7750 Service Router
Virtualized Service Router
Release 25.10.R1

Gy AVPs Reference Guide

3HE 21204 AAAC TQZZA 01
Edition: 01
October 2025

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

Table of contents

1 Getting started 6
1.1 About this guide 6
1.1.1 Audience 6
1.1.2 References 6

2 Diameter Gy interface specification 7

3 Diameter Gy - Credit-Control-Request (CCR) command 8
3.1 Diameter Gy – CCR message top level AVPs 9
3.2 Diameter Gy – CCR message grouped AVPs 26
3.2.1 Diameter Gy CCR – Subscription-Id grouped AVP 26
3.2.2 Diameter Gy CCR – Multiple-Services-Credit-Control grouped AVP 27
3.2.3 Diameter Gy CCR – Requested-Service-Unit grouped AVP 29
3.2.4 Diameter Gy CCR – Used-Service-Unit grouped AVP 29
3.2.5 Diameter Gy CCR - User-Equipment-Info grouped AVP 31
3.2.6 Diameter Gy CCR – Service-Information grouped AVP 32
3.2.7 Diameter Gy CCR – PS-Information grouped AVP 32

4 Diameter Gy – Credit-Control-Answer (CCA) command 34
4.1 Diameter Gy – CCA message top level AVPs 34
4.2 Diameter Gy – CCA message grouped AVPs 38
4.2.1 Diameter Gy CCA – Failed-AVP grouped AVP 38
4.2.2 Diameter Gy CCA – Multiple-Services-Credit-Control grouped AVP 38
4.2.3 Diameter Gy CCA – Final-Unit-Indication grouped AVP 40
4.2.4 Diameter Gy CCA - Redirect-Server grouped AVP 42
4.2.5 Diameter Gy CCA – Granted-Service-Unit grouped AVP 43

5 Diameter Gy – Re-Auth-Request (RAR) command 45
5.1 Diameter Gy – RAR message format 45
5.2 Diameter Gy – RAR message top level AVPs 45

6 Diameter Gy – Re-Auth-Answer (RAA) command 47
6.1 Diameter Gy – RAA message format 47
6.2 Diameter Gy – RAA message top level AVPs 47

7 Diameter Gy – Abort-Session-Request (ASR) command....49
7.1 Diameter Gy – ASR message format....49
7.2 Diameter Gy – ASR message top level AVPs....49

8 Diameter Gy – Abort-Session-Answer (ASA) command....51
8.1 Diameter Gy – ASA message format....51
8.2 Diameter Gy – ASA message top level AVPs....51

9 Standards and protocol support....53
9.1 Access Node Control Protocol (ANCP)....53
9.2 Bidirectional Forwarding Detection (BFD)....53
9.3 Border Gateway Protocol (BGP)....53
9.4 Bridging and management....55
9.5 Broadband Network Gateway (BNG) Control and User Plane Separation (CUPS)....56
9.6 Certificate management....56
9.7 Circuit emulation....57
9.8 Ethernet....57
9.9 Ethernet VPN (EVPN)....57
9.10 gRPC Remote Procedure Calls (gRPC)....58
9.11 Intermediate System to Intermediate System (IS-IS)....58
9.12 Internet Protocol (IP) Fast Reroute (FRR)....59
9.13 Internet Protocol (IP) general....60
9.14 Internet Protocol (IP) multicast....61
9.15 Internet Protocol (IP) version 4....62
9.16 Internet Protocol (IP) version 6....63
9.17 Internet Protocol Security (IPsec)....64
9.18 Label Distribution Protocol (LDP)....66
9.19 Layer Two Tunneling Protocol (L2TP) Network Server (LNS)....66
9.20 Multiprotocol Label Switching (MPLS)....67
9.21 Multiprotocol Label Switching - Transport Profile (MPLS-TP)....67
9.22 Network Address Translation (NAT)....68
9.23 Network Configuration Protocol (NETCONF)....68
9.24 Media Sanitization....68
9.25 Open Shortest Path First (OSPF)....69
9.26 OpenFlow....69

9.27 Path Computation Element Protocol (PCEP)..... 70
9.28 Point-to-Point Protocol (PPP)..... 70
9.29 Policy management and credit control..... 70
9.30 Pseudowire (PW)..... 71
9.31 Quality of Service (QoS)..... 71
9.32 Remote Authentication Dial In User Service (RADIUS)..... 72
9.33 Resource Reservation Protocol - Traffic Engineering (RSVP-TE)..... 72
9.34 Routing Information Protocol (RIP)..... 73
9.35 Segment Routing (SR)..... 73
9.36 Simple Network Management Protocol (SNMP)..... 74
9.37 Timing..... 76
9.38 Two-Way Active Measurement Protocol (TWAMP)..... 77
9.39 Virtual Private LAN Service (VPLS)..... 77
9.40 Voice and video..... 78
9.41 Yet Another Next Generation (YANG)..... 78
9.42 Yet Another Next Generation (YANG) OpenConfig Models..... 78

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 MD-CLI and the classic 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

3 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 ]~~
                                  [ User-Equipment-Info ]
                                 ~~*[ Proxy-Info ]~~
~~*[ Route-Record ]~~
                                 *[ 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 ]
```

3.1 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	RADIUS username
		The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy aaa-user-name`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp radius-user-name`
		default: not included

8	Framed-IP-Address	The IP address of the IPv4 subscriber host that triggered the creation of the Diameter Gy session.
		The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp address-avp`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp address-avp`
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`

AVP code	AVP name	Description
		• **classic CLI** `configure subscriber-mgmt diameter-application-policy gy include-avp ps-information` default: included

30	Called-Station-Id	The AVP is included if configured in the diameter application policy command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp called-station-id`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp called-station-id`
		Included at the command level or embedded within the [3GPP – 873] Service-Information / [3GPP – 874] PS-Information grouped AVPs using the following commands:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ps-information`
		value: string up to 64 characters
		default: no called-station-id

55	Event-Timestamp	Timestamp when the request was generated.
97	Framed-IPv6-Prefix	The IPv6 prefix of the SLAAC subscriber host that triggered the creation of the Diameter Gy session. The AVP is included if configured in the diameter application policy using the following command: • **MD-CLI** `configure subscriber-mgmt diameter-gy-policy gy include-avp address-avp` • **classic CLI** `configure subscriber-mgmt diameter-gy-policy gy include-avp address-avp`

AVP code	AVP name	Description

		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ps-information`
		default: included

123	Delegated-IPv6-Prefix	The IPv6 prefix of the DHCPv6 IA-PD subscriber host that triggered the creation of the Diameter Gy session.
		The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp address-avp`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp address-avp`
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ps-information`
		default: included

258	Auth-Application-Id	Fixed value: 4 = Diameter Credit Control Application
263	Session-Id	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. Format:

AVP code	AVP name	Description
		<DiameterIdentity>; <high 32 bits>; <low 32 bits> • <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 Example: bng.nokia.com;1326398325;1
264	Origin-Host	Diameter Identity. As configured in the corresponding diameter-peer-policy. Example: bng.nokia.com
278	Origin-State-Id	Initialized to the Diameter process startup time. Encoded as number of seconds since 1 January, 1970.
283	Destination-Realm	Diameter Identity. As configured in the corresponding diameter-peer-policy or learned from CCA/RAR. Example: nokia.com
293	Destination-Host	Diameter Identity. As configured in the corresponding diameter-peer-policy or learned from CCA/RAR. Omitted in CCR-I if not configured. Example: server.nokia.com
295	Termination-Cause	(CCR-T only) 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	Identifies the subscriber host or session. The value is as configured in the diameter application policy:

AVP code	AVP name	Description

	↳ (grouped AVP)	• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy avp-subscription-id origin`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy avp-subscription-id origin`
		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 to a category configured in a category-map using the following commands. `configure subscriber-mgmt category-map category rating-group`

458	User-Equipment-Info
	↳ (grouped AVP)
		(GTP access only)
		The AVP is included if configured in the diameter application policy:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp user-equipment-info-type type imeisv`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp user-equipment-info type imeisv`
		value: IMEI as signaled in the GTP Create Session Request message.
		default: not included

461	Service-Context-Id	The AVP is included if configured in the diameter application policy using the following command:

AVP code	AVP name	Description

		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp service-context-id`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp service-context-id`
		value: string of up to 32 characters
		default: no service-context-id

NOKIA – 99	Alc-IPv6-Address	The IPv6 address of the DHCPv6 IA-NA subscriber host that triggered the creation of the Diameter Gy session.
		The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp address-avp`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp address-avp`
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ps-information`
		default: included

3GPP – 1	3GPP-IMSI	The AVP is included if configured in the diameter application policy using the following command: • **MD-CLI** `configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-imsi`

AVP code	AVP name	Description

		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-imsi`
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ps-information`
		values:
		• circuit-id
		• imsi
		• subscriber-id
		default: included with value subscriber-id

3GPP – 2	3GPP-Charging-Id	The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-charging-id`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-charging-id`
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ps-information`
		.

AVP code	AVP name	Description
		values: • 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 default: included with esm-info value (auto)

3GPP – 5	3GPP-GPRS-QoS-Negotiated-Profile	The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-gprs-negotiated-qos-profile`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-gprs-negotiated-qos-profile`
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ps-information`
		value: the active SLA profile name
		default: included

3GPP – 7	3GPP-GGSN-Address	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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-ggsn-ipv4-address`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-ggsn-address`

AVP code	AVP name	Description

		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ps-information`
		Value:
		1. Use the configured IPv4 source address:
		• **MD-CLI**
		`configure aaa diameter-peer-policy ipv4-source-address`
		• **classic CLI**
		`configure aaa diameter-peer-policy source-address`
		2. If the router equals base or vprn service id, use the system interface IPv4 address
		else if the router equals management, use the active management port IP address configured in the BOF
		default: included

3GPP – 10	3GPP-NSAPI	The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-nsapi`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-nsapi`
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`

AVP code	AVP name	Description
		• **classic CLI** `configure subscriber-mgmt diameter-application-policy gy include-avp ps-information` value: <system name>;<service-id>;<sap-id> default: included

3GPP – 11	3GPP-Session-Stop-Indicator	(CCR-T only)
		The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-session-stop-indicator`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-session-stop-indicator`
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ps-information`
		Fixed value: 0x FF
		default: included

3GPP – 12	3GPP-Selection-Mode	The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-selection-mode`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-selection-mode`

AVP code	AVP name	Description

		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ps-information`
		Fixed value: 0x 00 00 00 00 (MS or network provided APN, subscribed verified)
		default: included

3GPP – 13	3GPP-Charging-Characteristics	The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-charging-characteristics`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-charging-characteristics`
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ps-information`
		Fixed value: "0000”
		default: included

3GPP – 16	3GPP-GGSN-v6-Address	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:

AVP code	AVP name	Description

		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-ggsn-ipv6-address`
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ps-information`
		value:
		1. Use the configured IPv6 source address:
		`configure aaa diameter peer-policy ipv6-source-address`
		2. If router = base or vprn service id: use the system interface IPv6 address
		else if router = management: use the active management port IP address configured in the BOF
		default: not included

3GPP – 21	3GPP-RAT-Type	The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp three-gpp-rat-type`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp 3gpp-rat-type`

AVP code	AVP name	Description
		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: `gy include-avp ps-information` value: [1 to 255] default: not included 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.

3GPP - 22	3GPP-User-Location-Info	(GTP access only)
		Provides UE location details
		The AVP is included if configured in the diameter application policy:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp 3gpp-user-location-info`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp three-gpp-user-location-info`
		value: ULI learned from the GTP Create Session Request message.
		default: not included

3GPP – 847	GGSN-Address	The local address used to setup the diameter peer.
		The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp ggsn-address type (ipv4 | ipv6)`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy include-avp ggsn-address {ipv4 | ipv6}`
		Either IPv4 or IPv6 address can be included.

AVP code	AVP name	Description

		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:
		`gy include-avp ps-information`
		value:
		1. Use the configured IP source address:
		• **MD-CLI**
		`configure aaa diameter peer-policy ipv6-source-address`
		`configure aaa diameter peer-policy ipv4-source-address`
		• **classic CLI**
		`configure aaa diameter-peer-policy ipv6-source-address`
		`configure aaa diameter-peer-policy ipv4-source-address`
		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
		default: not included

3GPP – 873	Service-Information ↳ (grouped AVP)	Grouped AVP containing the [3GPP – 874] PS-Information grouped AVP and embedding following AVPs: • [8] Framed-IP-Address • [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

AVP code	AVP name	Description
		• [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 The AVP is included if configured in the diameter application policy using the following command: • **MD-CLI** `configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information` • **classic CLI** `configure subscriber-mgmt diameter-gy-policy gy include-avp ps-information` When not configured the above listed AVPs are included at command level. default: no ps-information

3GPP – 1004	Charging-Rule-Base-Name	The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp charging-rule-base-name category-map`
		• **classic CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp charging-rule-base-name category-map-name`
		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:
		`gy include-avp ps-information`
		value:
		• category-map-name: the name of the category-map in use for this session
		• string: a string of max. 64 characters.
		default: charging-rule-base-name category-map-name

AVP code	AVP name	Description

3GPP – 1247	PDP-Context-Type	(CCR-I only)
		The AVP is included if configured in the diameter application policy using the following command:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp pdp-context-type`
		• **classic CLI**
		`configure subscriber-mgmt diameter-gy-policy gy include-avp pdp-context-type`
		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:
		`gy include-avp ps-information`
		Fixed value: 0 (primary)
		default: included

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
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

AVP code	AVP name	Standard	Data format	Flags
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
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

3.2 Diameter Gy – CCR message grouped AVPs

This section provides an overview of CCR message grouped AVPs.

3.2.1 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	Value as configured in the diameter application policy:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy avp-subscription-id origin`
		`configure subscriber-mgmt diameter-gy-policy gy avp-subscription-id type`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy avp-subscription-id origin (circuit-id|dual-stack-remote-id|imei|imsi|mac|msisdn|nas-port-id|subscriber-id|username) [type (e164|imsi|nai|private)]`
		values:
		• 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
		default: type private
		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.

444	Subscription-Id-Data	The value as configured in the diameter application policy: • **MD-CLI** `configure subscriber-mgmt diameter-gy-policy gy avp-subscription-id origin`

AVP code	AVP name	Description

		`configure subscriber-mgmt diameter-gy-policy gy avp-subscription-id type`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy avp-subscription-id origin [type]`
		Note that there is no check if the provided data is in the format of the following configured type.
		values:
		• circuit-id
		• subscriber-id
		• imsi
		• msisdn
		• imei
		default: avp-subscription-id subscriber-id
		For GTP access, the Subscription ID data is learned from GTP and contains the IMSI and MSISDN.

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

3.2.2 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 • 0 (Threshold): used quota reached time or volume threshold value (threshold value different from zero) • 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 Reauthorization): 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

3.2.3 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.

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

Grouped AVP format as defined in RFC 4006. ~~Strikethough~~ 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	Number of ingress bytes forwarded via queues or policers that are monitored in the ingress direction for this rating group.

AVP code	AVP name	Description

		• **MD-CLI**
		`configure subscriber-mgmt category-map category ingress policer value`
		`configure subscriber-mgmt category-map category ingress queue value`
		• classic CLI
		`configure subscriber-mgmt category-map category queue queue-id {ingress-only}`
		`configure subscriber-mgmt category-map category policer policer-id {ingress-only}`
		Value equals zero when credit type is time or when no queues/policers are monitored in ingress direction.

414	CC-Output-Octets	Number of egress bytes forwarded via queues or policers that are monitored in egress direction for this rating group.
		• **MD-CLI**
		`configure subscriber-mgmt category-map category egress policer value`
		`configure subscriber-mgmt category-map category egress queue value`
		• classic CLI
		`configure subscriber-mgmt category-map category queue queue-id {egress-only}`
		`configure subscriber-mgmt category-map category policer policer-id {egress-only}`
		Value equals zero when credit type is time. Or when no queues/policers are monitored in egress direction.

420	CC-Time	Total number of seconds during which activity is detected for queues or policers that are monitored for this rating group.
		• **MD-CLI**
		`configure subscriber-mgmt category-map category ingress policer value`
		`configure subscriber-mgmt category-map category ingress queue value`
		• **classic CLI**
		`configure subscriber-mgmt category-map category queue queue-id {ingress-only | egress-only | ingress-egress}`

AVP code	AVP name	Description

		`configure subscriber-mgmt category-map category policer policer-id {ingress-only | egress-only | ingress-egress}`
		Only sampling periods exceeding the configured activity-threshold are counted:
		`configure subscriber-mgmt category-map activity-threshold`
		Value equals zero when credit type is volume.

421	CC-Total-Octets	Total number of bytes used for this rating-group. Corresponds with the sum of CC-Input-Octets and CC-Output-Octets. Value equals zero when credit type is time.

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

3.2.5 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	

3.2.6 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

3.2.7 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 ]
```

4 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 ]
```

4.1 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 – CCA 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

AVP code	AVP name	Description
263	Session-id	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. Format: <DiameterIdentity>;<high 32 bits>;<low 32 bits> • <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 Example: bng.nokia.com;1326398325;1
264	Origin-Host	Diameter Identity. Used as destination host in the next Diameter message. Example: server.nokia.com
268	Result-Code	Values: 2001 = Diameter Success 3xxx = Protocol Errors 4001 = Diameter Authentication Rejected 4010 = Diameter End User Service Denied (CCA-U only) 4011 = Diameter Credit Control Not Applicable 4012 = Diameter Credit Limit Reached (CCA-U only) 5003 = Diameter Authorization Rejected 5030 = Diameter User Unknown 5031 = Diameter Rating Failed (CCA-U only) Values not listed result in a Diameter Session Failure and the Credit Control Failure Handling action is executed.
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

AVP code	AVP name	Description
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy on-failure failover [true | false] handling [terminate | continue | retry-and-terminate]`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy on-failure [failover {enabled | disabled}] [handling {continue | retry-and-terminate | terminate}]`
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy on-failure failover enabled handling [terminate | continue | retry-and-terminate]`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy on-failure [failover {enabled|disabled}] [handling {continue | retry-and-terminate | terminate}]`
		Values:
		0 = Terminate
		1 = Continue

AVP code	AVP name	Description
		2 = Retry and terminate
456	Multiple-Services-Credit-Control ↳ (grouped AVP)	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: `configure subscriber-mgmt category-map category rating-group`
3GPP – 1004	Charging-Rule-Base-Name	(CCA-I only) Assigns the category-map or overrides the category-map obtained in authentication. value: category-map-name: the name of the category-map to be used for this session

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
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

4.2 Diameter Gy – CCA message grouped AVPs

This section provides an overview of CCA message grouped AVPs.

4.2.1 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.

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

Grouped AVP 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.

```
  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	Values: 2001 = Diameter Success 4010 = Diameter End User Service Denied 4011 = Diameter Credit Control Not Applicable 4012 = Diameter Credit Limit Reached 5003 = Diameter Authorization Rejected 5031 = Diameter Rating Failed Values not listed result in a Diameter Session Failure and the Credit Control Failure Handling action is executed.

AVP code	AVP name	Description

430	Final-Unit-Indication
	↳ (grouped AVP)
		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:
		• **MD-CLI**
		`configure subscriber-mgmt diameter-gy-policy gy out-of-credit-reporting quota-exhausted`
		• **classic CLI**
		`configure subscriber-mgmt diameter-application-policy gy out-of-credit-reporting quota-exhausted`

431	Granted-Service-Unit ↳ (grouped AVP)	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.
432	Rating-Group	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. `configure subscriber-mgmt category-map category rating-group`
448	Validity-Time	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). Value in seconds
3GPP – 868	Time-Quota-Threshold	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). 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

4.2.3 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
434	Redirect-Server ↳ (grouped AVP)	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: • **MD-CLI** `configure subscriber-mgmt category-map category exhausted-credit-service-level ingress ip-filter entry 1 action http-redirect`

AVP code	AVP name	Description
		• **classic CLI** `configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry action http-redirect url allow-override` 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.

449	Final-Unit-Action	If the value is Terminate, then the session is terminated and the corresponding subscriber host deleted.
		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:
		`configure subscriber-mgmt credit-control-policy out-of-credit-action`
		Alternately, the following command can be used to configure out of credit action:
		`configure subscriber-mgmt category-map category out-of-credit-action-override`
		Values:
		0 = Terminate
		1 = Redirect
		2 = Restrict Access

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

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

4.2.4 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	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.
		The URL specified in the Redirect-Server-Address AVP is only used when all following conditions are met:
		• 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:
		`configure subscriber-mgmt credit-control-policy out-of-credit-action change-service-level`
		Alternately, the following command can be used to set the change service level:
		`configure subscriber-mgmt category-map category out-of-credit-action-override change-service-level`
		• An IPv4 HTTP redirect action with allow-override is specified as exhausted-credit-service-level for the corresponding rating group:
		– **MD-CLI**
		`configure subscriber-mgmt category-map category exhausted-credit-`

AVP code	AVP name	Description
		service-level ingress ip-filter entry action http-redirect url allow-override – **classic CLI** configure subscriber-mgmt category-map category exhausted-credit-service-level ingress-ip-filter-entries entry action http-redirect url allow-override
435 (continued)		In all other cases, the Redirect-Server-Address AVP is ignored. 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.

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

4.2.5 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

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

5.1 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 ]
```

5.2 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	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. Format: <DiameterIdentity>;<high 32 bits>;<low 32 bits> • <DiameterIdentity> is the configured origin host

AVP code	AVP name	Description
		• <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 Example: 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
285	Re-Auth-Request-Type	Values: 0 = Authorize-Only
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 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

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

6.1 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 ]~~
```

6.2 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	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. Format: <DiameterIdentity>;<high 32 bits>;<low 32 bits> • <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

AVP code	AVP name	Description
		Example: bng.nokia.com;1326398325;1
264	Origin-Host	Diameter Identity. As configured in the corresponding diameter-peer-policy Example: bng.nokia.com
268	Result-Code	Values: 2002 = Diameter Limited Success 5002 = Diameter Unknown Session ID 5012 = Diameter Unable To Comply - AVP parsing errors or message errors
296	Origin-Realm	Diameter Identity. As configured in the corresponding diameter-peer-policy Example: nokia.com

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

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

7.1 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 ]
```

7.2 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	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. Format: <DiameterIdentity>;<high 32 bits>;<low 32 bits> • <DiameterIdentity> is the configured origin host • <high 32 bits> are encoded as the Diameter initialization time (the number of seconds since 1 Jan 1970)

AVP code	AVP name	Description
		• <low 32 bits> are encoded as a sequentially increasing number starting at 1 Example: 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

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

8.1 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 ]~~
```

8.2 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	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. Format: <DiameterIdentity>;<high 32 bits>;<low 32 bits> • <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

AVP code	AVP name	Description
		Example: bng.nokia.com;1326398325;1
264	Origin-Host	Diameter Identity. As configured in the corresponding diameter-peer-policy Example: bng.nokia.com
268	Result-Code	Values: 2002 = Diameter Limited Success 5002 = Diameter Unknown Session ID 5012 = Diameter Unable To Comply — AVP parsing errors or message errors
296	Origin-Realm	Diameter Identity. As configured in the corresponding diameter-peer-policy Example: nokia.com

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

9 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.

9.1 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*

9.2 Bidirectional Forwarding Detection (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*

RFC 9247, *BGP - Link State (BGP-LS) Extensions for Seamless Bidirectional Forwarding Detection (S-BFD)*

9.3 Border Gateway Protocol (BGP)

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

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

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

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

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

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

draft-ietf-idr-bgp-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*

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 6368, *Internal BGP as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*

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 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*

RFC 9294, *Application-Specific Link Attributes Advertisement Using the Border Gateway Protocol - Link State (BGP LS)*

RFC 9351, *Border Gateway Protocol - Link State (BGP-LS) Extensions for Flexible Algorithm Advertisement*

RFC 9494, *Long-Lived Graceful Restart for BGP*

RFC 9552, *Distribution of Link-State and Traffic Engineering Information Using BGP*

9.4 Bridging and management

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*

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

3GPP TS 23.003, *Numbering, addressing and identification*

3GPP TS 23.007, *Restoration procedures*

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

3GPP TS 23.501, *System architecture for the 5G System (5GS)*

3GPP TS 23.502, *Procedures for the 5G System (5GS)*

3GPP TS 23.503, *Policy and charging control framework for the 5G System (5GS)*

3GPP TS 24.501, *Non-Access-Stratum (NAS) protocol for 5G System (5GS)*

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

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

3GPP TS 29.500, *Technical Realization of Service Based Architecture*

3GPP TS 29.501, *Principles and Guidelines for Services Definition*

3GPP TS 29.502, *Session Management Services*

3GPP TS 29.503, *Unified Data Management Services*

3GPP TS 29.512, *Session Management Policy Control Service*

3GPP TS 29.518, *Access and Mobility Management Services*

3GPP TS 32.255, *5G data connectivity domain charging*

3GPP TS 32.290, *Services, operations and procedures of charging using Service Based Interface (SBI)*

3GPP TS 32.291, *5G system, charging service*

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)*

RFC 8910, *Captive-Portal Identification in DHCP and Router Advertisements (RAs)*

9.6 Certificate management

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

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

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

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

RFC 7030, *Enrollment over Secure Transport*

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

9.7 Circuit emulation

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

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

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

9.8 Ethernet

IEEE 802.3ah, *Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks*

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*

9.9 Ethernet VPN (EVPN)

draft-ietf-bess-evpn-ip-aliasing-03, *EVPN Support for L3 Fast Convergence and Aliasing/Backup Path*

draft-ietf-bess-evpn-ipvpn-interworking-14, *EVPN Interworking with IPVPN*

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

draft-sr-bess-evpn-vpws-gateway-03, *Ethernet VPN Virtual Private Wire Services Gateway Solution*

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 9014, *Interconnect Solution for Ethernet VPN (EVPN) Overlay Networks*

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

RFC 9135, *Integrated Routing and Bridging in Ethernet VPN (EVPN)*

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)*

RFC 9541, *Flush Mechanism for Customer MAC Addresses Based on Service Instance Identifier (I-SID) in Provider Backbone Bridging EVPN (PBB-EVPN)*

RFC 9625, *EVPN Optimized Inter-Subnet Multicast (OISM) Forwarding* – ingress replication and mLDP

RFC 9784, *Virtual Ethernet Segments for EVPN and Provider Backbone Bridge EVPN*

RFC 9785, *Preference-Based EVPN Designated Forwarder (DF) Election*

RFC 9819, *Argument Signaling for BGP Services in Segment Routing over IPv6 (SRv6)*

9.10 gRPC Remote Procedure Calls (gRPC)

cert.proto version 0.1.0, *gNOI Certificate Management Service*

file.proto version 0.1.0, *gNOI File Service*

gnmi.proto version 0.8.0, *gNMI Service Specification*

gnmi_ext.proto, *gNMI Commit Confirmed Extension*

gnmi_ext.proto, *gNMI Config Subscription Extension*

gnmi_ext.proto, *gNMI Depth Extension*

system.proto version 1.0.0, *gNOI System Service*

tunnel.proto version 0.2, *gRPC Tunnel Service*

PROTOCOL-HTTP2, *gRPC over HTTP2*

9.11 Intermediate System to Intermediate System (IS-IS)

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

draft-ietf-lsr-igp-ureach-prefix-announce-01, *IGP Unreachable Prefix Announcement* – without U-Flag and UP-Flag

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

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

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

RFC 2973, *IS-IS Mesh Groups*

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

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

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

RFC 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 7981, *IS-IS Extensions for Advertising Router Information*

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*

9.12 Internet Protocol (IP) Fast Reroute (FRR)

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

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

RFC 7431, *Multicast-Only Fast Reroute*

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

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

9.13 Internet Protocol (IP) general

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 5289, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*

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*

RFC 8907, *The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol*

9.14 Internet Protocol (IP) multicast

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

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

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

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

RFC 1112, *Host Extensions for IP Multicasting*

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

RFC 2365, *Administratively Scoped IP Multicast*

RFC 2375, *IPv6 Multicast Address Assignments*

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

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

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

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

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

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

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

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

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

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

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

RFC 4607, *Source-Specific Multicast for IP*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RFC 9573, *MVPN/EVPN Tunnel Aggregation with Common Labels* – DCB and static service labels

9.15 Internet Protocol (IP) version 4

RFC 791, *Internet Protocol*

RFC 792, *Internet Control Message Protocol*

RFC 826, *An Ethernet Address Resolution Protocol*

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

RFC 1034, *Domain Names - Concepts and Facilities*

RFC 1035, *Domain Names - Implementation and Specification*

RFC 1191, *Path MTU Discovery* – router specification

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

RFC 1534, *Interoperation between DHCP and BOOTP*

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

RFC 1812, *Requirements for IPv4 Routers*

RFC 1918, *Address Allocation for Private Internets*

RFC 2003, *IP Encapsulation within IP*

RFC 2131, *Dynamic Host Configuration Protocol*

RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

RFC 2401, *Security Architecture for Internet Protocol*

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

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

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

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

9.16 Internet Protocol (IP) version 6

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

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

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

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

RFC 3587, *IPv6 Global Unicast Address Format*

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

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

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

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

RFC 3971, *SEcure Neighbor Discovery (SEND)*

RFC 3972, *Cryptographically Generated Addresses (CGA)*

RFC 4007, *IPv6 Scoped Address Architecture*

RFC 4191, *Default Router Preferences and More-Specific Routes* – Default Router Preference

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 6221, *Lightweight DHCPv6 Relay Agent*

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*

9.17 Internet Protocol Security (IPsec)

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

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

RFC 2401, *Security Architecture for the Internet Protocol*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RFC 3948, *UDP Encapsulation of IPsec ESP Packets*

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

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

RFC 4301, *Security Architecture for the Internet Protocol*

RFC 4303, *IP Encapsulating Security Payload*

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

RFC 4308, *Cryptographic Suites for IPsec*

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

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

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

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

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

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

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

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

RFC 5903, *ECP Groups for IKE and IKEv2*

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

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

RFC 6379, *Suite B Cryptographic Suites for IPsec*

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

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

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

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

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

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

RFC 8784, *Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security*

9.18 Label Distribution Protocol (LDP)

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

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

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

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

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

RFC 3037, *LDP Applicability*

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

RFC 5036, *LDP Specification*

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

RFC 5443, *LDP IGP Synchronization*

RFC 5561, *LDP Capabilities*

RFC 5919, *Signaling LDP Label Advertisement Completion*

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

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

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

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

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

RFC 7552, *Updates to LDP for IPv6*

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

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

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

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

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

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

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

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

9.20 Multiprotocol Label Switching (MPLS)

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

RFC 3031, *Multiprotocol Label Switching Architecture*

RFC 3032, *MPLS Label Stack Encoding*

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

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

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

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

RFC 4950, *ICMP Extensions for Multiprotocol Label Switching*

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*

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

RFC 5586, *MPLS Generic Associated Channel*

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

RFC 5960, *MPLS Transport Profile Data Plane Architecture*

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

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

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

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

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

RFC 6478, *Pseudowire Status for Static Pseudowires*

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

9.22 Network Address Translation (NAT)

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

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

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

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*

9.23 Network Configuration Protocol (NETCONF)

RFC 5277, *NETCONF Event Notifications*

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

RFC 6022, *YANG Module for NETCONF Monitoring*

RFC 6241, *Network Configuration Protocol (NETCONF)*

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

RFC 6243, *With-defaults Capability for NETCONF*

RFC 8071, *NETCONF Call Home and RESTCONF Call Home* – 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

9.24 Media Sanitization

NIST Special Publication 800-88 Revision 1, *Guidelines for Media Sanitization* – CF, MMC, SSD, SD, USB

9.25 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*

9.26 OpenFlow

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

9.27 Path Computation Element Protocol (PCEP)

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

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

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

draft-ietf-pce-pceps-tls13-04, *Updates for PCEPS: TLS Connection Establishment Restrictions*

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

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

RFC 8233, *Extensions to the Path Computation Element Communication Protocol (PCEP) to Compute Service-Aware Label Switched Paths (LSPs)* – Path Delay Metric

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*

9.28 Point-to-Point Protocol (PPP)

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

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

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

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*

9.29 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*

9.30 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*

9.31 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)*

9.32 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*

9.33 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 5712, *MPLS Traffic Engineering Soft Preemption*

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

9.34 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*

9.35 Segment Routing (SR)

draft-bashandy-rtgwg-segment-routing-uloop-15, *Loop avoidance using Segment Routing*

draft-filsfils-spring-net-pgm-extension-srv6-usid-15, *Network Programming extension: SRv6 uSID instruction*

draft-filsfils-spring-srv6-net-pgm-insertion-08, *SRv6 NET-PGM extension: Insertion*

draft-ietf-bess-mvpn-evpn-sr-p2mp-07, *Multicast and Ethernet VPN with Segment Routing P2MP and Ingress Replication* – MVPN

draft-ietf-idr-segment-routing-te-policy-23, *Advertising Segment Routing Policies in BGP*

draft-ietf-idr-ts-flowspec-srv6-policy-03, *Traffic Steering using BGP FlowSpec with SR Policy*

draft-ietf-pim-p2mp-policy-ping-03, *P2MP Policy Ping*

draft-ietf-pim-sr-p2mp-policy-06, *Segment Routing Point-to-Multipoint Policy* – MPLS

draft-ietf-rtgwg-segment-routing-ti-lfa-11, *Topology Independent Fast Reroute using Segment Routing*

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

draft-ietf-spring-sr-replication-segment-16, *SR Replication segment for Multi-point Service Delivery* – MPLS

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

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 8426, *Recommendations for RSVP-TE and Segment Routing (SR) Label Switched Path (LSP) Coexistence*

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 9085, *Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing*

RFC 9088, *Signaling Entropy Label Capability and Entropy Readable Label Depth Using IS-IS* – advertising ELC

RFC 9089, *Signaling Entropy Label Capability and Entropy Readable Label Depth Using OSPF* – advertising ELC

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

RFC 9256, *Segment Routing Policy Architecture*

RFC 9259, *Operations, Administration, and Maintenance (OAM) in Segment Routing over IPv6 (SRv6)*

RFC 9350, *IGP Flexible Algorithm*

RFC 9352, *IS-IS Extensions to Support Segment Routing over the IPv6 Data Plane*

RFC 9514, *Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing over IPv6 (SRv6)*

RFC 9800, *Compressed SRv6 Segment List Encoding*

9.36 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 3430, *Simple Network Management Protocol (SNMP) over Transmission Control Protocol (TCP) Transport Mapping*

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 3434, *Remote Monitoring MIB Extensions for High Capacity Alarms*

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 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 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*

9.37 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.811, *Timing characteristics of primary reference clocks*

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.8272 , *Timing characteristics of primary reference time clocks* – PRTC-A, PRTC-B

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

ITU-T G.8275.2, *Precision time protocol telecom profile for phase/time synchronization with partial 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*

RFC 8573, *Message Authentication Code for the Network Time Protocol*

9.38 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

RFC 9503, *Simple Two-Way Active Measurement Protocol (STAMP) Extensions for Segment Routing Networks* – excluding Sections 3, 4.1.2 and 4.1.3

RFC 9534, *Simple Two-Way Active Measurement Protocol Extensions for Performance Measurement on a Link Aggregation Group*

9.39 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)*

9.40 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*

9.41 Yet Another Next Generation (YANG)

RFC 6991, *Common YANG Data Types*

RFC 7950, *The YANG 1.1 Data Modeling Language*

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

9.42 Yet Another Next Generation (YANG) OpenConfig Models

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

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

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

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

openconfig-alarms.yang version 0.3.2, *OpenConfig System Alarms Model*

openconfig-bfd.yang version 0.2.2, *OpenConfig BFD Model*

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

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

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

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

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

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

openconfig-bgp-peer-group.yang version 6.1.0, *OpenConfig BGP Peer Group Model*

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

openconfig-if-aggregate.yang version 2.4.3, *OpenConfig Interfaces Aggregated Model*

openconfig-if-ethernet.yang version 2.12.2, *OpenConfig Interfaces Ethernet Model*

openconfig-if-ip.yang version 3.1.0, *OpenConfig Interfaces IP Model*

openconfig-if-ip-ext.yang version 2.3.1, *OpenConfig Interfaces IP Extensions Model*

openconfig-igmp.yang version 0.3.1, *OpenConfig IGMP Model*

openconfig-interfaces.yang version 3.0.0, *OpenConfig Interfaces Model*

openconfig-isis.yang version 1.1.0, *OpenConfig IS-IS Model*

openconfig-isis-policy.yang version 0.5.0, *OpenConfig IS-IS Policy Model*

openconfig-isis-routing.yang version 1.1.0, *OpenConfig IS-IS Routing Model*

openconfig-lacp.yang version 2.1.0, *OpenConfig LACP Model*

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

openconfig-local-routing.yang version 1.2.0, *OpenConfig Local Routing Model*

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

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

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

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

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

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

openconfig-ospfv2.yang version 0.4.0, *OpenConfig OSPFv2 Model*

openconfig-ospfv2-area.yang version 0.4.0, *OpenConfig OSPFv2 Area Model*

openconfig-ospfv2-area-interface.yang version 0.4.0, *OpenConfig OSPFv2 Area Interface Model*

openconfig-ospfv2-common.yang version 0.4.0, *OpenConfig OSPFv2 Common Model*

openconfig-ospfv2-global.yang version 0.4.0, *OpenConfig OSPFv2 Global Model*

openconfig-packet-match.yang version 1.1.0, *OpenConfig Packet Match Model*

openconfig-pim.yang version 0.4.3, *OpenConfig PIM Model*

openconfig-platform.yang version 0.15.0, *OpenConfig Platform Model*

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

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

openconfig-platform-port.yang version 0.4.2, *OpenConfig Port Model*

openconfig-platform-transceiver.yang version 0.9.0, *OpenConfig Transceiver Model*

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

openconfig-qos.yang version 0.11.2, *OpenConfig QoS Model*

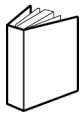
openconfig-qos-elements.yang version 0.11.2, *OpenConfig QoS Elements Model*

openconfig-qos-interfaces.yang version 0.11.2, *OpenConfig QoS Interfaces Model*

openconfig-qos-mem-mgmt.yang version 0.11.2, *OpenConfig QoS Memory Management Model*

openconfig-relay-agent.yang version 0.1.0, *OpenConfig Relay Agent Model*
openconfig-routing-policy.yang version 3.0.0, *OpenConfig Routing Policy Model*
openconfig-rsvp-sr-ext.yang version 0.1.0, *OpenConfig RSVP-TE and SR Extensions Model*
openconfig-system.yang version 0.10.1, *OpenConfig System Model*
openconfig-system-grpc.yang version 1.0.0, *OpenConfig System gRPC Model*
openconfig-system-logging.yang version 0.3.1, *OpenConfig System Logging Model*
openconfig-system-terminal.yang version 0.3.0, *OpenConfig System Terminal Model*
openconfig-telemetry.yang version 0.5.0, *OpenConfig Telemetry Model*
openconfig-terminal-device.yang version 1.9.0, *OpenConfig Terminal Device Model*
openconfig-vlan.yang version 3.2.2, *OpenConfig VLAN Model*

Customer document and product support



Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback