code | AVP name | Description |
|-------------|---|--|
| | | <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy on-failure failover enabled handling [terminate continue retry-and-terminate]</pre> classic CLI <pre>configure subscriber-mgmt diameter-application-policy on-failure [failover {enabled disabled}] [handling {continue retry-and-terminate terminate}]</pre> <p>Values: 0 = Terminate 1 = Continue 2 = Retry and terminate</p> |
| 456 | Multiple-Services-Credit-Control ↳ (grouped AVP) | <p>Up to sixteen Multiple-Services-Credit-Control AVPs, each corresponding to a rating group. A rating group maps to a category configured in a category-map:</p> <pre>configure subscriber-mgmt category-map category rating-group</pre> |
| 3GPP – 1004 | Charging-Rule-Base-Name | <p>(CCA-I only)</p> <p>Assigns the category-map or overrides the category-map obtained in authentication.</p> <p>value: category-map-name: the name of the category-map to be used for this session</p> |

Table 15: Diameter Gy CCA: top level AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|----------|-------------------------------|-------------------|-------------------|-------|
| 258 | Auth-Application-Id | RFC 6733/RFC 4006 | Unsigned 32 | M |
| 263 | Session-id | RFC 6733 | UTF8 String | M |
| 264 | Origin-Host | RFC 6733 | Diameter Identity | M |
| 268 | Result-Code | RFC 6733/RFC 4006 | Unsigned 32 | M |
| 278 | Failed-AVP ↳ (grouped AVP) | RFC 6733 | Grouped | M |
| 296 | Origin-Realm | RFC 6733 | Diameter Identity | M |
| 415 | CC-Request-Number | RFC 4006 | Unsigned 32 | M |

| AVP code | AVP name | Standard | Data format | Flags |
|-------------|---|-----------|--------------|-------|
| 416 | CC-Request-Type | RFC 4006 | Enumerated | M |
| 418 | CC-Session-Failover | RFC 4006 | Enumerated | M |
| 427 | Credit-Control-Failure-Handling | RFC 4006 | Enumerated | M |
| 456 | Multiple-Services-Credit-Control ↳ (grouped AVP) | RFC 4006 | Grouped | M |
| 3GPP – 1004 | Charging-Rule-Base-Name | TS 29.212 | Octet String | V, M |

2.2.2 Diameter Gy – CCA message grouped AVPs

This section provides an overview of CCA message grouped AVPs.

2.2.2.1 Diameter Gy CCA – Failed-AVP grouped AVP

Grouped AVP format as defined in RFC 6733:

```
<Failed-AVP> ::= < AVP Header: 279 >
                1* {AVP}
```

The failed-AVP AVP contains the entire AVP that could not be processed successfully.

2.2.2.2 Diameter Gy CCA – Multiple-Services-Credit-Control grouped AVP

Grouped AVP format as defined in RFC 4006: ~~Strike through~~ formatted AVPs should not appear or are ignored in CCA. *Italic* formatted AVPs listed after [AVP] are not defined in RFC 4006.

```
Multiple-Services-Credit-Control ::= < AVP Header: 456 >
    [ Granted-Service-Unit ]
    [Requested-Service-Unit]
    *[ Used-Service-Unit ]
[ Tariff-Change-Usage ]
    *[ Service-Identifier ]
    [ Rating-Group ]
    *[ G-S-U-Pool-Reference ]
    [ Validity-Time ]
    [ Result-Code ]
    [ Final-Unit-Indication ]
    *[ AVP ]
    [Time-Quota-Threshold]
    [ Volume-Quota-Threshold ]
    [ Quota-Holding-Time ]
```

Table 16: Diameter Gy CCA: Multiple-Services-Credit-Control grouped AVP description

| AVP code | AVP name | Description |
|------------|--|--|
| 268 | Result-Code | <p>Values:</p> <p>2001 = Diameter Success</p> <p>4010 = Diameter End User Service Denied</p> <p>4011 = Diameter Credit Control Not Applicable</p> <p>4012 = Diameter Credit Limit Reached</p> <p>5003 = Diameter Authorization Rejected</p> <p>5031 = Diameter Rating Failed</p> <p>Values not listed result in a Diameter Session Failure and the Credit Control Failure Handling action is executed.</p> |
| 430 | Final-Unit-Indication ↳ (grouped AVP) | <p>This AVP indicates that the Granted-Service-Unit contains the final units for the service. When this quota is consumed, a final reporting is started (CCR-U or CCR-T) with reporting reason "Final". The final reporting can be disabled with the following commands:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt diameter-gy-policy gy out-of-credit-reporting quota-exhausted</pre> classic CLI <pre>configure subscriber-mgmt diameter-applicaton-policy gy out-of-credit-reporting quota-exhausted</pre> |
| 431 | Granted-Service-Unit ↳ (grouped AVP) | <p>Amount of service units that the Diameter credit control client can provide to the end user until the service must be released or a new CCR message must be sent.</p> |
| 432 | Rating-Group | <p>Rating group for which the quota is allocated. The rating group corresponds with a category within a category-map defining the queues and policers and direction to monitor.</p> <pre>configure subscriber-mgmt category-map category rating-group</pre> |
| 448 | Validity-Time | <p>If the granted service units have not been consumed within the validity time, a CCR-U is triggered with Reporting Reason AVP set to 4 (Validity Time).</p> <p>Value in seconds</p> |
| 3GPP – 868 | Time-Quota-Threshold | <p>Threshold preventing time quota exhaustion before refreshing. When the used time quota exceeds the threshold, a CCR-U is triggered with Reporting Reason AVP set to 0 (Threshold).</p> |

| AVP code | AVP name | Description |
|------------|------------------------|--|
| | | Value in seconds |
| 3GPP – 869 | Volume-Quota-Threshold | Threshold preventing volume quota exhaustion before refreshing. When the used volume quota exceeds the threshold, a CCR-U is triggered with Reporting Reason AVP set to 0 (Threshold). Value in octets |
| 3GPP – 871 | Quota-Holding-Time | Specifies an idle-timeout associated with the granted service units. If no traffic associated with the quota is observed for the time specified by the quota holding time, then a CCR-U is triggered with Reporting Reason AVP set to 1 (Quota Holding Time). The idle time is measured per sampling period. Value in seconds |

Table 17: Diameter Gy CCA: Multiple-Services-Credit-Control grouped AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|------------|--|-------------------|-------------|-------|
| 268 | Result-Code | RFC 6733/RFC 4006 | Unsigned 32 | M |
| 430 | Final-Unit-Indication ↳ (grouped AVP) | RFC 4006 | Grouped | M |
| 431 | Granted-Service-Unit ↳ (grouped AVP) | RFC 4006 | Grouped | M |
| 432 | Rating-Group | RFC 4006 | Unsigned 32 | M |
| 448 | Validity-Time | RFC 4006 | Unsigned 32 | M |
| 3GPP – 868 | Time-Quota-Threshold | TS 32.299 | Unsigned 32 | V, M |
| 3GPP – 869 | Volume-Quota-Threshold | TS 32.299 | Unsigned 32 | V, M |
| 3GPP – 871 | Quota-Holding-Time | TS 32.299 | Unsigned 32 | V, M |

2.2.2.3 Diameter Gy CCA – Final-Unit-Indication grouped AVP

Grouped AVP format as defined in RFC 4006: Strikethrough formatted AVPs should not appear or are ignored in CCA.

```
Final-Unit-Indication ::= < AVP Header: 430 >
  { Final-Unit-Action }
  *[ Restriction-Filter-Rule ]
  *[ Filter-Id ]
  [ Redirect-Server ]
```

Table 18: Diameter Gy CCA: Final-Unit-Indication grouped AVP description

| AVP code | AVP name | Description |
|----------|------------------------------------|--|
| 443 | Redirect-Server ↳ (grouped AVP) | <p>This AVP is included when the Final-Unit-Action AVP is set to REDIRECT (1) and contains the URL to which the user must be redirected. The URL overrides the URL specified with the following commands:</p> <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt category-map category exhausted-credit-service- level ingress ip-filter entry 1 action http-redirect</pre> classic CLI <pre>configure subscriber-mgmt category-map category exhausted-credit-service- level ingress-ip-filter-entries entry action http-redirect url allow- override</pre> <p>The AVP is ignored when the out-of-credit action is different from change-service-level or when no http-redirect action with allow-override is configured.</p> |
| 449 | Final-Unit-Action | <p>If the value is Terminate, then the session is terminated and the corresponding subscriber host deleted.</p> <p>If the value is Redirect or Restrict Access, then the out-of-credit action as configured for that rating group (category) is executed using the following command:</p> <pre>configure subscriber-mgmt credit-control- policy out-of-credit-action</pre> <p>Alternately, the following command can be used to configure out of credit action:</p> <pre>configure subscriber-mgmt category-map category out-of-credit-action-override</pre> <p>Values: 0 = Terminate 1 = Redirect 2 = Restrict Access</p> |

Table 19: Diameter Gy CCA: Final-Unit-Indication grouped AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|----------|------------------------------------|----------|-------------|-------|
| 443 | Redirect-Server ↳ (grouped AVP) | RFC 4006 | Enumerated | M |
| 449 | Final-Unit-Action | RFC 4006 | Enumerated | M |

2.2.2.4 DIAMETER Gy CCA - Redirect-Server grouped AVP

Grouped AVP format as defined in RFC 4006.

```
Redirect-Server ::= < AVP Header: 434 >
                { Redirect-Address-Type }
                { Redirect-Server-Address }
```

Table 20: Diameter Gy CCA: Redirect-Server grouped AVP description

| AVP code | AVP name | Description |
|----------|-------------------------|---|
| 433 | Redirect-Address-Type | Must be set to URL (2). The Redirect-Server-Address AVP is ignored when set to a different value. |
| 435 | Redirect-Server-Address | <p>Contains the IPv4 HTTP redirect URL that is used when the Final-Unit-Action REDIRECT is triggered for the rating group that corresponds with the MSCC in which the Final-Unit-Indication AVP is included.</p> <p>The URL specified in the Redirect-Server-Address AVP is only used when all following conditions are met:</p> <ul style="list-style-type: none"> • The Final-Unit-Indication AVP is present in the Multiple-Services-Credit-Control AVP • The Final-Unit-Action is set to REDIRECT (1) • The Redirect-Address-Type is set to URL (2) • The out-of-credit action for the corresponding rating group is set to change-service-level: <pre>configure subscriber-mgmt credit- control-policy out-of-credit-action change-service-level</pre> |

| AVP code | AVP name | Description |
|-----------------|----------|--|
| | | <p>Alternately, the following command can be used to set the change service level:</p> <pre>configure subscriber-mgmt category-map category out-of-credit-action-override change-service-level</pre> <ul style="list-style-type: none"> An IPv4 HTTP redirect action with allow-override is specified as exhausted-credit-service-level for the corresponding rating group: <ul style="list-style-type: none"> MD-CLI <pre>configure subscriber-mgmt category- map category exhausted-credit- service-level ingress ip-filter entry action http-redirect url allow-override</pre> classic CLI <pre>configure subscriber-mgmt category- map category exhausted-credit- service-level ingress-ip-filter- entries entry action http-redirect url allow-override</pre> |
| 435 (continued) | | <p>In all other cases, the Redirect-Server-Address AVP is ignored.</p> <p>The maximum URL length is 255 characters and can include the same macro substitutions such as \$IP (customer's IP address), \$MAC (customer's MAC address), \$URL (original requested URL), as supported for a static configured HTTP redirect URL.</p> |

Table 21: Diameter Gy CCA: Redirect-Server grouped AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|----------|-------------------------|----------|-------------|-------|
| 433 | Redirect-Address-Type | RFC 4006 | Enumerated | M |
| 435 | Redirect-Server-Address | RFC 4006 | Enumerated | M |

2.2.2.5 Diameter Gy CCA – Granted-Service-Unit grouped AVP

Grouped AVP format as defined in RFC 4006. Strikethrough formatted AVPs should not appear or are ignored in CCA.

```
Granted-Service-Unit ::= < AVP Header: 431 >
```

```

      { Tariff-Time-Change }
      [ CC-Time ]
      { CC-Money }
      [ CC-Total-Octets ]
      { CC-Input-Octets }
{ CC-Output-Octets }
{ CC-Service-Specific-Units }
      *{ AVP }

```

For a single rating group (category), either Volume or Time quota can be granted. Granting both time and volume quota for a single rating group is not supported and results in a Diameter Session Failure and the execution of the Credit Control Failure Handling action.

Table 22: Diameter Gy CCA: Granted-Service-Unit grouped AVP description

| AVP code | AVP name | Description |
|----------|-----------------|--|
| 420 | CC-Time | Amount of granted time Value: in seconds |
| 421 | CC-Total-Octets | Total number of octets regardless of the direction (quota can be consumed for ingress or egress) Value: in octets |

Table 23: Diameter Gy CCA: Granted-Service-Unit grouped AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|----------|-----------------|----------|-------------|-------|
| 420 | CC-Time | RFC 4006 | Unsigned 32 | M |
| 421 | CC-Total-Octets | RFC 4006 | Unsigned 64 | M |

2.3 Diameter Gy – Re-Auth-Request (RAR) command

2.3.1 Diameter Gy – RAR message format

This section describes the Diameter Gy RAR message format as defined in RFC 6733. Strikethrough formatted AVPs should not appear or are ignored in RAR.

A RAR message triggers an intermediate interrogation (CCR-U) with Reporting-Reason set to "Forced Reauthorization".

```

<RAR> ::= < Diameter Header: 258, REQ, PXY >
      < Session-Id >
      { Origin-Host }
      { Origin-Realm }
      { Destination-Realm }
      { Destination-Host }
      { Auth-Application-Id }
      { Re-Auth-Request-Type }
      { User-Name }
{ Origin-State-Id }

```

* [~~Proxy-Info~~]
 * [~~Route-Record~~]
 * [~~AVP~~]

2.3.2 Diameter Gy – RAR message top level AVPs

[Table 24: Diameter Gy RAR: top level AVP description](#) provides a detailed description for each top level AVP present in a Diameter Gy RAR message.

Table 24: Diameter Gy RAR: top level AVP description

| AVP code | AVP name | Description |
|----------|----------------------|--|
| 258 | Auth-Application-Id | Fixed value: 4 = Diameter Credit Control Application |
| 263 | Session-id | <p>A session is a logical concept at the application layer that exists between the Diameter client and the Diameter server; it is identified via the Session-Id AVP.</p> <p>Format:</p> <p><DiameterIdentity>;<high 32 bits>;<low 32 bits></p> <ul style="list-style-type: none"> • <DiameterIdentity> is the configured origin host • <high 32 bits> are encoded as the Diameter initialization time (the number of seconds since 1 January, 1970) • <low 32 bits> are encoded as a sequentially increasing number starting at 1 <p>Example:</p> <p>bng.nokia.com;1326398325;1</p> |
| 264 | Origin-Host | <p>Diameter Identity. Used as destination host in the next Diameter message.</p> <p>Example: server.nokia.com</p> |
| 283 | Destination-Realm | <p>Diameter Identity.</p> <p>Example: nokia.com</p> |
| 285 | Re-Auth-Request-Type | <p>Values:</p> <p>0 = Authorize-Only</p> |
| 293 | Destination-Host | <p>Diameter Identity.</p> <p>Example: bng.nokia.com</p> |
| 296 | Origin-Realm | <p>Diameter Identity. Used as destination realm in the next Diameter message.</p> <p>Example: nokia.com</p> |

Table 25: Diameter Gy RAR: top level AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|----------|----------------------|-------------------|-------------------|-------|
| 258 | Auth-Application-Id | RFC 6733/RFC 4006 | Unsigned 32 | M |
| 263 | Session-id | RFC 6733 | UTF8 String | M |
| 264 | Origin-Host | RFC 6733 | Diameter Identity | M |
| 283 | Destination-Realm | RFC 6733 | Diameter Identity | M |
| 285 | Re-Auth-Request-Type | RFC 6733 | Enumerated | M |
| 293 | Destination-Host | RFC 6733 | Diameter Identity | M |
| 296 | Origin-Realm | RFC 6733 | Diameter Identity | M |

2.4 Diameter Gy – Re-Auth-Answer (RAA) command

2.4.1 Diameter Gy – RAA message format

This section describes the Diameter Gy RAA message format as defined in RFC 6733. Strikethrough formatted AVPs are not included in RAA.

```

<RAA> ::= < Diameter Header: 258, PXY >
        < Session-Id >
        { Result-Code }
        { Origin-Host }
        { Origin-Realm }
        { User-Name }
{ Origin-State-Id }
{ Error-Message }
{ Error-Reporting-Host }
{ Failed-AVP }
        * { Redirect-Host }
{ Redirect-Host-Usage }
{ Redirect-Max-Cache-Time }
        * { Proxy-Info }
        * { AVP }

```

2.4.2 Diameter Gy – RAA message top level AVPs

[Table 26: Diameter Gy RAA: top level AVP description](#) provides a detailed description for each top level AVP present in a Diameter Gy RAA message.

Table 26: Diameter Gy RAA: top level AVP description

| AVP code | AVP name | Description |
|----------|--------------|--|
| 263 | Session-id | <p>A session is a logical concept at the application layer that exists between the Diameter client and the Diameter server; it is identified via the Session-Id AVP.</p> <p>Format:</p> <p><DiameterIdentity>;<high 32 bits>;<low 32 bits></p> <ul style="list-style-type: none"> • <DiameterIdentity> is the configured origin host • <high 32 bits> are encoded as the Diameter initialization time (the number of seconds since 1 January, 1970) • <low 32 bits> are encoded as a sequentially increasing number starting at 1 <p>Example:</p> <p>bng.nokia.com;1326398325;1</p> |
| 264 | Origin-Host | <p>Diameter Identity. As configured in the corresponding diameter-peer-policy</p> <p>Example: bng.nokia.com</p> |
| 268 | Result-Code | <p>Values:</p> <p>2002 = Diameter Limited Success</p> <p>5002 = Diameter Unknown Session ID</p> <p>5012 = Diameter Unable To Comply - AVP parsing errors or message errors</p> |
| 296 | Origin-Realm | <p>Diameter Identity. As configured in the corresponding diameter-peer-policy</p> <p>Example: nokia.com</p> |

Table 27: Diameter Gy RAA: top level AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|----------|--------------|-------------------|-------------------|-------|
| 263 | Session-id | RFC 6733 | UTF8 String | M |
| 264 | Origin-Host | RFC 6733 | Diameter Identity | M |
| 268 | Result-Code | RFC 6733/RFC 4006 | Unsigned 32 | M |
| 296 | Origin-Realm | RFC 6733 | Diameter Identity | M |

2.5 Diameter Gy – Abort-Session-Request (ASR) command

2.5.1 Diameter Gy – ASR message format

This section describes the Diameter Gy ASR message format as defined in RFC 6733. Strikethrough formatted AVPs should not appear or are ignored in ASR.

An Abort-Session-Request message triggers a deletion of the Diameter session: an Abort-Session-Answer is generated, followed by a CCR-T. The corresponding subscriber host is deleted from the system.

```
<ASR> ::= < Diameter Header: 274, REQ, PXY >
        < Session-Id >
        { Origin-Host }
        { Origin-Realm }
        { Destination-Realm }
        { Destination-Host }
        { Auth-Application-Id }
        { User-Name }
{ Origin-State-Id }
        * { Proxy-Info }
        * { Route-Record }
        * { AVP }
```

2.5.2 Diameter Gy – ASR message top level AVPs

[Table 28: Diameter Gy ASR: top level AVP description](#) provides a detailed description for each top level AVP present in a Diameter Gy ASR message.

Table 28: Diameter Gy ASR: top level AVP description

| AVP code | AVP name | Description |
|----------|---------------------|---|
| 258 | Auth-Application-Id | Fixed value: 4 = Diameter Credit Control Application |
| 263 | Session-id | <p>A session is a logical concept at the application layer that exists between the Diameter client and the Diameter server; it is identified via the Session-Id AVP.</p> <p>Format:</p> <p><DiameterIdentity>;<high 32 bits>;<low 32 bits></p> <ul style="list-style-type: none"> <DiameterIdentity> is the configured origin host <high 32 bits> are encoded as the Diameter initialization time (the number of seconds since 1 Jan 1970) <low 32 bits> are encoded as a sequentially increasing number starting at 1 <p>Example:</p> |

| AVP code | AVP name | Description |
|----------|-------------------|--|
| | | bng.nokia.com;1326398325;1 |
| 264 | Origin-Host | Diameter Identity. Used as destination host in the next Diameter message. Example: server.nokia.com |
| 283 | Destination-Realm | Diameter Identity. Example: nokia.com |
| 293 | Destination-Host | Diameter Identity. Example: bng.nokia.com |
| 296 | Origin-Realm | Diameter Identity. Used as destination realm in the next Diameter message. Example: nokia.com |

Table 29: Diameter Gy ASR: top level AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|----------|---------------------|-------------------|-------------------|-------|
| 258 | Auth-Application-Id | RFC 6733/RFC 4006 | Unsigned 32 | M |
| 263 | Session-id | RFC 6733 | UTF8 String | M |
| 264 | Origin-Host | RFC 6733 | Diameter Identity | M |
| 283 | Destination-Realm | RFC 6733 | Diameter Identity | M |
| 293 | Destination-Host | RFC 6733 | Diameter Identity | M |
| 296 | Origin-Realm | RFC 6733 | Diameter Identity | M |

2.6 Diameter Gy – Abort-Session-Answer (ASA) command

2.6.1 Diameter Gy – ASA message format

This section describes the Diameter Gy ASA message format as defined in RFC 6733. Strikethrough formatted AVPs are not included in ASA.

```
<ASA> ::= < Diameter Header: 274, PXY >
        < Session-Id >
        { Result-Code }
        { Origin-Host }
        { Origin-Realm }
        { User-Name }
        { Origin-State-Id }
        { Error-Message }
```



```

{ Error-Reporting-Host }
{ Failed-AVP }
    * { Redirect-Host }
{ Redirect-Host-Usage }
{ Redirect-Max-Cache-Time }
    * { Proxy-Info }
    * { AVP }

```

2.6.2 Diameter Gy – ASA message top level AVPs

[Table 30: Diameter Gy ASA: top level AVP description](#) provides a detailed description for each top level AVP present in a Diameter Gy ASA message.

Table 30: Diameter Gy ASA: top level AVP description

| AVP code | AVP name | Description |
|----------|--------------|---|
| 263 | Session-id | <p>A session is a logical concept at the application layer that exists between the Diameter client and the Diameter server; it is identified via the Session-Id AVP.</p> <p>Format:</p> <p><DiameterIdentity>;<high 32 bits>;<low 32 bits></p> <ul style="list-style-type: none"> • <DiameterIdentity> is the configured origin host • <high 32 bits> are encoded as the Diameter initialization time (the number of seconds since 1 Jan 1970) • <low 32 bits> are encoded as a sequentially increasing number starting at 1 <p>Example:</p> <p>bng.nokia.com;1326398325;1</p> |
| 264 | Origin-Host | <p>Diameter Identity. As configured in the corresponding diameter-peer-policy</p> <p>Example: bng.nokia.com</p> |
| 268 | Result-Code | <p>Values:</p> <p>2002 = Diameter Limited Success</p> <p>5002 = Diameter Unknown Session ID</p> <p>5012 = Diameter Unable To Comply — AVP parsing errors or message errors</p> |
| 296 | Origin-Realm | <p>Diameter Identity. As configured in the corresponding diameter-peer-policy</p> <p>Example: nokia.com</p> |

Table 31: Diameter Gy ASA: top level AVP format

| AVP code | AVP name | Standard | Data format | Flags |
|----------|--------------|-------------------|-------------------|-------|
| 263 | Session-id | RFC 6733 | UTF8 String | M |
| 264 | Origin-Host | RFC 6733 | Diameter Identity | M |
| 268 | Result-Code | RFC 6733/RFC 4006 | Unsigned 32 | M |
| 296 | Origin-Realm | RFC 6733 | Diameter Identity | M |

3 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.

3.1 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*

3.2 Bidirectional Forwarding Detection (BFD)

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

draft-ietf-lsr-ospf-bfd-strict-mode-10, *OSPF BFD Strict-Mode*

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*

3.3 Border Gateway Protocol (BGP)

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

draft-hares-idr-update-attr-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*

3.4 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*
BBF TR-459.2, *Multi-Service Disaggregated BNG with CUPS: Integrated Carrier Grade NAT function*
RFC 8300, *Network Service Header (NSH)*

3.5 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*

3.6 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*

3.7 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*

3.8 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 9047, *Propagation of ARP/ND Flags in an Ethernet Virtual Private Network (EVPN)*

RFC 9135, *Integrated Routing and Bridging in Ethernet VPN (EVPN) – Asymmetric IRB Procedures and Mobility Procedure*

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)*

3.9 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 0.8.0, *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*

3.10 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 routing 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 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 – sections 2.1 and 2.3*

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*

3.11 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*

3.12 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*

3.13 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 Rendezvous 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)*

3.14 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*

3.15 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*

3.16 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)*

3.17 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-ldp-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*

3.18 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"*

3.19 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 7308, *Extended Administrative Groups in MPLS Traffic Engineering (MPLS-TE)*
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*

3.20 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*

3.21 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*

3.22 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*

3.23 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 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*

3.24 OpenFlow

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

3.25 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 8253, *PCEPS: Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)*
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*

3.26 Point-to-Point Protocol (PPP)

RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*
RFC 1990, *The PPP Multilink Protocol (MP)*
RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*
RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*
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*

3.27 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*

3.28 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*

3.29 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)*

3.30 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*

3.31 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 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 5712, *MPLS Traffic Engineering Soft Preemption*
RFC 5817, *Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks*

3.32 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*

3.33 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-bgp-ls-srv6-ext-13, *BGP Link State Extensions for SRv6*

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 coexistence*

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)*

3.34 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*

3.35 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*

3.36 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*

3.37 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)*

3.38 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*

3.39 Wireless Local Area Network (WLAN) gateway

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

3.40 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*

3.41 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 0.2.2, *OpenConfig BFD Module*

openconfig-bgp.yang version 6.1.0, *OpenConfig BGP Module*

openconfig-bgp-common.yang version 6.0.0, *OpenConfig BGP Common Module*

openconfig-bgp-common-multiprotocol.yang version 6.0.0, *OpenConfig BGP Common Multiprotocol Module*

openconfig-bgp-common-structure.yang version 6.0.0, *OpenConfig BGP Common Structure Module*

openconfig-bgp-global.yang version 6.0.0, *OpenConfig BGP Global Module*

openconfig-bgp-neighbor.yang version 6.1.0, *OpenConfig BGP Neighbor Module*

openconfig-bgp-peer-group.yang version 6.1.0, *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 1.2.0, *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 0.15.0, *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 0.4.2, *OpenConfig Port Module*

openconfig-platform-transceiver.yang version 0.9.0, *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 0.10.1, *OpenConfig System Module*

openconfig-system-grpc.yang version 1.0.0, *OpenConfig System gRPC 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 1.9.0, *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](#)