containerized Multi-Access Gateway – controller

Release 26.10

PFCP Interface Description Guide

3HE 31071 AAAA 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 **4**

List of figures **5**

1 Getting started **6**
1.1 About this guide 6
1.2 Conventions 6
1.2.1 Precautionary and information messages 6
1.2.2 Options or substeps in procedures and sequential workflows 7

2 Introduction to PFCP and CUPS concepts **8**
2.1 PFCP in the CUPS architecture 8
2.2 CUPS concepts 8
2.2.1 PFCP association and path 8
2.2.2 PFCP session 9
2.2.3 Packet data rule 9

3 Forwarding between cMAG-c and MAG-u **11**
3.1 IBCP 11
3.2 GTP-U encapsulation and decapsulation 12

4 Session handling **14**

5 PFCP protocol **15**
5.1 Protocol stack 15
5.2 Generic PFCP message header 15
5.3 PFCP messages overview 17
5.4 Example call flows 18
5.4.1 Initial PFCP association and session setup 18
5.4.2 IPoE session setup 19
5.4.3 CoA handling 20
5.4.4 cMAG-c triggered updates 20

Appendix: References **22**

© 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)..... 13

Table 2: Generic PFCP message header..... 15

Table 3: PFCP messages overview..... 17

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

List of figures

Figure 1: Control plane communication for fixed access....11
Figure 2: Protocol stack for IBCP....12
Figure 3: PFCP protocol stack for the control plane....15
Figure 4: PFCP session ID allocation and use....16
Figure 5: Initial PFCP association and session setup....18
Figure 6: IPoE session setup....19
Figure 7: CoA handling....20
Figure 8: cMAG-c triggered accounting update....20

© 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 containerized Multi-Access Gateway – controller (cMAG-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 cMAG-c functions as the control plane (CP) and has the ability to control the MAG-u nodes.

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

For more information, see the Appendix: References, and other guides mentioned in the *cMAG-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 *cMAG-c Release Notes* for information about features supported in each load of the software release.

1.2 Conventions

This section describes the general conventions used in this guide.

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.

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



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 cMAG-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 cMAG-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 cMAG-c and the MAG-u.

- **SCi, Sx, N4**
  The cMAG-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 accordingly. 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 the Sx/N4 interface.
- **CPRi, Sx-u, N4-u**
  The MAG-u and cMAG-c use these interfaces to forward and tunnel control packets; for example, DHCP discovery and PPPoE Active Discovery Initiation (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 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 cMAG-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 cMAG-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.

- **PFCP association**
  A PFCP association must be set up before sessions can be established between the MAG-u and the cMAG-c. Only one association per cMAG-c and MAG-u pair is allowed. The identifiers of the association

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

are the cMAG-c and the MAG-u node IDs, which can be IP addresses or domain names (FQDNs). Nokia recommends using an FQDN as identifier because it is more stable.

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

Note: Both the cMAG-c and MAG-u use PFCP heartbeat messages to verify that all peering PFCP entities are alive. The heartbeat parameters are configured in the context of the PFCP profile.

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 that specifies the match criteria for the packet. It contains detailed flow matching criteria and is usually set to "any flow". It also contains a reference to a traffic endpoint that contains the session matching criteria.
- **TE**
  The traffic endpoint (TE) specifies the identifying criteria for the session, for example the Layer 2 access ID, VLANs, MAC address, and IP addresses. The PDR refers to one TE via the PDI. TEs can be shared between multiple PDRs within a session.
- **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.

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

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.

- **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.

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

3 Forwarding between cMAG-c and MAG-u

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

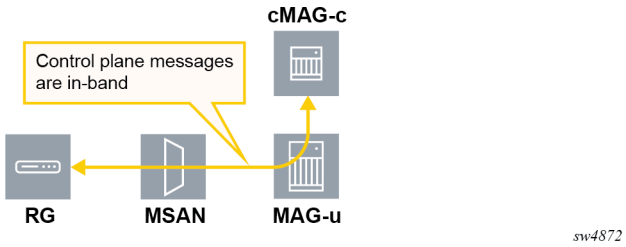
3.1 IBCP

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 cMAG-c. Examples include DHCP, DHCPv6, and ICMPv6 RS.

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 cMAG-c.

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

Figure 1: Control plane communication for fixed access



The cMAG-c installs basic PDRs for the per Layer 2 access ID 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 cMAG-c.

Immediately after the PFCP association is created, the cMAG-c learns all Layer 2 access IDs configured on the MAG-u. Layer 2 access ID are learned via PFCP Node Report signaling; see Initial PFCP association and session setup for more information. The cMAG-c subsequently installs one GTP-U tunnel per Layer 2 access ID, using a dedicated PFCP session for unknown in-band control plane packets. That tunnel is called the per Layer 2 access ID IBCP tunnel. The Layer 2 access ID is a generalized representation of any L2 access technology such as a physical port, pseudowire port, or LAG.

Similarly, for cases where network-facing control plane traffic is required (for example, L2TP signaling for LAC/LNS), the cMAG-c learns all network instances configured on the MAG-u, and subsequently installs one GTP-U tunnel per network instance using a dedicated PFCP session for control plane packets. That tunnel is called the per network instance IBCP tunnel. A network instance is a generalized representation of a routed network, for example a plain router or IP VRF.

After the cMAG-c handles the initial control plane messages, it 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.

See GTP-U encapsulation and decapsulation for more information.

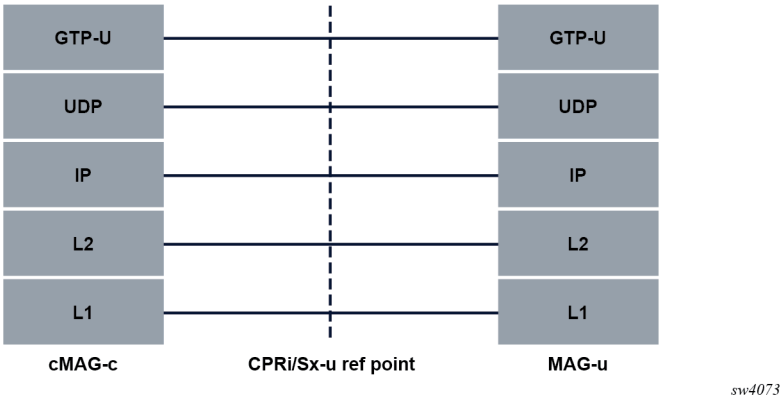
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

3.2 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 the GTP-U tunnel, unmodified (that is, including the VLAN tags).

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

Figure 2: Protocol stack for IBCP



The MAG-u inserts an NSH header to provide context on the cMAG-c. The NSH header contains the following fields:

- **Layer 2 access ID**
  The cMAG-creceives IBCP packets over the Layer 2 access ID, which identifies, for example, the physical port, LAG, or pseudowire port. This uses the Logical Port type (Metadata Class 0x0200, Type 0x00) as defined in BBF TR459.
- **Local MAC address 2**
  This is the local MAC address on the MAG-u, belonging to the Layer 2 access ID. This uses the MAC type (Metadata Class 0x0200, Type 0x01) as defined in BBF TR459.
- **Network instance**
  This is the network instance over which the IBCP packet is received. This only applies to per-network-instance IBCP tunnels. This uses the Network Instance type (Metadata Class 0x0200, Type 0x02) as defined in BBF TR459.
- **PFCP node ID**
  This is the PFCP node ID that identifies the MAG-u node. This uses the Ingress Network Node ID (Metadata Class 0x0000, type 0x06) as defined in RFC 9263. The MAG-u includes the PFCP node ID in this field, using the exact same contents as the PFCP Node ID IE as defined in 3GPP TS29.244, including the node ID type octet.

The cMAG-c sets up a PFCP session using the logical port in the PDR/FAR, and uses the MAC address as the 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.

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, instead 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 cMAG-c.

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.

[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.

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.

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 cMAG-c.

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

5 PFCP protocol

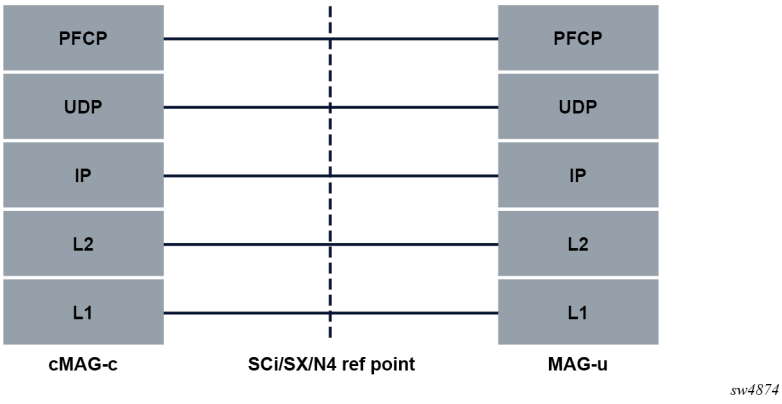
The core of session management is the PFCP protocol as defined in 3GPP TS 29.244, with BNG-specific extensions defined in BBF TR-459.

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 cMAG-c.

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 2: 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)							

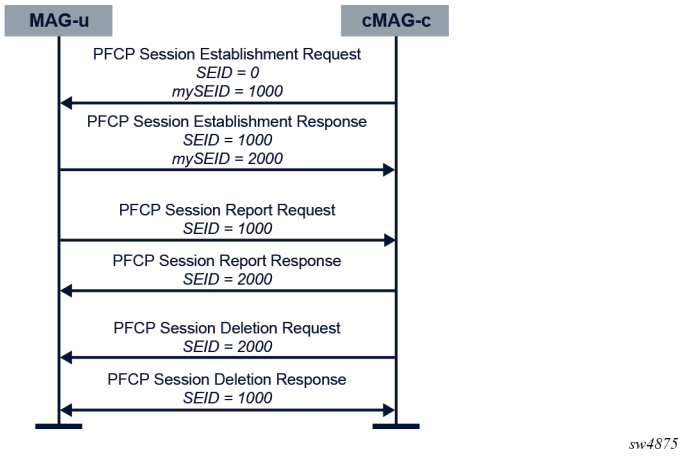
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

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 cMAG-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 the following figure 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

The following table describes the PFCP messages supported by the cMAG-c. See TS 29.244 for more information.

Table 3: PFCP messages overview

Message type	Message	Description
0	Reserved	—
1	PFCP Heartbeat Request	Checks connectivity
2	PFCP Heartbeat Response	Confirms connectivity
5	PFCP Association Setup Request	Starts a PFCP association to exchange feature capabilities and node-wide parameters
6	PFCP Association Setup Response	Confirms a PFCP Association Setup Request
7	PFCP Association Update Request	Signals feature capabilities or node-wide parameter updates
8	PFCP Association Update Response	Confirms the update
9	PFCP Association Release Request	Tears down the PFCP association
10	PFCP Association Release Response	Confirms the teardown
12	PFCP Node Report Request	Reports general, non-session-specific events
13	PFCP Node Report Response	Confirms the node report
50	PFCP Session Establishment Request	Creates a new PFCP session, with message containing all the parameters necessary to correctly create the forwarding state or in-band control plane state
51	PFCP Session Establishment Response	Confirms the creation of the PFCP session and contains the value of related MAG-u parameters, such as the SEID
52	PFCP Session Modification Request	Updates parameters of a PFCP session or requests an update of the usage information (counters)
53	PFCP Session Modification Response	Confirms the modification and can contain updated related MAG-u parameters or usage information (counters) or both

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

Message type	Message	Description
54	PFCP Session Deletion Request	Removes a PFCP session and its related state information
55	PFCP Session Deletion Response	Confirms the removal and includes a final usage update (counters)
56	PFCP Session Report Request	Notifies the cMAG-c of usage information updates (counters) or other state changes (for example, LCP keep-alive failures)
57	PFCP Session Report Response	Confirms receipt of the report

5.4 Example call flows

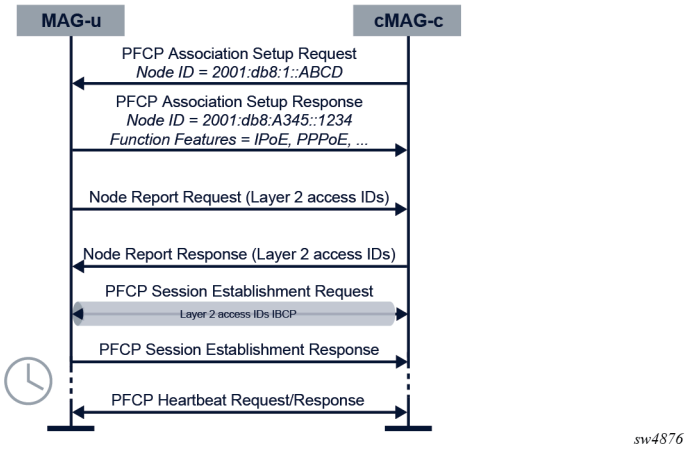
Review call flow examples, including PFCP association and session setup, CoA handling, cMAG-c triggered updates, and PFCP connectivity failure.

5.4.1 Initial PFCP association and session setup

When either a cMAG-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 cMAG-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 cMAG-c initializes the PFCP association setup and the MAG-u responds. During the association setup, both the MAG-u and the cMAG-c exchange parameters.
2. The MAG-u immediately sends one or more PFCP Node Report Request messages to signal each Layer 2 access ID on that MAG-u.

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

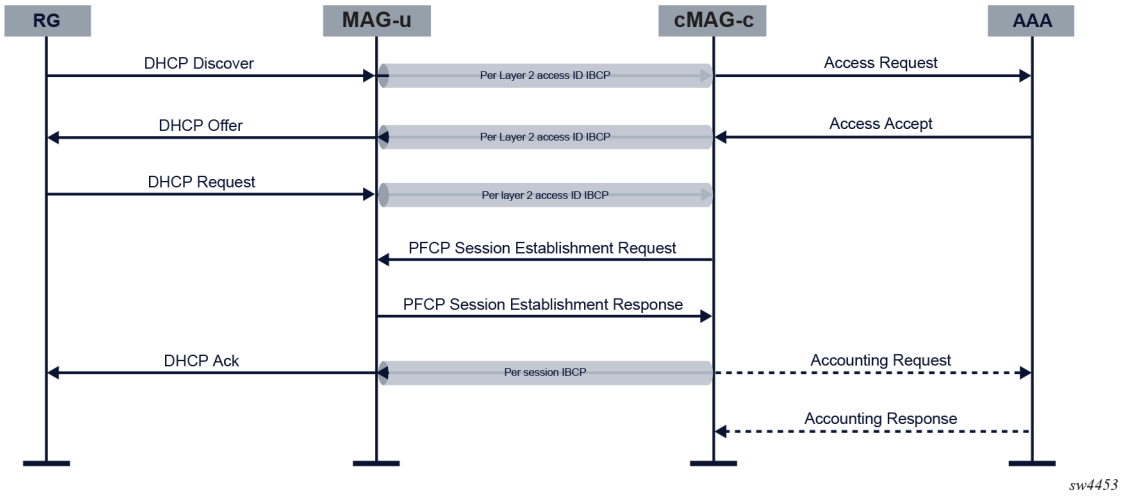
3. For each Layer 2 access ID, the cMAG-c creates a PFCP session on the MAG-u with both uplink and downlink PDRs for the forwarding of initial in-band control plane packets. See IBCP for more information.
4. To monitor connectivity, the MAG-u and the cMAG-c exchange periodic heartbeat messages.

5.4.2 IPoE session setup

When the MAG-u receives a DHCP Discover message from an RG, it forwards the message to the cMAG-c over the the per Layer 2 access ID IBCP tunnel. The cMAG-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 cMAG-c.
- The cMAG-c initialized the MAG-u with per Layer 2 access ID tunnels 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 cMAG-c over the per Layer 2 access ID IBCP tunnel.
2. The cMAG-c authorizes the IPoE session based on parameters in the DHCP message.
3. The cMAG-c sends a DHCP Offer over the per Layer 2 access ID IBCP tunnel to the MAG-u, which decapsulates the DHCP packet and sends it to the RG.
4. The MAG-u forwards the DHCP Request packet to the cMAG-c over the per Layer 2 access ID IBCP tunnel.
5. The cMAG-c initializes the PFCP session and creates data plane rules and per-session IBCP tunnels on the MAG-u (PFCP session establishment procedure).

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

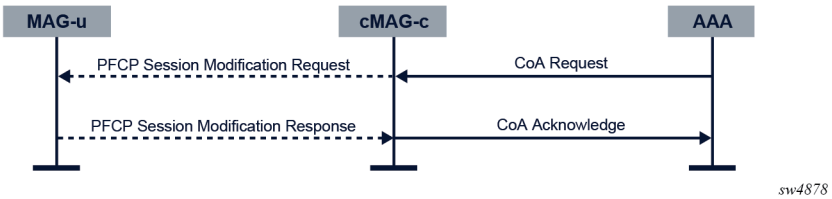
6. The cMAG-c sends the DHCP Ack over the per-session IBCP tunnel to the MAG-u. The MAG-u decapsulates the DHCP packet and sends the packet to the RG.
7. If accounting is provisioned, the cMAG-c starts accounting for the session.

5.4.3 CoA handling

When the RADIUS server requests a change in client authorization for an active session, the cMAG-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

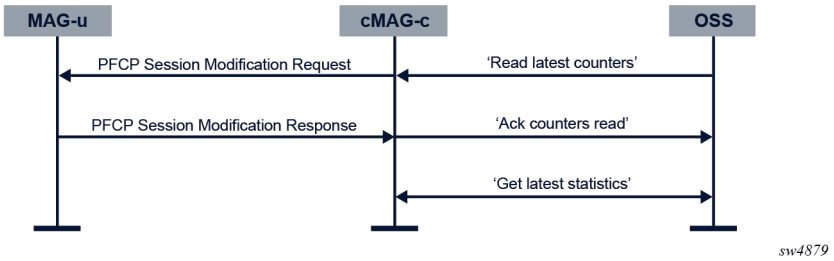
1. The AAA server sends a CoA request directly to the cMAG-c.
2. The cMAG-c processes the message and translates it to the necessary MAG-u state changes. The state changes are signaled via a PFCP session modification procedure.
   If the cMAG-c determines that no MAG-u changes are required, the PFCP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

5.4.4 cMAG-c triggered updates

To perform specific tasks, such as getting up-to-date forwarding statistics for a specific subscriber session, the OSS may send a trigger to the cMAG-c.

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

Figure 8: cMAG-c triggered accounting update



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

Description of the call flow

1. The OSS requests up-to-date forwarding statistics from the cMAG-c using the following command.

   ```
   tools subscriber-management session fetch-statistics-from-up
   ```

2. The cMAG-c processes the message and sends a PFCP Session Modification Request containing the Query URR IE to the MAG-u.
3. The MAG-u sends the requested report in a PFCP Session Modification Response.
4. The MAG-u finalizes the fetch operation.
5. The OSS fetches up-to-date forwarding statistics.

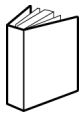
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

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