7750 Service Router
Virtualized Service Router
Release 23.7.R1

Gx AVPs Reference Guide

3HE 19218 AAAB TQZZA 01
Edition 01
July 2023

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

Table of contents

1 Gx AVP

This guide provides an overview of supported Gx Attribute Value Pairs (AVP) for the 7750 SR. The implementation is based on Gx Release v11.12, doc 3GPP 29212-bc0.doc.

The AVP descriptions are organized per application.

Table 1: Attribute conventions displays the conventions used in this guide.

Table 1: Attribute conventions

Attribute	Description
0	This attribute must not be present in packet.
0+	Zero or more instances of this attribute may be present in packet.
0-1	Zero or one instance of this attribute may be present in packet.
1	Exactly one instance of this attribute must be present in packet.

2 AVPs

Certain AVPs are applicable in only one direction, while others are applicable to both directions.

AVPs sent by the 7750 SR are used to:

- inform the PCRF of the host creation/termination and the subscriber host identity in the 7750 SR
- inform the PCRF of the functionality supported in the 7750 SR
- report specific events related to the subscriber-host
- report the status of the rules
- report usage monitoring
- report status of the host (existent/non-existent)

AVPs sent by PCRF toward the 7750 SR are used to:

- install or activate policies
- request usage monitoring
- terminate the subscriber-host
- request status of the subscriber-host (existent/non-existent)

AVPs that apply to both directions are used for base Diameter functionality such as peering establishment, routing of the Diameter messages, session identification and reporting of catastrophic failures (OSI change).

3 Reserved keywords in the 7750 SR

The reserved keywords used to identify referenced object type within the 7750 SR are listed in Reserved keywords in the 7750 SR. See Standard diameter AVPs (description) for further reference.

Table 2: Reserved keywords in the 7750 SR

Reserved keywords in the 7750 SR	Used in AVP	Comments
ingr-v4:	charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).
ingr-v6:	charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).
egr-v4:	charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).
egr-v6:	charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).
in-othr-v4:	charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).
in-othr-v6:	charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).
sub-id	charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).
sla-profile:	charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).
sub-profile:	charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).
inter-dest:	charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).

Reserved keywords in the 7750 SR	Used in AVP	Comments
cat-map:	charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).
aa-functions:	adc-rule-name, charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).
aa-functions:app:<string>	charging-rule-name	Used to identify the AA app-profile directly in the charging-rule-name AVP in a charging-rule-install. See Table 3: Standard diameter AVPs (description) and .
aa-functions:aso:<char>:val	charging-rule-name	Used to identify the AA ASO characteristic and value directly in a charging-rule-name AVP in a charging rule-install. Table 4: Standard diameter AVPs (format) and Table 5: NOKIA-specific AVPs.
aa-functions:urlparam:<string>	charging-rule-name	Used to identify the AA Sub HTTP URL parameter directly in a charging-rule-name AVP in a charging rule-install. See Table 4: Standard diameter AVPs (format) and Table 5: NOKIA-specific AVPs.
aa-functions:subscope:<val>	charging-rule-name	Used to identify the AA Sub scope directly in a charging-rule-name AVP in a charging rule-install. See Table 4: Standard diameter AVPs (format) and Table 5: NOKIA-specific AVPs.
aa-um	charging-rule-name	Used to identify referenced object type within 7x50. See Table 3: Standard diameter AVPs (description).

4 Standard diameter AVPs

Applications for which the described AVPs apply:

- Gx-PM-ESM—Policy Management for Enhanced Subscriber Management
- Gx-UM-ESM—Usage Monitoring for Enhanced Subscriber Management
- Gx-PM-AA—Policy Management for Application Assurance
- Gx-UM-AA—Usage Monitoring Application Assurance

The AVPs listed in Table 3: Standard diameter AVPs (description) that do not have an associated application are AVPs that are used for generic purposes and their use can extend through all applications.

Table 3: Standard diameter AVPs (description)

AVP ID	AVP name	Section defined	Application	Description
5	NAS-Port	RFC 2865 / §5.5 RFC 4005 / §4.2	—	See the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*.
8	Framed-IP-Address	RFC 4005 / §6.11.1	—	This AVP specifies the IPv4 address of the subscriber host. The IPv4 address is obtained before Gx session establishment. The IPv4 address cannot be assigned to the subscriber host by PCRF via Gx but is instead used only for reporting.
18	3GPP-SGNS-MCC-MNC	29.061	—	GTP S11 Access uses the value configured with the following command: `configure subscriber-mgmt gtp serving-network`
22	3GPP-User-Location-Info	29.061	—	In CCR-I, this contains the User Location Information as signaled in the incoming GTP-C message for GTP Access hosts. For a CCR-U triggered by either USER_LOCATION_CHANGE (ULC), ECGI_CHANGE, or TAI_CHANGE will include ULI values as follows: • If the trigger was ULC and the ULI contains anything other than ECGI or TAI, the ULI is signaled as received in GTP. • If the trigger was ULC and either TAI or ECGI changed from its last known value, both TAI and ECGI will be included.

AVP ID	AVP name	Section defined	Application	Description
				• If the trigger was ECGI_CHANGE and ECGI changed from its last known value, ECGI is included. • If the trigger was TAI_CHANGE and TAI change from its last known value, TAI is included.
25	Class	RFC 2865 / §5.25	—	This attribute is available to be sent by the PCRF to the 7750 SR and is echoed unmodified by the 7750 SR to the PCRF. The 7750 SR does not interpret this attribute locally.
30	Called-Station-Id	RFC 2865 / §5.30 RFC 4005 / §4.5	—	See the*7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*.
31	Calling-Station-ID	RFC 4005 / §4.6	—	See the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*.
55	Event-Timestamp	RFC 6733 / §8.21	—	This AVP records the time that this event occurred on the 7750 SR, in seconds since January 1, 1900 00:00 UTC.
61	NAS-Port-Type	RFC 2865 / §5.41 RFC 4005 / §4.4 RFC 4603	—	See the*7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*.
87	NAS-Port-Id	RFC 2869 / §5.17 RFC 4005 / §4.3	—	See the*7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*.
92	NAS-Filter-Rule	RFC 4849	Gx-PM-ESM	See the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*. This AVP is nested within the Charging-Rule-Definition AVP.
97	Framed-IPv6-Prefix	RFC 4005 / §6.11.6	—	This AVP specifies the IPv6-prefix and prefix-length that is assigned to the host via SLAAC (Router Advertisement) to the WAN side of the user. The IPv6-prefix and prefix-length is obtained before Gx session establishment. The facilities to provide the IPv6-prefix and prefix-length to the subscriber-host are DHCP server/local pools, RADIUS or LUDB. The IPv6-prefix/ prefix-length cannot be assigned to the subscriber host by PCRF via Gx. Instead the IPv6-prefix and prefix-length is the one being reported to the PCRF during the host instantiation phase.

AVP ID	AVP name	Section defined	Application	Description
123	Delegated-IPv6-Prefix	RFC 4818	—	This attribute carries the Prefix (ipv6-prefix/prefix-length) assigned to the host via DHCPv6 (IA-PD) for the LAN side of the user (IPoE, PPPoE). The IPv6-prefix/prefix-length is obtained before Gx session establishment. The facilities to provide the IPv6-prefix/prefix-length to the subscriber-host are DHCP server/local pools, RADIUS or LUDB. The IPv6-prefix/prefix-length cannot be assigned to the subscriber host by PCRF via Gx. Instead the IPv6-prefix/prefix-length is the one being reported to the PCRF during the host instantiation phase.
257	Host-IP-Address	RFC 6733 / §5.3.5	—	This AVP is used to inform a Diameter peer of the sender's IP address. The IPv4 address used is the one configured in the **diameter-peer-policy**. If none is configured, then the system IP address is used.
258	Auth-Application-Id	RFC 6733 / §6.8	—	This AVP indicates supported Diameter applications. The application support is exchanged in CER/CEA when the peering sessions is established. The diameter base protocol does not require application ID because its support is mandatory. The Gx application ID value is 16777238 and it is advertised in Auth-Application-Id AVP within the grouped Vendor-Specific-Application-Id AVP in CER message. In addition, each Gx specific message carries Auth-Application-Id AVP with the value of 16777238.
260	Vendor-Specific-Application-Id	RFC 6733 / §6.11	—	This is a Grouped AVP that is used to advertise support of a vendor-specific Diameter application in CER/CEA messages. Gx is one such application. This AVP contains the Vendor-Id AVP of the application and the auth-application-id AVP.
263	Session-id	RFC 6733 / §8.8	—	This AVP must be present in all messages and it is used to identify a specific IP-Can session. IP-Can session corresponds to

AVP ID	AVP name	Section defined	Application	Description
				a subscriber host, which can be DHCPv4/v6, PPPoX or ARP host. Session-id AVP is unique per host. Dual stack host (IPoE or PPPoX) share a single session-id.
264	Origin-Host	RFC 6733 / §6.3	—	This AVP must be present in all messages and it is used to identify the endpoint (Diameter peer) that originated the message.
265	Supported-Vendor-Id	RFC 6733 / §5.3.6	—	This AVP is used in CER/CEA messages to inform the peer that the sender supports a subset of) the vendor-specific AVPs defined by the vendor identified in this AVP. Supported vendors in the 7750 SR are: 3GPP — 10415 ETSI — 13019 NOKIA — 6527 BBF — 3561
266	Vendor-Id	RFC 6733 / §5.3.3	—	The value of this AVP is the IANA assigned code to a specific vendor. This AVP may be part of the Vendor-Specific-Application-Id AVP, Failed-AVP AVP, Experimental-Result AVP to identify the vendor associated with the relevant message/AVP. In case of a standalone Vendor-Id AVP (outside of any grouped AVP) that is conveyed in CER/CEA messages, it is envisioned that this AVP along with the Product-Name AVP and the Firmware-Revision AVP may provide useful debugging information. Supported Vendor-Id AVPs in the 7750 SR are: 3GPP — 10415 ETSI — 13019 NOKIA — 6527
267	Firmware-Revision	RFC 6733 / §5.3.4	—	The SR OS version is reported.

AVP ID	AVP name	Section defined	Application	Description
268	Result-Code	RFC 6733 / §7.1	—	This AVP indicates whether a particular request was completed successfully or an error occurred. All answer messages in Diameter/Gx must include one Result-Code AVP or Experimental-Result AVP. For the list of supported error codes see Table 10: Result codes (Result-Code AVP).
269	Product-Name	RFC 6733 / §5.3.7	—	This AVP specifies the vendor-assigned name.
278	Origin-State-Id	RFC 6733 / §8.16	—	This AVP is used to inform the PCRF of the loss of the state on the 7750 SR side. Its value monotonically increases each time the PCRF is rebooted with the loss of the previous state. Because Gx sessions are not persistent in the 7750 SR, Origin-State-Id increases each time the 7750 SR is rebooted.
279	Failed-AVP	RFC 6733 / §7.5	—	This is a Grouped AVP that provides debugging information in cases where a request is rejected or not fully processed because of the erroneous information in specific AVP. The value of the Result-Code AVP will provide information about the reason for the Failed-AVP AVP. The Failed-AVP AVP contains the entire AVP that could not be processed successfully.
281	Error-Message	RFC 6733 / §7.3	—	This AVP provides more information of the failure that is indicated in the Result-Code AVP.
282	Route Record	RFC 6733 / §6.7.1		This AVP identifies the peer from which the request is received and is used for routing loop detection. An SR node inserts the origin-host of the peer in the Route-Record AVP of all transit request messages.
283	Destination-Realm	RFC 6733 / §6.6	—	This AVP represents the realm to which this message is to be routed. The value of this AVP is either explicitly configured in the 7750 SR.

AVP ID	AVP name	Section defined	Application	Description
285	Re-Auth-Request-Type	RFC 6733 / §8.12	—	This AVP is mandatory in RAR requests. The content of this AVP is ignored by the 7750 SR.
293	Destination-Host	RFC 6733 / §6.5	—	This AVP represents the host to which this message is to be sent. The value of this AVP can be explicitly configured. In case that it is omitted, the DRA (Diameter relay-agent) that receives the message selects the destination host to which the message is sent.
295	Termination-Cause	RFC 6733 / §8.15	—	This AVP is used to indicate the reason why a session was terminated on the 7750 SR. The supported termination causes in the 7750 SR are specified in Table 13: Termination causes (Termination-Cause AVP) .
296	Origin-Realm	RFC 6733 / §6.4	—	This AVP contains the realm of the originator of message. In the 7750 SR, the Origin-Realm is explicitly configured per Diameter peer.
297	Experimental-Result	RFC 6733 / §7.6	—	This is a Grouped AVP that indicates whether a particular vendor-specific request completed successfully or whether an error occurred. It contains a vendor-assigned value representing the result of processing a request. The result-code AVP values defined in Diameter Base RFC (6733, §7.1) are also applicable to Experimental-Result AVP. For a list of Gx-specific Experimental-Result-Code values supported in the 7750 SR, see Table 10: Result codes (Result-Code AVP). For Gx application, the Vendor-Id AVP is set to 10415 (3GPP). All answer messages defined in vendor-specific application must include either one Result-Code AVP or one Experimental-Result AVP.
298	Experimental-Result-Code	RFC 6733 / §7.7 29.214 / §5.5	—	This AVP specifies vendor-assigned (3GPP — Gx) values representing the result of processing the request.

AVP ID	AVP name	Section defined	Application	Description
				For a list of the 7750 SR supported values for Gx see Table 10: Result codes (Result-Code AVP).
302	Logical-Access-Id	ETSI TS 283 034 / §7.3.3 BBF TR-134 (§7.1.4.1)	—	This AVP contains information describing the subscriber agent circuit identifier corresponding to the logical access loop port of the Access Node from which the subscriber's requests are initiated, namely: • **circuit-id** from DHCPv4 Option (82,1) • **circuit-id** from PPPoE tag (0x105, 0x00000de9 [dsl forum], 0x01 — DSL Forum TR-101) • **interface-id** from DHCPv6 option 18. The Vendor-Id in CER is set to ETSI (13019).
313	Physical-Access-Id	ETSI TS283 034 / §7.3.14 BBF TR-134 (§7.1.4.1)	—	This AVP contains information about the identity of the physical access to which the user device is connected, namely: • **remote-id** from DHCPv4 Option (82,2) • **remote-id** from PPPoE tag (0x105, 0x00000de9 [dsl forum], 0x02 — DSL Forum TR-101) • **remote-id** from DHCPv6 option 37. The Vendor-Id in CER is set to ETSI (13019).
412	CC-Input-Octets	RFC 4006 / §8.24	Gx-UM-ESM Gx-UM-AA	This AVP contains the number of requested, granted or used octets from the user.
414	CC-Output-Octets	RFC 4006 / §8.25	Gx-UM-ESM Gx-UM-AA	This AVP contains the number of requested, granted or used octets toward the user.
415	CC-Request-Number	RFC 4006 / §8.2	—	This AVP identifies each request within one session. Each request within a session has a unique CC-Request-Number that is used for matching requests with answers.
416	CC-Request-Type	RFC 4006 / §8.3	—	This AVP identifies the request type: INITIAL_REQUEST (CCR-I) UPDATE_REQUEST (CCR-U) TERMINATION_REQUEST (CCR-T)

AVP ID	AVP name	Section defined	Application	Description
418	CC-Session-Failover	RFC 4006 / §8.4	—	This AVP controls whether the secondary peer will be used in case that the primary peer is unresponsive (peer failover behavior). The unresponsiveness is determined by the timeout of the previously sent message. If this AVP is not supplied via PCRF, the locally configured options in the 7750 SR will determine the peer failover behavior. For further details on the peer failover behavior, see "Gx Fallback Function" section in the Gx Configuration Guide.
421	CC-Total-Octets	RFC 4006 / §8.23	Gx-UM-ESM Gx-UM-AA	This AVP contains the number of requested, granted or used octets regardless of the direction (sent or received).
427	Credit-Control-Failure-Handling	RFC 4006 / §8.14	—	This AVP controls whether the subscriber is terminated or instantiated with default parameters in case that the PCRF is unresponsive. The unresponsiveness is determined by the timeout of the previously sent message. If this AVP is not supplied via PCRF, the locally configured options in the 7750 SR determines the behavior. For further details, see the "Gx Fallback Function" section in the Gx Configuration Guide.
431	Granted-Service-Unit	RFC 4006 / §8.17	Gx-UM-ESM Gx-UM-AA	This grouped AVP is sent by PCRF to the 7750 SR for usage monitoring purposes. When the granted amount of units is consumed by the user, a report is sent from the 7750 SR to the PCRF. The amount of consumed units can be measured on three different levels: • Session level (host level) • PCC rule level (credit category in the 7750 SR) • ADC rule level (AA level in the 7750 SR)
433	Redirect-Address-Type	RFC 4006 / §8.38	Gx-PM-ESM	This AVP specifies the address type of the HTTP redirect server. URL (2) type is the only address type supported in the 7750 SR.

AVP ID	AVP name	Section defined	Application	Description
435	Redirect-Server-Address	RFC 4006 / §8.39	Gx-PM-ESM	This AVP specifies the URL string of the redirect server.
443	Subscription-Id	RFC 4006 / §8.46	—	This AVP is of type Grouped and is used to identify the subscriber host in the 7750 SR. The nested AVPs are subscription-id-data and subscription-id-type.

444	Subscription-Id-Data	RFC 4006 / §8.48	—	This AVP is part of the subscription-id AVP and is used to identify the host by:
				• Circuit-id
				• Dual-stack-remote-id
				• Imei
				• Imsi
				• Mac of the host
				• Msisdn
				• Subscriber-id
				• Username (ppp-username or a string returned in the Username attribute via RADIUS or NASREQ)
				Subscription type (subscription-id-type AVP) has to be explicitly set via CLI. The data is formatted according to the type set.
				For GTP S11 access, the value configured with the following command is ignored and the session always includes two subscription-Id AVPs for both IMSI and MSISDN.
				• **MD-CLI**
				`configure subscriber-mgmt diameter-gx-policy gx avp-subscription-id`
				• **classic CLI**
				`configure subscriber-mgmt diameter-application-policy gx avp-subscription-id`

446	Used-Service-Unit	RFC 4006 / §8.19	Gx-UM-ESM Gx-UM-AA	This AVP is of type Grouped and it represents the measured volume threshold for usage monitoring control purposes. It is sent in the Usage-Monitoring-Report AVP from the 7750 SR to the PCRF when

AVP ID	AVP name	Section defined	Application	Description
				the granted unit threshold is reached or in response to a usage-report request from the PCRF.
450	Subscription-Id-Type	RFC 4006 / §8.47	—	This AVP is used to determine which type of identifier is carried by the subscription-id AVP. The following formats (types) are supported in the 7750 SR: • E.164 format (ITU-T E.164) • IMSI format (ITU-T E.212) • NAI format (RFC 2486) • Private format
458	User-Equipment-Info	RFC 4006 / §8.49	—	This is a Grouped AVP that carries information about the identity and the capabilities of the host.
459	User-Equipment-Info-Type	RFC 4006 / §8.50	—	This AVP is nested within the User-Equipment-Info AVP. The following types are supported in the 7750 SR: • IMEISV – contains the IMEI and software version according to 3GPP TS 23.003 document. • MAC address • Eui64 based on 48-bit MAC address with 0xfffe inserted in the middle. • Modified_eui64 — similar to eui64 but with inverted 'u' bit as defined in: http://standards.ieee.org/develop/regauth/tut/eui64.pdf and RFC 4291. The equipment type must be explicitly set through the CLI. For GTP S11 access, the configuration is ignored and always uses IMEISV.
460	User-Equipment-Info-Value	RFC 4006 / §8.51	—	This AVP carries the value that is defined by the User-Equipment-Info-Type AVP.
507	Flow-Description	29.214 / §5.3.8	Gx-PM-ESM	This AVP is nested within Flow-Information AVP. It identifies traffic within the PCC rule based on the 5 tuple.
511	Flow-Status	29.214 / §5.3.11	Gx-PM-ESM	This AVP is used to set the service gating action for the service represented by the PCC rule. It is nested inside of Charging-Rule-Definition AVP. Supported values are:

AVP ID	AVP name	Section defined	Application	Description
				• ENABLED (2) • DISABLED (3) The service identified by PCC rule is by default enabled (Flow-Status = ENABLED). If explicitly configured within the PCC rule, it must be accompanied with one or more additional actions. Otherwise, the entire PCC rule instantiation fails. Flow-Status = DISABLED can be the sole action within the PCC rule. Traffic associated with this action, is dropped.
515	Max-Requested-Bandwidth-DL	29.214 / §5.3.14	Gx-PM-ESM	Depending on the context in which it is configured (nested), this AVP represents the egress PIR of a queue or a policer.
516	Max-Requested-Bandwidth-UL	29.214 / §5.3.15	Gx-PM-ESM	Depending on the context in which it is configured (nested), this AVP represents the ingress PIR of a queue or a policer.
554	Extended-Max-Requested-BW-DL	29.214 / §5.3.52	Gx-PM-ESM	For higher rate requirements, this AVP can be used in place of the Max-Requested-Bandwidth-DL AVP.
555	Extended-Max-Requested-BW-UL	29.214 / §5.3.52	Gx-PM-ESM	For higher rate requirements, this AVP can be used in place of the Max-Requested-Bandwidth-UL AVP.
628	Supported-Features	29.229 / §6.3.29 29.212 / §5.4.1	—	This is a Grouped AVP that is used during Gx session establishment to inform the destination host about the required and optional features that the origin-host supports. One instance of Supported-Features AVP is needed per Feature-List-id. The 7750 SR supports the following features from 3GPP document 29.212, section §5.4.1: • Gx Rel 8, 9, 10 • ADC • Extended-BW-NR (optional) The Vendor-Id AVP in Supported-Features AVP is set to 10415 (3GPP).
629	Feature-List-Id	29.229 / §6.3.30	—	This AVP contains the identity of a feature list. This AVP allows differentiation between multiple feature lists in case that

AVP ID	AVP name	Section defined	Application	Description
				an application has multiple feature lists defined. Gx reference point and ADC are advertised in Feature-List-Id=1 and Extended-BW-NR is advertised in Feature-List-Id=2.
630	Feature-List	29.229 / §6.3.31	—	This AVP contains a bitmask indicating the supported feature in Gx. The Gx features in the Feature-List AVP are defined in 3GPP TS 29.212, §5.4.1.
909	RAI	29.061	—	For GTP S11 access this contains the RAI if it was signaled in GTP.
1001	Charging-Rule-Install	29.212 / §5.3.2	—	This AVP is of type Grouped and is used to enforce overrides, install NAS filter inserts and install or modify PCC rules in the node as instructed by PCRF. Each override, NAS filter insert or a PCC rule that is to be instantiated is identified by the charging-rule-name AVP.
1002	Charging-Rule-Remove	29.212 / §5.3.3	—	This AVP is of type Grouped and is used to remove PCC rules from an IP CAN session. Be aware that Gx overrides (ESM string overrides, updates of queue and policer rates, filter overrides, category-map overrides), cannot be removed. For those cases, the Charging-Rule-Remove AVP is ignored, even if the M-bit in the AVP is set.
1003	Charging-Rule-Definition	29.212 / §5.3.4	—	This AVP is of type Grouped and is used for rule overrides, NAS filter inserts or PCC rules installation. It contains nested AVPs that define the overrides (rate changes of a subscriber, a queue or a policer, and so on), NAS filter insert or a completely new PCC rule definition. The override/PCC rule (defined by the Charging-Rule-Definition) is instantiated via Charging-Rule-Install AVP.
1005	Charging-Rule-Name	29.212 / §5.3.6	—	This AVP is used to: • Reference a predefined rule in the node. This predefined rule represents an override of an existing rule. The

AVP ID	AVP name	Section defined	Application	Description
				override is activated by including Charging-Rule-Name AVP nested within the Charging-Rule-Install AVP sent from the PCRF to the 7750 SR. • Name the PCC rule which is defined through Charging-Rule-Definition AVP. When the PCC rule is installed, it can be removed by referencing the PCC rule name. • Report rule/override status in case of a rule/override activation failure. The status is reported within Charging-Rule-Report AVP sent from the node to the PCRF.
1006	Event-Trigger	29.212 / §5.3.7	—	This AVP can be sent from the PCRF to subscribe to a particular event in the 7750 SR. When specific events occur on the 7750 SR, they are reported to the PCRF in the related AVP along with the event trigger indication. The supported events are listed in Table 12: Event triggers (Event-Trigger AVP).
1010	Precedence	29.212 / §5.3.11	Gx-PM-ESM	This AVP is carried within a PCC rule definition (Charging-Rule-Definition) and it determines the order in which PCC rules are installed for the subscriber-host. PCC rules with lower values are evaluated before PCC rules with higher values. PCC rules without the Precedence value will be automatically ordered by the system to optimize the use of system resource. In case that there is a mix of PCC rules with and without the Precedence value, PCC rules without the explicit Precedence value are ordered after the PCC rules with the explicitly set Precedence value.
1014	ToS-Traffic-Class	29.212 / §5.3.15	Gx-PM-ESM	This AVP is nested within Flow-Information AVP. It identifies traffic within the PCC rule based on DSCP bits. The only supported mask in this AVP is 11111100 (6 bits denoting DSCP field).

AVP ID	AVP name	Section defined	Application	Description

1016	QoS-Information	29.212 / §5.3.16	Gx-PM-ESM	This AVP has a multi-faceted function:
				• As part of PCC rule definition in CCA or RAR, this AVP is used to rate-limit a flow.
				• The AVP defines QoS overrides that can be submitted from PCRF to the SR OS router in a CCA or RAR message. The overrides are nested in Charging-Rule-Definition AVP and are activated in 7x50 through the Charging-Rule-Install AVP.
				The supported QoS overrides are:
				• Queue rates, bursts sizes, and weights
				• Policer rates and burst sizes
				• Subscriber egress aggregate rate limit
				• Arbiter rates
				The AVP defines APN Uplink and Downlink Aggregate Maximum Bitrate (AMBR) in a CCA or RAR message. In this case, the AVP is included on the message level. The SR OS can map the AMBR on QoS overrides using the following commands.
				• **MD-CLI**
				`configure groups group subscriber-mgmt diameter-gx-policy gx three-gpp-qos-mapping`
				• **classic CLI**
				`configure subscriber-mgmt diameter-application-policy gx 3gpp-qos-mapping`
				For GTP S11 access, the AVP can also be used to signal the APN AMBR value received in GTP in a CCR message. In this case the AVP is included on message level.

1018	Charging-Rule-Report	29.212 / §5.3.18	—	This AVP is of type Grouped and is used to report the status of PCC rules in the 7750 SR. Failure to install or activate one or more policy rules is always reported in CCR-u messages. One or more Charging-

AVP ID	AVP name	Section defined	Application	Description
				Rule-Report AVPs in CCR-u command is included, indicating the failed rules. The report about successful rule activation or rule resource allocation is not sent to the PCRF even in the cases when the PCRF specifically demands such reports from the 7750 SR.
1019	PCC-Rule-Status	29.212 / §5.3.19	—	This AVP describes the status of the rules as active or inactive and is nested within the Charging-Rule-Report AVP.
1025	Guaranteed-Bitrate-DL	29.212 / §5.3.25	Gx-PM-ESM	Depending on the context in which it is configured (nested), this AVP represents the egress CIR of a queue or a policer.
1026	Guaranteed-Bitrate-UL	29.212 / §5.3.26	Gx-PM-ESM	Depending on the context in which it is configured (nested), this AVP represents the ingress CIR of a queue or a policer.
1027	IP-CAN-Type	29.212 / §5.3.27	—	This AVP indicates the type of Connectivity Access Network in which the user is connected. For GTP S11 access, the AVP value is set to 3GPP-EPS (code 5). For any other access type the AVP value is set to xDSL (code 2).
1028	QoS-Class-Identifier	29.212 / §5.3.17	—	This AVP identifies a QoS forwarding class within the router. Mapping between QCIs and forwarding classes in the 7750 SR is the following: • QCI 1 — FC H1 • QCI 2 — FC H2 • QCI 3 — FC EF • QCI 4 — FC L1 • QCI 5 — FC NC • QCI 6 — FC AF • QCI 7 — FC L2 • QCI 8 — FC BE
1031	Rule-Failure-Code	29.212 / §5.3.38	—	This AVP is sent from the router to the PCRF within a Charging-Rule-Report or ADC-Rule-Report AVP to identify the reason a rule is being reported. For the list of supported failure codes in the 7750 SR,

AVP ID	AVP name	Section defined	Application	Description
				see Table 11: Rule failure codes (Rule-Failure-Code AVP).
1032	RAT-Type	29.212 / §5.3.31	—	This AVP identifies the radio access technology used for this connection. For WLAN-GW UEs, the AVP value is fixed and set to WLAN(0). For GTP S11 access, the AVP value is set to the value signaled in GTP.

1040	APN-Aggregate-Max-Bitrate-DL	29.212	—	When received in an RAR or CCA, this value can be mapped to a local egress QoS override with the following commands.
				• **MD-CLI**
				`configure groups group subscriber-mgmt diameter-gx-policy gx three-gpp-qos-mapping apn-ambr-dl`
				• **classic CLI**
				`configure subscriber-mgmt diameter-application-policy gx 3gpp-qos-mapping apn-amb-dl`
				This uses the generic ESM override mechanism and any override received from another source (such as RADIUS or Alc-Queue AVP) can remove or change this value.
				For GTP S11 access, the value received in GTP is also reflected in a CCR.

1041	APN-Aggregate-Max-Bitrate-UL	29.212	—	When received in an RAR or CCA, this value can be mapped to a local ingress qos override with the following commands.
				• **MD-CLI**
				`configure groups group subscriber-mgmt diameter-gx-policy gx three-gpp-qos-mapping apn-ambr-ul`
				• **classic CLI**
				`configure subscriber-mgmt diameter-application-policy gx 3gpp-qos-mapping apn-amb-ul`

AVP ID	AVP name	Section defined	Application	Description
				This uses the generic ESM override mechanism and any override received from another source (such as RADIUS or Alc-Queue AVP) can remove or change this value. For GTP S11, the access value received in GTP also reflected in a CCR.
1045	Session-Release-Cause	29.212 / §5.3.33	Gx-PM-ESM Gx-PM-AA	This AVP terminates the Gx session from the PCRF side. The reason for session termination is included in this AVP. The reason for the session termination is ignored by the router.
1050	AN-GW-Address	29.212 / § 5.3.49	—	This AVP is the system IPv4 address of the 7750 SR.
1058	Flow-Information	29.212 / §5.3.53	Gm-PM-ESM	This is a Grouped AVP carrying information about traffic identification with the PCC rule. This AVP is nested within Charging-Rule-Definition AVP. Possible traffic identifiers within this AVP are: • Flow-Description AVP — 5 tuple information • ToS-Traffic-Class AVP — DSCP bits • Flow-Direction AVP — ingress or egress direction of the traffic
1065	PDN-Connection-ID	29.212	—	For GTP S11, the access value contains the APN as received in GTP.
1066	Monitoring-Key	29.212 / §5.3.59	Gx-UM-ESM Gx-UM-AA	This AVP is used for usage monitoring, as an identifier for a usage monitoring control instance. This AVP can be nested within: • **Charging-Rule-Definition AVP** In this case, the Monitoring-Key AVP is used to represent the PCC rule for which usage monitoring may be needed. • **Usage-Monitoring-Information AVP** In this case, the Monitoring-Key AVP is used to trigger or report the usage monitoring action for the entity

AVP ID	AVP name	Section defined	Application	Description
				represented by the Monitoring-Key AVP. The usage monitoring can be performed on multiple levels as requested by the Usage-Monitoring-Level AVP nested within the Usage-Monitoring-Information AVP: • If the level is IP-CAN session, then the monitoring-key is an arbitrary octet string set by the PCRF – usage monitoring is performed for the entire IP-CAN session (which represent a host/sla-profile instance) • If the level is pcc rule, then the Monitoring-Key refers to either the predefined category (name) in the 7750 SR, or the PCC rule represented by the Monitoring-Key AVP as defined in the Charging-Rule-Definition AVP. • If the level is adc rule, then the monitoring-key is an arbitrary unique name that refers to a unique Tdf-App-Id defined in an Adc-Rule. There can be up to three monitoring-keys in a single Gx messages.
1067	Usage-Monitoring-Information	29.212/ §5.3.60	Gx-UM-ESM Gx-UM-AA	This AVP is of type Grouped and it contains the usage monitoring control information. It is used to activate usage monitoring and grant service units when it is sent from the PCRF toward the 7750 SR. The 7750 SR uses this AVP to report usage monitoring to the PCRF.
1068	Usage-Monitoring-Level	29.212 / §5.3.61	Gx-UM-ESM Gx-UM-AA	This AVP is sent by PCRF to indicate the level on which usage monitoring is performed in the 7750 SR: • IP-CAN session level • PCC rule level • ADC rule level If usage-monitoring-level AVP is not provided, its absence indicates the pcc rule level usage monitoring.
1069	Usage-Monitoring-Report	29.212 / §5.3.62	Gx-UM-ESM	This AVP is sent by the PCRF to indicate that the accumulated usage monitoring is

AVP ID	AVP name	Section defined	Application	Description
			Gx-UM-AA	to be reported by the 7750 SR regardless of whether a usage monitoring threshold is reached. In other words, this AVP indicated immediate request for a usage monitoring report. A single value for this AVP is defined: 0 — usage_monitoring_report_required
1070	Usage-Monitoring-Support	29.212 / §5.3.63	Gx-UM-ESM Gx-UM-AA	This AVP is sent by the PCRF to indicate whether the usage monitoring is disabled for specific monitoring key. The following value is defined: 0 — usage_monitoring_disabled When usage-monitoring is disabled for a specific monitoring-key in this fashion, the 7750 SR generates a new CCR-u with the event-trigger AVP set to 'usage_report' to report the accumulated usage for the disabled usage monitoring entities.
1080	Flow-Direction	29.212 / §5.3.65	Gx-PM-ESM	This AVP is nested within the Flow-Information AVP. It identifies the direction in which the PCC rule is applied (ingress or egress). Supported values are: • DOWNLINK (1) for egress direction • UPLINK (2) for ingress direction The direction to which the PCC rule is applied can come from the following two sources, in the order of preference: • Flow-Direction AVP inside of the Flow-Information AVP. • Inside of the Flow-Description AVP as part of IPFilterRule type (direction field).
1085	Redirect-Information	29.212/§5.3.82	Gx-PM-ESM	This is a Grouped AVP that contains HTTP redirect information. This can be used in: • PCC rules to HTTP redirect a flow or a group of flows. • HTTP redirect overrides to override currently applied URL within the subscriber filter.
1086	Redirect-Support	29.212/§5.3.83	Gx-PM-ESM	This AVP is nested inside of Redirect-Information AVP.

AVP ID	AVP name	Section defined	Application	Description
				The values of this AVPs are: • REDIRECTION_DISABLED (0) • REDIRECTION-ENABLED (1) The behavior for Redirect-Support in the 7750 SR is the following: • If the AVP value is REDIRECTION_ ENABLED, the 7750 SR accepts it and HTTP redirect is in effect. • If the AVP value is different from REDIRECTION_ENABLED and M-bit is set (or inherited from parent AVP), the 7750 SR rejects it and the rule fails. • If the AVP value is different from REDIRECTION_ENABLED and M-bit is not set in this AVP or any of parent AVPs, the 7750 SR ignores it and the HTTP redirect is not explicitly disabled. Not receiving this AVP has the same effect as it was received with value REDIRECTION_ENABLED.
1088	TDF-Application-Identifier	29.212/§5.3.77	Gx-UM-AA	This AVP is of type OctetString. This AVP can be used in both PCC and ADC rules. For AA, this identifier is a reference to a preconfigured charging-group, app-group or application.
1092	ADC-Rule-Install	29.212 / §5.3.85	Gx-PM-AA Gx-UM-AA	This AVP is of type Grouped and is used to install or modify ADC (AA) rules in the 7750 SR as instructed by the PCRF.
1093	ADC-Rule-Remove	29.212/§5.3.86	Gx-PM-AA Gx-UM-AA	This AVP is of type Grouped, and it is used to deactivate or remove ADC rules in the 7750 SR as instructed from the PCRF.
1094	ADC-Rule-Definition	29.212 / §5.3.87	Gx-PM-AA Gx-UM-AA	This AVP is of type Grouped and it contains the rules that are to be activated. AA rules that can be applied to a subscriber via Gx are: • Application-profile activation/override. A preexisting application-profile must be defined in the 7750 SR. • Application characteristic overrides.

AVP ID	AVP name	Section defined	Application	Description
				• Monitoring Key and a TDF-Application-Identifier. This installation of this rule has the effect of creating a usage monitoring instance for the subscriber for the specified TDF-Application-Identifier.
1096	ADC-Rule-Name	29.212 / §5.3.89	Gx-PM-AA Gx-UM-AA	This AVP specifies the name of the ADC rule that is applied. This is an arbitrary string assigned by the PCRF and is used by the 7750 SR to report the rule status. In case that AA-Functions AVP is used (app-profile and ASO assignment/ modification), this arbitrary name string must be prepended with a 7750 SR reserved keyword "AA-Functions:".
1097	ADC-Rule-Report	29.212 / §5.3.90	Gx-PM-AA Gx-UM-AA	This AVP is of type Grouped and is used to report the status of ADC rules which cannot be activated or enforced in the 7750 SR.
2848	Extended-APN-AMBR-DL	29.212 / §5.3.134		For higher rate requirements, this AVP can be used in place of the APN-Aggregate-Max-Bitrate-DL AVP.
2849	Extended-APN-AMBR-UL	29.212 / §5.3.135		For higher rate requirements, this AVP can be used in place of the APN-Aggregate-Max-Bitrate-UL AVP.
2850	Extended-GBR-DL	29.212 / §5.3.136	Gx-PM-ESM	For higher rate requirements, this AVP can be used in place of the Guaranteed-Bitrate-DL AVP.
2851	Extended-GBR-UL	29.212 / §5.3.137	Gx-PM-ESM	For higher rate requirements, this AVP can be used in place of the Guaranteed-Bitrate-UL AVP.

4.1 Standard diameter AVPs (format)

Table 4: Standard diameter AVPs (format) lists standard diameter AVPs.

Incl/Excl – The attribute can be suppressed via CLI.

Flags (as set by the 7750 SR when the AVP is constructed):

- V indicates Vendor specific bit.
- M indicates Mandatory bit.

Note: The P flag bit is always set to 0.

UTF8String is a human-readable string using UTF-8 transformation format (which is for 7-bit encoding the same as US-ASCII).

OctetString is a basic data type which contains an arbitrary data. For example, Charging-Rule-Name AVP is OctetString according to RFC 6733 but in the 7750 SR it is displayed as readable string (UTF8String).

Flags for Gx specific AVPs are defined in RFC 6733, §4.5; 29.212, §5.3.

Flags for the Gx re-used AVPs are set as described in RFC 6733, §4.5 and in 3GPP 29.219, §5.4 — "The AVPs from Diameter base protocol are not included in Table 5.4, but they are re-used for the Gx reference point. Unless otherwise stated, re-used AVPs shall maintain their 'M', 'P' and 'V' flag settings. Where 3GPP RADIUS AVPs are re-used, unless otherwise stated, they shall be translated to Diameter AVPs as described in RFC 4005 [12] with the exception that the 'M' flag shall be set and the 'P' flag may be set".

The NOKIA-specific AVPs will have the M-bit cleared.

NA — This keyword (Not Advertised) denotes that the AVP is not originated by the 7750 SR and therefore the 7750 SR does not set the flag bits. However, the 7750 SR recognizes the AVPs and corresponding values listed in the table, regardless of the M-bit flags set by PCRF. However, if the V-bit is present in the received AVP, then the Vendor-Id filed in the AVP layout also must be present and set to the correct value because the AVP with V-bit set is identified by the <**avp-id**, **vendor-id**> pair.

Table 4: Standard diameter AVPs (format)

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
5	NAS-Port	Yes	Unsigned32	M	4 octets	See the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*.
8	Framed-IP-Address	No	OctetString	M	4 octets	Example: ip-address 10.11.12.13 Framed-IP-Address = 0a0b0c0d As defined in RFC 4005, §6.11.1.
22	3GPP-User-Location-Info	Yes	Octetstring	V	—	Vendor-Id = 10415 (3GPP) See 3GPP TS 29.061 for encoding details. For example: 3GPP-User-Location-Info = 130 (TAI and ECGI), MNC 001, MCC 001, ECI 1, TAC 1
30	Called-Station-Id	Yes	UTF8String	M	64 chars	Example: Called-Station-Id = mac:ssid or mac only if ssid is not available.
31	Calling-Station-ID	Yes	UTF8String	M	64 chars	llid | mac | remote-id | sap-id | sap-string (a 64 character string configured at the SAP level)

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format

						Example: include-avp calling-station-id sap-id
						• **MD-CLI**
						`configure subscriber-mgmt diameter-gx-policy gx include-avp calling-station-id type sap-id`
						• **classic CLI**
						`configure subscriber-mgmt diameter-application-policy gx include-avp calling-station-id sap-id`
						Calling-Station-Id = 1/1/2:1.1

55	Event-Time stamp	No	Time	M	4 octets	See the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*.
61	NAS-Port-Type	Yes	Enumerated	M	4 octets	The values for this attribute are defined in the RFC 2865, 4005 and 4603. See the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*.
87	NAS-Port-Id	Yes	UTF8String	M	253 octets	See the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*.
92	NAS-Filter-Rule	NA	UTF8String	NA	Max 10 attributes per message or max 10 filter entries per message.	See the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*.
97	Framed-IPv6-Prefix	No	OctetString	M	—	SLAAC wan-host <ipv6-prefix/prefix-length> with prefix-length 64 The AVP layout is: <1 octet Reserved> <1 octet Length> <max 16 octets for Prefix>
123	Delegated-IPv6-Prefix	No	OctetString	M	—	<ipv6-prefix/prefix-length> with prefix-length [48 to 64] The AVP layout is:

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
						<1 octet Reserved> <1 octet Length> <max 16 octets for Prefix>
257	Host-IP-Address	No	Address	M	—	IPv4 Address
258	Auth-Application-Id	No	Unsigned32	M	—	Example: Gx Auth-Application-Id = 16777238
260	Vendor-Specific-Application-Id	No	Grouped	M	—	This AVP contains the Vendor-Id AVP and Auth-Application-Id AVP. For Gx, the Vendor-Id = 10415 (3GPP) and the Auth-Application-Id = 16777238.
263	Session-id	No	UTF8String	M	102 bytes	The session-id must be globally and eternally unique. The format of the session-id is the following: <DiameterIdentity>;<high 32 bits>;<low 32 bits> In the 7750 SR the session-id is defined as: diameter-identity;boxuptime; seq-number Example: router.workstation.be;1391362206;1
264	Origin-Host	No	Diameter Identity	M	80 bytes	Example: Origin-Host = host-name-1@domain-name-1
265	Supported-Vendor-Id	No	Unsigned32	M	—	IANA assigned vendor number: 3GPP — 10415 ETSI — 13019 NOKIA — 6527
266	Vendor-Id	No	Unsigned32	M	—	IANA assigned vendor number: 3GPP — 10415 ETSI — 13019 NOKIA — 6527 BBF — 3561
267	Firmware-Revision	No	Unsigned32	—	—	Reference to the major/minor release version.

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
						Example: 805 — Release 8R5
268	Result-Code	No	Unsigned32	M	—	See Table 10: Result codes (Result-Code AVP) for Error Codes.
269	Product-Name	No	UTF8String	—	—	Vendor-assigned name for the product. Example: "SR OS"
278	Origin-State-Id	No	Unsigned32	M	—	Example: Origin-State-Id = 10
279	Failed-AVP	No	Grouped	M	—	This AVP contains the AVP that could not be processed successfully.
281	Error-Message	No	UTF8String	—	—	String describing the cause of the failure.
282	Route-Record	No	Diameter Identity	M	80 bytes	Example: Route-Record: host-1
283	Destination-Realm	No	Diameter Identity	M	80 bytes	Example: Destination-Realm = domain.com
285	Re-Auth-Request-Type	No	Enumerated	NA	—	This AVP is always received in RAR message and it is never sent by the 7750 SR. 0 — AUTHORIZE_ONLY 1 — AUTHORIZE_AUTHENTICATE Example: Re-Auth-Request-Type = 0
293	Destination-Host	No	Diameter Identity	M	80 bytes	Operator configurable.
295	Termination-Cause	No	Enumerated	M	—	For a list of the 7750 SR supported values for Gx see Table 13: Termination causes (Termination-Cause AVP) .
296	Origin-Realm	No	Diameter Identity	M	80 bytes	Example: Origin-Realm = origin-domain.com
297	Experimental-Result	No	Grouped	M	—	A grouped AVP containing: • Vendor-Id AVP • Experimental-Result-Code AVP

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
						Example: Experimental-Result = {Vendor-Id = 10415 (3GPP) Experimental-Result-Code = DIAMETER_PCC_RULE_EVENT (5142)}
298	Experimental-Result-Code	No	Unsigned32	M	—	For a list of the 7750 SR supported values for Gx see Table 10: Result codes (Result-Code AVP).
302	Logical-Access-Id	Yes	OctetString	V	—	Vendor ID = 13019 (ETSI)
313	Physical-Access-Id	Yes	UTF8String	V	—	Vendor ID = 13019 (ETSI)
412	CC-Input-Octets	No	Unsigned64	M	—	Example: CC-Input-Octets = 1000000
414	CC-Output-Octets	No	Unsigned64	M	—	Example: CC-Output-Octets = 1000000
415	CC-Request-Number	No	Unsigned32	M	—	Monotonically increasing from 0 for all requests within one session.
416	CC-Request-Type	No	Enumerated	M	—	Example: CC-Request-Type = 1 (CCR-i) 3. CC-Request-Type = 2 (CCR-u) CC-Request-Type = 3 (CCR-t)
418	CC-Session-Failover	No	Enumerated	M	—	FAILOVER_NOT_SUPPORTED (0) FAILOVER_SUPPORTED (1) Example: CC-Session-Failover = 1
421	CC-Total-Octets	No	Unsigned64	M	—	Example: CC-Total-Octets = 2000000
427	Credit-Control-Failure-Handling	No	Enumerated	M	—	TERMINATE (0) CONTINUE (1) RETRY_AND_TERMINATE (2) Example: Credit-Control-Failure-Handling = 1

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
431	Granted-Service-Unit	No	Grouped	M	—	This AVP can contain the following AVPs: • CC-Total-Octets • CC-Input-Octets • CC-Output-Octets
433	Redirect-Address-Type	No	Enumerated	M	—	Example: Redirect-Address-Type = 2 (URL type)
435	Redirect-Server-Address	No	UTF8String	M	255 chars	Example: Redirect-Server-Address = http://www.operator.com/portal.php&
443	Subscription-Id	Yes	Grouped	M	—	This AVP contains the following AVPs: • Subscription-Id-Type • Subscription-Id-Data
444	Subscription-Id-Data	Yes	UTF8String	M	—	Example: Username — Subscription-Id-Data = user1@domain.com Mac — Subscription-Id-Data = 11:22:33:44:55:66 Circuit-id — Subscription-Id-Data = dslam1 eth 2/1:100 Dual-stack-remote-id — Subscription-Id-Data = myRemoteId Subscriber-id — Subscription-Id-Data = sub-id-1 Imsi Subscription-Id-Data = 204047910000598 Msisdn Subscription-Id-Data = 13109976224 Imei — Subscription-Id-Data = 356938035643809
446	Used-Service-Unit	No	Grouped	M	—	This AVP contains the following AVPs: • CC-Total-Octets • CC-Input-Octets • CC-Output-Octets

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
450	Subscription-Id-Type	Yes	Enumerated	M	—	Example: Subscription-Id-Type = 0 (end_user_e164) Subscription-Id-Type = 1 (end_user_imsi) Subscription-Id-Type = 3 (end_user_nai) Subscription-Id-Type = 4 (end_user_private)
458	User-Equipment-Info	Yes	Grouped	M	—	This AVP contains the following AVPs: • User-Equipment-Info-Type • User-Equipment-Info-Value
459	User-Equipment-Info-Type	Yes	Enumerated	—	—	Example: User-Equipment-Info-Type = 0 (emissive) User-Equipment-Info-Type =1 (mac) User-Equipment-Info-Type = 2 (eui64) User-Equipment-Info-Type = 3 (modified_eui64)
460	User-Equipment-Info-Value	Yes	OctetString	—	—	—
507	Flow-Description	No	IPFilterRule (RFC6733, §4.3.1)	NA,M	—	The IPFilterRule format within PCC rule in the 7750 SR has the following syntax: action dir proto from src to dst action — permit dir — direction: in or out proto — an IP protocol specified by number. The **ip** keyword means any protocol matches. src and dest — <address/mask> and ports (including port ranges) Example: Flow-Description = allow in 6 from 192.168.7.0/24 3000-40000 to 172.16.10.0/26 10000-20000

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
511	Flow-Status	No	Enumerated	NA,M	—	Example: Flow-Status = 3 — matched traffic inside of the PCC rule is dropped.
515	Max-Requested-Bandwidth-DL	No	Unsigned32	NA, V	—	The units of this parameter are kb/s for overrides and b/s when used within PCC rules. The rate accounts for the IP header and above (no L2 header). Vendor-Id = 10415 (3GPP) Example: Max-Requested-Bandwidth-DL = 1000 — 1 Mb/s in overrides Max-Requested-Bandwidth-DL = 1000000 — 1 Mb/s in PCC rules
516	Max-Requested-Bandwidth-UL	No	Unsigned32	NA, V	—	The units of this parameter are kb/s for overrides and b/s when used within PCC rules. The rate accounts for the IP header and above (no Layer 2 header). Vendor-Id = 10415 (3GPP) Example: Max-Requested-Bandwidth-UL = 1000 — 1 Mb/s for overrides Max-Requested-Bandwidth-UL = 1000000 — 1 Mb/s in PCC rules
554	Extended-Max-Requested-BW-DL	NA	Unsigned32	NA, V	—	The units of this parameter are kb/s. Vendor-Id = 10415 (3GPP) Example: Extended-Max-Requested-BW-DL = 1000 — 1 Mb/s
555	Extended-Max-Requested-BW-UL	NA	Unsigned32	NA, V	—	The units of this parameter are kb/s. Vendor-Id = 10415 (3GPP) Example: Extended-Max-Requested-BW-UL = 1000 — 1 Mb/s
628	Supported-Features	No	Grouped	V	—	This AVP contains the following AVPs: • Vendor-Id

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
						• Feature-List-Id • Feature-List Vendor-Id = 10415 (3GPP) Example for Extended-BW-NR: Supported-Features • Vendor-Id = 10415 3GPP • Feature-List-Id = 2 • Feature-List = 128
629	Feature-List-Id	No	Unsigned32	V	—	Vendor-Id = 10415 (3GPP) Example: Feature-List-Id = 2
630	Feature-List	No	Unsigned32	V	—	Vendor-Id = 10415 (3GPP) Example: Feature-List = 128
909	RAI	Yes	Octetstring	V	12 octets	Vendor-Id = 10415 (3GPP) See 3GPP TS 29.061 for encoding details. For example: RAI = MCC 001, MNC 001, LAC 0xA2C1, RAC 0x0A
1001	Charging-Rule-Install	No	Grouped	NA, V	—	Vendor-Id = 10415 (3GPP) This AVP contains the following AVPs: • Charging-Rule-Definition • Charging-Rule-Name
1002	Charging-Rule-Remove	No	Grouped	NA, V	—	Vendor-Id = 10415 (3GPP) This AVP contains the following AVP: Charging-Rule-Name
1003	Charging-Rule-Definition	No	Grouped	NA, V	—	Vendor-Id = 10415 (3GPP) This AVP contains the following nested AVPs: • Charging-Rule-Name (provides the name to the overrides so that they can be referred in the Charging-Rule-Report – successful or failed rule instantiation)

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
						• QoS-Information (defines Qos overrides) • NAS-Filter-Rule • Alc-NAS-Filter-Rule-Shared • AA-Functions
1005	Charging-Rule-Name	No	OctetString	V,M	100 chars for PCC rules (defined via Charging-Rule-Definition AVP) 128 chars for overrides.	Vendor-Id = 10415 (3GPP) This is an arbitrary rule name for PCC rules or a predefined string representing the overrides in the 7750 SR. Syntax for predefined names used in overrides are: Filters: • Ingr-v4:<id> • Ingr-v6:<id> • Egr-v4:<id> • Egr-v6:<id> • In-Othr-v4:<id> (one-time-http-redirect) ESM Strings: • Sub-Id: (64 Byte) • Sla-Profile:sla-profile-string (16 Byte) • Sub-Profile:sub-profile-string (16 Byte) • Inter-Dest:Inter-Dest-String to associate subscriber with Vport HTTP Redirect Override • V4-http-url:url-string • V6-http-url:url-string Category-Map (for usage monitoring): Cat-Map:category-map-name HTTP Redirect Override: • V4-http-url:url-string • V6-http-url:url-string AA Strings: • **AA-Functions: <name-string>**

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
						This prefix indicates that the rule contains aa-specific information. • **AA-UM: <name-string>** This prefix indicates that the rule contains aa-specific usage-monitoring information, or points to a predefined aa-specific usage-monitoring rule. Example: Charging-Rule-Name = ingr-v4:5–reference to the predefined ingress IPv4 filter in 7450 ESS, 7750 SR, 7950 XRS, and VSR. The filter ID is 5. Charging-Rule-Name =sla-profile:my-premium-sla–reference to the predefined sla-profile in 7450 ESS, 7750 SR, 7950 XRS, and VSR. The sla-profile name is 'my-premium-sla'.
1006	Event-Trigger	No	Enumerated	V	—	Vendor-Id = 10415 (3GPP) For the list of supported event-triggers in the 7750 SR, see Table 12: Event triggers (Event-Trigger AVP).
1010	Precedence	No	Unsigned32	NA, M	0 to 65535	Vendor-Id = 10415 (3GPP) Example: Precedence = 100
1014	Tos-Traffic-Class	No	OctetString	NA, M	—	Encoded as two octets. The first octet contains the IPv4 Type-of-Service or the IPv6 Traffic-Class field and the second octet contains the ToS/Traffic Class mask field. The only supported mask is 11111100 (6 bits denoting DSCP support). Example: ToS-Traffic-Class = 00101000 11111100 — DSCP AF11
1016	QoS-Information	NA	Grouped	NA, V	—	Vendor-Id 10415 (3GPP) When used to signal a flow rate limiter in a PCC rule, this AVP contains the following nested AVPs: • Max-Requested-Bandwidth-UL

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
						• Max-Requested-Bandwidth-DL • Guaranteed-Bitrate-UL • Guaranteed-Bitrate-DL

1018	Charging-Rule-Report	No	Grouped	V,M	—	Vendor-Id = 10415 (3GPP)
						This AVP contains the following nested AVPs:
						• Charging-Rule-Name
						• PCC-Rule-Status
						• Rule-Failure-Code
						Example: Charging-Rule-Report {
						Charging-Rule-Name = sla-profile:failed-profile
						PCC-Rule-Status = 1 (inactive)
						Rule-Failure-Code = 4 (GW/7750 SR_MALFUNCTION)
						}

1019	PCC-Rule-Status	No	Enumerated	V,M	—	Vendor-Id = 10415 (3GPP) Supported values in the 7750 SR: 1 – inactive Example: PCC-Rule-Status = 0 — rule is active
1025	Guaranteed-Bitrate-DL	NA	Unsigned32	NA,V	—	The units of this parameter are kb/s for overrides and b/s when used within PCC rules. The rate accounts for the IP header and above (no Layer 2 header). Vendor-Id = 10415 (3GPP) Example: Guaranteed-Bandwidth-DL = 1000 — 1 Mb/s in overrides Guaranteed-Bandwidth-DL = 1000000 — 1 Mb/s in PCC rules
1026	Guaranteed-Bitrate-UL	NA	Unsigned32	V	—	The units of this parameter are kb/s for overrides and b/s when used within PCC rules. The rate accounts for the IP header and above (no Layer 2 header).

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
						Vendor-Id = 10415 (3GPP) Example: Guaranteed-Bandwidth-UL = 1000 — 1 Mb/s in overrides Guaranteed-Bandwidth-UL = 1000000 — 1 Mb/s in PCC rules
1027	IP-CAN-Type	Yes	Enumerated	V	—	Vendor-Id = 10415 (3GPP) Example: IP-CAN-Type = 2 — xDSL IP-CAN-Type = 5 — 3GPP-EPS
1028	QoS-Class-Identifier	NA	Enumerated	NA,M	—	Vendor-Id = 10415 (3GPP) Example: QoS-Class-Identifier = 3 — maps to FC EF.
1031	Rule-Failure-Code	No	Enumerated	V,M	—	Vendor-Id = 10415 (3GPP) Example: Rule-Failure-Code = 1 — UNKNOWN_RULE_NAME
1032	RAT-Type	Yes	Enumerated	V	—	Vendor-Id = 10415 (3GPP) Example: RAT-Type = 0 — WLAN RAT-Type = 1004 — EUTRAN
1040	APN-Aggregate-Max-Bitrate-DL	Yes	Unsigned32	V	2^32-1 b/s	Vendor-Id = 10415 (3GPP) Rate in bits per second (b/s) For example: APN-Aggregate-Max-Bitrate-DL = 100000000 (100 Mb/s)
1041	APN-Aggregate-Max-Bitrate-UL	Yes	Unsigned32	V	2^32-1 b/s	Vendor-Id = 10415 (3GPP) Rate in bits per second (b/s) For example: APN-Aggregate-Max-Bitrate-UL = 10000000 (10 Mb/s)
1045	Session-Release-Cause	NA	Enumerated	V,M	—	Vendor-Id = 10415 (3GPP)

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
						This AVP is only received by the 7750 SR and it is never sent by the 7750 SR. 0 — UNSPECIFIED-REASON 1 — UE_SUBSCRIPTION_REASON This value is used to indicate that the subscription of UE has changed (for example, removed) and the session needs to be terminated. 2 — INSUFFICIENT_SERVER_ RESOURCES This value is used to indicate that the server is overloaded and needs to abort the session. Example: Session-Release-Cause = 0
1050	AN-GW-Address	Yes	IPv4Address	V	—	Vendor-Id = 10415 (3GPP) Example: AN-GW-Address = 10.10.10.10
1058	Flow-Information	No	Grouped	V	—	Vendor-Id = 10415 (3GPP) The following AVPs can be nested inside: • Flow-Description • ToS-Traffic-Class • Flow-Direction
1065	PDN-Connection-ID	Yes	UTF8String	V	100 chars	Vendor-Id = 10415 (3GPP) For example: PDN-Connection-ID = example-apn.mnc001.mcc001.gprs
1066	Monitoring-Key	No	OctetString	NA,V	32 bytes	Vendor-Id = 10415 (3GPP) Category name configured in the 7750 SR, a string used for session monitoring or a Monitoring-Key AVP set in PCC rule definition with the Charging-Rule-Definition AVP. Example: Monitoring-Key = monitor-pcc-rule-1

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
1067	Usage-Monitoring-Information	No	Grouped	V	—	Vendor-Id = 10415 (3GPP) This AVP contains the following nested AVPs: • Monitoring-Key • Granted-Service-Unit • Used-Service-Unit • Usage-Monitoring-Level • Usage-Monitoring-Report • Usage-Monitoring-Support
1068	Usage-Monitoring-Level	No	Enumerated	V	—	Vendor-Id = 10415 (3GPP) The following values are defined: 0 – session_level 1 – pcc_rule_level 2 – adc_rule_level Example: Usage-Monitoring-Level = 0 — usage monitoring is performed based on sla-profile (IP-CAN session level) of the host. Usage-Monitoring-Level = 1 — usage monitoring is performed based on predefined category as indicated by the monitoring-key AVP Usage-Monitoring-Level = 2 — usage monitoring is performed based on ADC rule, as indicated by the monitoring-key AVP
1069	Usage-Monitoring-Report	No	Enumerated	V	—	Vendor-Id = 10415 (3GPP) Example: Usage-Monitoring-Report = 0 (usage_monitoring_report_required)
1070	Usage-Monitoring-Support	No	Enumerated	NA,V	—	Vendor-Id = 10415 (3GPP) Example: Usage-Monitoring-Support = 0 — usage_ monitoring_disabled

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
1080	Flow-Direction	No	Enumerated	NA,M	—	Vendor-Id = 10415 (3GPP) Example: Flow-Direction = 1 — egress Flow-Direction = 2 — ingress
1085	Redirect-Information	No	Grouped	NA,V	—	Vendor-Id = 10415 (3GPP) This AVP can contain the following AVPs: • Redirect-Support • Redirect-Address-Type • Redirect-Server-Address
1086	Redirect-Support	No	Enumerated	NA,V	—	Vendor-Id = 10415 (3GPP) Example: Redirect-Support = 1 — redirection is enabled
1088	TDF-Application-Identifier		OctetString	NA,V	32 chars long	Vendor-Id = 10415 (3GPP) Example: 0_rated, BitTorrent
1092	ADC-Rule-Install	No	Grouped	NA,V	—	Vendor-Id = 10415 (3GPP) This AVP contains the following nested AVPs: ADC-Rule-Definition
1093	ADC-Rule-Remove		Grouped	NA,V	—	Vendor-Id = 10415 (3GPP) This AVP contains the following nested AVPs: ADC-Rule-Name

1094	ADC-Rule-Definition	No	Grouped	NA,V	—	Vendor-Id = 10415 (3GPP)
						This AVP contains the following nested AVPs:
						• ADC-Rule-Name
						• MonitoringKey
						• TDF-Application-Id
						• AA-Functions {
						– AA profile
						– AA-App-Service-Options {
						– AA-App-Service-Options-Name

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
						– AA-App-Service-Options-Value } }
1096	ADC-Rule-Name	No	OctetString	V	17 chars for prefix/ separator (optional) plus 32 chars for name	Vendor-Id = 10415 (3GPP) Example: For app-profile and ASO changes: ADC-Rule-Name = "AA-Functions: Adc RuleWithAAFtn" For usage monitoring: ADC-Rule-Name = "AdcRule WithoutAAFtn"
1097	ADC-Rule-Report	No	Grouped	V	—	Vendor-Id = 10415 (3GPP) This AVP contains the following nested AVPs: • ADC-Rule-Name • PCC-Rule-Status • Rule-Failure-Code
2848	Extended-APN-AMBR-DL	NA	Unsigned32	NA, V	—	The units of this parameter are kb/s. Vendor-Id = 10415 (3GPP) Example: Extended-APN-AMBR-DL = 1000 — 1 Mb/s
2849	Extended-APN-AMBR-UL	NA	Unsigned32	NA, V	—	The units of this parameter are kb/s. Vendor-Id = 10415 (3GPP) Example: Extended-APN-AMBR-UL = 1000 — 1 Mb/s
2850	Extended-GBR-DL	NA	Unsigned32	NA, V	—	The units of this parameter are kb/s. Vendor-Id = 10415 (3GPP) Example: Extended-GBR-DL = 1000 — 1 Mb/s
2851	Extended-GBR-UL	NA	Unsigned32	NA, V	—	The units of this parameter are kb/s. Vendor-Id = 10415 (3GPP) Example:

AVP ID	AVP name	Incl/ Excl	Type	Flags	Limits	Format
						Extended-GBR-UL = 1000 — 1 Mb/s

5 NOKIA-specific AVPs

Table 5: NOKIA-specific AVPs

AVP ID	AVP name	Application	Description
92	Alc-PPPoE-LCP-Keepalive-Interval	Gx-PM-ESM	Specifies the interval in seconds at which PPPoE LCP Echo-Request messages are sent. Overrides the LCP keepalive interval value configured in **subscriber-mgmt ppp-policy** for PPPoE PTA sessions or in the Base router or VPRN service **l2tp group** context for L2TP LNS sessions.
93	Alc-PPPoE-LCP-Keepalive-Multiplier	Gx-PM-ESM	Specifies the number of PPPoE Echo-Request messages that can be missed before the PPPoE session is terminated. Overrides the LCP keepalive multiplier value configured in **subscriber-mgmt ppp-policy** for PPPoE PTA sessions or in the Base router or VPRN service **l2tp group** context for L2TP LNS sessions.
99	Alc-IPv6-Address (IA-NA)	Gx-PM-ESM Gx-PM-AA	Attribute that carries the IPv6 address assigned to the IPoE/PPPoE host via DHCPv6 (IA-NA). The IPv6address is obtained before Gx session establishment. The facilities to provide the IPv6 address to the subscriber-host are DHCP server, RADIUS or LUDB. The IPv6 address cannot be assigned to the subscriber host by PCRF via Gx. Instead the IPv6 address is the one being reported to the PCRF during the host instantiation phase.
158	Alc-NAS-Filter-Rule-Shared	Gx-PM-ESM	See the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*. This AVP is nested within Charging-Rule-Definition AVP.
1001	AA-Functions	Gx-PM-AA	This is a grouped AVP that contains a set AA related AVPs used to apply overrides to the AA subscriber. AA-Function AVP encompasses application-profile instantiation and overrides as well as the overrides of the ASOs within the application profile. (AA subscriber state must exist for application profiles and ASO overrides to be applied).
1002	AA-App-Profile-Name	Gx-PM-AA	The name of the application profile (app-profile) that is to be applied (instantiated or overridden) to the subscriber. The app-profile must be predefined in the 7750 SR.

AVP ID	AVP name	Application	Description
1003	AA-App-Service-Options	Gx-PM-AA	This AVP is of type grouped and it contains AVPs related to application service options (ASO) which are configurable strings in AA context used to further refine identification criteria within the same application and consequently apply more targeted actions.
1004	AA-App-Serv-Options-Name	Gx-PM-AA	AA service option name.
1005	AA-App-Serv-Options-Value	Gx-PM-AA	AA service option value.
1006	Alc-Queue	Gx-PM-ESM	This AVP is a grouped AVP that contains AVPs related to the queue parameters that can be overridden.
1007	Alc-Queue-Id	Gx-PM-ESM	Queue ID of a queue for which the parameters are being modified.
1008	Alc-Committed-Burst-Size-UL	Gx-PM-ESM	Committed burst size (CBS) of an ingress queue or an ingress policer in bytes. Specifies the CBS value of the dynamic policer used for an ingress PCC rule when included in the QoS-Information -> Alc-Dynamic-Policer AVP grouped AVP.
1009	Alc-Maximum-Burst-Size-UL	Gx-PM-ESM	Maximum burst size (MBS) of an ingress queue or an ingress policer in bytes. Specifies the MBS value of the dynamic policer used for an ingress PCC rule when included in the QoS-Information -> Alc-Dynamic-Policer AVP grouped AVP.
1010	Alc-Committed-Burst-Size-DL	Gx-PM-ESM	Committed burst size (CBS) of an egress queue or an egress policer in bytes. Specifies the CBS value of the dynamic policer used for an egress PCC rule when included in the QoS-Information -> Alc-Dynamic-Policer AVP grouped AVP.
1011	Alc-Maximum-Burst-Size-DL	Gx-PM-ESM	Maximum burst size (MBS) of an egress queue or an egress policer in bytes. Specifies the MBS value of the dynamic policer used for an egress PCC rule when included in the QoS-Information --> Alc-Dynamic-Policer AVP grouped AVP.
1014	Alc-Policer	Gx-PM-ESM	This AVP is a grouped AVP that contains AVPs related to the policer parameters that can be overridden.
1015	Alc-Policer-Id	Gx-PM-ESM	Policer ID of a policer for which the parameters are being modified.
1016	Alc-Sub-Egress-Rate-Limit	Gx-PM-ESM	This AVP contains the aggregate egress rate for the subscriber.

AVP ID	AVP name	Application	Description
1017	Alc-Arbiter-Rate-Limit-DL	Gx-PM-ESM	This AVP contains the egress arbiter rate for the subscriber.
1018	Alc-Arbiter-Rate-Limit-UL	Gx-PM-ESM	This AVP contains the ingress arbiter rate for the subscriber.
1021	Alc-Arbiter	Gx-PM-ESM	This AVP is a grouped AVP that contains AVPs related to the arbiter parameters that can be overridden.
1022	Alc-Arbiter-Name	Gx-PM-ESM	Arbiter name for which the parameters are being modified: **root** for the root arbiter **arbiter name** for an intermediate arbiter **_tmnx_no_parent** (PCC rule only) sets no parent for the dynamic policer Specifies the parent arbiter name of the dynamic policer used for a PCC rule when included in the QoS-Information -> Alc-Dynamic-Policer -> Alc-Policer-Parent grouped AVP.
1024	Alc-Next-Hop-IP	Gx-PM-ESM	This AVP contain IPv4 or IPv6 next-hop address which can be within the same routing context or within a different routing context as specified by Alc-v4-Next-Hop-Service-Id or Alc-v6-Next-Hop-Service-Id AVPs.
1025	Alc-v4-Next-Hop-Service-Id	Gx-PM-ESM	This AVP contains the service ID of the routing context where the IPv4 traffic is redirected. The next-hop IPv4 address can be explicitly set via Alc-Next-Hop-IP AVP or it can be implicitly determined via routing lookup.
1026	Alc-v6-Next-Hop-Service-Id	Gx-PM-ESM	This AVP contains the service ID of the routing context where the IPv6 traffic is redirected. The next-hop IPv6 address can be explicitly set via Alc-Next-Hop-IP AVP or it can be implicitly determined via routing lookup.
1027	Alc-Filter-Action	Gx-PM-ESM	This AVP sets the gating action within the filter portion of the PCC rule. The support values in the node are: • FORWARD (1) • DROP (2)
1028	Alc-QoS-Action	Gx-PM-ESM	This AVP is used to create an allowlist entry related to the QoS part of the PCC rule. The supported value is: FORWARD (1) Alc-QoS-Action = Forward–Assuming that traffic is not dropped by the filtering action, it transparently passes

AVP ID	AVP name	Application	Description
			traffic through the QoS policy, without any QoS-related action taken.
1029	AA-Sub-Http-Url-Param	GX-PM-AA	This AVP is used to indicate an **http url** parameter to be applied to the subscriber AA context.
1030	AA-Sub-Scope	GX-PM-AA	This AVP is used to indicate the scope of an AA application on the subscriber. AA can be applied on the overall subscriber level (all subscriber hosts) or at a specific subscriber-host level (MAC or device).
1036	Alc-SPI-Sharing	Gx-PM-ESM	Grouped AVP This can be included in a Gx CCA or Gx RAR message to set or override the SPI sharing method for this subscriber session to SPI sharing per group or to the default SPI sharing method as specified in the SLA profile. `configure subscriber-mgmt sla-profile def-instance-sharing {per-sap | per-session}` To set SPI sharing per group, a group is identified with an integer SPI group ID. An SPI is shared by all subscriber sessions with the same subscriber ID, SAP, SLA profile and SPI group ID. The Alc-SPI-Sharing-Type must be set to "per group" and the Alc-SPI-Sharing-Id must contain the SPI group ID. To set SPI sharing to the default SPI sharing method as specified in the SLA profile, set the Alc-SPI-Sharing-Type to "default". The Alc-SPI-Sharing-Id AVP must not be present. Setting this AVP for an IPoE host with IPoE session disabled on the group interface results in a setup failure. Unsupported values result in a subscriber session setup failure.
1037	Alc-SPI-Sharing-Type	Gx-PM-ESM	Values: 0= default 2= per group
1038	Alc-SPI-Sharing-Id	Gx-PM-ESM	Value is function of the Alc-SPI-Sharing-Type: "default" (0) — The Alc-SPI-Sharing-Id AVP must not be present. "per group" (2) — The group ID used for SPI sharing. Valid values are 0 to 65535.

AVP ID	AVP name	Application	Description
1039	Alc-Policer-Parent	Gx-PM-ESM	Grouped AVP included in the Alc-Dynamic-Policer AVP to specify the Arbiter parent parameters of the dynamic policer used for the PCC Rule.
1040	Alc-Parent-Level	Gx-PM-ESM	Specifies the parent level of the dynamic policer used for a PCC rule. Included in the QoS-Information -> Alc-Dynamic-Policer -> Alc-Policer-Parent grouped AVP.
1041	Alc-Parent-Weight	Gx-PM-ESM	Specifies the parent weight of the dynamic policer used for a PCC rule. Included in the QoS-Information -> Alc-Dynamic-Policer -> Alc-Policer-Parent grouped AVP.
1042	Alc-Stat-Mode-UL	Gx-PM-ESM	Specifies the stat-mode of the dynamic policer used for an ingress PCC rule. Included in the QoS-Information -> Alc-Dynamic-Policer AVP grouped AVP.
1043	Alc-Stat-Mode-DL	Gx-PM-ESM	Specifies the stat-mode of the dynamic policer used for an egress PCC rule. Included in the QoS-Information -> Alc-Dynamic-Policer AVP grouped AVP.
1044	Alc-Packet-Byte-Offset-UL	Gx-PM-ESM	Specifies the packet-byte-offset of the dynamic policer used for an ingress PCC rule. Included in the QoS-Information -> Alc-Dynamic-Policer AVP grouped AVP.
1045	Alc-Packet-Byte-Offset-DL	Gx-PM-ESM	Specifies the packet-byte-offset of the dynamic policer used for an egress PCC rule. Included in the QoS-Information -> Alc-Dynamic-Policer AVP grouped AVP.
1046	Alc-Dynamic-Policer	Gx-PM-ESM	Grouped AVP included in the QoS-Information AVP for a PCC Rule definition to specify the dynamic policer parameters for the PCC Rule. Parameters not specified are taken from the dynamic-policer configuration in the **sap-ingress** or **sap-egress** QoS policy. The PCC rule instantiation fails when this AVP is included for a PCC rule that does not require a dynamic policer.

1047	Alc-Spi-Host-And-Session-Limits	Gx-PM-ESM	Grouped AVP included in a Charging-Rule-Definition AVP to override the per SLA profile instance .
			`configure subscriber-mgmt sla-profile host-limits`
			`configure subscriber-mgmt sla-profile session-limits`

1048	Alc-Sub-Host-And-Session-Limits	Gx-PM-ESM	Grouped AVP included in a Charging-Rule-Definition AVP to override the per subscriber **host-limits** and **session-limits** configured in the subscriber profile. `configure subscriber-mgmt sub-profile sub-profile-name`

AVP ID	AVP name	Application	Description
1049	Alc-Host-Limits-IPv4-Arp	Gx-PM-ESM	Overrides the IPv4 ARP limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1050	Alc-Host-Limits-IPv4-Dhcp	Gx-PM-ESM	Overrides the IPv4 DHCP limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1051	Alc-Host-Limits-IPv4-Overall	Gx-PM-ESM	Overrides the IPv4 overall limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1052	Alc-Host-Limits-IPv4-Ppp	Gx-PM-ESM	Overrides the IPV4 PPP limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1053	Alc-Host-Limits-IPv6-Overall	Gx-PM-ESM	Overrides the IPv6 IPoE DHCP PD host limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1054	Alc-Host-Limits-IPv6-Pd-Ipoe-Dhcp	Gx-PM-ESM	Overrides the IPv6 IPoE DHCP PD host limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context. (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1055	Alc-Host-Limits-IPv6-Pd-Overall	Gx-PM-ESM	Overrides the IPv6 DHCP PD host limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1056	Alc-Host-Limits-IPv6-Pd-Ppp-Dhcp	Gx-PM-ESM	Overrides the IPv6 PPPoE DHCP PD host limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.

AVP ID	AVP name	Application	Description
1057	Alc-Host-Limits-IPv6-Wan-Ipoe-Dhcp	Gx-PM-ESM	Overrides the IPv6 IPoE DHCP WAN host limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1058	Alc-Host-Limits-IPv6-Wan-Ipoe-Slaac	Gx-PM-ESM	Overrides the IPv6 IPoE SLAAC WAN host limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1059	Alc-Host-Limits-IPv6-Wan-Overall	Gx-PM-ESM	Overrides the IPv6 IPoE DHCP WAN host limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1060	Alc-Host-Limits-IPv6-Wan-Ppp-Dhcp	Gx-PM-ESM	Overrides the IPv6 PPPoE DHCP WAN host limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1061	Alc-Host-Limits-IPv6-Wan-Ppp-Slaac	Gx-PM-ESM	Overrides the **ipv6-wan-ppp-slaac** limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1062	Alc-Host-Limits-Lac-Overall	Gx-PM-ESM	Overrides the **lac-overall** limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1063	Alc-Host-Limits-Overall	Gx-PM-ESM	Overrides the **overall** limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **host-limits** context.
1064	Alc-Session-Limits-IPoE	Gx-PM-ESM	Overrides the **ipoe** limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **session-limits** context.
1065	Alc-Session-Limits-PPPoE-Local	Gx-PM-ESM	Overrides the **pppoe-local** limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the

AVP ID	AVP name	Application	Description
			Alc-Sub-Host-And-Session-Limits grouped AVP) **session-limits** context.
1066	Alc-Session-Limits-PPPoE-Lac	Gx-PM-ESM	Overrides the **pppoe-lac** limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **session-limits** context.
1067	Alc-Session-Limits-PPPoE-Overall	Gx-PM-ESM	Overrides the **pppoe-overall** limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **session-limits** context.
1068	Alc-Session-Limits-L2TP-Lns	Gx-PM-ESM	Overrides the **l2tp-lns** limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **session-limits** context.
1069	Alc-Session-Limits-L2TP-Lts	Gx-PM-ESM	Overrides the **l2tp-lts** limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **session-limits** context.
1070	Alc-Session-Limits-L2TP-Overall	Gx-PM-ESM	Overrides the **l2tp-overall** limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **session-limits** context.
1071	Alc-Session-Limits-Overall	Gx-PM-ESM	Overrides the **overall** limit configured in the **sla-profile** (when included in the Alc-Spi-Host-And-Session-Limits grouped AVP) or **sub-profile** (when included in the Alc-Sub-Host-And-Session-Limits grouped AVP) **session-limits** context.

5.1 NOKIA-specific AVPs (format)

Table 6: NOKIA-specific AVPs (format)

AVP ID	AVP name	Conf	Type	Flags	Limits	Format
92	Alc-PPPoE-LCP-	NA	integer32	NA, V	[4..300]	Alc-PPPoE-LCP-Keepalive-Interval = 10

AVP ID	AVP name	Conf	Type	Flags	Limits	Format
	Keepalive-Interval					
93	Alc-PPPoE-LCP-Keepalive-Multiplier	NA	integer32	NA, V	[1..5]	Alc-PPPoE-LCP-Keepalive-Multiplier = 2
99	Alc-IPv6-Address (IA-NA)	No	OctetString	V	—	The AVP layout is: <16 octets for address>
158	Alc-NAS-Filter-Rule-Shared	NA	UTF8String	NA,V	Max 50 attributes per message or max 50 filter entries per message.	See the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*.

1001	AA-Functions	NA	Grouped	NA,V	One per ADC rule.
					AA-Functions AVP must contain at least one AA-App-Profile-Name or one AA-App-Service-Options AVP.
						This AVP contains the following nested AVPs:
						• AA-App-Profile-Name
						• AA-App-Service-Options {
						– AA-App-Service-Options-Name
						– AA-App-Service-Options-Value
						}

1002	AA-App-Profile-Name	NA	UTF8String	NA,V	32 chars	Example: AA-App-Profile-Name = MyAppProfile
1003	AA-App-Service-Options	NA	Grouped	NA,V	Max 32 per AA-Functions	This AVP contains the following nested AVPs: • AA-App-Serv-Options-Name • AA-App-Serv-Options-Value
1004	AA-App-Serv-Options-Name	NA	UTF8String	NA,V	32 chars Max one AVP per AA-App-	Example: A-App-Serv-Options-Name = p2p

AVP ID	AVP name	Conf	Type	Flags	Limits	Format
					Service-Options AVP	
1005	AA-App-Serv-Options-Value	NA	UTF8String	NA,V	32 chars Max one AVP per AA-App-Service-Options AVP	AA-App-Serv-Options-Value = HiPrioSub
1006	Alc-Queue	NA	Grouped	NA,V	—	This AVP contains the following nested AVPs: • Alc-Queue-Id • Max-Requested-Bandwidth-UL • Max-Requested-Bandwidth-DL • Guaranteed_Bitrate_UL • Guaranteed_Bitrate_DL • Alc-Committed-Burst-Size-UL • Alc-Maximum-Burst-Size-UL • Alc-Committed-Burst-Size-DL • Alc-Maximum-Burst-Size-DL • AAlc-Wrr-Weight-DL
1007	Alc-Queue-Id	NA	Unsigned32	NA,V	—	Example: Alc-Queue-Id = 3
1008	Alc-Committed-Burst-Size-UL	NA	Unsigned32	NA,V	—	Example: Alc-Committed-Burst-Size-UL = 300000 Burst size of 300,000 bytes.
1009	Alc-Maximum-Burst-Size-UL	NA	Unsigned32	NA,V	—	Example: Alc-Maximum-Burst-Size-UL = 300000 Burst size of 300,000 bytes.
1010	Alc-Committed-Burst-Size-DL	NA	Unsigned32	NA,V	—	Example: Alc-Committed-Burst-Size-DL = 300000 Burst size of 300,000 bytes.
1011	Alc-Maximum-Burst-Size-DL	NA	Unsigned32	NA,V	—	Example: Alc-Maximum-Burst-Size-DL = 300000 Burst size of 300,000 bytes.

AVP ID	AVP name	Conf	Type	Flags	Limits	Format
1013	Alc-Wrr-Weight-DL	NA	Unsigned32	NA,V	—	Example: Alc-Wrr-Weight-DL = 2
1014	Alc-Policer	NA	Grouped	NA,V	—	This AVP contains the following nested AVPs: • Alc-Policer-Id • Max-Requested-Bandwidth-UL • Max-Requested-Bandwidth-DL • Guaranteed_Bitrate_UL • Guaranteed_Bitrate_DL • Alc-Committed-Burst-Size-UL • Alc-Maximum-Burst-Size-UL • Alc-Committed-Burst-Size-DL • Alc-Maximum-Burst-Size-DL
1015	Alc-Policer-Id	NA	Unsigned32	NA,V	—	Example: Alc-Policer-Id = 10
1016	Alc-Sub-Egress-Rate-Limit	NA	Unsigned32	NA,V	—	Example: Alc-Sub-Egress-Rate-Limit = 10000000
1017	Alc-Arbiter-Rate-Limit-DL	NA	Unsigned32	NA,V	—	Example: Alc-Arbiter-Rate-Limit-DL = 10000000
1018	Alc-Arbiter-Rate-Limit-UL	NA	Unsigned32	NA,V	—	Example: Alc-Arbiter-Rate-Limit-UL = 10000000
1021	Alc-Arbiter	NA	Grouped	NA,V	—	This AVP contains the following nested AVPs: • Alc-Arbiter-Name • Alc-Arbiter-Rate-Limit-UL • Alc-Arbiter-Rate-Limit-DL
1022	Alc-Arbiter-Name	NA	UTF8String	NA,V	32 chars	Example: Alc-Arbiter-Name = arbiter-1
1023	Alc-Next-Hop	NA	Grouped	NA,V	—	This AVP can contain the following AVPS: • Alc-Next-Hop-IP • Alc-v4-Next-Hop-Service-Id

AVP ID	AVP name	Conf	Type	Flags	Limits	Format
						• Alc-v6-Next-Hop-Service-Id
1024	Alc-Next-Hop-IP	NA	Address	NA,V	16 octets	IPvv4 or IPv6 address. Example: Alc-Next-Hop-IP = 10.10.10.10 Alc-Next-Hop-IP = 2001:0db8::1
1025	Alc-v4-Next-Hop-Service-Id	NA	Unsigned32	NA,V	1 to 2148007978	Example: Alc-v4-Next-Hop-Service-Id = 10
1026	Alc-v6-Next-Hop-Service-Id	NA	Unsigned32	NA,V	1 to 2148007978	Example: Alc-v6-Next-Hop-Service-Id = 10
1027	Alc-Filter-Action	NA	Enumerated	NA,V	1 or 2	Example: Alc-Filter-Action = 2–matched traffic inside of the PCC rule is dropped.
1028	Alc-QoS-Action	NA	Enumerated	NA,V	1	Example: Alc-QoS-Action = 1–matched traffic inside of the PCC rule is not subjected to QoS related actions.
1029	AA-Sub-Http-Url-Param	NA	UTF String	NV	32 chars	—
1030	AA-Sub-Scope	NA	Enumerated	NV	—	1 = subscriber scope 2 = MAC or device scope
1036	Alc-SPI-Sharing	NA	Grouped	V	—	This AVP contains the following nested AVPs: • Alc-SPI-Sharing-Type • Alc-SPI-Sharing-Id
1037	Alc-SPI-Sharing-Type	NA	Enumerated	V	0 or 2	For example: Alc-SPI-Sharing-Type = 2 -> SLA Profile Instance sharing per group
1038	Alc-SPI-Sharing-Id	NA	Unsigned32	V	0 to 65535 (per group)	For example: Alc-SPI-Sharing-Id = 100
1039	Alc-Policer-Parent	NA	Grouped	NA,V	—	This AVP can contain the following nested AVPs: • Alc-Arbiter-Name

AVP ID	AVP name	Conf	Type	Flags	Limits	Format
						• Alc-Parent-Level • Alc-Parent-Weight
1040	Alc-Parent-Level	NA	Unsigned32	NA,V	1 to 8	For example: Alc-Parent-Level = 8
1041	Alc-Parent-Weight	NA	Unsigned32	NA,V	1 to 100	For example: Alc-Parent-Weight = 20
1042	Alc-Stat-Mode-UL	NA	Enumerated	NA,V	0 to 9	Values: 0 = no_stats 1 = minimal 2 = offered_profile_no_cir 3 = offered_total_cir 4 = offered_priority_no_cir 5 = offered_profile_cir 6 = offered_priority_cir 7 = offered_limited_profile_cir 8 = offered_profile_capped_cir 9 =offered_limited_capped_cir Example: Example: Alc-Stat-Mode-UL = 1
1043	Alc-Stat-Mode-DL	NA	Enumerated	NA,V	0 to 6 and 8 to 10	Values: 0 = no_stats 1 = minimal 2 = offered_profile_no_cir 3 = offered_total_cir 4 = offered_profile_cir 5 = offered_limited_capped_cir 6 = offered_profile_capped_cir 8 = offered_total_cir_exceed 9 = offered_four_profile_no_cir 10 = offered_total_cir_four_profile Example: Alc-Stat-Mode-DL = 1

AVP ID	AVP name	Conf	Type	Flags	Limits	Format
1044	Alc-Packet-Byte-Offset-UL	NA	integer32	NA,V	-32 to +31	Example: Alc-Packet-Byte-Offset-UL = 8
1045	Alc-Packet-Byte-Offset-DL	NA	integer32	NA,V	-64 to +31	Example: Alc-Packet-Byte-Offset-DL = -22
1046	Alc-Dynamic-Policer	NA	Grouped	NA,V	—	For an ingress PCC rule, this AVP can contain the following nested AVPs: • Alc-Policer-Parent • Alc-Committed-Burst-Size-UL • Alc-Maximum-Burst-Size-UL • Alc-Stat-Mode-UL • Alc-Packet-Byte-Offset-UL For an egress PCC rule, this AVP can contain the following nested AVPs: • Alc-Policer-Parent • Alc-Committed-Burst-Size-DL • Alc-Maximum-Burst-Size-DL • Alc-Stat-Mode-DL • Alc-Packet-Byte-Offset-DL
1047	Alc-Spi-Host-And-Session-Limits	NA	Grouped	NA,V	—	This AVP can contain the following nested AVPs: • NOKIA-1049 Alc-Host-Limits-IPv4-Arp • NOKIA-1050 Alc-Host-Limits-IPv4-Dhcp • NOKIA-1051 Alc-Host-Limits-IPv4-Overall • NOKIA-1052 Alc-Host-Limits-IPv4-Ppp • NOKIA-1053 Alc-Host-Limits-IPv6-Overall • NOKIA-1054 Alc-Host-Limits-IPv6-Pd-Ipoe-Dhcp • NOKIA-1055 Alc-Host-Limits-IPv6-Pd-Overall • NOKIA-1056 Alc-Host-Limits-IPv6-Pd-Ppp-Dhcp • NOKIA-1057 Alc-Host-Limits-IPv6-Wan-Ipoe-Dhcp

AVP ID	AVP name	Conf	Type	Flags	Limits	Format
						• NOKIA-1058 Alc-Host-Limits-IPv6-Wan-Ipoe-Slaac • NOKIA-1059 Alc-Host-Limits-IPv6-Wan-Overall • NOKIA-1060 Alc-Host-Limits-IPv6-Wan-Ppp-Dhcp • NOKIA-1061 Alc-Host-Limits-IPv6-Wan-Ppp-Slaac • NOKIA-1062 Alc-Host-Limits-Lac-Overall • NOKIA-1063 Alc-Host-Limits-Overall • NOKIA-1064 Alc-Session-Limits-IPoE • NOKIA-1065 Alc-Session-Limits-PPPoE-Local • NOKIA-1066 Alc-Session-Limits-PPPoE-Lac • NOKIA-1067 Alc-Session-Limits-PPPoE-Overall • NOKIA-1068 Alc-Session-Limits-L2TP-Lns • NOKIA-1069 Alc-Session-Limits-L2TP-Lts • NOKIA-1070 Alc-Session-Limits-L2TP-Overall • NOKIA-1071 Alc-Session-Limits-Overall
1048	Alc-Sub-Host-And-Session-Limits	NA	Grouped	NA,V	—	This AVP can contain the following nested AVPs: • NOKIA-1049 Alc-Host-Limits-IPv4-Arp • NOKIA-1050 Alc-Host-Limits-IPv4-Dhcp • NOKIA-1051 Alc-Host-Limits-IPv4-Overall • NOKIA-1052 Alc-Host-Limits-IPv4-Ppp • NOKIA-1053 Alc-Host-Limits-IPv6-Overall • NOKIA-1054 Alc-Host-Limits-IPv6-Pd-Ipoe-Dhcp

AVP ID	AVP name	Conf	Type	Flags	Limits	Format
						• NOKIA-1055 Alc-Host-Limits-IPv6-Pd-Overall • NOKIA-1056 Alc-Host-Limits-IPv6-Pd-Ppp-Dhcp • NOKIA-1057 Alc-Host-Limits-IPv6-Wan-Ipoe-Dhcp • NOKIA-1058 Alc-Host-Limits-IPv6-Wan-Ipoe-Slaac • NOKIA-1059 Alc-Host-Limits-IPv6-Wan-Overall • NOKIA-1060 Alc-Host-Limits-IPv6-Wan-Ppp-Dhcp • NOKIA-1061 Alc-Host-Limits-IPv6-Wan-Ppp-Slaac • NOKIA-1062 Alc-Host-Limits-Lac-Overall • NOKIA-1063 Alc-Host-Limits-Overall • NOKIA-1064 Alc-Session-Limits-IPoE • NOKIA-1065 Alc-Session-Limits-PPPoE-Local • NOKIA-1066 Alc-Session-Limits-PPPoE-Lac • NOKIA-1067 Alc-Session-Limits-PPPoE-Overall • NOKIA-1068 Alc-Session-Limits-L2TP-Lns • NOKIA-1069 Alc-Session-Limits-L2TP-Lts • NOKIA-1070 Alc-Session-Limits-L2TP-Overall • NOKIA-1071 Alc-Session-Limits-Overall
1049	Alc-Host-Limits-IPv4-Arp	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv4-Arp = 2
1050	Alc-Host-Limits-IPv4-Dhcp	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv4-Dhcp = 2

AVP ID	AVP name	Conf	Type	Flags	Limits	Format
1051	Alc-Host-Limits-IPv4-Overall	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv4-Overall = 2
1052	Alc-Host-Limits-IPv4-Ppp	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv4-Ppp = 2
1053	Alc-Host-Limits-IPv6-Overall	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv6-Overall = 2
1054	Alc-Host-Limits-IPv6-Pd-Ipoe-Dhcp	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv6-Pd-Ipoe-Dhcp = 2
1055	Alc-Host-Limits-IPv6-Pd-Overall	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv6-Pd-Overall = 2
1056	Alc-Host-Limits-IPv6-Pd-Ppp-Dhcp	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv6-Pd-Ppp-Dhcp = 2
1057	Alc-Host-Limits-IPv6-Wan-Ipoe-Dhcp	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv6-Wan-Ipoe-Dhcp = 2
1058	Alc-Host-Limits-IPv6-Wan-Ipoe-Slaac	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv6-Wan-Ipoe-Slaac = 2
1059	Alc-Host-Limits-IPv6-Wan-Overall	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv6-Wan-Overall = 2
1060	Alc-Host-Limits-IPv6-Wan-Ppp-Dhcp	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv6-Wan-Ppp-Dhcp = 2

AVP ID	AVP name	Conf	Type	Flags	Limits	Format
1061	Alc-Host-Limits-IPv6-Wan-Ppp-Slaac	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-IPv6-Wan-Ppp-Slaac = 2
1062	Alc-Host-Limits-Lac-Overall	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-Lac-Overall = 2
1063	Alc-Host-Limits-Overall	NA	integer32	NA,V	-2, -1, [1..131071]	-2 = use the configured value -1 = no limit Alc-Host-Limits-Overall = 2
1064	Alc-Session-Limits-IPoE	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Session-Limits-IPoE = 2
1065	Alc-Session-Limits-PPPoE-Local	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Session-Limits-PPPoE-Local = 2
1066	Alc-Session-Limits-PPPoE-Lac	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Session-Limits-PPPoE-Lac = 2
1067	Alc-Session-Limits-PPPoE-Overall	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Session-Limits-PPPoE-Overall = 2
1068	Alc-Session-Limits-L2TP-Lns	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Session-Limits-L2TP-Lns = 2
1069	Alc-Session-Limits-L2TP-Lts	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Session-Limits-L2TP-Lts = 2
1070	Alc-Session-Limits-L2TP-Overall	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Session-Limits-L2TP-Overall = 2

AVP ID	AVP name	Conf	Type	Flags	Limits	Format
1071	Alc-Session-Limits-Overall	NA	integer32	NA,V	-2, -1, [0..131071]	-2 = use the configured value -1 = no limit Alc-Session-Limits-Overall = 2

6 Diameter-based AVP applicability

The following tables use the following symbols:

- **0**

  The AVP must not be present in the message.
- **0+**

  Zero or more instances of the AVP may be present in the message.
- **0-1**

  Zero or one instance of the AVP may be present in the message. It is considered an error if there is more than one instance of the AVP.
- **1**

  One instance of the AVP must be present in the message.
- **1+**

  At least one instance of the AVP must be present in the message.
- **N**

  The AVP is nested inside of a grouped AVP that is present in this message.

Table 7: Diameter-based AVP applicability

AVP ID	AVP name	CER	CEA	DPR	DPA	DWR	DWA	ASR	ASA
257	Host-IP-Address	1	1+	0	0	0	0	0	0
258	Auth-Application-Id	1	0+	0	0	0	0	1	0
260	Vendor-Specific-Application-Id	0+	0+	0	0	0	0	0	0
263	Session-id	0	0	0	0	0	0	1	1
264	Origin-Host	1	1	1	1	1	1	1	1
265	Supported-Vendor-Id	1+	0+	0	0	0	0	0	0
266	Vendor-Id	1	1	0	0	0	0	0	0
267	Firmware-Revision	1	0-1	0	0	0	0	0	0
268	Result-Code	0	1	0	1	0	1	0	1
269	Product-Name	1	1	0	0	0	0	0	0
273	Disconnect-Cause	0	0	1	0	0	0	0	0

AVP ID	AVP name	CER	CEA	DPR	DPA	DWR	DWA	ASR	ASA
278	Origin-State-Id	1	0-1	0	0	0	0-1	0-1	0-1
279	Failed-AVP	0	0-1	0	0-1	0	0-1	0	0-1
281	Error-Message	0	0	0	0	0	0	0	0
283	Destination-Realm	0	0	0	0	0	0	1	0
293	Destination-Host	0	0	0	0	0	0	1	0
294	Error-Reporting-Host	0	0	0	0	0	0	0	0-1
296	Origin-Realm	1	1	1	1	1	1	1	1

7 Gx AVP applicability

Table 8: Gx AVP applicability

AVP ID	AVP name	CCR	CCA	RAR	RAA
5	NAS-Port	0-1	0	0	0
8	Framed-IP-Address	0-1	0	0	0-1
18	3GPP-SGNS-MCC-MNC	0-1	0	0	0-1
22	3GPP-User-Location-Info	0-1	0	0	0
30	Called-Station-Id	0-1	0	0	0
31	Calling-Station-ID	0-1	0	0	0
55	Event-Timestamp	0-1	0-1	0-1	1
61	NAS-Port-Type	0-1	0	0	0
87	NAS-Port-Id	0-1	0	0	0
92	NAS-Filter-Rule	0	0+	0+	0
97	Framed-IPv6-Prefix	0-1	0	0	0-1
123	Delegated-IPv6-Prefix	0-1	0	0	0-1
258	Auth-Application-Id	1	1	1	0
263	Session-id	1	1	1	1
264	Origin-Host	1	1	1	1
266	Vendor-Id	0	N	0	0
268	Result-Code	0	1	0	0-1
278	Origin-State-Id	1	0-1	0-1	1
279	Failed-AVP	0-1	0+	0	0-1
281	Error-Message	0-1	0-1	0	0-1
282	Route-Record	0+	0	0+	0
283	Destination-Realm	1	0	1	0
285	Re-Auth-Request-Type	0	0	1	0

AVP ID	AVP name	CCR	CCA	RAR	RAA
293	Destination-Host	0-1	0	1	0
295	Termination-Cause	0-1	0	0	0
296	Origin-Realm	1	1	1	1
297	Experimental-Result	0	0-1	0	0-1
298	Experimental-Result-Code	0	N	0	N
302	Logical-Access-Id	0-1	0	0	0
313	Physical-Access-Id	0-1	0	0	0
412	CC-Input-Octets	N	N	N	0
414	CC-Output-Octets	N	N	N	0
415	CC-Request-Number	1	1	0	0
416	CC-Request-Type	1	1	0	0
418	CC-Session-Failover	0	0-1	0	0
421	CC-Total-Octets	N	N	N	0
427	Credit-Control-Failure-Handling	0	0-1	0	0
431	Granted-Service-Unit	0	0-1	N	0
433	Redirect-Address-Type	0	N	N	0
433	Redirect-Server-Address	0	N	N	0
443	Subscription-Id	1-2	0	0	0
444	Subscription-Id-Data	N	0	0	0
446	Used-Service-Unit	N	0	0	0
450	Subscription-Id-Type	N	0	0	0
458	User-Equipment-Info	0-1	0	0	0
459	User-Equipment-Info-Type	N	0	0	0
460	User-Equipment-Info-Value	N	0	0	0
507	Flow-Description	0	N	N	0
511	Flow-Status	0	N	N	0

AVP ID	AVP name	CCR	CCA	RAR	RAA
515	Max-Requested-Bandwidth-DL	0	N	N	0
516	Max-Requested-Bandwidth-UL	0	N	N	0
554	Extended-Max-Requested-BW-DL	0	N	N	0
555	Extended-Max-Requested-BW-UL	0	N	N	0
628	Supported-Features	0-1	0+	0	0
629	Feature-List-Id	N	N	0	0
630	Feature-List	N	N	0	0
909	RAI	0-1	0	0	0
1001	Charging-Rule-Install	0	0+	0+	0
1002	Charging-Rule-Remove	0	0+	0+	0
1003	Charging-Rule-Definition	0	N	N	0
1005	Charging-Rule-Name	N	N	N	N
1006	Event-Trigger	0+	0+	0+	0
1010	Precedence	0	N	N	0
1014	ToS-Traffic-Class	0	N	N	0
1016	QoS-Information	0-1	0-1, N	0-1, N	0
1018	Charging-Rule-Report	0+	0	0	0+
1019	PCC-Rule-Status	N	0	0	N
1025	Guaranteed-Bitrate-DL	0	N	N	0
1026	Guaranteed-Bitrate-UL	0	N	N	0
1027	IP-CAN-Type	0-1	0	0	0-1
1028	QoS-Class-Identifier	0	N	N	0
1031	Rule-Failure-Code	N	0	0	N
1032	RAT-Type	0-1	0	0	0-1
1033	Event-Report-Indication	0	0	0-1	0

AVP ID	AVP name	CCR	CCA	RAR	RAA
1040	APN-Aggregate-Max-Bitrate-DL	N	N	N	0
1041	APN-Aggregate-Max-Bitrate-UL	N	N	N	0
1045	Session-Release-Cause	0	0	0-1	0
1050	AN-GW-Address	0-1	0	0	0-1
1058	Flow-Information	0	0+	0+	0
1065	PDN-Connection-ID	0-1	0	0	0
1066	Monitoring-Key	N	N	N	0
1067	Usage-Monitoring-Information	0+	0+	0+	0
1068	Usage-Monitoring-Level	0	N	N	0
1069	Usage-Monitoring-Report	0	N	N	0
1070	Usage-Monitoring-Support	0	N	N	0
1080	Flow-Direction	0	N	N	0
1085	Redirect-Information	0	0-1	0-1	0
1086	Redirect-Support	0	N	N	0
1088	TDF-Application-Identifier	0	N	N	0
1092	ADC-Rule-Install	0	0+	0+	0
1093	ADC-Rule-Remove	0	0	0	0
1094	ADC-Rule-Definition	0	0	0	0
1096	ADC-Rule-Name	N	N	N	N
1097	ADC-Rule-Report	0+	0+	0	0+
2848	Extended-APN-AMBR-DL	0	N	N	0
2849	Extended-APN-AMBR-UL	0	N	N	0
2850	Extended-GBR-DL	0	N	N	0
2850	Extended-GBR-UL	0	N	N	0

8 NOKIA-specific AVP applicability

Table 9: NOKIA-specific AVP applicability

AVP ID	AVP name	CCR	CCA	RAR	RAA
92	Alc-PPPoE-LCP-Keepalive-Interval	0	0-1	0	0
93	Alc-PPPoE-LCP-Keepalive-Multiplier	0	0-1	0	0
99	Alc-IPv6-Address (IA-NA)	0-1	0	0	0-1
158	Alc-NAS-Filter-Rule-Shared	0	0+	0+	0
1001	AA-Functions	0	0+	0+	0
1002	AA-App-Profile-Name	0	N	N	0
1003	AA-App-Service-Options	0	N	N	0
1004	AA-App-Serv-Options-Name	0	N	N	0
1005	AA-App-Serv-Options-Value	0	N	N	0
1006	Alc-Queue	0	N	N	0
1007	Alc-Queue-Id	0	N	N	0
1008	Alc-Committed-Burst-Size-UL	0	N (0-1)	N (0-1)	0
1009	Alc-Maximum-Burst-Size-UL	0	N (0-1)	N (0-1)	0
1010	Alc-Committed-Burst-Size-DL	0	N (0-1)	N (0-1)	0
1011	Alc-Maximum-Burst-Size-DL	0	N (0-1)	N (0-1)	0
1013	Alc-Wrr-Weight-DL	0	N	N	0
1014	Alc-Policer	0	N	N	0
1015	Alc-Policer-Id	0	N	N	0
1016	Alc-Sub-Egress-Rate-Limit	0	N	N	0
1017	Alc-Arbiter-Rate-Limit-DL	0	N	N	0
1018	Alc-Arbiter-Rate-Limit-UL	0	N	N	0
1021	Alc-Arbiter	0	N	N	0

AVP ID	AVP name	CCR	CCA	RAR	RAA
1022	Alc-Arbiter-Name	0	N (0-1)	N (0-1)	0
1023	Alc-Next-Hop	0	N	N	0
1024	Alc-Next-Hop-IP	0	N	N	0
1025	Alc-v4-Next-Hop-Service-Id	0	N	N	0
1026	Alc-v6-Next-Hop-Service-Id	0	N	N	0
1027	Alc-Filter-Action	0	0+	0+	0
1028	Alc-QoS-Action	0	0+	0+	0
1036	Alc-SPI-Sharing	0	0-1	0-1	0
1037	Alc-SPI-Sharing-Type	0	N	N	0
1038	Alc-SPI-Sharing-Id	0	N	N	0
1039	Alc-Policer-Parent	0	N (0-1)	N (0-1)	0
1040	Alc-Parent-Level	0	N (0-1)	N (0-1)	0
1041	Alc-Parent-Weight	0	N (0-1)	N (0-1)	0
1042	Alc-Stat-Mode-UL	0	N (0-1)	N (0-1)	0
1043	Alc-Stat-Mode-DL	0	N (0-1)	N (0-1)	0
1044	Alc-Packet-Byte-Offset-UL	0	N (0-1)	N (0-1)	0
1045	Alc-Packet-Byte-Offset-DL	0	N (0-1)	N (0-1)	0
1046	Alc-Dynamic-Policer	0	N (0-1)	N (0-1)	0
1047	Alc-Spi-Host-And-Session-Limits	0	0-1	0-1	0
1048	Alc-Sub-Host-And-Session-Limits	0	0-1	0-1	0
1049	Alc-Host-Limits-IPv4-Arp	0	0-1	0-1	0
1050	Alc-Host-Limits-IPv4-Dhcp	0	0-1	0-1	0
1051	Alc-Host-Limits-IPv4-Overall	0	0-1	0-1	0
1052	Alc-Host-Limits-IPv4-Ppp	0	0-1	0-1	0
1053	Alc-Host-Limits-IPv6-Overall	0	0-1	0-1	0
1054	Alc-Host-Limits-IPv6-Pd-Ipoe-Dhcp	0	0-1	0-1	0

AVP ID	AVP name	CCR	CCA	RAR	RAA
1055	Alc-Host-Limits-IPv6-Pd-Overall	0	0-1	0-1	0
1056	Alc-Host-Limits-IPv6-Pd-Ppp-Dhcp	0	0-1	0-1	0
1057	Alc-Host-Limits-IPv6-Wan-Ipoe-Dhcp	0	0-1	0-1	0
1058	Alc-Host-Limits-IPv6-Wan-Ipoe-Slaac	0	0-1	0-1	0
1059	Alc-Host-Limits-IPv6-Wan-Overall	0	0-1	0-1	0
1060	Alc-Host-Limits-IPv6-Wan-Ppp-Dhcp	0	0-1	0-1	0
1061	Alc-Host-Limits-IPv6-Wan-Ppp-Slaac	0	0-1	0-1	0
1062	Alc-Host-Limits-Lac-Overall	0	0-1	0-1	0
1063	Alc-Host-Limits-Overall	0	0-1	0-1	0
1064	Alc-Session-Limits-IPoE	0	0-1	0-1	0
1065	Alc-Session-Limits-PPPoE-Local	0	0-1	0-1	0
1066	Alc-Session-Limits-PPPoE-Lac	0	0-1	0-1	0
1067	Alc-Session-Limits-PPPoE-Overall	0	0-1	0-1	0
1068	Alc-Session-Limits-L2TP-Lns	0	0-1	0-1	0
1069	Alc-Session-Limits-L2TP-Lts	0	0-1	0-1	0
1070	Alc-Session-Limits-L2TP-Overall	0	0-1	0-1	0
1071	Alc-Session-Limits-Overall	0	0-1	0-1	0

9 Result codes (Result-Code AVP)

Table 10: Result codes (Result-Code AVP)

Result code ID	Result code name	Description
Success		
2001	DIAMETER_SUCCESS	The request was successfully completed.
Protocol errors		
3001	DIAMETER_COMMAND_ UNSUPPORTED	Rx: treated as an error. Tx: not supported.
3002	DIAMETER_UNABLE_TO_ DELIVER	Rx: peer failover procedure on the Diameter base level is invoked. After the same response (3002) is received from all eligible peers, the application level (NASREQ/Gx/Gy) is notified. The message can then be retransmitted one last time with the destination-host AVP cleared. For a message to be retransmitted on the application level, server failover procedure must be enabled. Tx: diameter base replies with 3002 if it cannot route the received request message to its destination (this applies to Diameter multi-chassis configuration).
3003	DIAMETER_REALM_NOT_ SERVED	Rx: treated as an error. Tx: not supported.
3004	DIAMETER_TOO_BUSY	Rx - The peer failover procedure on the Diameter base level is invoked. After the same response (3004) is received from all eligible peers, the application level (NASREQ, Gx, Gy) is notified. The message can then be retransmitted one last time with the destination-host AVP cleared. For a message to be retransmitted on the application level, server failover procedure must be enabled. Tx: not supported.
3005	DIAMETER_LOOP_DETECTED	Rx: treated as an error. Tx: not supported.
3006	DIAMETER_REDIRECT_ INDICATION	Rx: treated as an error. Tx: not supported.

Result code ID	Result code name	Description
3007	DIAMETER_APPLICATION_ UNSUPPORTED	Rx: treated as an error. Tx: not supported.
3008	DIAMETER_INVALID_HDR_BITS	Rx: treated as an error. Tx: not supported.
3009	DIAMETER_INVALID_AVP_BITS	Rx: treated as an error. Tx: not supported.
3010	DIAMETER_UNKNOWN_PEER	Rx: treated as an error. Tx: not supported.
Permanent failures		
5001	DIAMETER_AVP_ UNSUPPORTED	Rx: treated as an error. Tx: Reception of an unrecognized AVP with M-bit set triggers a response (RAA) message that contains the Result-Code AVP whose value is set to DIAMETER_AVP_UNSUPORTED, and the Failed-AVP AVP containing the offending AVP.
5002	DIAMETER_UNKNOWN_ SESSION	Rx: treated as an error. Tx: In case that a message from PCRF is received for a non-existing session, the 7750 SR replies with this value.
5004	DIAMETER_INVALID_AVP_ VALUE	Rx: treated as an error. Tx: Reception of an AVP with invalid value triggers a response message (RAA) that contains the Result-Code AVP whose value is set to DIAMETER_INVALID_AVP_VALUE, and the Failed-AVP containing the AVP that caused the error.
5005	DIAMETER_MISSING_AVP	Rx: treated as an error. Tx: not supported.
5007	DIAMETER_CONTRADICTING_ AVPS	Rx: treated as an error. Tx: not supported.
5008	DIAMETER_AVP_NOT_ ALLOWED	Rx: treated as an error. Tx: not supported.
5009	DIAMETER_AVP_OCCURS_ TOO_MANY_TIMES	Rx: treated as an error. Tx: not supported.

Result code ID	Result code name	Description
5010	DIAMETER_NO_COMMON_ APPLICATION	Rx: treated as an error. Tx: not supported.
5011	DIAMETER_UNSUPPORTED_ VERSION	Rx: treated as an error. Tx: As an example, a RAA message carries this AVP as a response to a RAR message that was received by a SR OS node while the Gx session was in a session terminating state. A session terminating state is considered a state where the SR OS node is waiting for a CCA-T message as a response to a previously initiated CCR-T message by the SR OS node.
5012	DIAMETER_UNABLE_TO_ COMPLY	Rx: treated as an error. Tx: For example, a RAA message carries this AVP as a response to a RAR message that was received by a SR OS node while the Gx session was in a session terminating state. A session terminating state is considered a state where the SR OS node is waiting for a CCA-T message as a response to a previously initiated CCR-T message by the SR OS node.
5013	DIAMETER_INVALID_BIT_IN_ HEADER	Rx: treated as an error. Tx: not supported.
5014	DIAMETER_INVALID_AVP_ LENGTH	Rx: treated as an error. Tx: not supported.
5015	DIAMETER_INVALID_ MESSAGE_LENGTH	Rx: treated as an error. Tx: not supported.
5016	DIAMETER_INVALID_AVP_BIT_ COMBO	Rx: treated as an error. Tx: not supported.
5017	DIAMETER_NO_COMMON_ SECURITY	Rx: treated as an error. Tx: not supported.
Gx specific permanent failures		
5140	DIAMETER_ERROR_INITIAL_ PARAMETERS	Rx: treated as an error. Tx: not supported.
5141	DIAMETER_ERROR_TRIGGER_ EVENT	Rx: treated as an error. Tx: not supported.
5142	DIAMETER_PCC_RULE_EVENT	Rx: treated as an error.

Result code ID	Result code name	Description
		Tx: not supported.
5148	DIAMETER_ADC_RULE_EVENT	Rx: treated as an error. Tx: not supported.

10 Rule failure codes (Rule-Failure-Code AVP)

Table 11: Rule failure codes (Rule-Failure-Code AVP)

Rule failure code ID	Rule failure name	Description
1	UNKNOWN_RULE_NAME	Rx: treated as an error. Tx: not supported.
4	GW/7750 SR_ MALFUNCTION	This value indicates the problem related to the value carried in the AVP. For example, the value references a non-existing object (rule), the value is out of bounds or any other unexpected error. The error-message AVP in CCR/RAA carried on the top level or Failed-AVP provides more information about the event for debugging purposes.
5	RESOURCE_LIMITATION	Rx: treated as an error. Tx: not supported.
14	TDF_APPLICATION_ IDENTIFIER_ERROR	Rx: treated as an error. Tx: not supported.

11 Event triggers (Event-Trigger AVP)

Table 12: Event triggers (Event-Trigger AVP)

Event trigger ID	Event trigger name	Description
2	RAT_CHANGE	For GTP S11 access, this is triggered if a new RAT Type is received in GTP.
13	USER_LOCATION_CHANGE	For WLAN-GW, this is triggered for any UE location change. For GTP S11 access, this is triggered if a ULI was received in GTP with either non-ECGI/TAI values or a ECGI/TAI value that changed.
14	NO_EVENT_TRIGGERS	Sent in CCA and RAR by the PCRF to indicate that PCRF does not require any Event Trigger notification except for those events that do not require subscription and are always provisioned.
18	UE_IP_ADDRESS_ALLOCATE	When used in a CCR command, this value indicates that the 7750 SR generated the request because a client's IPv4 address is allocated. The Framed-IP-Address, Framed-IPv6-Prefix, Delegated-IPv6-Prefix or Alc-IPv6-Address AVPs is provided in the same request. This event trigger is reported when the corresponding event occurs, even if the event trigger is not provisioned by the PCRF.
19	UE_IP_ADDRESS_RELEASE	When used in a CCR command, this value indicates that the 7750 SR generated the request because a client's IP address/prefix is released. The Framed-IP-Address, Framed-IPv6-Prefix, Delegated-IPv6-Prefix or Alc-IPv6-Address AVPs is provided in the same request. This event trigger shall be reported when the corresponding event occurs, even if the event trigger is not provisioned by the PCRF.
21	AN_GW_CHANGE	This value is sent by the PCRF to inform the Diameter client in the SR to trigger a notification for every subscriber during a switchover in a multi-chassis configuration. This notification contains the IP address of the newly active BNG (AN_GW_ADDRESS) sent in a CCR-U message. If the Diameter client in the SR OS node is not armed with this event-trigger, the subscriber switchover is not reported to the PCRF.

Event trigger ID	Event trigger name	Description
22	SUCCESSFUL_RESOURCE_ ALLOCATION	Not supported.
26	TAI_CHANGE	For GTP S11 access, this is triggered if a ULI is signaled in GTP with a TAI that changed from the last value received.
27	ECGI_CHANGE	For GTP S11 access, this is triggered if a ULI is signaled in GTP with a ECGI that changed from the last value received.
33	USAGE_REPORT	This value is used in a CCA and RAR commands by the PCRF when requesting usage monitoring on the 7750 SR. The PCRF also provides in the CCA or RAR command the Usage-Monitoring-Information AVPs including the Monitoring-Key AVP and the Granted-Service-Unit AVP. When used in a CCR command, this value indicates that the 7750 SR generated the request to report the accumulated usage for one or more monitoring keys. The 7750 SR provides the accumulated usage volume using the Usage-Monitoring-Information AVPs including the Monitoring-Key AVP and the Used-Service-Unit AVP.

12 Termination causes (Termination-Cause AVP)

Table 13: Termination causes (Termination-Cause AVP)

Termination cause ID	Termination cause name	Description	Reference
1	DIAMETER_LOGOUT	Example reasons: • Clear subscriber via CLI • PADT Received	[RFC 3588][RFC 6733]
2	DIAMETER_SERVICE_NOT_PROVIDED	Example reason: Subscriber-host is terminated via force-NACK received via RADIUS CoA	[RFC 3588][RFC 6733]
3	DIAMETER_BAD_ANSWER	Example reason: Problem with initial parameters during sub-host instantiation while Gx fallback is disabled or default subscriber parameters are not available.	[RFC 3588][RFC 6733]
4	DIAMETER_ADMINISTRATIVE	Example reasons: • Host deleted via RADIUS DISCONNECT • Service shutdown for PPPoE subscriber	[RFC 3588][RFC 6733]
5	DIAMETER_LINK_BROKEN	Example reasons: • SAP is deleted • SHCV check fails	[RFC 3588][RFC 6733]
8	DIAMETER_SESSION_TIMEOUT	Example reason: When idle timeout for the subscriber-host is enabled and its value is reached.	[RFC 3588][RFC 6733]

13 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.

13.1 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*

13.2 Bidirectional Forwarding Detection (BFD)

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

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

RFC 5880, *Bidirectional Forwarding Detection (BFD)*

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

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

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

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

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

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

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

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

13.3 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-ls-app-specific-attr-16, *Application-Specific Attributes Advertisement with BGP Link-State*

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

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

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

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

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

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

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

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

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

RFC 1997, *BGP Communities Attribute*

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

RFC 2439, *BGP Route Flap Damping*

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

RFC 2858, *Multiprotocol Extensions for BGP-4*

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

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

RFC 4360, *BGP Extended Communities Attribute*

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

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

RFC 4486, *Subcodes for BGP Cease Notification Message*

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

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

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

RFC 4760, *Multiprotocol Extensions for BGP-4*

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

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

RFC 5065, *Autonomous System Confederations for BGP*

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

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

RFC 5492, *Capabilities Advertisement with BGP-4*

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

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

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

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

RFC 6811, *Prefix Origin Validation*

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

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

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

RFC 7607, *Codification of AS 0 Processing*

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

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

RFC 7854, *BGP Monitoring Protocol (BMP)*

RFC 7911, *Advertisement of Multiple Paths in BGP*

RFC 7999, *BLACKHOLE Community*

RFC 8092, *BGP Large Communities Attribute*

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

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

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

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

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

RFC 8955, *Dissemination of Flow Specification Rules*

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

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

13.4 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 23.501, *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*

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)*

13.5 Certificate management

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

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

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

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

RFC 7030, *Enrollment over Secure Transport*

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

13.6 Circuit emulation

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

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

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

13.7 Ethernet

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

IEEE 802.1ad, *Provider Bridges*

IEEE 802.1ag, *Connectivity Fault Management*

IEEE 802.1ah, *Provider Backbone Bridges*

IEEE 802.1ak, *Multiple Registration Protocol*

IEEE 802.1aq, *Shortest Path Bridging*

IEEE 802.1ax, *Link Aggregation*

IEEE 802.1D, *MAC Bridges*

IEEE 802.1p, *Traffic Class Expediting*

IEEE 802.1Q, *Virtual LANs*

IEEE 802.1s, *Multiple Spanning Trees*

IEEE 802.1w, *Rapid Reconfiguration of Spanning Tree*

IEEE 802.1X, *Port Based Network Access Control*

IEEE 802.3ac, *VLAN Tag*

IEEE 802.3ad, *Link Aggregation*

IEEE 802.3ah, *Ethernet in the First Mile*

IEEE 802.3x, *Ethernet Flow Control*

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

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

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

13.8 Ethernet VPN (EVPN)

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

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

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

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

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

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

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

RFC 7432, *BGP MPLS-Based Ethernet VPN*

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

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

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

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

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

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

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

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

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

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

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

13.9 gRPC Remote Procedure Calls (gRPC)

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

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

gnmi.proto version 0.8.0, *gRPC Network Management Interface (gNMI) Service Specification*

PROTOCOL-HTTP2, *gRPC over HTTP2*

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

13.10 Intermediate System to Intermediate System (IS-IS)

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

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

ISO/IEC 10589:2002 Second Edition, *Intermediate system to Intermediate system intra-domain 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*

13.11 Internet Protocol (IP) Fast Reroute (FRR)

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

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

RFC 7431, *Multicast-Only Fast Reroute*

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

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

13.12 Internet Protocol (IP) general

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

RFC 768, *User Datagram Protocol*

RFC 793, *Transmission Control Protocol*

RFC 854, *Telnet Protocol Specifications*

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

RFC 2347, *TFTP Option Extension*

RFC 2348, *TFTP Blocksize Option*

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

RFC 2428, *FTP Extensions for IPv6 and NATs*

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

RFC 2784, *Generic Routing Encapsulation (GRE)*

RFC 2818, *HTTP Over TLS*

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

RFC 3164, *The BSD syslog Protocol*

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

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

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

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

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

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

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

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

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

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

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

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

RFC 5925, *The TCP Authentication Option*

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

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

RFC 6528, *Defending against Sequence Number Attacks*

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

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

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

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

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

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

RFC 7616, *HTTP Digest Access Authentication*

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

13.13 Internet Protocol (IP) multicast

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

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

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

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

RFC 1112, *Host Extensions for IP Multicasting*

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

RFC 2365, *Administratively Scoped IP Multicast*

RFC 2375, *IPv6 Multicast Address Assignments*

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

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

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

RFC 3446, *Anycast 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)*

13.14 Internet Protocol (IP) version 4

RFC 791, *Internet Protocol*

RFC 792, *Internet Control Message Protocol*

RFC 826, *An Ethernet Address Resolution Protocol*

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

RFC 1034, *Domain Names - Concepts and Facilities*

RFC 1035, *Domain Names - Implementation and Specification*

RFC 1191, *Path MTU Discovery* – router specification

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

RFC 1534, *Interoperation between DHCP and BOOTP*

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

RFC 1812, *Requirements for IPv4 Routers*

RFC 1918, *Address Allocation for Private Internets*

RFC 2003, *IP Encapsulation within IP*

RFC 2131, *Dynamic Host Configuration Protocol*

RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

RFC 2401, *Security Architecture for Internet Protocol*

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

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

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

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

13.15 Internet Protocol (IP) version 6

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

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

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

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

RFC 3587, *IPv6 Global Unicast Address Format*

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

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

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

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

RFC 3971, *SEcure Neighbor Discovery (SEND)*

RFC 3972, *Cryptographically Generated Addresses (CGA)*

RFC 4007, *IPv6 Scoped Address Architecture*

RFC 4193, *Unique Local IPv6 Unicast Addresses*

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

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

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

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

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

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

RFC 5007, *DHCPv6 Leasequery*

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

RFC 5722, *Handling of Overlapping IPv6 Fragments*

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

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

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

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

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

RFC 6437, *IPv6 Flow Label Specification*

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

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

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

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

13.16 Internet Protocol Security (IPsec)

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

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

RFC 2401, *Security Architecture for the Internet Protocol*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RFC 3948, *UDP Encapsulation of IPsec ESP Packets*

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

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

RFC 4301, *Security Architecture for the Internet Protocol*

RFC 4303, *IP Encapsulating Security Payload*

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

RFC 4308, *Cryptographic Suites for IPsec*

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

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

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

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

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

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

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

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

RFC 5903, *ECP Groups for IKE and IKEv2*

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

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

RFC 6379, *Suite B Cryptographic Suites for IPsec*

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

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

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

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

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

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

13.17 Label Distribution Protocol (LDP)

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

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

draft-pdutta-mpls-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*

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

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

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

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

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

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

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

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

13.19 Multiprotocol Label Switching (MPLS)

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

RFC 3031, *Multiprotocol Label Switching Architecture*

RFC 3032, *MPLS Label Stack Encoding*

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

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

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

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

RFC 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*

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

RFC 5586, *MPLS Generic Associated Channel*

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

RFC 5960, *MPLS Transport Profile Data Plane Architecture*

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

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

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

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

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

RFC 6478, *Pseudowire Status for Static Pseudowires*

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

13.21 Network Address Translation (NAT)

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

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

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

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

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

RFC 5382, *NAT Behavioral Requirements for TCP*

RFC 5508, *NAT Behavioral Requirements for ICMP*

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

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

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

RFC 6887, *Port Control Protocol (PCP)*

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

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

RFC 7915, *IP/ICMP Translation Algorithm*

13.22 Network Configuration Protocol (NETCONF)

RFC 5277, *NETCONF Event Notifications*

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

RFC 6022, *YANG Module for NETCONF Monitoring*

RFC 6241, *Network Configuration Protocol (NETCONF)*

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

RFC 6243, *With-defaults Capability for NETCONF*

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

RFC 8525, *YANG Library*

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

13.23 Open Shortest Path First (OSPF)

RFC 1765, *OSPF Database Overflow*

RFC 2328, *OSPF Version 2*

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

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

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

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

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

RFC 4552, *Authentication/Confidentiality for OSPFv3*

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

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

RFC 5185, *OSPF Multi-Area Adjacency*

RFC 5187, *OSPFv3 Graceful Restart* – helper mode

RFC 5243, *OSPF Database Exchange Summary List Optimization*

RFC 5250, *The OSPF Opaque LSA Option*

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

RFC 5340, *OSPF for IPv6*

RFC 5642, *Dynamic Hostname Exchange Mechanism for OSPF*

RFC 5709, *OSPFv2 HMAC-SHA Cryptographic Authentication*

RFC 5838, *Support of Address Families in OSPFv3*

RFC 6549, *OSPFv2 Multi-Instance Extensions*

RFC 6987, *OSPF Stub Router Advertisement*

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

RFC 7684, *OSPFv2 Prefix/Link Attribute Advertisement*

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

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

RFC 8920, *OSPF Application-Specific Link Attributes*

13.24 OpenFlow

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

13.25 Path Computation Element Protocol (PCEP)

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

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

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

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

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

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

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

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

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

13.26 Point-to-Point Protocol (PPP)

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

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

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

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

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

RFC 5072, *IP Version 6 over PPP*

13.27 Policy management and credit control

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

RFC 4006, *Diameter Credit-Control Application*

RFC 6733, *Diameter Base Protocol*

13.28 Pseudowire (PW)

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

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

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

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

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

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

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

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

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

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

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

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

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

RFC 6073, *Segmented Pseudowire*

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

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

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

RFC 6718, *Pseudowire Redundancy*

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

RFC 6870, *Pseudowire Preferential Forwarding Status bit*

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

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

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

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

13.29 Quality of Service (QoS)

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

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

RFC 2597, *Assured Forwarding PHB Group*

RFC 3140, *Per Hop Behavior Identification Codes*

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

13.30 Remote Authentication Dial In User Service (RADIUS)

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

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

RFC 2866, *RADIUS Accounting*

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

RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

RFC 2869, *RADIUS Extensions*

RFC 3162, *RADIUS and IPv6*

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

RFC 5176, *Dynamic Authorization Extensions to RADIUS*

RFC 6613, *RADIUS over TCP* – with TLS

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

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

RFC 6911, *RADIUS attributes for IPv6 Access Networks*

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

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

RFC 2702, *Requirements for Traffic Engineering over MPLS*

RFC 2747, *RSVP Cryptographic Authentication*

RFC 2961, *RSVP Refresh Overhead Reduction Extensions*

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

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

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

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

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

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

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

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

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

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

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

RFC 5712, *MPLS Traffic Engineering Soft Preemption*

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

13.32 Routing Information Protocol (RIP)

RFC 1058, *Routing Information Protocol*

RFC 2080, *RIPng for IPv6*

RFC 2082, *RIP-2 MD5 Authentication*

RFC 2453, *RIP Version 2*

13.33 Segment Routing (SR)

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

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

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

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

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

draft-ietf-idr-bgpls-srv6-ext-13, *BGP Link State Extensions for SRv6*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RFC 8661, *Segment Routing MPLS Interworking with LDP*

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

RFC 8665, *OSPF Extensions for Segment Routing*

RFC 8666, *OSPFv3 Extensions for Segment Routing*

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

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

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

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

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

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

RFC 9256, *Segment Routing Policy Architecture*

13.34 Simple Network Management Protocol (SNMP)

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

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

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

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

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

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

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

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

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

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

IANAifType-MIB revision 200505270000Z, *ianaifType*

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

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

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

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

LLDP-MIB revision 200505060000Z, *lldpMIB*

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

RFC 1212, *Concise MIB Definitions*

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

RFC 1724, *RIP Version 2 MIB Extension*

RFC 1901, *Introduction to Community-based SNMPv2*

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

RFC 2206, *RSVP Management Information Base using SMIv2*

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

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

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

RFC 2579, *Textual Conventions for SMIv2*

RFC 2580, *Conformance Statements for SMIv2*

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

RFC 2819, *Remote Network Monitoring Management Information Base*

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

RFC 2863, *The Interfaces Group MIB*

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

RFC 2933, *Internet Group Management Protocol MIB*

RFC 3014, *Notification Log MIB*

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

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

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

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

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

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

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

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

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

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

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

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

RFC 3419, *Textual Conventions for Transport Addresses*

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

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

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

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

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

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

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

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

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

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

RFC 4001, *Textual Conventions for Internet Network Addresses*

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

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

RFC 4220, *Traffic Engineering Link Management Information Base*

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

RFC 4292, *IP Forwarding Table MIB*

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

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

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

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

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

SFLOW-MIB revision 200309240000Z, *sFlowMIB*

13.35 Timing

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

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

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

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

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

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

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

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

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

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

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

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

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

13.36 Two-Way Active Measurement Protocol (TWAMP)

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

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

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

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

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

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

13.37 Virtual Private LAN Service (VPLS)

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

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

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

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

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

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

13.38 Voice and video

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

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

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

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

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

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

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

RFC 4588, *RTP Retransmission Payload Format*

13.39 Wireless Local Area Network (WLAN) gateway

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

13.40 Yet Another Next Generation (YANG)

RFC 6991, *Common YANG Data Types*

RFC 7950, *The YANG 1.1 Data Modeling Language*

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

13.41 Yet Another Next Generation (YANG) OpenConfig Modules

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

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

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

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

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

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

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

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

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

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

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

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

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

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

openconfig-if-ethernet.yang version 2.12.1, *OpenConfig Interfaces Ethernet Module*

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

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

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

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

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

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

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

openconfig-lacp.yang version 1.3.0, *OpenConfig LACP Module*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

openconfig-system.yang version 0.10.1, *OpenConfig System Module*

openconfig-system-grpc.yang version 1.0.0, *OpenConfig System gRPC Module*

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

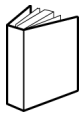
openconfig-system-terminal.yang version 0.3.0, *OpenConfig System Terminal Module*

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

openconfig-terminal-device.yang version 1.9.0, *OpenConfig Terminal Optics Device Module*

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

Customer document and product support



Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback