Multi-Access Gateway – controller

Release 26.10

PFCP Interface Description Guide

3HE 22207 AAAC TQZZA
Edition: 01
October 2026

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

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

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

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

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

No part of this document may be modified.

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

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

© 2026 Nokia.

Table of contents

List of tables **7**

List of figures **11**

1 Getting started **12**
1.1 About this guide 12
1.2 Conventions 12
1.2.1 Precautionary and information messages 13
1.2.2 Options or substeps in procedures and sequential workflows 13

2 Introduction to PFCP and CUPS concepts **14**
2.1 PFCP in the CUPS architecture 14
2.2 CUPS concepts 14
2.2.1 PFCP association and path 14
2.2.2 PFCP session 15
2.2.3 Packet data rule 15

3 Forwarding between the MAG-c and MAG-u **17**
3.1 IBCP 17
3.2 Default IBCP session 18
3.3 GTP-U encapsulation and decapsulation 19

4 Session handling **20**
4.1 Overview 20
4.2 PFCP session example 20

5 PFCP protocol **23**
5.1 Protocol stack 23
5.2 Generic PFCP message header 23
5.3 PFCP messages overview 25
5.4 Example call flows 26
5.4.1 Initial PFCP association and session setup 26
5.4.2 IPoE session setup 27
5.4.3 CoA handling 28

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

5.4.4 MAG-c triggered updates....28
5.4.5 PFCP connectivity failure and headless mode....29

6 PFCP messages....30
6.1 Message types....30
6.2 PFCP node-related messages....31
6.2.1 PFCP association messages....31
6.2.1.1 PFCP Association Setup Request....31
6.2.1.2 PFCP Association Setup Response....32
6.2.1.3 PFCP Association Update Request....33
6.2.1.4 PFCP Association Update Response....34
6.2.2 Heartbeat messages....35
6.2.2.1 PFCP Heartbeat Request....35
6.2.2.2 PFCP Heartbeat Response....35
6.3 PFCP session-related messages....35
6.3.1 PFCP Session Establishment Request....35
6.3.1.1 Create PDR IE....37
6.3.1.2 Create FAR IE....39
6.3.1.3 Create URR IE....40
6.3.1.4 Create QER IE....41
6.3.1.5 Create Traffic Endpoint IE....41
6.3.1.6 Nokia UP Aggregate Route IE....46
6.3.2 PFCP Session Establishment Response....46
6.3.2.1 Created Traffic Endpoint IE....47
6.3.3 PFCP Session Modification Request....47
6.3.3.1 Update PDR IE....50
6.3.3.2 Update FAR IE....51
6.3.3.3 Update URR IE....52
6.3.3.4 Update QER IE....53
6.3.3.5 Update Traffic Endpoint IE....53
6.3.3.6 Remove PDR IE....54
6.3.3.7 Remove FAR IE....55
6.3.3.8 Remove URR IE....55
6.3.3.9 Remove QER IE....55
6.3.3.10 Remove Traffic Endpoint IE....55
6.3.3.11 Query URR IE....56

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

6.3.4 PFCP Session Modification Response....56
6.3.4.1 Usage Report IE....57
6.3.5 PFCP Session Deletion Request....57
6.3.6 PFCP Session Deletion Response....57
6.3.7 PFCP Session Report Request....58
6.3.8 PFCP Session Report Response....58

7 Nokia-specific information elements....59
7.1 Format of the information elements....59
7.2 Nokia Detailed Error IE....60
7.3 Nokia SAP Template IE....60
7.4 Nokia Group Interface Template....61
7.5 Nokia QoS Override IE....61
7.6 Nokia Create Filter Override....62
7.7 Nokia Delete Filter Override IE....62
7.8 Nokia Intermediate Destination IE....63
7.9 Nokia Measurement Information IE....63
7.10 Nokia UP Function Features IE....64
7.11 Nokia PFCPHB-Flags IE....64
7.12 Nokia PFCPSMReq-Flags IE....65
7.13 Nokia State ID IE....65
7.14 Nokia NAT ISA Members IE....66
7.15 Nokia format for QoS policy in the Activate Predefined Rules IE....66
7.16 Nokia L2TP Init Rx LCP Conf Request IE....66
7.17 Nokia L2TP Last Tx LCP Conf Request IE....67
7.18 Nokia L2TP Last Rx LCP Conf Request IE....67
7.19 Nokia L2TP Authentication Type IE....68
7.20 Nokia L2TP Authentication Name IE....68
7.21 Nokia L2TP Authentication ID IE....69
7.22 Nokia L2TP Authentication Challenge IE....69
7.23 Nokia L2TP Authentication Response IE....70
7.24 Nokia L2TP Client Endpoint IE....70
7.25 Nokia L2TP Server Endpoint IE....71
7.26 Nokia L2TP Client Auth ID IE....71
7.27 Nokia L2TP Server Auth ID IE....71
7.28 Nokia L2TP Password IE....72

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

7.29 Nokia L2TP Assignment ID IE....72
7.30 Nokia L2TP Private Group ID IE....73
7.31 Nokia L2TP Parameters IE....73
7.32 Nokia Access Line Parameters IE....75
7.33 Nokia L2TP IDs IE....77
7.34 Nokia Access Line Circuit ID IE....78
7.35 Nokia Access Line Remote ID IE....78

Appendix: References....80

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

List of tables

Table 1: GTP-U header for in-band control plane messages (CPRi interface)..... 18
Table 2: Default IBCP PFCP session example for a PPPoE-only deployment..... 19
Table 3: Top level IEs for an example PPPoE session..... 20
Table 4: PDR and FARs for an example PPPoE session..... 21
Table 5: Generic PFCP message header..... 23
Table 6: PFCP messages overview..... 25
Table 7: Message types..... 30
Table 8: IEs in a PFCP Association Setup Request..... 31
Table 9: IEs in a PFCP Association Setup Response..... 32
Table 10: IEs in a PFCP Association Update Request..... 33
Table 11: IEs in a PFCP Association Update Response..... 34
Table 12: IEs in a PFCP Heartbeat Request..... 35
Table 13: IEs in a PFCP Heartbeat Response..... 35
Table 14: IEs in a PFCP Session Establishment Request..... 35
Table 15: Create PDR IE..... 37
Table 16: PDI IE..... 38
Table 17: Ethernet Packet Filter IE..... 38
Table 18: Create FAR IE..... 39
Table 19: Forwarding Parameters IE..... 39
Table 20: Create URR IE..... 40
Table 21: Create QER IE..... 41

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Table 22: Create Traffic Endpoint IE....41
Table 23: Nokia L2TP Tunnel IE....44
Table 24: Nokia UP Aggregate Route IE....46
Table 25: IEs in PFCP Session Establishment Response....46
Table 26: Created Traffic Endpoint IE....47
Table 27: IEs in a PFCP Session Modification Request....47
Table 28: Update PDR IE (PFCP Session Modification Request)....50
Table 29: Update FAR IE (PFCP Session Modification Request)....51
Table 30: Update Forwarding Parameters IE....52
Table 31: Update URR IE (PFCP Session Modification Request)....52
Table 32: Update QER IE (PFCP Session Modification Request)....53
Table 33: Update Traffic Endpoint IE (PFCP Session Modification Request)....53
Table 34: Remove PDR IE (PFCP Session Modification Request)....54
Table 35: Remove FAR IE (PFCP Session Modification Request)....55
Table 36: Remove URR IE (PFCP Session Modification Request)....55
Table 37: Remove QER IE (PFCP Session Modification Request)....55
Table 38: Remove Traffic Endpoint IE (PFCP Session Modification Request)....55
Table 39: Query URR IE (PFCP Session Modification Request)....56
Table 40: IEs in a PFCP Session Modification Response....56
Table 41: Usage Report IE (PFCP Session Modification Response)....57
Table 42: IEs in a PFCP Session Deletion Response....58
Table 43: IEs in a PFCP Session Report Request....58
Table 44: IEs in a PFCP Session Report Response....58

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Table 45: IE format....59
Table 46: 3GPP IE format....59
Table 47: Vendor-specific IE format....60
Table 48: Nokia Detailed Error IE....60
Table 49: Nokia SAP Template IE....60
Table 50: Nokia Group Interface Template IE....61
Table 51: Nokia QoS Override IE....61
Table 52: Nokia Create Filter Override IE....62
Table 53: Nokia Delete Filter Override IE....62
Table 54: Nokia Intermediate Destination IE....63
Table 55: Nokia Measurement Information IE....63
Table 56: Nokia UP Function Features IE....64
Table 57: Nokia PFCPHB-Flags IE....64
Table 58: Nokia PFCPSMReq-Flags IE....65
Table 59: Nokia State ID IE....65
Table 60: Nokia NAT ISA Members IE....66
Table 61: Nokia L2TP Init Rx LCP Conf Request IE....66
Table 62: Nokia L2TP Last Tx LCP Conf Request IE....67
Table 63: Nokia L2TP Last Rx LCP Conf Request IE....67
Table 64: Nokia L2TP Authentication Type IE....68
Table 65: Nokia L2TP Authentication Name IE....68
Table 66: Nokia L2TP Authentication ID IE....69
Table 67: Nokia L2TP Authentication Challenge IE....69

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Table 68: Nokia L2TP Authentication Response IE....70
Table 69: Nokia L2TP Client Endpoint IE....70
Table 70: Nokia L2TP Server Endpoint IE....71
Table 71: Nokia L2TP Client Auth ID IE....71
Table 72: Nokia L2TP Server Auth ID IE....71
Table 73: Nokia L2TP Password IE....72
Table 74: Nokia L2TP Assignment ID IE....72
Table 75: Nokia L2TP Private Group ID IE....73
Table 76: Nokia L2TP Parameters IE....73
Table 77: L2TP parameters....73
Table 78: Nokia Access Line Parameters IE....75
Table 79: Access line parameters....76
Table 80: Nokia L2TP IDs IE....77
Table 81: Nokia Access Line Circuit ID IE....78
Table 82: Nokia Access Line Remote ID IE....78

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

List of figures

Figure 1: Control plane communication for fixed access....17
Figure 2: Protocol stack for IBCP....19
Figure 3: PFCP protocol stack for the control plane....23
Figure 4: PFCP session ID allocation and use....24
Figure 5: Initial PFCP association and session setup....26
Figure 6: IPoE session setup....27
Figure 7: CoA handling....28
Figure 8: MAG-c triggered accounting update....28
Figure 9: Example headless mode call flow....29

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

1 Getting started

Find general information about this guide.

1.1 About this guide

This guide describes the applicability of PFCP for fixed broadband access and the extensions to the protocol.

The PFCP interface serves as the control layer between the Nokia MAG-c and the SR OS-based user plane (MAG-u). The PFCP interface is designed to perform the following functions:

- handle all dynamic states
- create packet matching rules and corresponding QoS
- provide usage reporting and monitoring and packet action parameters

Note:
The MAG-c functions as the control plane (CP) and has the ability to control the MAG-u nodes.

Note:
The MAG-c is the generic converged name for any type of control plane, including the BNG CP, the 4G combined SGW-C + PGW-C, and the 5G CP function (SMF).

The MAG-u is the generic converged name for any type of user plane, including the BNG UP, the 4G combined SGW-u + PGW-u, and the 5G UP function (UPF).

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

For more information, see the Appendix: References, and other guides mentioned in the MAG-c Guide to Documentation.

Note: This guide generically covers content for the release specified on the title page of the guide, and may also contain some content that will be released in later maintenance loads. See the applicable *MAG-c Release Notes* for information about features supported in each load of the software release.

Note: The information in this guide is intended to be used in conjunction with the SR OS software user guides. The SR OS software user guides describe SR OS service features that are supported by the MAG-c. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR Documentation Suite Overview Card 20.10.R1* for specific guide titles.

1.2 Conventions

This section describes the general conventions used in this guide.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

1.2.1 Precautionary and information messages

The following information symbols are used in the documentation.



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



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



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



Note: Note provides additional operational information.



Tip: Tip provides suggestions for use or best practices.

1.2.2 Options or substeps in procedures and sequential workflows

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

Example: Options in a procedure

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

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

Example: Substeps in a procedure

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

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

2 Introduction to PFCP and CUPS concepts

The interfaces between the MAG-c and the MAG-u that are related to PFCP are the SCi, CPRi, Sx, N4, Sx-u, and N4-u interfaces. Get a brief overview of those interfaces and of general CUPS and BNG concepts, including PFCP association and path, PFCP session, and PDR.

2.1 PFCP in the CUPS architecture

The interfaces between the MAG-c and the MAG-u that are related to PFCP are the SCi, CPRi, Sx, N4, Sx-u, and N4-u interfaces.

The following lists the interfaces between the MAG-c and the MAG-u.

- **SCi, Sx, N4**
  The MAG-c creates traffic forwarding rules and related states on the MAG-u via these interfaces. When the rules and states are created, the MAG-u forwards subscriber data traffic according to the rules. The Sx interface is defined by 3GPP for 4G sessions, while the N4 interface is defined for 5G sessions. 3GPP defines these interfaces mainly in TS 29.244. The SCi interface is an extension added for pure BNG sessions as defined in TR-459 and is based on TS 29.244.
- **CPRi, Sx-u, N4-u**
  The MAG-u and MAG-c use these interfaces to forward and tunnel control packets; for example, DHCP discovery, PPPoE PADI. All these interfaces use GTP-U as the tunnel transport layer and these tunnels are configured using the PFCP protocol. Sx-u and N4-u are the 3GPP terms defined in TS 29.244 in context of 4G and 5G sessions, while CPRi is the BBF term defined in TR-459, but all imply the same concept. Nokia often uses the term in-band control plane (IBCP) to indicate any of these interfaces.

2.2 CUPS concepts

Get a brief overview of general CUPS and BNG concepts. See 3GPP TS 29.244 for more information about the CUPS concepts.

2.2.1 PFCP association and path

The PFCP association and path define the connectivity between the MAG-c and MAG-u.

To send a session to a MAG-u, a PFCP association needs to be established. While establishing this association, the MAG-u and the MAG-c exchange capabilities, functional features, and parameters; for example, a MAG-u sends functional features such as PPPoE support, IPoE support, and LCP Keep-alive Offload support. Capability exchange can influence the IE applicability in PFCP session messages.

- **PFCP association**
  A PFCP association must be set up before sessions can be established between the MAG-u and the MAG-c. Only one association per MAG-c and MAG-u pair is allowed. The identifiers of the association are the MAG-c and the MAG-u node IDs, which can be IP addresses or domain names. Provisioning commands specific to PFCP associations are available to enable the PFCP protocol.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- **PFCP path**
  Multiple paths are possible per PFCP association. The identifier of a PFCP path is the pair of IP addresses that the MAG-c and the MAG-u use to communicate. Paths are not negotiated, but are learned while using PFCP signaling. Each IP address is called a PFCP entity. Each pair of MAG-c and MAG-u IP addresses is called a PFCP path.

Note:

- The Nokia MAG-c uses only one IP address per association, although in general a MAG-c or MAG-u (also called a PFCP node) could use multiple IP addresses for communication within the same PFCP association. Because the Nokia MAG-c and MAG-u use only one PFCP path per association, the terms path and association are often used interchangeably.
- Both the MAG-c and MAG-u use PFCP heartbeat messages to verify that all known paths are alive. The heartbeat parameters are configured in the PFCP profile context. When a path fails, all related sessions are removed.

2.2.2 PFCP session

A session is the basic operational object of the MAG, and represents the connectivity of a single device such as a residential gateway. The following are done in the scope of a single session:

- address assignment
- authentication
- accounting
- communication

A PFCP association is required to create a PFCP session.

2.2.3 Packet data rule

Packet data rules (PDRs) are the building blocks to create a correct forwarding state on the MAG-u.

The PFCP sessions are containers for PDRs. Each PDR defines a unidirectional traffic flow and the rules associated with that flow. The MAG-u adheres to the PDR rules when treating the traffic for the defined traffic flow.

A PDR consists of the following sub-objects and references.

- **PDI**
  The packet detection information (PDI) is a sub-object and specifies the match criteria for the packet. It also contains a reference to a traffic endpoint.
- **FAR ID**
  The forwarding action rule (FAR) specifies the action (for example, drop, forward, mirror) for matching packets. The PDR refers to one FAR. FARs can be shared between multiple PDRs within a session.
- **QER ID**
  The QoS enforcement rule (QER) specifies the QoS treatment for matching packets (for example, GBR, MBR). The PDR refers to one or multiple QERs. QERs can be shared between multiple PDRs within a session and between sessions.

  Multiple PDRs of one session share the same QER using the QER ID, while multiple PDRs of different sessions share the same QER using the QER correlation ID.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

- **URR ID**
  The usage reporting rule (URR) specifies the usage reporting and charging for matching packets. The PDR refers to one or multiple URRs. URRs can be shared between multiple PDRs within a session.



Note: The Nokia BNG CUPS solution supports only one QER and one URR per PDR.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

3 Forwarding between the MAG-c and MAG-u

The forwarding of control plane messages is in-band and sent using an IBCP tunnel.

3.1 IBCP

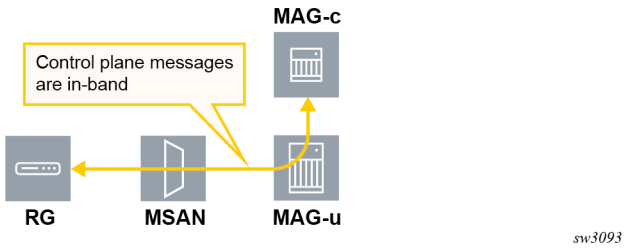
In-band control plane (IBCP) packets are sent by a residential gateway over the data path to the MAG-u, but must be handled by the MAG-c. Examples include DHCP, DHCPv6, and ICMPv6 RS.

This contrasts for example with out-of-band NAS signaling in case of fixed wireless access (FWA) sessions which do not reach the MAG-u, but are sent to the MAG-c through an MME (4G) or AMF (5G).

IBCP packets for fixed access sessions arrive before any session state is created. The MAG-u sends the initial control plane packets over GTP-U to the MAG-c.

The following figure shows the control plane communication for fixed access.

Figure 1: Control plane communication for fixed access



Immediately after the PFCP association is created, the MAG-c signals at least one GTP-U tunnel using a dedicated PFCP session for unknown in-band control plane packets. That tunnel is called the default IBCP tunnel.

After handling the initial control plane message, the MAG-c instructs the MAG-u to forward any subsequent control plane packets over a per-session GTP-U tunnel. The per-session GTP-U tunnel is signaled as part of the regular PFCP session for that connection.

The default IBCP tunnel is only used for packets from the MAG-u to the MAG-c, return packets use a dedicated per-session GTP-U tunnel.

GTP-U runs over UDP, using port 2152, and is defined in 3GPP TS 29.281. GTP-U is extended to allow transport of Ethernet packets. This is not explicitly added in the GTP-U encoding, rather the content type is defined at tunnel setup in PFCP.

The following table describes the format of the basic GTP-U header for IBCP packets on the CPRi interface between the MAG-u and the MAG-c.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Table 1: GTP-U header for in-band control plane messages (CPRi interface)

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	Version=1			PT=0	0	E	S=0	PN=0
2	Message Type = 255							
3	Message Length (1st Octet)							
4	Message Length (2nd Octet)							
5 to 8	TEID							
9	Next Extension Header Type [1]							

The following clarifies the fields in the message header.

- PT indicates the protocol type. The protocol type is 0 for IBCP messages on the CPRi interface.
- E indicates the presence of a meaningful value in the Next Extension Header field. When it is set to 0, the Next Extension Header field either is not present or, if present, is not interpreted. When it is set to 1, the Next Extension Header field is present, and is interpreted.
- S indicates whether the SEID field is present. IBCP messages on the CPRi interface do not contain a session ID.
- PN indicates the presence of a meaningful value in the N-PDU Number field. PN is 0 for IBCP packets on the CPRi interface. The N-PDU number is not used.
- Message Type indicates the type of the message and determines the content of the message beyond the header.
- Message Length is the total length of the packet.
- TEID is signaled during PFCP session establishment for the IBCP packets.
- Next Extension Header Type is only evaluated when E is set to 1. It defines the type of the extension header that follows this field in the GTP PDU.

3.2 Default IBCP session

After a PFCP association is created, the MAG-c signals at least one GTP-U tunnel using a PFCP session for unknown IBCP packets. That tunnel is called the default IBCP tunnel

The MAG-c installs basic PDRs for the default IBCP session using PFCP. The MAG-u uses the SDF filters and Ethernet packet filters in the PDR to filter out control plane traffic packets; for example, to only allow PPPoE or DHCP packets. The FAR that is linked to the PDR defines the GTP-U encapsulation between the MAG-u and the MAG-c.

The default IBCP session is only relevant to fixed access sessions. For Fixed Wireless Access (FWA) sessions, initial setup is always done out of band and creates a dedicated PFCP session. Subsequent in-band control plane messages can use the IBCP associated with that dedicated PFCP session.

[1] This field is only evaluated when indicated by the E flag set to 1.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

The following table describes an example of a default IBCP PFCP session for a PPPoE-only deployment.

Table 2: Default IBCP PFCP session example for a PPPoE-only deployment

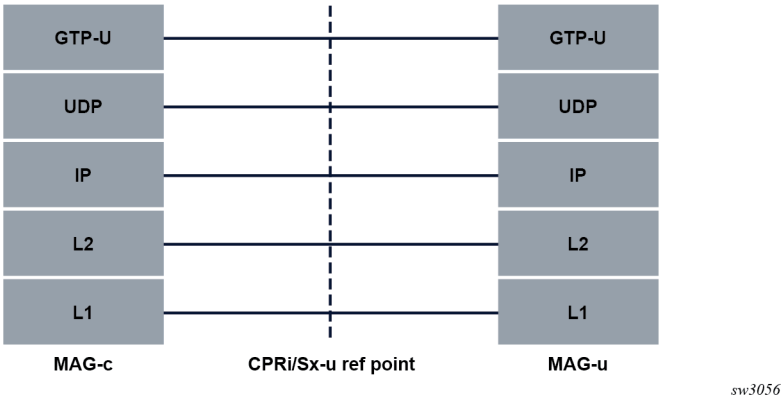
PDR	PDI	FAR
PDR 1 UP to CP	Source Interface = Access Ethernet Packet Filter: Ethertype = 0x8863	FAR 1 Action = forward Forwarding Parameters: Destination Interface = CP-Function Outer Header Creation = GTP-U/UDP/IPv4, TEID 1000, IPv4 Address 203.0.113.1 BBF Outer Header Creation = CPR-NSH

3.3 GTP-U encapsulation and decapsulation

The MAG-u encapsulates a received control plane packet from the access side in a GTP-U tunnel, using the TEIDs as signaled during the PFCP session setup procedure. The MAG-u passes the received Ethernet frame as payload in GTP-U, unmodified (that is, including VLAN tags).

The following figure shows the protocol stack for IBCP over the CPRi interface.

Figure 2: Protocol stack for IBCP



When control plane packets only match the default IBCP session, the MAG-u inserts an NSH header to provide context on the control plane. The NSH header contains the following mandatory fields:

- an opaque logical port; for example, the physical port, also known as the Layer 2 Access ID on the Nokia MAG-c
- the local MAC address on the MAG-u, belonging to the Layer 2 Access ID

The MAG-c sets up a PFCP session using the logical port in the PDR/FAR and uses the MAC address as source MAC when sending control plane messages. Control plane packets matching these dedicated sessions do not use NSH.

See BBF TR-459 for a description of the NSH header and metadata fields.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

4 Session handling

A PFCP session is set up to control the creation, modification, and deletion of a bundle of PDRs. There is a single PFCP session per connected device.

4.1 Overview

PFCP sessions adhere to the following generic scope rules as defined in TS 29.244.

- Identifiers (for example, FAR ID, QER ID, URR ID) are only unique within a session unless explicitly stated otherwise.
- PDRs belonging to different sessions must not have the same PDI matching criteria.

PFCP messages are used to add, update, or delete rules as follows.

- PFCP Session Establishment adds rules.
- PFCP Session Modification can add, modify, and delete specific rules.
- PFCP Session Deletion deletes all rules.

PFCP Session Modification and PFCP Session Report are used to send statistics or other information from the MAG-u to the MAG-c.

4.2 PFCP session example

The following tables describe an example for a dual-stack PPPoE session, with session ID 100, IP anti-spoofing enabled, and single-session per MAC.

The following table describes the reused and top-level IEs, such as Traffic Endpoint IEs, QER IE, URR IE, and LCP PPP Connectivity IE. Table 4: PDR and FARs for an example PPPoE session lists the PDRs with their accompanying PDR and related FAR. FARs are directly in the table for convenience.

Table 3: Top level IEs for an example PPPoE session

IE	Contents
PDN Type	`Ethernet`

Traffic Endpoint 1	`BBF) Logical Port = 1/2/3,`
	`S-TAG = 4,`
	`C-TAG = 5,`
	`MAC address = SOUR-00:00:5E:00:53:01`

Traffic Endpoint 2	`(BBF) Logical Port = 1/2/3,` `S-TAG = 4,`

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

IE	Contents
	C-TAG = 5, MAC address = SOUR-00:00:5E:00:53:01, (BBF) PPPoE Session ID = 100, UE IP Address = 192.0.2.2, 2001:db8:1::/56 (IPv6D=8), 2001:db8:2:1::/64
Traffic Endpoint 3	UE IP Address = 192.0.2.2, 2001:db8:1::/56 (IPv6D=8), 2001:db8:2:1::/64, Network-Instance = 'network'
Traffic Endpoint 4	Local F-TEID = v46, F-TEID CHOOSE
QER 1	QER Correlation ID = 1
URR 1	Measurement Method = VOLUM Reporting Triggers = PERIO Measurement Period = 600 //10m
(BBF) PPP LCP Connectivity	Traffic Endpoint ID = 1 (BBF) PPP LCP Magic Number = 0x12345678 (BBF) Verification Timers = interval 3000, count 3
Nokia UP Aggregate Route	Network-Instance = 'network' Framed-Route = 192.0.2.1/24 Framed-IPv6-Route = 2001:db8:1::/48 Framed-IPv6-Route = 2001:db8:2::/56

Table 4: PDR and FARs for an example PPPoE session

PDR	PDI	FAR

PDR 1 (UP to CP)	Source Interface = Access
	Traffic-Endpoint = 1
	Ethernet Packet Filter: //PADI, PADR
	Ethertype = 0x8863,
	Ethernet Packet Filter: //PPP ctl
	Ethertype = 0x8864,
	(BBF) PPP Protocol = control
	Ethernet Packet Filter: //DHCPv6
	Ethertype = 0x8864,
	(BBF) PPP Protocol = data
	SDF: Permit out 17 from any to any
	547,
	Ethernet Packet Filter: //RS
	Ethertype = 0x8864,
	(BBF) PPP Protocol = data
		FAR 1
		Apply Action = forward
		Forwarding Parameters:
		Destination Interface = CP-Function
		Outer Header Creation = GTP-U/UDP/
		IPv4, TEID 2000, IPv4 203.0.113.1,
		IPv6 2001:db8:1234::1

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

PDR	PDI	FAR
	SDF: Permit out 58 from any to FF02::2	
PDR 2 (CP to UP) Outer Header Removal = GTP/UDP/IPv4	Source Interface = CP Function Traffic-Endpoint = 4	FAR 2 Apply Action = forward Forwarding Parameters: - Destination Interface = Access - Linked Traffic Endpoint ID = 1
PDR 3 (upstream data) BBF Outer Header Removal = PPP/PPPoE/Ethernet QER ID = 1 URR ID = 1 Activate Predefined Rules = 'IPoE-HQoS'	Source-interface = access Traffic Endpoint = 2	FAR 3 Apply Action = forward Forwarding Parameters: - Destination-Interface = SGi-LAN - Network-Instance = 'network'
PDR 4 (downstream data) QER ID = 1 URR ID = 1 Activate Predefined Rules = 'IPoE-HQoS'	Source-interface = SGi-LAN Traffic-Endpoint = 3	FAR 4 Action = forward Forwarding Parameters: - Destination Interface = access - BBF Outer Header Creation = Traffic-Endpoint - BBF Outer Header Creation = Traffic-Endpoint - Linked Traffic Endpoint ID = 2 - (BBF) MTU = 1400

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

5 PFCP protocol

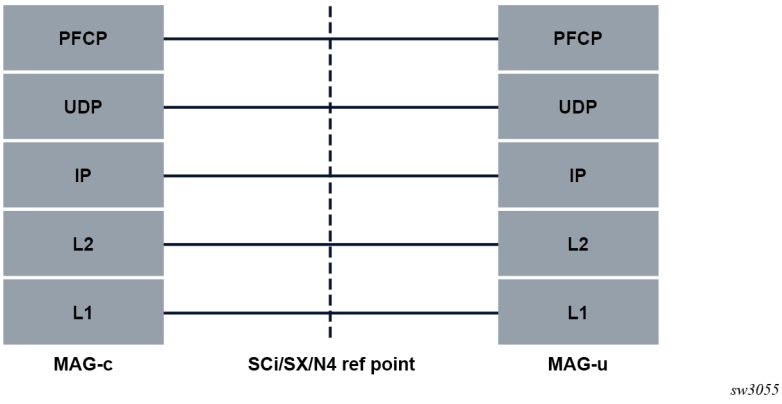
The core of session management is the PFCP protocol as defined in 3GPP TS 29.244, with BNG-specific extensions defined in BBF TR-459.

5.1 Protocol stack

The PFCP protocol runs on top of UDP/IP. The UDP destination port for a request message uses port 8805, which is the registered port number for the PFCP protocol.

The following figure shows the PFCP protocol stack for the control plane.

Figure 3: PFCP protocol stack for the control plane



Note: The maximum supported PFCP message size is 8192 bytes. If the PFCP link MTU size is limited to 1500 bytes, Nokia recommends enabling IP address reassembly.

5.2 Generic PFCP message header

The following table describes the format of the generic PFCP message header.

Table 5: Generic PFCP message header

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	Version			Spare	Spare	Spare	MP	S
2	Message Type							
3	Message Length (1st Octet)							

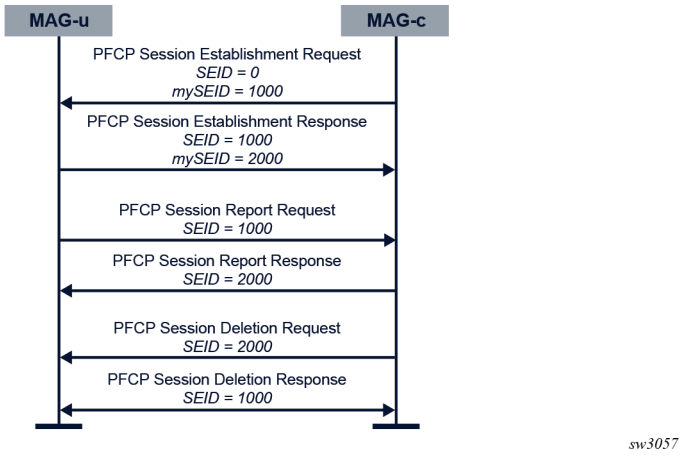
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
4	Message Length (2nd Octet)							
m to (m+7)	If S=1, octets 5 to 12 contain the SEID If S=0, the SEID field is not present							
n to (n+2)	Sequence Number							
n+3	Message Priority				Spare			

The following clarifies the fields in the message header.

- MP indicates whether the Message Priority field is set. The Message Priority field is only set for messages related to a PFCP session.
- S indicates whether the SEID field is present. Messages related to a PFCP session always contain a session ID.
- Message Type indicates the type of the message and determines the content of the message beyond the header.
- Message Length is the total length of the packet.
- SEID is the session ID. When the session ID is not known (for example, for the first message in a session), the session ID is set to 0. During PFCP session establishment, both the MAG-u and the MAG-c allocate an SEID and signal their SEID to the other peer. Any subsequent message must use the SEID of the peer in the message header. See Figure 4: PFCP session ID allocation and use for an example of SEID allocation and use.
- Sequence Number is used to detect retransmission of PFCP packets.
- Message Priority defines a relative strict priority for the message processing. See TS 29.244 for more information.

Figure 4: PFCP session ID allocation and use



© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

5.3 PFCP messages overview

Table 6: PFCP messages overview

Message	Description
PFCP Association Setup Request	The MAG-u or the MAG-c starts a PFCP association. Feature capabilities and node-wide parameters are exchanged.
PFCP Association Setup Response	The MAG-u or the MAG-c confirms the PFCP association.
PFCP Association Update Request	The MAG-u or the MAG-c updates feature capabilities or node-wide parameters. The MAG-u can request the MAG-c to gracefully tear down the PFCP association.
PFCP Association Update Response	The MAG-u or the MAG-c confirms the update.
PFCP Association Release Request	The MAG-c tears down the PFCP association.
PFCP Association Release Response	The MAG-u confirms the teardown.
PFCP Heartbeat Request	The MAG-u or the MAG-c checks connectivity.
PFCP Heartbeat Response	The MAG-u or the MAG-c confirms connectivity.
PFCP Session Establishment Request	The MAG-c creates a new PFCP session. The message contains all parameters necessary to correctly create the forwarding state or in-band control plane state.
PFCP Session Establishment Response	The MAG-u confirms the creation of the PFCP session. The message contains the value of related MAG-u parameters, such as the SEID.
PFCP Session Modification Request	The MAG-c updates parameters of a PFCP session or requests an update of the usage information (counters).
PFCP Session Modification Response	The MAG-u confirms the modification. The message can contain updated related MAG-u parameters or usage information (counters) or both.
PFCP Session Deletion Request	The MAG-c removes a PFCP session and its related state information. Possible reasons for removal include the following. • The subscriber session triggers removal (DHCP release or PADT). • The AAA service triggers removal (RADIUS Disconnect).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Message	Description
	• The operator triggers removal for administrative purposes (clear command).
PFCP Session Deletion Response	The MAG-u confirms the removal. The message includes a final usage update (counters).
PFCP Session Report Request	The MAG-u notifies the MAG-c of usage information updates (counters) or other state changes (for example, LCP keep-alive failures).
PFCP Session Report Response	The MAG-c confirms receipt of the report.

5.4 Example call flows

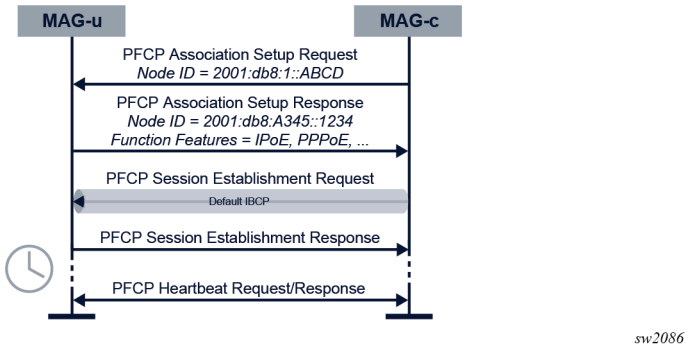
Get a description of call flow examples, including PFCP association and session setup, CoA handling, MAG-c triggered updates, and PFCP connectivity failure.

5.4.1 Initial PFCP association and session setup

When either a MAG-c or a MAG-u comes online, it sets up a PFCP association. The association request can be triggered either from the MAG-u or from the MAG-c.

The following figure shows the initial PFCP association and session setup.

Figure 5: Initial PFCP association and session setup



Description of the call flow

1. The MAG-c initializes the PFCP association setup and the MAG-u responds. During the association setup, both the MAG-u and the MAG-c exchange parameters.
2. The MAG-c immediately initializes the MAG-u with PDRs for the forwarding of initial in-band control plane packets using the PFCP session establishment procedure. For more information, see Default IBCP session.
3. To monitor connectivity, periodic heartbeat messages are exchanged between the MAG-u and the MAG-c.

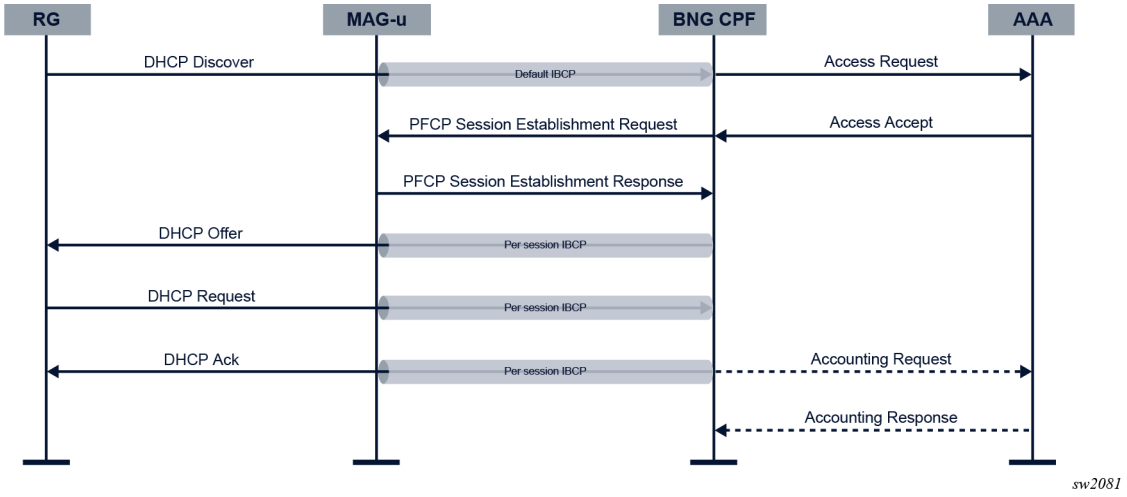
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

5.4.2 IPoE session setup

When the MAG-u receives a DHCP Discover message from an RG, it forwards the message to the MAG-c over the CPRi interface. The MAG-c initiates the setup of the IPoE session.

The following figure shows the IPoE session setup.

Figure 6: IPoE session setup



Prerequisites

- The MAG-u has a PFCP association with the MAG-c.
- The MAG-c initialized the MAG-u with PDRs for the forwarding of control plane packets over the CPRi interface (GTP-U).

Description of the call flow

1. The MAG-u forwards a DHCP Discover packet to the MAG-c over the CPRi interface (GTP-U, default IBCP tunnel).
2. The MAG-c authorizes the IPoE session based on parameters in the DHCP message.
3. The MAG-c initializes the PFCP session and creates data plane rules and per-session IBCP tunnels on the MAG-u (PFCP session establishment procedure).
4. The MAG-c sends a DHCP Offer over the CPRi interface (GTP-U, per- session IBCP tunnel) to the MAG-u. The MAG-u decapsulates the DHCP packet and sends the packet to the RG.
5. The MAG-u forwards the DHCP Request packet to the MAG-c over the CPRi interface (GTP-U, per-session IBCP tunnel).
6. The MAG-c sends the DHCP Ack over the CPRi interface (GTP-U, per- session IBCP tunnel) to the MAG-u. The MAG-u decapsulates the DHCP packet and sends the packet to the RG.
7. If accounting is provisioned, the MAG-c starts accounting for the session.

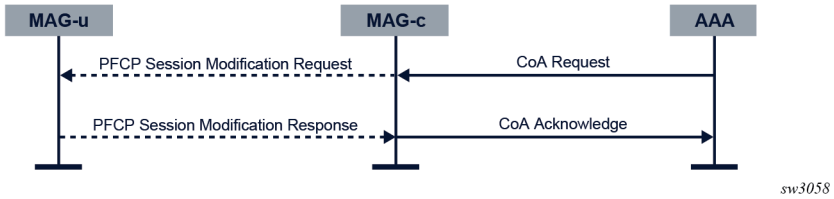
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

5.4.3 CoA handling

When the RADIUS server requests a change in client authorization for an active session, the MAG-c triggers the MAG-u with the needed modifications.

The following figure shows the call flow process.

Figure 7: CoA handling



Description of the call flow

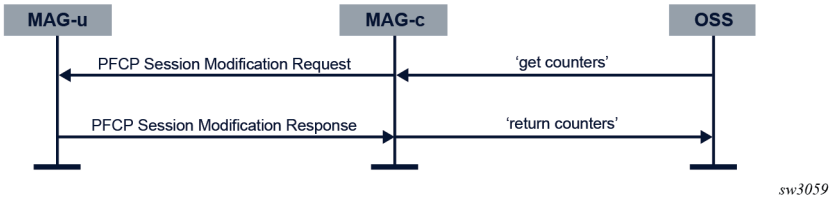
1. The AAA server sends a CoA request directly to the MAG-c.
2. The MAG-c processes the message and translates it to the necessary MAG-u state changes. The state changes are signaled via a PFCP session modification procedure.
   If the MAG-c determines that no MAG-u changes are required, the PFCP session modification procedure is skipped.
3. The MAG-c sends the CoA Ack to the AAA server.

5.4.4 MAG-c triggered updates

To perform specific tasks, the OSS may send a trigger to the MAG-c. An example of a specific task is getting up-to-date forwarding statistics for a specific subscriber session.

The following figure shows a MAG-c triggered accounting update.

Figure 8: MAG-c triggered accounting update



Description of the call flow

1. The OSS requests up-to-date forwarding statistics from the MAG-c.
2. The MAG-c processes the message and sends a PFCP Session Modification Request to the MAG-u. The request contains the Query URR IE.
3. The MAG-u sends the requested report in a PFCP Session Modification Response.
4. The MAG-c sends up-to-date forwarding statistics to the OSS.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

5.4.5 PFCP connectivity failure and headless mode

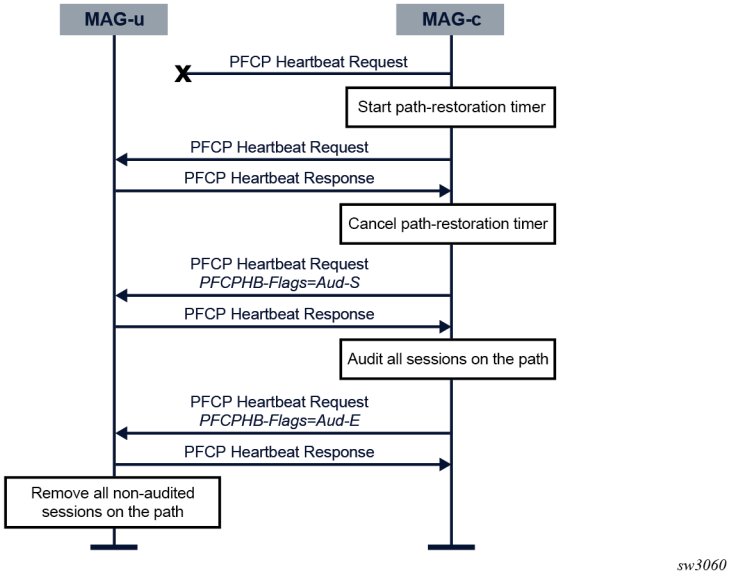
PFCP heartbeat messages check the connectivity of a PFCP path. When the heartbeat procedure fails, all state information for the corresponding path is removed and all sessions using that path are terminated. The association remains in place.

To protect against temporary failures, the MAG-c and the MAG-u support a headless mode. When headless mode is enabled, the sessions are not removed when there is a heartbeat failure. Instead, a configured timer is started and heartbeats continue to be sent.

The following figure shows an example call flow of the heartbeat procedure with headless mode in case of a PFCP connectivity failure. In the example call flow, the path is restored and a PFCP audit procedure is started.

For more information, see *MAG-c Control Plane Function Guide*, section *PFCP connectivity failure*.

Figure 9: Example headless mode call flow



Description of the call flow

1. The MAG-c discovers a connectivity failure on the PFCP path and starts the path-restoration timer.
2. The MAG-c and the MAG-u exchange heartbeat messages successfully before the path-restoration timer period ends.
3. The MAG-c signals the start of an audit to the MAG-u.
4. The MAG-u acknowledges the start of the audit. The MAG-c audits all known sessions on the path.
5. The MAG-c signals the end of the audit to the MAG-u.
6. The MAG-u acknowledges the end of the audit and removes all non-audited sessions on the path.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

6 PFCP messages

Get a description of the PFCP messages that are applicable for the MAG-c.

Table 7: Message types defines which PFCP messages are applicable for the MAG-c.

The applicability of the messages and the applicability of the information elements that are defined in 3GPP TS 29.244 remain as specified in 3GPP TS 29.244.

Information elements that are added and defined by BBF in TR-459 are prefixed with (BBF) in the tables of this chapter. However, their name does not include the (BBF) prefix.

Vendor-specific information elements are prefixed with Nokia. Their name includes the Nokia prefix.

For the applicable messages, only the IEs used by the MAG-c are listed in the tables. .

Note: The abbreviations listed in the P (Presence) column in the tables in this section represent the following:

- M = Mandatory
- C = Conditional
- O = Optional

6.1 Message types

Table 7: Message types

Message type value (decimal)	Message	Applicability MAG-c
0	Reserved	
	PFCP node-related messages	
1	PFCP Heartbeat Request	✓
2	PFCP Heartbeat Response	✓
5	PFCP Association Setup Request	✓
6	PFCP Association Setup Response	✓
7	PFCP Association Update Request	✓
8	PFCP Association Update Response	✓
9	PFCP Association Release Request (see TS 29.244)	✓
10	PFCP Association Release Response (see TS 29.244)	✓
12	PFCP Node Report Request (see TS 29.244)	✓
13	PFCP Node Report Response (see TS 29.244)	✓

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Message type value (decimal)	Message	Applicability MAG-c
16 to 49	For future use	
	PFCP session-related messages	
50	PFCP Session Establishment Request	✓
51	PFCP Session Establishment Response	✓
52	PFCP Session Modification Request	✓
53	PFCP Session Modification Response	✓
54	PFCP Session Deletion Request	✓
55	PFCP Session Deletion Response	✓
56	PFCP Session Report Request	✓
57	PFCP Session Report Response	✓
58 to 99	For future use	
	Other messages	
100 to 255	For future use	

6.2 PFCP node-related messages

6.2.1 PFCP association messages

6.2.1.1 PFCP Association Setup Request

The PFCP Association Setup Request message can be initiated either from the MAG-c or from the MAG-u.

Table 8: IEs in a PFCP Association Setup Request

Information elements	P	Description
Node ID	M	This IE contains the unique identifier of the sending node.
Recovery Time Stamp	M	This IE contains the time stamp when the node was started. This IE is ignored on the SCi interface.
UP Function Features	C	This IE is present if the MAG-u sends the message and supports at least one UP feature defined in this IE. When present, this IE indicates the features that the MAG-u supports.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Information elements	P	Description
CP Function Features	C	This IE is present if the MAG-c sends the message and supports at least one CP feature defined in this IE. When present, this IE indicates the features that the MAG-c supports.
(BBF) BBF UP Function Features	C	This IE is present if the MAG-u sends the message and supports at least one BBF UP feature defined in this IE. When present, this IE indicates the BBF features that the MAG-u supports.
Nokia UP Function Features See Table 56: Nokia UP Function Features IE	C	This IE is present if the MAG-u sends the message and supports at least one Nokia UP feature defined in this IE. When present, this IE indicates the Nokia-specific features that the MAG-u supports.
Nokia NAT ISA members See Table 60: Nokia NAT ISA Members IE	C	This IE is present if the MAG-u sends the message and the Nokia UP Function Features IE indicates NAT support. When present, this IE includes the number of ISA members on the NAT group. When not present, the number of ISA members on the NAT group is assumed to be 1.

6.2.1.2 PFCP Association Setup Response

Table 9: IEs in a PFCP Association Setup Response

Information elements	P	Description
Node ID	M	This IE contains the unique identifier of the sending node.
Cause	M	This IE indicates the acceptance or the rejection of the corresponding request message.
Recovery Time Stamp	M	This IE contains the time stamp when the node was started. This IE is ignored on the SCi interface.
UP Function Features	C	This IE is present if the MAG-u sends the message and supports at least one UP feature defined in this IE. When present, this IE indicates the features that the MAG-u supports.
CP Function Features	C	This IE is present if the MAG-c sends the message and supports at least one CP feature defined in this IE. When present, this IE indicates the features that the MAG-c supports.
(BBF) BBF UP Function Features	C	This IE is present if the MAG-u sends the message and supports at least one BBF UP feature defined in this IE.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Information elements	P	Description
		When present, this IE indicates the BBF features that the MAG-u supports.
Nokia UP Function Features See Table 56: Nokia UP Function Features IE	C	This IE is present if the MAG-u sends the message and supports at least one Nokia UP feature defined in this IE. When present, this IE indicates the Nokia-specific features that the MAG-u supports.
Nokia NAT ISA members See Table 60: Nokia NAT ISA Members IE	C	This IE is present if the MAG-u sends the message and the Nokia UP Function Features IE indicates NAT support. When present, this IE includes the number of ISA members on the NAT group. When not present, the number of ISA members on the NAT group is assumed to be 1.

6.2.1.3 PFCP Association Update Request

The PFCP Association Update Request message can be initiated either from the MAG-c or from the MAG-u.

Table 10: IEs in a PFCP Association Update Request

Information elements	P	Description
Node ID	M	This IE contains the unique identifier of the sending node.
UP Function Features	O	This IE may be present if the MAG-u sends the message and supports at least one UP feature defined in this IE. When present, this IE indicates the features that the MAG-u supports.
CP Function Features	O	This IE may be present if the MAG-c sends the message and supports at least one CP feature defined in this IE. When present, this IE indicates the features that the MAG-c supports.
PFCP Association Release Request	C	This IE is present if the MAG-u requests the MAG-c to release the PFCP association.
Graceful Release Period	C	This IE is present if the MAG-u requests a graceful release of the PFCP association.
(BBF) BBF UP Function Features	C	This IE is present if the MAG-u sends the message and supports at least one BBF UP feature defined in this IE. When present, this IE indicates the BBF features that the MAG-u supports.
Nokia UP Function Features See Table 56: Nokia UP Function Features IE	C	This IE is present if the MAG-u sends the message and supports at least one Nokia UP feature defined in this IE.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Information elements	P	Description
		When present, this IE indicates the Nokia-specific features that the MAG-u supports.
Nokia NAT ISA members See Table 60: Nokia NAT ISA Members IE	C	This IE is present if the MAG-u sends the message and the Nokia UP Function Features IE indicates NAT support. When present, this IE includes the number of ISA members on the NAT group. When not present, the number of ISA members on the NAT group is assumed to be 1.

6.2.1.4 PFCP Association Update Response

Table 11: IEs in a PFCP Association Update Response

Information elements	P	Description
Node ID	M	This IE contains the unique identifier of the sending node.
Cause	M	This IE indicates the acceptance or the rejection of the corresponding request message.
UP Function Features	O	This IE may be present if the MAG-u sends the message and supports at least one UP feature defined in this IE. When present, this IE indicates the features that the MAG-u supports.
CP Function Features	O	This IE may be present if the MAG-c sends the message and supports at least one CP feature defined in this IE. When present, this IE indicates the features that the MAG-c supports.
(BBF) BBF UP Function Features	C	This IE is present if the MAG-u sends the message and supports at least one BBF UP feature defined in this IE. When present, this IE indicates the BBF features that the MAG-u supports.
Nokia UP Function Features See Table 56: Nokia UP Function Features IE	C	This IE is present if the MAG-u sends the message and supports at least one Nokia UP feature defined in this IE. When present, this IE indicates the Nokia-specific features that the MAG-u supports.
Nokia NAT ISA members See Table 60: Nokia NAT ISA Members IE	C	This IE is present if the MAG-u sends the message and the Nokia UP Function Features IE indicates NAT support. When present, this IE includes the number of ISA members on the NAT group. When not present, the number of ISA members on the NAT group is assumed to be 1.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

6.2.2 Heartbeat messages

6.2.2.1 PFCP Heartbeat Request

Table 12: IEs in a PFCP Heartbeat Request

Information elements	P	Description
Recovery Time Stamp	M	This IE contains the time stamp when the node was started.
Nokia PFCPHB-Flags See Table 57: Nokia PFCPHB-Flags IE	C	The MAG-u includes this IE to trigger an audit request. The MAG-c includes this IE to signal the start or the end of an audit.

6.2.2.2 PFCP Heartbeat Response

Table 13: IEs in a PFCP Heartbeat Response

Information elements	P	Description
Recovery Time Stamp	M	This IE contains the time stamp when the node was started.

6.3 PFCP session-related messages

6.3.1 PFCP Session Establishment Request

The PFCP Session Establishment Request message is initiated from the MAG-c function to create a new PFCP session on the MAG-u.

Table 14: IEs in a PFCP Session Establishment Request

Information elements	P	Description
Node ID	M	This IE contains the unique identifier of the sending node.
F-SEID	M	This IE uniquely identifies the session. The ID is allocated by the MAG-c.
Create PDR See Table 15: Create PDR IE	M	This IE includes a PDR to be associated with the PFCP session. Several IEs with this IE type may be present to represent a list of PDRs to create.
Create FAR See Table 18: Create FAR IE	M	This IE includes one or more FARs to be associated with the PFCP session.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Information elements	P	Description
Create URR See Table 20: Create URR IE	C	This IE is present if a measurement action is applied to packets matching one or more PDRs of this PFCP session. Only one Create URR IE may be present on the SCi interface.
Create QER See Table 21: Create QER IE	C	This IE is present if a QoS enforcement action is applied to packets matching one or more PDRs of this PFCP session. Only one Create QER IE may be present on the SCi interface.
Create Traffic Endpoint See Table 22: Create Traffic Endpoint IE	C	When present, this IE contains the information associated with the traffic endpoint to be created.
PDN Type	C	This IE is present if the PFCP session is set up for an individual PDN connection or a PDU session. For SCi sessions, this must be Ethernet. For default IBCP sessions, this IE must not be present.
(BBF) PPP LCP connectivity	C	This IE is present if periodic LCP echo hello is required.
Nokia UP Aggregate Route See Table 24: Nokia UP Aggregate Route IE	C	This IE is present if any aggregate routes need to be installed on the MAG-u.
Nokia SAP Template See Table 49: Nokia SAP Template IE	C	This IE is present if a specific SAP template needs to be used to construct SAP structures on the MAG-u.
Nokia Group Interface Template See Table 50: Nokia Group Interface Template IE	C	This IE is present if a specific group interface template needs to be used to construct group interface structures on an SR OS MAG-u.
Nokia Create Filter Override See Table 52: Nokia Create Filter Override IE	C	This IE is present if a Nokia-specific filter needs to be installed. This is signaled as out of scope of any PDR or FAR because Nokia filters are installed per session.
Nokia Intermediate Destination See Table 54: Nokia Intermediate Destination IE	C	This IE is present if an intermediate destination identifier (for example, access line ID) needs to be signaled to the MAG-u. This is signaled as out of scope of any PDR or FAR because this can apply to both QoS (for example, vport) and access identification (for example, mc-ring).
Nokia State ID See Table 59: Nokia State ID IE	C	This IE is present if the MAG-u indicated support for the bulk audit feature. It must be stored unmodified by the MAG-u.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

6.3.1.1 Create PDR IE

Table 15: Create PDR IE

Octet 1 and 2	Create PDR IE Type = 1 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
PDR ID	M	This IE uniquely identifies the PDR among all the PDRs configured for the PFCP session.
Precedence	M	This IE indicates the precedence of the PDR among all PDRs of the PFCP session. The MAG-u applies the precedence when looking for a PDR matching an incoming packet.
PDI See Table 16: PDI IE	M	This IE specifies the match criteria for incoming packets. It also contains a reference to a traffic endpoint.
Outer Header Removal	C	This IE is present if the MAG-u is required to remove one or more outer headers from the packets matching this PDR.
FAR ID	C	This IE is present if the Activate Predefined Rules IE is not included or if it is included but it does not result in activating a predefined FAR. When present, this IE contains the FAR ID to be associated with the PDR.
QER ID	C	This IE is present if a QoS enforcement action is applied to packets matching the PDR. When present, this IE contains the QER ID to be associated with the PDR.
URR ID	C	This IE is present if a measurement action is applied to packets matching this PDR. When present, this IE contains the URR ID to be associated with the PDR.
Activate Predefined Rules See Nokia format for QoS policy in the Activate Predefined Rules IE	C	This IE is present if predefined rules are activated for the PDR. When present, this IE contains one predefined rules name. Several IEs with the same IE type may be present to represent multiple predefined rules names.
(BBF) BBF Outer Header Removal	C	This IE is present if the MAG-u must remove one or more headers from the packets matching the PDR.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Table 16: PDI IE

Octet 1 and 2	PDI IE Type = 2 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
Source Interface	M	This IE identifies the source interface of the incoming packet.
Traffic Endpoint ID	C	This IE is present if the MAG-u indicated the support of PDI optimization. If present, this IE uniquely identifies the traffic endpoint for the PFCP session.
Ethernet Packet Filter See Table 17: Ethernet Packet Filter IE	O	If present, this IE identifies the Ethernet PDU to match for the incoming packet. Several IEs with the same IE type may be present to provision a list of Ethernet packet filters. When present, the full set of applicable Ethernet packet filters is provided during the creation or modification of the PDI.
SDF Filter	O	If present, this IE identifies the SDF filter to match for the incoming packet. Several IEs with the same IE type may be present to represent a list of SDF filters.

Table 17: Ethernet Packet Filter IE

Octet 1 and 2	Ethernet Packet Filter IE Type = 132 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
Ethernet Filter ID	C	This IE identifies the source interface of the incoming packet.
MAC address	O	If present, this IE identifies the MAC address. The IE may be present up to 16 times.
Ethertype	O	If present, this IE identifies the Ethertype.
C-TAG	O	If present, this IE identifies the Customer-VLAN tag.
S-TAG	O	If present, this IE identifies the Service-VLAN tag.
SDF Filter	O	If packet filtering is required, this IE describes the IP packet filter set for Ethernet frames with Ethertype indicating IPv4 or IPv6 payload. Several IEs with the same IE type may be present to represent a list of SDF filters.
(BBF) PPP Protocol	O	If present, this IE identifies the PPP protocol to match for the incoming packet.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

6.3.1.2 Create FAR IE

Table 18: Create FAR IE

Octet 1 and 2	**Create FAR IE Type = 3 (decimal)**	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
FAR ID	M	This IE uniquely identifies the FAR among all the FARs configured for the PFCP session.
Apply Action	M	This IE indicates the action to apply to the packets.
Forwarding Parameters See Table 19: Forwarding Parameters IE	C	This IE is present if the Apply Action IE requests the packets to be forwarded. For other values of the Apply Action IE, it may be present. When present, this IE contains the forwarding instructions to be applied by the MAG-u when the Apply Action IE requests the packets to be forwarded.

Table 19: Forwarding Parameters IE

Octet 1 and 2	**Forwarding Parameters IE Type = 4 (decimal)**	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
Destination Interface	M	This IE identifies the destination interface of the outgoing packet.
Network Instance	O	When present, this IE identifies the network instance where the outgoing packet is sent to.[2]
Outer Header Creation	C	This IE is present if the MAG-u is required to add one or more outer headers to the outgoing packet. If present, it contains the F-TEID of the remote GTP-U peer when adding a GTP-U/UDP/IP header, or the destination IP address and port number when adding a UDP/IP header.
Linked Traffic Endpoint ID	C	This IE is present if the MAG-u indicated support of the PDI optimization feature. When present, it identifies the traffic endpoint ID allocated for the PFCP session to receive the traffic in the reverse direction.

[2] The following are examples of the need for a Network Instance IE.

- The PGW/TDF UP function supports multiple PDNs with overlapping IP addresses.
- The SGW UP function is connected to PGWs in different IP domains (S5/S8).
- The SGW UP function is connected to eNodeBs in different IP domains.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Octet 1 and 2	Forwarding Parameters IE Type = 4 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
		A BBF Outer Header Creation IE indicating Traffic-Endpoint indicates which fields must be added. In this case, any SRC/DST fields must be reversed before creating the header.
(BBF) BBF Outer Header Creation	C	This IE is present if the MAG-u is required to add one or more outer headers to the outgoing packet.
(BBF) MTU	O	When present, this IE enforces an MTU on outgoing packets. In the case of PPPoE, this may be based on the negotiated MRU value.

6.3.1.3 Create URR IE

Table 20: Create URR IE

Octet 1 and 2	Create URR IE Type = 6 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
URR ID	M	This IE uniquely identifies the URR among all the URRs configured for this PFCP session.
Measurement Method	M	This IE indicates the method for measuring the network resources usage; that is, whether the data volume, duration (time), or combined volume and duration are measured.
Reporting Triggers	M	This IE indicates the triggers for reporting network resources usage to the MAG-c; for example, periodic reporting.
Measurement Period	C	This IE is present if periodic reporting is required. When present, it indicates the period for generating and reporting usage reports.
Measurement Information	C	This IE contains the Measurement of Number of Packets flag. This IE is only included if that flag is set to 1. The Measurement of Number of Packets flag is set to 1 when packet-based measurement applies. For packet-based measurement, the MAG-u reports the number of packets in the uplink direction, the number of packets in the downlink direction, and the total number of packets. The MAG-u sends the packet-based measurements as well as the measurements in bytes, which apply by default.
Nokia Measurement Information	C	This IE is present if any of the flags in this IE are set to 1.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Octet 1 and 2	Create URR IE Type = 6 (decimal)	
Octet 3 and 4	Length = n	
Information elements	**P**	**Condition/Comment**
See Table 55: Nokia Measurement Information IE		

6.3.1.4 Create QER IE

Table 21: Create QER IE

Octet 1 and 2	Create QER IE Type = 7 (decimal)	
Octet 3 and 4	Length = n	
Information elements	**P**	**Condition/Comment**
QER ID	M	This IE uniquely identifies the QER among all the QERs configured for the PFCP session.
QER Correlation ID	C	This IE is present if the MAG-u is required to correlate the QERs of several PFCP sessions. For the SCi interface, this IE is used to encode a subscriber ID.
Gate Status	M	This IE indicates whether the packets are allowed to be forwarded (the gate is open) or discarded (the gate is closed) in the uplink and, or downlink directions.
Nokia QoS Override See Table 51: Nokia QoS Override IE	C	This IE is present if a Nokia-specific QoS override is required. Multiple IEs may be present in case multiple overrides are required.

6.3.1.5 Create Traffic Endpoint IE

Table 22: Create Traffic Endpoint IE

Octet 1 and 2	Create Traffic Endpoint IE Type = 127 (decimal)	
Octet 3 and 4	Length = n	
Information elements	**P**	**Condition/Comment**
Traffic Endpoint ID	M	This IE uniquely identifies the traffic endpoint for the PFCP session.
Local F-TEID	O	If present, this IE identifies the local F-TEID to match for an incoming packet. The MAG-c sets the CHOOSE (CH) bit to 1 if the MAG-u supports the allocation of F-TEID and if the MAG-c requests the MAG-u to assign a local F-TEID to the traffic endpoint.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Octet 1 and 2	Create Traffic Endpoint IE Type = 127 (decimal)	
Octet 3 and 4	Length = n	
Information elements	**P**	**Condition/Comment**
		For the SCi interface, this IE is only valid for IBCP sessions.
Network Instance	O	This IE is present if the MAG-c requests the MAG-u to allocate a UE IP address/prefix. If present, this IE identifies the network instance to match for the incoming packet.
UE IP address	O	If present, this IE identifies the source or destination IP address to match for the incoming packet.
Framed-Route	O	This IE may be present for a DL PDR if the MAG-u indicated support of framed routing (see clause 8.2.5 of 3GPP TS 29.244). When present, this IE describes a framed route. Several IEs with the same IE type may be present to provision a list of framed routes.
Framed-IPv6-Route	O	This IE may be present for a DL PDR if the MAG-u indicated support of framed routing (see clause 8.2.25 of 3GPP TS 29.244). When present, this IE describes a framed IPv6 route. Several IEs with the same IE type may be present to provision a list of framed IPv6 routes.
MAC address	O	If present, this IE identifies the MAC address.
C-TAG	O	If present, this IE identifies the Customer-VLAN tag. The PCP and DEI values are not specified.
S-TAG	O	If present, this IE identifies the Service-VLAN tag. The PCP and DEI values are not specified.
(BBF) Logical Port	O	If present, this IE provides an opaque value obtained from the NSH header to indicate the logical port for the subscriber.
(BBF) PPPoE Session ID	O	If present, this IE identifies the PPPoE session ID of the subscriber.
Nokia L2TP Tunnel Group Assignment ID See Table 74: Nokia L2TP Assignment ID IE	C	A name for the group of L2TP tunnels this session belongs to. It is used to correlate sessions connecting to the same set of LNS servers and to apply server selection and load-balancing. It is also used to assist in operational commands such as state retrieval and debugging.
Nokia L2TP Client Endpoint See Table 69: Nokia L2TP Client Endpoint IE	C	The endpoint IP address to be used by the MAG-u to set up a tunnel. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia L2TP Client Auth ID See Table 71: Nokia L2TP Client Auth ID IE	C	An identifier for the L2TP LAC, sent to the LNS using the L2TP Host Name AVP. This IE requires at least one Nokia L2TP Tunnel IE to be present.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Octet 1 and 2	Create Traffic Endpoint IE Type = 127 (decimal)	
Octet 3 and 4	Length = n	
Information elements	**P**	**Condition/Comment**
Nokia L2TP Server Auth ID See Table 72: Nokia L2TP Server Auth ID IE	C	An identifier for the L2TP LNS. It is compared to the Host Name AVP as received from the LNS in L2TP. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia L2TP Init Rx LCP Conf Request See Table 61: Nokia L2TP Init Rx LCP Conf Request IE	C	Used to proxy PPP negotiated information to the LNS. This IE contains the initial PPP LCP configure request as received by the MAG-c from the PPPoE client. It is sent to the LNS using the L2TP Initial Received LCP CONFREQ AVP. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia L2TP Last Rx LCP Conf Request See Table 63: Nokia L2TP Last Rx LCP Conf Request IE	C	Used to proxy PPP negotiated information to the LNS. This IE contains the last PPP LCP configure request as received by the MAG-c from the PPPoE client. It is sent to the LNS using the L2TP Last Received LCP CONFREQ AVP. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia L2TP Last Tx LCP Conf Request See Table 62: Nokia L2TP Last Tx LCP Conf Request IE	C	Used to proxy PPP negotiated information to the LNS. This IE contains the last PPP LCP configure request as sent by the MAG-c to the PPPoE client. It is sent to the LNS using the L2TP Last Sent LCP CONFREQ AVP. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia L2TP Authentication Type See Table 64: Nokia L2TP Authentication Type IE	C	Used to proxy PPP negotiated information to the LNS. This IE indicates which authentication type (for example, PAP or CHAP) was performed toward the MAG-c. It is sent to the LNS using the Proxy Authen Type AVP. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia L2TP Authentication Name See Table 65: Nokia L2TP Authentication Name IE	C	Used to proxy PPP negotiated information to the LNS. This IE contains the username that was used during authentication toward the MAG-c. It is sent to the LNS using the Proxy Authen Name AVP. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia L2TP Authentication ID See Table 66: Nokia L2TP Authentication ID IE	C	Used to proxy PPP negotiated information to the LNS. This IE contains the authenticator ID used during authentication. It is sent to the LNS using the Proxy Authen ID AVP. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia L2TP Authentication Challenge See Table 67: Nokia L2TP Authentication Challenge IE	C	Used to proxy PPP negotiated information to the LNS. This IE is included if the client performed CHAP authentication and contains the challenge used toward the MAG-c. It is sent to the LNS using the Proxy Authen Challenge AVP. This IE requires at least one Nokia L2TP Tunnel IE to be present.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Octet 1 and 2	Create Traffic Endpoint IE Type = 127 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
Nokia L2TP Authentication Response See Table 68: Nokia L2TP Authentication Response IE	C	Used to proxy PPP negotiated information to the LNS. This IE contains the password or challenge response that was used during authentication toward the MAG-c. It is sent to the LNS using the Proxy Authen Response AVP. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia L2TP Password See Table 73: Nokia L2TP Password IE	C	Indicates that the MAG-u needs to do CHAP based tunnel authentication, using the shared secret in this IE. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia L2TP Private Group ID See Table 75: Nokia L2TP Private Group ID IE	C	An identifier that the LNS can use to correlate sessions of a particular customer group. It is sent to the LNS in the L2TP Private Group ID AVP. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia L2TP Parameters See Table 76: Nokia L2TP Parameters IE	C	L2TP Parameters that are common for all L2TP tunnels. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia Access Line Circuit ID See Table 81: Nokia Access Line Circuit ID IE	C	Circuit ID as learned by the MAG-c, to be reflected in L2TP. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia Access Line Remote ID See Table 82: Nokia Access Line Remote ID IE	C	Remote ID as learned by the MAG-c, to be reflected in L2TP. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia Access Line Parameters See Table 78: Nokia Access Line Parameters IE	C	TR 101 Access Line Characteristics as learned by the MAG-c, to be reflected in L2TP. This IE requires at least one Nokia L2TP Tunnel IE to be present.
Nokia L2TP Tunnel See Table 23: Nokia L2TP Tunnel IE	C	When present, indicates that the MAG-u must initiate an L2TP tunnel to an L2TP LNS and forward the PPP traffic to the LNS. Multiple IEs of this type can be present to indicate a set of tunnels from which the MAG-u can choose. Tunnel selection is subject to MAG-u configuration and a preference as indicated in the L2TP Params IE.

Table 23: Nokia L2TP Tunnel IE

Octet 1 and 2	Nokia L2TP Tunnel IE Type = 32808 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
Nokia L2TP Server Endpoint	M	The endpoint IP address toward which the L2TP tunnel is set up.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Octet 1 and 2	Nokia L2TP Tunnel IE Type = 32808 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
See Table 70: Nokia L2TP Server Endpoint IE		
Nokia L2TP Tunnel Assignment ID See Table 74: Nokia L2TP Assignment ID IE	C	A name for the L2TP tunnel, for operational commands on the MAG-u.
Nokia L2TP Client Endpoint See Table 69: Nokia L2TP Client Endpoint IE	C	In a Create Traffic Endpoint context, indicates the IP address that the MAG-u must use to set up a tunnel. This value has precedence over the same IE on Traffic Endpoint level, if both are present. In a Created Traffic Endpoint context, indicates the IP address that the MAG-u used to set up the tunnel.
Nokia L2TP Client Auth ID See Table 71: Nokia L2TP Client Auth ID IE	C	In a Create Traffic Endpoint context, sent to the LNS using the L2TP Host Name AVP. This value has precedence over the same IE on Traffic Endpoint level, if both are present. In a Created Traffic Endpoint context, indicates the Host Name that the MAG-u used to set up the tunnel.
Nokia L2TP Server Auth ID See Table 72: Nokia L2TP Server Auth ID IE	C	In a Create Traffic Endpoint context, this value is compared to the Host Name AVP as received from the LNS in L2TP. This value has precedence over the same IE on Traffic Endpoint level, if both are present. In a Created Traffic Endpoint context, indicates the Host Name that the LNS sent.
Nokia L2TP Private Group ID See Table 75: Nokia L2TP Private Group ID IE	C	An identifier that the LNS can use to correlate sessions of a customer group. It is sent to the LNS in the L2TP Private Group ID AVP. This value has precedence over the same IE on Traffic Endpoint level, if both are present. This IE may only be present in a Create Traffic Endpoint IE context.
Nokia L2TP Parameters See Table 76: Nokia L2TP Parameters IE	C	L2TP parameters for tunnel setup. Any parameter specified in this IE overrides that parameter's value in the Traffic Endpoint IE, if present. This IE may only be present in a Create Traffic Endpoint IE context.
Nokia L2TP IDs See Table 80: Nokia L2TP IDs IE	C	Identifiers of the created tunnel. This IE contains the remote (LNS) tunnel and session IDs, the local (LAC) tunnel and session IDs, and the CSN. This IE may only be present in a Created Traffic Endpoint IE context.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

6.3.1.6 Nokia UP Aggregate Route IE

Table 24: Nokia UP Aggregate Route IE

Octet 1 and 2	Nokia UP Aggregate Route IE Type = 32774 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
Network Instance	O	If present, this IE identifies the network instance for the IP prefix.
Framed-Route	O	If present, this IE describes an IP prefix assigned to the MAG-u. Optionally, the prefix may contain a /32 address that may be used as a local address on the MAG-u and that must be used to answer ARPs for this session. Several IEs with the same IE type may be present to provision a list of framed routes.
Framed IPv6-Route	O	If present, this IE describes an IPv6 prefix assigned to the MAG-u. Several IEs with the same IE type may be present to provision a list of framed IPv6 routes.

6.3.2 PFCP Session Establishment Response

The PFCP Session Establishment Response message is sent from the MAG-u to the MAG-c as a reply to the PFCP Session Establishment Request.

Table 25: IEs in PFCP Session Establishment Response

Information elements	P	Condition/Comment
Node ID	M	This IE contains the unique identifier of the sending node.
Cause	M	This IE indicates the acceptance or the rejection of the corresponding request message.
Offending IE	C	This IE is included if the rejection is caused by a conditional or a mandatory missing or faulty IE.
UP F-SEID	M	This IE contains the unique identifier allocated by the MAG-u identifying the session.
Failed Rule ID	C	This IE is included if the Cause IE indicates a rejection because of a rule creation failure or a rule modification failure.
Created Traffic Endpoint See Table 22: Create Traffic Endpoint IE	C	This IE is present if the Cause IE is set to success and the MAG-u was requested to allocate a local F-TEID or a UE IP address/prefix in a Create Traffic Endpoint IE. When present, this IE contains the local F-TEID or UE IP address/prefix to be used for this traffic endpoint.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Information elements	P	Condition/Comment
		Several instances of this IE may be present.
Nokia Detailed Error See Table 48: Nokia Detailed Error IE	C	This IE is present if the Cause IE indicates an error.

6.3.2.1 Created Traffic Endpoint IE

Table 26: Created Traffic Endpoint IE

Octet 1 and 2	Created Traffic Endpoint IE Type = 128 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
Traffic Endpoint ID	M	This IE uniquely identifies the traffic endpoint for the PFCP session.
Local F-TEID	C	This IE is present if the MAG-u allocates the F-TEID. When present, this IE contains the local F-TEID to be used for the traffic endpoint.
Nokia L2TP Tunnel See Table 23: Nokia L2TP Tunnel IE	C	When present, indicates that the MAG-u successfully initiated an L2TP connection to this tunnel. Only one IE of this type can be present.

6.3.3 PFCP Session Modification Request

The PFCP Session Modification Request message is initiated from the MAG-c to request the MAG-u to modify the PFCP session.

Table 27: IEs in a PFCP Session Modification Request

Information elements	P	Condition/Comment
CP F-SEID	C	This IE is present if the MAG-c decides to change its F-SEID for the PFCP session. The MAG-u uses the new CP F-SEID for subsequent PFCP session messages related to this PFCP session.
Remove PDR See Table 34: Remove PDR IE (PFCP Session Modification Request)	C	When present, this IE contains the PDR rule that is requested to be removed. Several IEs with this IE type may be present to represent a list of PDRs to remove.
Remove FAR	C	When present, this IE contains the FAR rule that is requested to be removed.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Information elements	P	Condition/Comment
See Table 35: Remove FAR IE (PFCP Session Modification Request)		Several IEs with this IE type may be present to represent a list of FARs to remove.
Remove URR See Table 36: Remove URR IE (PFCP Session Modification Request)	C	When present, this IE contains the URR rule that is requested to be removed.[3]
Remove QER See Table 37: Remove QER IE (PFCP Session Modification Request)	C	When present, this IE contains the QER rule that is requested to be removed. Several IEs with this IE type may be present to represent a list of QERs to remove.
Remove Traffic Endpoint See Table 38: Remove Traffic Endpoint IE (PFCP Session Modification Request)	C	This IE is present if the MAG-u indicated support for PDI optimization and the MAG-c requests to remove a traffic endpoint. When present, this IE contains the traffic endpoint ID of the traffic endpoint to be removed. All PDRs referring to the removed traffic endpoint are deleted as well.
Create PDR	C	This IE is present if the MAG-c requests the MAG-u to create a new PDR. Several IEs with this IE type may be present to represent a list of PDRs to create.
Create FAR	C	This IE is present if the MAG-c requests the MAG-u function to create a new FAR. Several IEs with this IE type may be present to represent a list of FARs to create.
Create URR	C	This IE is present if the MAG-c requests the MAG-u to create a new URR.[3]
Create QER	C	This IE is present if the MAG-c requests the MAG-u to create a new QER.
Create Traffic Endpoint	C	This IE is present if the MAG-u indicated support for PDI optimization and the MAG-c requests the MAG-u to create a new traffic endpoint. When present, this IE contains the information associated with the traffic endpoint to be created.
(BBF) PPP LCP Connectivity	C	This IE is present if periodic LCP echo hello is required.
Update PDR See Table 28: Update PDR IE (PFCP Session Modification Request)	C	This IE is present if a PDR previously created for the PFCP session needs to be modified. Several IEs with this IE type may be present to represent a list of PDRs to update.

[3] Only one URR may be active for a PFCP session.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Information elements	P	Condition/Comment
Update FAR See Table 29: Update FAR IE (PFCP Session Modification Request)	C	This IE is present if a FAR previously created for the PFCP session needs to be modified. Several IEs with this IE type may be present to represent a list of FARs to update.
Update URR See Table 31: Update URR IE (PFCP Session Modification Request)	C	This IE is present if the URR previously created for the PFCP session needs to be modified.[3]
Update QER See Table 32: Update QER IE (PFCP Session Modification Request)	C	This IE is present if QERs previously created for the PFCP session need to be modified. Several IEs with this IE type may be present to represent a list of modified QERs. Previously created QERs that are not modified are not included.
Update Traffic Endpoint See Table 33: Update Traffic Endpoint IE (PFCP Session Modification Request)	C	This IE is present if the MAG-c requests the MAG-u to update a traffic endpoint. When present, this IE contains the information associated with the traffic endpoint to be updated. All the PDRs that point to the traffic endpoint use updated traffic endpoint information.
PFCPSMReq-Flags	C	This IE is included if the QAURR (Query All URRs) flag in this IE is set to 1. The QAURR flag indicates that the MAG-c requests immediate usage reports for the URRs provisioned for this PFCP session.[3, 4]
Query URR See Table 39: Query URR IE (PFCP Session Modification Request)	C	This IE is present if the MAG-c requests immediate usage reports from the MAG-u for the specified URR.[3, 4]
Nokia UP Aggregate Route See Table 24: Nokia UP Aggregate Route IE	C	This IE is present if any aggregate routes need to change. When present, all routes must be included. When absent, no changes to aggregate routes are done.
Nokia SAP Template See Table 49: Nokia SAP Template IE	C	This IE is present if a specific SAP template needs to be used to construct SAP structures on a MAG-u.
Nokia Group Interface Template See Table 50: Nokia Group Interface Template IE	C	This IE is present if a specific group interface template needs to be used to construct group interface structures on a MAG-u.
Nokia Create Filter Override	C	This IE is present if a new override has to be created or an existing override needs to be changed.

4 The QAURR (Query All URRs) flag in the PFCPSMReq-Flags IE and the Query URR IE are mutually exclusive in a PFCP Session Modification Request.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Information elements	P	Condition/Comment
See Table 52: Nokia Create Filter Override IE		Multiple IEs may be present, as long as they indicate distinct filter types and the filter types are not present in the Nokia Delete Filter Override IE.
Nokia Delete Filter Override See Table 53: Nokia Delete Filter Override IE	C	This IE is present if an override has to be removed. Multiple IEs may be present, as long as they indicate distinct filter types and the filter types are not present in the Nokia Create Filter Override IE.
Nokia Intermediate Destination See Table 54: Nokia Intermediate Destination IE	C	This IE is present if the intermediate destination changed.
Nokia State ID See Table 59: Nokia State ID IE	C	This IE is included if the MAG-u indicated support for the bulk audit feature. When present, the MAG-u stores the state unmodified. The state overrides the last signaled value for this session. When not present, the last value is kept.
Nokia PFCPSMReq-Flags See Table 58: Nokia PFCPSMReq-Flags IE	C	This IE is present if any of the flags in the IE is set to 1.

6.3.3.1 Update PDR IE

Table 28: Update PDR IE (PFCP Session Modification Request)

Octet 1 and 2	Update PDR IE Type = 9 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
PDR ID	M	This IE uniquely identifies the PDR among all the PDRs configured for that PFCP session.
Outer Header Removal	C	This IE is present if it needs to be changed.
Precedence	C	This IE is present if there is a change in the precedence of the PDR among all PDRs of the PFCP session. The MAG-u applies the precedence when matching an incoming packet.
PDI	C	This IE is present if there is a change within the PDI against which incoming packets are matched. When present, this IE replaces the PDI previously stored in the MAG-u for this PDR.
FAR ID	C	This IE is present if it needs to be changed.
QER ID	C	This IE is present if a QoS enforcement action is applied or no longer applied to packets matching this PDR.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Octet 1 and 2	Update PDR IE Type = 9 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
		When present, this IE contains the QER ID to be associated with the PDR.
URR ID	C	This IE is present if a measurement action is applied or no longer applied to packets matching this PDR. When present, this IE contains the URR ID to be associated with the PDR.
Activate Predefined Rules	C	This IE is present if a new predefined rule needs to be activated for the PDR. When present, this IE contains one predefined rule name. Several IEs with the same IE type may be present to represent multiple predefined rule names.
Deactivate Predefined Rules	C	This IE is present if a predefined rule needs to be deactivated for the PDR. When present, this IE contains one predefined rule name. Several IEs with the same IE type may be present to represent multiple predefined rule names.
(BBF) BBF Outer Header Removal	C	This IE is present if it needs to be changed. When present, this IE requests the MAG-u to remove one or more headers from the packets matching this PDR.

Note: The IEs that do not need to be modified are not included in the Update PDR IE. The MAG-u continues to behave according to the values previously received for IEs not present in the Update PDR IE.

6.3.3.2 Update FAR IE

Table 29: Update FAR IE (PFCP Session Modification Request)

Octet 1 and 2	Update FAR IE Type = 10 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
FAR ID	M	This IE identifies the FAR to be updated.
Apply Action	C	This IE is present if it is changed.
Update Forwarding Parameters See Table 30: Update Forwarding Parameters IE	C	This IE is present if it is changed.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Table 30: Update Forwarding Parameters IE

Octet 1 and 2	**Update Forwarding Parameters IE Type = 11 (decimal)**	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
Destination Interface	C	This IE is present if it is changed. When present, it indicates the destination interface of the outgoing packet.
Network Instance	C	This IE is present if it is changed.
Outer Header Creation	C	This IE is present if it is changed.
Linked Traffic Endpoint ID	C	This IE is present if it is changed.
(BBF) BBF Outer Header Creation	C	This IE is present if it is changed. When present, the MAG-u is required to add one or more outer headers to the outgoing packet.
(BBF) MTU	O	This IE is present to enforce an MTU on outgoing packets. In the case of PPPoE, the MTU may be based on the negotiated MRU value.

6.3.3.3 Update URR IE

Table 31: Update URR IE (PFCP Session Modification Request)

Octet 1 and 2	**Update URR IE Type = 13 (decimal)**	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
URR ID	M	This IE uniquely identifies the URR among all the URRs configured for the PFCP session.
Measurement Method	C	This IE is present if the measurement method is modified. When present, this IE indicates the method for measuring the network resources usage; that is, whether the data volume, the duration (time), or the combined volume and duration are measured.
Reporting Triggers	C	This IE is present if the reporting triggers are modified. When present, this IE indicates the triggers for reporting network resources usage to the MAG-c; for example, periodic reporting.
Measurement Period	C	This IE is present if the measurement period is modified. When present, it indicates the period for generating and reporting usage reports.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

6.3.3.4 Update QER IE

Table 32: Update QER IE (PFCP Session Modification Request)

Octet 1 and 2	Update QER IE Type = 14 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
QER ID	M	This IE uniquely identifies the QER among all the QERs configured for the PFCP session.
QER Correlation ID	C	This IE is present if the QER correlation ID in this QER needs to be modified.
Gate Status	C	This IE is present if the gate status needs to be modified. When present, it indicates whether the packets are allowed to be forwarded (the gate is open) or discarded (the gate is closed) in the uplink, the downlink, or both directions.
Nokia QoS Override See Table 51: Nokia QoS Override IE	C	This IE is present if changed. When not present, no change is done to previous QoS overrides. When present, any previous QoS overrides are removed and only the new overrides are retained. When an empty IE is present (n = 2), any previous QoS overrides are removed. Only one empty IE of this IE type may be present. Multiple non-empty IEs of this IE type may be present.

6.3.3.5 Update Traffic Endpoint IE

Table 33: Update Traffic Endpoint IE (PFCP Session Modification Request)

Octet 1 and 2	Update Traffic Endpoint IE Type = 129 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
Traffic Endpoint ID	M	This IE uniquely identifies the traffic endpoint for the PFCP session.
Local F-TEID	C	This IE is present if it needs to be changed. When present, this IE identifies the local F-TEID to match for an incoming packet. The MAG-c sets the CHOOSE (CH) bit to 1 if the MAG-u supports the allocation of F-TEID and if the MAG-c requests the MAG-u to assign a local F-TEID to the traffic endpoint.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Octet 1 and 2	Update Traffic Endpoint IE Type = 129 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
		For the SCi interface, this IE is only valid for IBCP sessions.
Network Instance	O	When present, this IE identifies the network instance to match for the incoming packet.
UE IP address	C	This IE is present if it needs to be changed.
Framed-Route	C	This IE is present for a DL PDR if it needs to be changed. When present, this IE describes a framed route. Several IEs with the same IE type may be present to provision a list of framed routes.
Framed-IPv6-Route	C	This IE is present for a DL PDR if it needs to be changed. When present, this IE describes a framed IPv6 route. Several IEs with the same IE type may be present to provision a list of framed IPv6 routes.
MAC address	O	This IE is present if it needs to be changed.
C-TAG	O	This IE is present if it needs to be changed.
S-TAG	O	This IE is present if it needs to be changed.
(BBF) Logical Port	O	This IE is present if it needs to be changed. When present, this IE provides an opaque value obtained from the NSH header to indicate the logical port for the subscriber.
(BBF) PPPoE Session ID	O	This IE is present if it needs to be changed. When present, this IE identifies the PPPoE session ID of the subscriber.

6.3.3.6 Remove PDR IE

Table 34: Remove PDR IE (PFCP Session Modification Request)

Octet 1 and 2	Remove PDR IE Type = 15 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
PDR ID	M	This IE identifies the PDR to be deleted.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

6.3.3.7 Remove FAR IE

Table 35: Remove FAR IE (PFCP Session Modification Request)

Octet 1 and 2	Remove FAR IE Type = 16 (decimal)	
Octet 3 and 4	Length = n	
Information elements	P	Condition/Comment
FAR ID	M	This IE identifies the FAR to be deleted.

6.3.3.8 Remove URR IE

Table 36: Remove URR IE (PFCP Session Modification Request)

Octet 1 and 2	Remove URR IE Type = 17 (decimal)	
Octet 3 and 4	Length = n	
Information elements	P	Condition/Comment
URR ID	M	This IE identifies the URR to be deleted.

6.3.3.9 Remove QER IE

Table 37: Remove QER IE (PFCP Session Modification Request)

Octet 1 and 2	Remove QER IE Type = 18 (decimal)	
Octet 3 and 4	Length = n	
Information elements	P	Condition/Comment
QER ID	M	This IE identifies the QER to be deleted.

6.3.3.10 Remove Traffic Endpoint IE

Table 38: Remove Traffic Endpoint IE (PFCP Session Modification Request)

Octet 1 and 2	Remove Traffic Endpoint IE Type = 130 (decimal)	
Octet 3 and 4	Length = n	
Information elements	P	Condition/Comment
Traffic Endpoint ID	M	This IE identifies the traffic endpoint to be deleted.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

6.3.3.11 Query URR IE

Table 39: Query URR IE (PFCP Session Modification Request)

Octet 1 and 2	Query URR IE Type = 77 (decimal)	
Octet 3 and 4	Length = n	
Information elements	**P**	**Condition/Comment**
URR ID	M	This IE identifies the URR to be queried.

6.3.4 PFCP Session Modification Response

The PFCP Session Modification Response message is sent from the MAG-u to the MAG-c as a reply to the PFCP Session Modification Request message.

Table 40: IEs in a PFCP Session Modification Response

Information elements	P	Condition/Comment
Cause	M	This IE indicates the acceptance or the rejection of the corresponding request message.
Offending IE	C	This IE is included if the rejection is caused by a conditional or mandatory IE that is missing or faulty.
Usage Report See Table 41: Usage Report IE (PFCP Session Modification Response)	C	This IE is present if the Query URR IE was present in the PFCP Session Modification Request and traffic usage measurements for that URR are available at the MAG-u. Several IEs with the same IE type may be present to represent a list of usage reports.
Failed Rule ID	C	This IE is present if the Cause IE indicates a rejection because of a rule creation failure or a rule modification failure.
Created Traffic Endpoint	C	This IE is present if the cause is set to success, traffic endpoints were created, and the MAG-u allocated a local F-TEID for the traffic endpoints. When present, this IE contains the traffic endpoint information associated with the PFCP session.
Updated Traffic Endpoint	C	This IE is present if the cause is set to success, traffic endpoints were updated, and the MAG-u allocated a local F-TEID for the traffic endpoints. When present, this IE contains the traffic endpoint information associated with the PFCP session.
Nokia Detailed Error See Table 48: Nokia Detailed Error IE	C	This IE is present if the Cause IE indicates a failure.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Information elements	P	Condition/Comment
Nokia State ID See Table 59: Nokia State ID IE	C	This IE is present if the MAG-u knows its value.

6.3.4.1 Usage Report IE

Table 41: Usage Report IE (PFCP Session Modification Response)

Octet 1 and 2	Usage Report IE Type = 78 (decimal)	
Octet 3 and 4	**Length = n**	
Information elements	**P**	**Condition/Comment**
URR ID	M	This IE identifies the URR for which usage is reported.
UR-SEQN	M	This IE uniquely identifies the usage report for the URR.
Usage Report Trigger	M	This IE identifies the trigger for this report.
Start Time	C	This IE is always present, except if the Usage Report Trigger IE indicates START (Start of Traffic) or STOPT (Stop of Traffic). When present, this IE provides the timestamp when the collection of the information in this report was started.
End Time	C	This IE is always present, except if the Usage Report Trigger indicates START (Start of Traffic) or STOPT (Stop of Traffic). When present, this IE provides the timestamp when the collection of the information in this report was generated.
Volume Measurement	C	This IE is present if a volume measurement needs to be reported.
UE IP address	O	This IE is present if the start or stop of an application was detected and no UE IP address was provisioned in the PDI. On the SCi interface, this IE is included to indicate any learned addresses for shared prefixes. This IE may only contain IPv6 addresses with IP6PL bit set and prefix-length equal to 128.
Vendor Specific	C	This IE can be any vendor-specific IE related to usage reports.

6.3.5 PFCP Session Deletion Request

The PFCP Session Deletion Request message is initiated from the MAG-c to request the MAG-u to delete the PFCP session. It uses the F-SEID in the PFCP header and does not include any IEs.

6.3.6 PFCP Session Deletion Response

The PFCP Session Deletion Response message is sent from the MAG-u to the MAG-c as a reply to the PFCP Session Deletion Request message.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Table 42: IEs in a PFCP Session Deletion Response

Information elements	P	Condition/Comment
Cause	M	This IE indicates the acceptance or the rejection of the corresponding request message.
Offending IE	C	This IE is included if the rejection is caused by a conditional or mandatory IE that is missing or faulty.
Nokia Detailed Error See Table 48: Nokia Detailed Error IE	C	This IE is included if the Cause IE indicates a failure.

6.3.7 PFCP Session Report Request

The PFCP Session Report Request message is initiated from the MAG-u to the MAG-c to report information related to a PFCP session.

Table 43: IEs in a PFCP Session Report Request

Information elements	P	Condition/Comment
Report Type	M	This IE indicates the type of the report.
Usage Report	C	This IE is present if the Report Type IE indicates a usage report. Several IEs with the same IE type may be present to represent a list of usage reports.
Nokia State ID See Table 59: Nokia State ID IE	C	This IE is present if the MAG-u knows its value.

6.3.8 PFCP Session Report Response

The PFCP Session Report Response message is sent from the MAG-c to the MAG-u as a reply to the PFCP Session Report Request.

Table 44: IEs in a PFCP Session Report Response

Information elements	P	Condition/Comment
Cause	M	This IE indicates the acceptance or the rejection of the corresponding request message.
Offending IE	C	This IE is included if the rejection is caused by a conditional or mandatory IE that is missing or faulty.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

7 Nokia-specific information elements

Get a description of the new and modified vendor-specific information elements required for the MAG-c.

7.1 Format of the information elements

A PFCP message may contain several IEs with support for TLV coded PFCP IEs and PFCP grouped IEs.

Table 45: IE format

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = xxx (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID							
7 to (n+4)	IE-specific data or content of a grouped IE							

An IE has the following fields.

- **Type**
  This field is mandatory and indicates the type of the information element. IE type values within the range of 0 to 32767 are reserved for IEs defined by 3GPP. IE type values within the range of 32768 to 65535 are used for vendor-specific IEs. The vendor controls the value allocation of vendor-specific IEs.
- **Length**
  This field is mandatory and contains the length of the IE excluding the first four octets, which are common for all IEs (type and length). Bit 8 of the lowest numbered octet is the most significant bit and bit 1 of the highest numbered octet is the least significant bit.
- **Enterprise ID**
  This field is optional. If the IE type value is within the range of 32768 to 65535, this field contains the IANA-assigned SMI Network Management Private Enterprise Codes value of the vendor defining the IE.

The following table describes the format of a 3GPP-defined IE. The range of the IE type is 0 to 32767.

Table 46: 3GPP IE format

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = xxx (decimal)							
3 to 4	Length = n							
5 to (n+4)	IE-specific data or content of a grouped IE							

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

The following table describes the format of a vendor-specific IE. The range of the IE type is 32768 to 65535.

Table 47: Vendor-specific IE format

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = xxx (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID							
7 to (n+4)	IE-specific data or content of a grouped IE							

Note: If the last field of an IE contains the statement “Present only if explicitly specified”, the IE can be extended in a later version.

7.2 Nokia Detailed Error IE

Table 48: Nokia Detailed Error IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32779 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to (n+4)	Detailed Error							

The MAG-u sends this IE in response messages to the MAG-c when the Cause IE does not indicate success. The IE contains detailed error information in addition to the generic error indicated by the Cause IE.

The Detailed Error field is encoded as a printable ASCII string without zero-byte termination. The string length is derived from the IE length.

7.3 Nokia SAP Template IE

Table 49: Nokia SAP Template IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32775 (decimal)							

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to (n+4)	SAP Template							

The MAG-c sends this IE to the MAG-u to indicate a SAP template. The MAG-u uses the SAP template to construct a new internal SAP structure for the creation of a forwarding state.

The SAP Template field is encoded as a printable ASCII string without zero-byte termination. The string length is derived from the IE length.

7.4 Nokia Group Interface Template

Table 50: Nokia Group Interface Template IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32776 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to (n+4)	Group Interface Template							

The MAG-c sends this IE to the MAG-u to indicate the group interface template that needs to be used to create a forwarding state on the MAG-u.

The Group Interface Template field is encoded as a printable ASCII string without zero-byte termination. The string length is derived from the IE length.

7.5 Nokia QoS Override IE

Table 51: Nokia QoS Override IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32780 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to (n+4)	QoS-Overrides							

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

The QoS-Overrides field is encoded as described in the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide* for the VSA Alc-Subscriber-QoS-Override.

7.6 Nokia Create Filter Override

Table 52: Nokia Create Filter Override IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32788 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7	Filter Type							
8 to (n+4)	Filter Override							

The type of the Filter Type field is an enumeration of the following values:

- 0: ingress IPv4 filter
- 1: egress IPv4 filter
- 2: ingress IPv6 filter
- 3: egress IPv6 filter

If n = 3, the Filter Override field is not present. All filtering for the specified filter type is disabled.

If n > 3, the Filter Override field contains a filter name.

7.7 Nokia Delete Filter Override IE

Table 53: Nokia Delete Filter Override IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32789 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7	Filter Type							
8 to (n+4)	Present only if explicitly specified							

The type of the Filter Type field is the same enumeration as defined for the Nokia Create Filter Override IE.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

This IE indicates that the filter override needs to be removed. The system falls back to the default filters configured for the session. This differs from an absent Filter Override field in the Nokia Create Filter Override IE (see Nokia Create Filter Override). The absent Filter Override field in the Nokia Create Filter Override IE explicitly disables all filtering, including the default filters.

7.8 Nokia Intermediate Destination IE

Table 54: Nokia Intermediate Destination IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32790 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to (n+4)	Intermediate Destination							

The Intermediate Destination field is encoded as described in the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide* for VSA Alc-Int-Dest-Id-Str.

7.9 Nokia Measurement Information IE

Table 55: Nokia Measurement Information IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32781 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7	Spare							DET
8 to (n+4)	Present only if explicitly specified							

This IE is an extension to the 3GPP Measurement Information IE. It defines how measurements are reported. The following additional bit is defined:

DET (7/1): includes detailed per queue and policer statistics in usage reports related to the URR for which this is signaled.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

7.10 Nokia UP Function Features IE

Table 56: Nokia UP Function Features IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32787 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7	Nokia-supported features							
8 to (n+4)	Present only if explicitly specified							

The MAG-u sends this IE to indicate the support for vendor-specific functions that are not available on each version of the Nokia MAG-u.

The following Nokia UP function features are defined.

- **Bulk (7/1)**
  The MAG-u supports the bulk audit feature.
- **NAT (7/2)**
  The MAG-u supports Nokia-specific extensions to subscriber-aware NAT.
- **LAC (7/3)**
  The MAG-u supports the Nokia LAC implementation where the UP is responsible for L2TP control plane signaling.
- **SSSG (7/3)**
  The MAG-u supports shared subscriber subnet signaling (SSSG) with each session to announce in routing.

7.11 Nokia PFCPHB-Flags IE

Table 57: Nokia PFCPHB-Flags IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32797 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7	Spare					Aud-E	Aud-S	Aud-R
8 to (n+4)	Present only if explicitly specified							

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

The audit flags indicate the following.

- **Aud-R**
  The MAG-u sends this flag to the MAG-c to indicate a mass audit request on this path. This flag may only be set if the MAG-c indicated support for the bulk audit feature.
- **Aud-S**
  The MAG-c sends this flag to the MAG-u to indicate the start of mass audit on this path. This flag may only be set if the MAG-u indicated support for the bulk audit feature.
- **Aud-E**
  The MAG-c sends this flag to the MAG-u to indicate the end of mass audit on this path. This flag may only be set if the MAG-u indicated support for the bulk audit feature.

7.12 Nokia PFCPSMReq-Flags IE

Table 58: Nokia PFCPSMReq-Flags IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32783 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7	Spare							Abs
8 to (n+4)	Present only if explicitly specified							

The Abs flag field indicates that the modification is absolute and not relative. Any rules or traffic endpoints that were not explicitly created in this message must be deleted. This flag may only be set if the MAG-u indicated support for the bulk audit feature.

7.13 Nokia State ID IE

Table 59: Nokia State ID IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32777 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to (n+4)	State							

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

The State field is an opaque value that is not interpreted by the MAG-u but reflected as-is, in PFCP Session Modification Response and PFCP Session Report Request messages.

7.14 Nokia NAT ISA Members IE

Table 60: Nokia NAT ISA Members IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32791 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7	Number of ISA members							
8 to (n+4)	Present only if explicitly specified							

The MAG-u sends this IE to indicate the number of ISA members in a NAT group. When not signaled, the Nokia MAG-c assumes the number to be 1.

7.15 Nokia format for QoS policy in the Activate Predefined Rules IE

To create BNG QoS profiles, Nokia formats the Activate Predefined Rules IE as follows:

```
qos_policy ::= (profile-name ':' value ';')+
```

where **profile-name** is **slaprof** or **subprof**. Each **profile-name** can occur at most one time.

- **slaprof**
  This is an SLA profile as directly defined on the MAG-u. No string-to-profile mappings are used.
- **subprof**
  This is a subscriber profile as directly defined on the MAG-u. No string-to-profile mappings are used.

7.16 Nokia L2TP Init Rx LCP Conf Request IE

Table 61: Nokia L2TP Init Rx LCP Conf Request IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32800 (decimal)							
3 to 4	Length = n							

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
5 to 6	Enterprise ID = 3729							
7 to n+4	LCP Configure Request message							

This IE includes the first LCP Configure Request Message received by a LAC MAG-c. It is used to proxy to an LNS.

This IE is used to proxy PPP setup parameters from a LAC MAG-c to an LNS. For more details, see RFC 1661, section 4.4.5.

7.17 Nokia L2TP Last Tx LCP Conf Request IE

Table 62: Nokia L2TP Last Tx LCP Conf Request IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32801 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to n+4	LCP Configure Request message							

This IE includes the last LCP Configure Request Message received by a LAC MAG-c. It is used to proxy to an LNS.

This IE is used to proxy PPP setup parameters from a LAC MAG-c to an LNS. For more details, see RFC 1661, section 4.4.5.

7.18 Nokia L2TP Last Rx LCP Conf Request IE

Table 63: Nokia L2TP Last Rx LCP Conf Request IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32802 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to n+4	LCP Configure Request message							

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

This IE includes the last LCP Configure Request Message received by a LAC MAG-c. It is used to proxy to an LNS.

This IE is used to proxy PPP setup parameters from a LAC MAG-c to an LNS. For more details, see RFC 1661, section 4.4.5.

7.19 Nokia L2TP Authentication Type IE

Table 64: Nokia L2TP Authentication Type IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32803 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7	Authentication Type							
8 to n+4	Present only if explicitly specified							

This IE indicates which authentication method was used between the LAC MAG-c and the PPPoE client. The type of the Authentication Type field is an enumeration of the following values:

- 0: CHAP
- 1: PAP

This IE is used to proxy PPP setup parameters from a LAC MAG-c to an LNS. For more details, see RFC 1661, section 4.4.5.

7.20 Nokia L2TP Authentication Name IE

Table 65: Nokia L2TP Authentication Name IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32804 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to n+4	Username							

This IE includes the username used during authentication between the LAC MAG-c and the PPPoE Client.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

This IE is used to proxy PPP setup parameters from a LAC MAG-c to an LNS. For more details, see RFC 1661, section 4.4.5.

7.21 Nokia L2TP Authentication ID IE

Table 66: Nokia L2TP Authentication ID IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32805 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7	Authentication ID							
8 to n+4	Present only if explicitly specified							

This IE includes the ID used during authentication between the LAC MAG-c and the PPPoE client.

This IE is used to proxy PPP setup parameters from a LAC MAG-c to an LNS. For more details, see RFC 1661, section 4.4.5.

7.22 Nokia L2TP Authentication Challenge IE

Table 67: Nokia L2TP Authentication Challenge IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32806 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to n+4	Challenge							

This IE includes the challenge used during CHAP authentication between the LAC MAG-c and the PPPoE Client.

This IE is used to proxy PPP setup parameters from a LAC MAG-c to an LNS. For more details, see RFC 1661, section 4.4.5.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

7.23 Nokia L2TP Authentication Response IE

Table 68: Nokia L2TP Authentication Response IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32807 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to n+4	Challenge							

This IE includes the challenge response or password used during the authentication between the LAC MAG-c and the PPPoE Client.

This IE is used to proxy PPP setup parameters from a LAC MAG-c to an LNS. For more details, see RFC 1661, section 4.4.5.

7.24 Nokia L2TP Client Endpoint IE

Table 69: Nokia L2TP Client Endpoint IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32809 (decimal)							
3 to 4	Length = 6							
5 to 6	Enterprise ID = 3729							
7 to 10	IPv4 address							

The LAC MAG-u uses the IP address in this IE to set up an L2TP tunnel.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

7.25 Nokia L2TP Server Endpoint IE

Table 70: Nokia L2TP Server Endpoint IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32810 (decimal)							
3 to 4	Length = 6							
5 to 6	Enterprise ID = 3729							
7 to 10	IPv4 address							

The LAC MAG-u sets up an L2TP tunnel toward the IP address in this IE.

7.26 Nokia L2TP Client Auth ID IE

Table 71: Nokia L2TP Client Auth ID IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32811 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to n+4	Name							

The Name field in this ID identifies the hostname of the LAC.

7.27 Nokia L2TP Server Auth ID IE

Table 72: Nokia L2TP Server Auth ID IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32812 (decimal)							
3 to 4	Length = n							

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
5 to 6	Enterprise ID = 3729							
7 to n+4	Name							

The Name field in this ID identifies the hostname of the LNS.

7.28 Nokia L2TP Password IE

Table 73: Nokia L2TP Password IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32813 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to n+4	Password							

This IE includes the password used for tunnel authentication.

7.29 Nokia L2TP Assignment ID IE

Table 74: Nokia L2TP Assignment ID IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32814 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to n+4	Name							

This IE includes a name for a tunnel or a group of tunnels.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

7.30 Nokia L2TP Private Group ID IE

Table 75: Nokia L2TP Private Group ID IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32815 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to n+4	Group ID							

An LNS can use the Group ID in this IE to correlate a group of customers.

7.31 Nokia L2TP Parameters IE

Table 76: Nokia L2TP Parameters IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32816 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to 11	Parameter Inclusion Flags							
12 to n+4	Parameters							

This IE contains a set of fixed-width parameters that influence tunnel set up. The Parameter Inclusion Flags field contains a list of flags that indicates whether a specific parameter is present or not.

The following table lists for all supported parameters the name, the description, the flag number (1 to 32), and the number of bytes used by the parameter. The flag number correlates to a bit in the Parameter Inclusion Flags field, that is, flag 1 corresponds with 0x00000001 and flag 32 with 0x80000000. The parameters that are flagged for inclusion are included in the Parameters field in order of flag number.

Table 77: L2TP parameters

Parameter	Description	Flag	Number of bytes
Algorithm	The algorithm for tunnel selection:	1	1

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Parameter	Description	Flag	Number of bytes
	• 1: weighted-access • 2: existing-first • 3: weighted-random		
AVP Hiding	The level of AVP hiding: • 1: nothing • 2: sensitive-only • 3: all	2	1
Challenge	Indicates whether to use L2TP tunnel authentication: • 1: never • 2: always	3	1
DF BIT	Indicates whether the LAC clears the DF bit: • 0: clr-lac-data • 1: set-lac-data	4	1
Preference	The relative preference of the tunnel	5	3
Session Limit	The maximum number of sessions per tunnel or group of tunnels	6	3
Idle Timeout	The time for which a tunnel without sessions is kept after removal of the last session	7	3
Hello Interval	The interval between sending Hello messages	8	3
Destruct Timeout	The time during which the tunnel data is operationally kept on the MAG-u after a tunnel is disconnected	9	3
Max Retries Established	The maximum number of times a message (for example, ICRQ) can be retried on an established tunnel before the peer is declared unreachable	10	3

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Parameter	Description	Flag	Number of bytes
	and the tunnel is disconnected		
Max Retries Not Established	The maximum number of times a message (for example, SCCRQ) can be retried on a not yet established tunnel before the peer is declared unreachable	11	3
Rx Window Size	The maximum number of outstanding messages the L2TP peer may send	12	3

7.32 Nokia Access Line Parameters IE

Table 78: Nokia Access Line Parameters IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32822 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to 11	Parameter Inclusion Flags							
12 to n+4	Parameters							

This IE contains a set of fixed-width access line parameters; for example, the access line characteristics as defined in BBF TR-101 and signaled in DHCP, DHCPv6 or PPPoE discovery. The Parameter Inclusion Flags field contains a list of flags that indicates whether a specific parameter is present or not. These values are signaled to be reflected in other MAG-u specific protocols such as L2TP.

The following table lists for all supported parameters the name, the description, the flag number (1 to 32), and the number of bytes used by the parameter. The flag number correlates to a bit in the Parameter Inclusion Flags field, that is, flag 1 corresponds with 0x00000001 and flag 32 with 0x80000000. The parameters that are flagged for inclusion are included in the Parameters field in order of flag number.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Table 79: Access line parameters

Parameter	Description	Flag	Number of bytes
Actual Data rate Upstream	The actual upstream data rate of an access line, in Kbps	1	4
Actual Data rate Downstream	The actual downstream data rate of an access line, in Kbps.	2	4
Minimum Data rate Upstream	The minimum upstream data rate at which an access line is set to operate, in Kbps	3	4
Minimum Data rate Downstream	The minimum downstream data rate at which an access line is set to operate, in Kbps	4	4
Attainable Data rate Upstream	The maximum upstream data rate that can be achieved, in Kbps	5	4
Attainable Data rate Downstream	The maximum downstream data rate that can be achieved, in Kbps	6	4
Maximum Data rate Upstream	The maximum upstream data rate at which an access line is set to operate, in Kbps	7	4
Maximum Data rate Downstream	The maximum downstream data rate at which an access line is set to operate, in Kbps	8	4
Minimum Data rate Upstream in low power state	The minimum upstream data rate at which an access line is set to operate in low power state, in Kbps	9	4
Minimum Data rate Downstream in low power state	The minimum downstream data rate at which an access line is set to operate in low power state, in Kbps	10	4

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Parameter	Description	Flag	Number of bytes
Maximum interleaving delay upstream	The maximum one-way interleaving delay, in milliseconds	11	4
Actual interleaving delay upstream	The actual one-way interleaving delay, in milliseconds	12	4
Maximum interleaving delay downstream	The maximum one-way interleaving delay, in milliseconds	13	4
Actual interleaving delay upstream	The actual one-way interleaving delay, in milliseconds	14	4
Access Loop Encapsulation	The encapsulation type of the access link, as defined in BBF TR 101	15	3
IWF Session	Indicates whether the IWF function was performed for this session to carry PPPoA traffic over PPPoE **Note:** This field does not contain data, setting the flag in the Parameter Inclusion Flags indicates IWF.	16	0

7.33 Nokia L2TP IDs IE

Table 80: Nokia L2TP IDs IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32817 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
7 to 8	Local Tunnel ID							
9 to 10	Remote Tunnel ID							
11 to 12	Local Session ID							
13 to 14	Remote Session ID							
15 to 18	Call Serial Number							
19 to n+4	Present only if explicitly specified							

This IE contains identifiers that are negotiated during L2TP setup.

7.34 Nokia Access Line Circuit ID IE

Table 81: Nokia Access Line Circuit ID IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32820 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							
7 to n+4	Circuit ID							

This IE includes the circuit ID as learned from the access connection protocols such as DHCP, PPPoE discovery, and DHCPv6.

7.35 Nokia Access Line Remote ID IE

Table 82: Nokia Access Line Remote ID IE

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1 to 2	Type = 32821 (decimal)							
3 to 4	Length = n							
5 to 6	Enterprise ID = 3729							

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
7 to n+4	Remote ID							

This IE includes the remote ID as learned from the access connection protocols such as DHCP, PPPoE discovery, and DHCPv6.

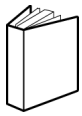
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Appendix: References

1. 3GPP TS 29.244: Interface between the Control Plane and the User Plane nodes
   See 3GPP Specifications Home
2. 3GPP TS 29.281: General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)
   See 3GPP Specifications Home
3. BBF TR-459: Control and User Plane Separation for a disaggregated BNG
   See Technical Reports - Broadband Forum
4. RFC 8300: Network Service Header (NSH)
   See RFC 8300

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

Customer document and product support



Customer documentation

Customer documentation welcome page



Technical support

Product support portal



Documentation feedback

Customer documentation feedback