containerized Multi-Access Gateway – controller

Release 26.10

Control Plane Function Guide

3HE 22220 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 **8**

List of figures **9**

1 Getting started **11**
1.1 About this guide 11
1.2 Conventions 11
1.2.1 Precautionary and information messages 11
1.2.2 Options or substeps in procedures and sequential workflows 12

2 cMAG-c configuration quick start **13**
2.1 Configuring cMAG-c for subscriber management 13
2.1.1 Configuration overview 13
2.1.2 Configuring cMAG-c 13

3 Session management **18**
3.1 PFCP session 18
3.2 General session functionality 18
3.2.1 PFCP protocol 18
3.2.1.1 PFCP association and path 18
3.2.1.2 MAG-u selection 19
3.2.1.3 PFCP session state 19
3.2.1.4 PFCP provisioning 19
3.2.1.5 Session message priority 22
3.2.2 PFCP connectivity failure 22
3.2.2.1 Headless mode 23
3.2.2.2 Session timer alignment 24
3.2.3 Subscribers 25
3.2.4 QoS 25
3.2.5 Service selection 26
3.2.6 Operational commands and debugging 28
3.2.7 Session state storage 29
3.2.8 Prefix delegation as a framed route 30
3.3 Fixed access sessions 30

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

3.3.1 Layer 2 circuit....30
3.3.2 In-band control plane and MAG-u selection....31
3.3.3 Session keys and anti-spoofing....32
3.3.4 Subscriber identification....33
3.3.5 Session limits....34
3.3.6 IBCP rate limiting....35
3.3.7 IPoE....36
3.3.7.1 SHCV....37
3.3.8 PPPoE....38
3.3.9 Application assurance for fixed subscriber sessions....46
3.4 Address assignment protocols....47
3.4.1 DHCP....47
3.4.2 ICMPv6 Router Advertisements and SLAAC....48
3.4.3 DHCPv6....50
3.5 Call trace....51
3.5.1 Always-on tracing....52
3.5.2 Packet tracing....53
3.5.3 Enabling automatic tracing based on error conditions....53
3.5.4 Accessing the call trace GUI....54
3.5.5 Managing session tracing filters....55
3.5.5.1 Managing static filters using the CLI....57
3.5.5.2 Managing dynamic filters using the Call Trace GUI tool....57
3.5.6 Inspecting call trace captures....60
3.5.6.1 Searching for session traces....61
3.5.6.2 Reviewing the details of a trace....63
3.5.7 Trace retention....65
3.6 Session lockout....65
3.6.1 Configuring and applying a session-lockout profile....66
3.6.2 Disable session lockout....67

4 Address assignment....68
4.1 Overview of address assignment....68
4.2 ODSA and local address assignment....68
4.2.1 ODSA....68
4.2.2 Variable prefix and micro-net lengths....70
4.2.3 Local address assignment....73

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

4.3 AAA-based address assignment....74
4.4 AAA framed routes....75
4.5 Managed routes from the ADB....75
4.6 Unmatching prefixes....76
4.7 Local static address assignment via authentication database....77
4.8 External DHCPv4 and DHCPv6 server address assignment....78
4.8.1 Local ODSA pool tracking....78
4.8.2 DHCPv4 relay....78
4.8.3 DHCPv6 relay....79
4.8.4 DHCP options....82
4.8.5 DHCP relay and MAG-u redundancy....83

5 Authentication....84
5.1 Overview of the authentication process....84
5.2 BNG entry point....84
5.3 Authentication database....85
5.4 Authentication flow....86
5.5 BNG EP and ADB lookup....87
5.6 VLAN list-based lookups....91
5.7 Required minimal configuration for a session creation....93
5.8 RADIUS authentication profile....94
5.9 RADIUS fallback to ADB....95
5.10 RADIUS CoA and DM....96
5.11 Example configuration....97

6 Accounting and charging....100
6.1 BNG charging profiles....100
6.2 Statistics collection from the MAG-u....101
6.3 cMAG-c-based charging....103
6.4 RADIUS accounting....104
6.4.1 Enabling RADIUS accounting....104
6.4.2 Session accounting....105
6.4.3 Message retransmission and buffering....106
6.4.4 Sending Accounting-On and Accounting-Off messages....108

7 Lawful intercept....109

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

7.1 LI overview ... 109
7.2 LI strict licensing ... 109
7.3 LI architecture ... 110
7.4 LI administrative interface ... 111
7.4.1 Configuring passwords and seeds ... 112
7.4.2 Setting up the LI infrastructure ... 112
7.5 LI solution for wireline application ... 113
7.5.1 Setting up LI targets ... 113
7.5.2 LI information related interface ... 114
7.5.3 LI contents of communication ... 114

8 Python support ... 116
8.1 Configuring a Python script ... 119

9 MAG-u resiliency ... 120
9.1 Terminology for MAG-u resiliency ... 120
9.2 Introduction to cMAG-c-driven MAG-u resiliency ... 120
9.3 Modeling a resilient MAG-u deployment using UP groups ... 122
9.3.1 Modifying UP groups ... 123
9.3.1.1 Validating UP group changes ... 124
9.3.2 Fate sharing group creation ... 125
9.3.3 Fixed access with active/standby pseudowire access ... 125
9.3.3.1 Configuring health reporting for an A/S PW port on the Nokia MAG-u ... 127
9.3.3.2 Maintenance on a Nokia MAG-u in an A/S PW setup ... 128
9.3.3.3 Bringing down the PW in headless conditions ... 130
9.3.3.4 Moving an FSG to standby in headless mode ... 131
9.3.4 Fixed access with broadcast access ... 132
9.3.4.1 Blocking the setup of non-resilient sessions ... 134
9.3.4.2 Hot-standby resiliency examples ... 136
9.3.4.3 Warm-standby resiliency examples ... 141
9.3.5 Performing maintenance on a Nokia MAG-u ... 147
9.3.6 Operational commands ... 151
9.4 Fate sharing groups ... 153
9.4.1 Session-to-FSG mapping ... 154
9.4.2 Traffic steering parameters ... 154
9.4.3 MAG-u health determination ... 156

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

9.4.4 Active/standby selection triggers 159
9.4.5 Active/standby selection 160
9.4.6 Active/standby change or switchover 162
9.4.7 MAG-u lockout 164
9.5 Standby modes 165
9.6 Interaction with headless mode 166

10 cMAG-c management 168
10.1 cMAG-c-specific system management 168
10.2 Accessing the cMAG-c GUI 170

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

List of tables

Table 1: cMAG-c configuration components and quick-start steps....13

Table 2: Message header for session-related PFCP messages....22

Table 3: PPPoE entry-point properties....39

Table 4: PPPoE profile LCP negotiation properties....41

Table 5: Address assignment protocols per session type....47

Table 6: Minimal configuration for a session creation....93

Table 7: Supported direction for RADIUS messages....116

Table 8: Supported direction for RADIUS CoA messages....117

Table 9: Supported direction for PPPoE messages....117

Table 10: Supported direction for DHCPv4 messages....117

Table 11: Supported direction for DHCPv6 messages....118

Table 12: Summary of MAG-u states....158

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

List of figures

Figure 1: HQoS example....26
Figure 2: IPoE session setup with RADIUS authentication....36
Figure 3: PPPoE session setup flow....39
Figure 4: Resiliency based on PADO delay....45
Figure 5: High-level call trace elements....52
Figure 6: Administratively disabling a filter using the Call Trace GUI tool....56
Figure 7: Viewing event details in the Call Trace tool....64
Figure 8: DHCPv4 call flow....79
Figure 9: DHCPv6 call flow with RS message....80
Figure 10: DHCPv6 call flow without RS message....81
Figure 11: Statistics collection using the pull model....101
Figure 12: Statistics collection using the push model....101
Figure 13: High-level cMAG-c LI architecture....111
Figure 14: High-level overview of communication for MAG-u resiliency....121
Figure 15: Multiple MAG-u backup nodes....122
Figure 16: A/S PW deployment....126
Figure 17: Multiple Layer 2 access IDs per UP group....133
Figure 18: 1:1 hot standby resiliency example....138
Figure 19: Per S-tag 1:1 hot standby resiliency example....140
Figure 20: N:1 warm standby resiliency example....143
Figure 21: N:K warm standby resiliency example....146

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

Figure 22: Example of the relationship between FSGs, MAC addresses, and subnets.....156

Figure 23: GARP race conditions..... 164

© 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 Nokia containerized Multi-Access Gateway – controller (cMAG-c) for the BNG CUPS solution.

The cMAG-c is based on the Packet Forwarding Control Protocol (PFCP) interface as defined in 3GPP TS 29.244 for mobile 4G CUPS and 5G, and extended by BBF TR-459.

The cMAG-c installs session forwarding state on one or more MAG-u nodes. The term MAG-u is a generic converged name for any type user plane, and includes for example a BNG-UP.

This guide is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as command line interface (CLI) syntax and command usage.

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

The CLI command descriptions can be found in the *cMAG-c CLI and Data Model Explorer*.

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.

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

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

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 cMAG-c configuration quick start

The quick start steps configure the main components required to prepare the cMAG-c for subscriber management.

2.1 Configuring cMAG-c for subscriber management

Set up and configure basic components to prepare the cMAG-c for subscriber management.

2.1.1 Configuration overview

The cMAG-c basic configuration for subscriber management requires specific configuration tasks to be completed in a particular order.

The following table lists the main components and links to the specific configuration step that you must complete to prepare the cMAG-c for subscriber management.

Table 1: cMAG-c configuration components and quick-start steps

Configuration component	Configuration task
Configure a system name.	Step 1
Configure PFCP connectivity between the cMAG-c and MAG-u.	Step 2
Configure a service and network instance.	Step 3
Configure a local address pool for IP address assignment within the network instance.	Step 4
Configure the authentication database (ADB).	Step 5
Configure the entry point.	Step 6
Configure IBCP to terminate fixed access sessions.	Step 7

2.1.2 Configuring cMAG-c

These quick-start instructions provide the basic steps required to configure the cMAG-c for subscriber management, including references to additional topics for users who want more information.

Prerequisites

- Identify the name of the IES or VPRN service used to host subscriber sessions on the MAG-u; see Service selection.
- Ensure the MAG-u is configured; see "PFCP association" and "Session management" in the *7750 SR and VSR BNG CUPS User Plane Function Guide* for more information.

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

About this task

This procedure describes the minimal configuration required to create subscriber sessions on the cMAG-c.

Procedure

Step 1. Optional: Configure a cMAG-c system name.

The cMAG-c system name is used as the hostname for the CLI session prompt and as the default value for any protocol that reflects a system identifier; for example, the NAS ID in RADIUS and the node ID in PFCP. Nokia recommends selecting a system name that is concise and adheres to the FQDN encoding rules.

Example

System name configuration

```
# info from running with-context /subscriber-management system name
    subscriber-management {
        system {
            name cmag-c
        }
    }
```

Step 2. Configure PFCP connectivity between the cMAG-c and MAG-u.

The following example shows a cMAG-c connected to a MAG-u with node ID mag-u and IP 192.0.2.11.

Example

PFCP connectivity between the cMAG-c and MAG-u

```
# info from running with-context /subscriber-management ref-points up
    subscriber-management {
        ref-points {
            up {
                peer mag-u {
                    admin-state enable
                    address-resolution {
                        static-ip [
                            192.0.2.11
                        ]
                    }
                }
            }
        }
    }
```

Step 3. Configure a service and network instance.

Sessions are assigned to a service, which maps to a network instance. A service is a generic concept describing the type of service a session receives; for example, high speed Internet, video, or voice. A network instance maps to a routing context on the UP. See Service selection for more information about network instance configuration.

Example

Network instance configuration for the service

```
# info from running with-context /subscriber-management services
    subscriber-management {
        services {
            network-instance hsi {
```


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

```
            }
            service hsi {
                network-instance hsi
            }
        }
    }
```

Step 4. Configure a local address pool for IP address assignment within the network instance.

The following example shows a simple address pool configuration that uses the prefix 192.0.2.0/24 for IPv4 address assignment and 2001:db8:b00::/40 for IPv6 PD prefix assignment. Other methods can be used. See Local address assignment for more information about IP address assignment.

Example

Local address pool configuration for IP address assignment

```
# info from running with-context /subscriber-management services network-instance hsi
 pool hsi
    subscriber-management {
        services {
            network-instance hsi {
                pool hsi {
                    hold-time 300
                    ipv4 {
                        micro-net-length 28
                        prefix 192.0.2.0/24 {
                        }
                    }
                    ipv6 {
                        na {
                            micro-net-length 120
                            prefix 2001:db8:a00::/116 {
                            }
                        }
                        pd {
                            micro-net {
                                length 48
                            }
                            prefix 2001:db8:b00::/40 {
                            }
                        }
                        slaac {
                            micro-net-length 56
                            prefix 2001:db8:c00::/48 {
                            }
                        }
                    }
                }
            }
        }
    }
```

Step 5. Configure the ADB.

The ADB configuration determines the authentication process and address assignment method, and retrieves attributes associated with the subscriber session. The following example uses the ADB to provide the address assignment and the subscriber and SLA profiles for the subscriber session. The address pool refers to the local address assignment configured in step 4. See Authentication database for more information.

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

Example

ADB configuration

```
# info from running with-context /subscriber-management authentication-database basic-
adb
    subscriber-management {
        authentication-database basic-adb {
            admin-state enable
            match 1 {
                attribute c-vlan
                optional true
            }
            entry default {
                admin-state enable
                service-name hsi
                ip-anti-spoof true
                action {
                    accept
                }
                up-parameters {
                    sla-profile default
                    sub-profile default
                }
                address-assignment {
                    local-dynamic {
                        ipv4-pool hsi
                        ipv6-pd-pool hsi
                        ipv6-na-pool hsi
                    }
                }
            }
        }
    }
```

Step 6. Configure the entry point.

The entry point informs the cMAG-c about the authentication flow and other aspects of session management and setup. See BNG entry point for more information. The following example shows a simple configuration that refers to the ADB configured in step 5.

Example

Entry point configuration

```
# info from running with-context /subscriber-management entry-point fixed-access
    subscriber-management {
        entry-point fixed-access {
            admin-state enable
            match 1 {
                attribute up-node-id
                optional true
            }
            entry default {
                admin-state enable
                ipoe {
                    authentication-flow {
                        authentication-database [
                            basic-adb
                        ]
                    }
                }
            }
        }
```


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

```
    }
```

Step 7. Configure IBCP to terminate fixed access sessions.

For fixed access sessions, configure IBCP to allow tunneling of control plane messages. The default IBCP tunnel supports tunneling of control packets from the MAG-u to the cMAG-c. The following example configures IBCP to terminate dual stack IPoE sessions. See In-band control plane and MAG-u selection for more information about IBCP.

Example

Configuration for the IBCP tunnel

```
# info from running with-context /subscriber-management ref-points up fixed-access
    subscriber-management {
        ref-points {
            up {
                fixed-access {
                    entry-point fixed-access
                    ibcp-triggers {
                        pppoe-discover true
                        ipoe-dhcp true
                        ipoe-dhcpv6 true
                        ipoe-router-solicit true
                    }
                }
            }
        }
    }
```


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

3 Session management

Get a general overview of the session functionality and the address assignment protocols, and details on the IPoE and PPPoE fixed access session types.

3.1 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.

3.2 General session functionality

Get a high-level overview of the PFCP protocol and general session related functionality including grouping sessions for a subscriber, QoS, service selection, session state, and lawful intercept.

3.2.1 PFCP protocol

Get a high-level overview of the core protocol of session management.

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.

3.2.1.1 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 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**

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

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.

3.2.1.2 MAG-u selection

The cMAG-c selects a MAG-u for each session depending on the session type.

The MAG-u selection varies from very static to very dynamic.

See In-band control plane and MAG-u selection for more information about the selection process for fixed access session.

3.2.1.3 PFCP session state

PFCP sessions require the creation of a forwarding state on the MAG-u device. Session operations allow to manage the forwarding state on the MAG-u.

The forwarding state includes rules (for example, encapsulation and decapsulation), information about routing context forwarding, QoS rules, and requested charging functionality.

The PFCP session establishment procedure creates the initial forwarding state. The path used for the PFCP session establishment procedure is tied to the session.

The following operations are supported for an established session:

- **PFCP session modification**
  The cMAG-c modifies the state or performs a state query (for example, to fetch statistics).
- **PFCP session deletion**
  The cMAG-c removes all state information.
- **PFCP session report**
  The MAG-u sends information unsolicited (for example, to report statistics or a connectivity failure).

In stable conditions, the MAG-u only modifies or deletes the state if instructed by the cMAG-c. If the MAG-u detects a failure, for example, a link failure, it does not delete the state but sends a report and keeps the local state. The MAG-u deletes the state only when the cMAG-c sends a delete request.

3.2.1.4 PFCP provisioning

The PFCP protocol uses components that must be provisioned and verified using the CLI.

Components for PFCP provisioning

To enable the PFCP protocol, provision and reference the following components in the reference-point configuration:

- **IP interface**
  The IP interface for signaling is provisioned at the infrastructure layer. See the cMAG-c Installation Guide for more information.

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

- **Node ID**
  The cMAG-c requires an FQDN-based node ID for the PFCP association. By default, the cMAG-c system name, which is set to **cmag-c** by default, serves as the node ID. Use the following command to configure the system name.

  ```
  subscriber-management system name
  ```

  Use the following command to override the used node ID.

  ```
  subscriber-management ref-points up mag-c-node-id
  ```

- **PFCP association peer list**
  Use the following command to configure the list of peer MAG-u devices.

  ```
  subscriber-management ref-points up peer
  ```

- **PFCP profile**
  Use the commands in the following context to configure PFCP profile options.

  ```
  subscriber-management profiles pfcp-profile
  ```

  Note: The heartbeat and the retransmit options must be configured with the same values in both the MAG-u and cMAG-c, to prevent the MAG-u and cMAG-c from going out of sync if a link failure occurs. See the *7750 SR and VSR BNG CUPS User Plane Function Guide* for more information about the MAG-u configuration.

Example: PFCP provisioning

Note: In this example the system interface is referenced. However, other interface types (for example, direct and loopback interfaces) are also allowed.

```
# info from running with-context /subscriber-management ref-points up
    subscriber-management {
        ref-points {
            up {
                fixed-access {
                    entry-point fixed-access
                    ibcp-triggers {
                        pppoe-discover true
                        ipoe-dhcp true
                        ipoe-dhcpv6 true
                        ipoe-router-solicit true
                    }
                }
                peer up-east {
                    admin-state enable
                    address-resolution {
                        static-ip [
                            192.0.2.11
                        ]
                    }
                }
            }
        }
    }
```


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

Verifying PFCP association setup

Use the following command to view the PFCP association establishment for the cMAG-c.

```
info from state /subscriber-management ref-points up
```

Output example: PFCP association reference point peers

```
# info detail depth 1 from state /subscriber-management ref-points up peer up-east
    subscriber-management {
        ref-points {
            up {
                peer up-east {
                    association-state up
                    setup-time 2025-04-03T15:35:30Z
                    last-change 2025-04-03T15:35:30Z
                    up-state active
                    admin-state enable
                    node-id-type fqdn
                    drain false
                    oper-mag-c-node-id cmag-c
                    apply-state applied
                    up-function-features-3gpp [
                        ip6pl
                        adpdp
                        mnop
                        empu
                        pdiu
                        frrt
                        ftup
                        treu
                    ]
                    up-function-features-bbf [
                        agf-direct
                        b-upf
                        pppoe
                        ipoe
                        lcp-keepalive-offload
                    ]
                    up-function-features-nokia [
                        bulk-audit
                        lac
                        session-subnet-signaling
                        fsg
                        per-l2-access-id-tunnels
                        partial-audit
                    ]
                    fsg {
                    }
                    path 192.0.2.11 {
                        path-state up
                        last-successful-heartbeat 2025-04-03T16:25:30Z
                        ongoing-heartbeat 2025-04-03T16:25:30Z
                        recovery-timestamp 2025-04-03T15:27:21Z
                        last-changed 2025-04-03T15:35:30Z
                    }
                    statistics {
                    }
                    address-resolution {
                        static-ip [
                            192.0.2.11
                        ]
                    }
```


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

```
                }
            }
        }
    }
```

Related topics
Headless mode

3.2.1.5 Session message priority

To prioritize PFCP session-related messages toward the MAG-u, the cMAG-c uses the message priority field of the PFCP header. The value of the message priority ranges from 0 to 15, with 0 indicating the highest priority. For more information about how the MAG-u enforces the priority, see the *7750 SR and VSR BNG CUPS User Plane Function Guide*.

Table 2: Message header for session-related PFCP messages

Bits								
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	Version			Spare	Spare	FO	**MP**	S=1
2	Message Type							
3	Message Length (1st Octet)							
4	Message Length (2nd Octet)							
5 to 12	Session Endpoint Identifier							
13 to 15	Sequence Number							
16	**Message Priority**				Spare			

The MP bit, which can only be set for session-related PFCP messages, indicates whether the message priority field is set. If the MP bit is not set, the message priority field is ignored and the MAG-u determines the priority. The Nokia MAG-u usually uses priority 15 if the MP bit is not set. See the 7750 SR and VSR BNG CUPS User Plane Function Guide for more information.

The message priority field indicates the actual priority of a message. The cMAG-c uses a part of the priority field to assign priority between different transaction types as part of its overload handling. For example, mid-session modifications are prioritized over the creation of new sessions, making sure that existing sessions are less likely to be affected than new sessions in the event of overload.

3.2.2 PFCP connectivity failure

To protect against temporary PFCP connectivity failures, cMAG-c supports a headless mode. Following the rules for configuring sessions timers ensures that the headless mode works as expected.

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

3.2.2.1 Headless mode

To prevent the removal of sessions with a temporary heartbeat failure, cMAG-c supports a short-lived headless mode to restore connectivity.

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.

Use the following command to configure the heartbeat parameters.

```
subscriber-management profiles pfcp-profile heart-beat
```

To protect against temporary failures, the cMAG-c and MAG-u support a headless mode. Use the following command to enable the headless mode.

```
subscriber-management profiles pfcp-profile path-restoration
```

Note: When using headless mode, Nokia recommends configuring the total message retransmit timeout for all other messages to be longer than the time to detect headless mode. To accomplish this, configure the message retransmit to be higher than the value of the **interval** command plus the **retry-count** command times the **timeout** command, as configured in the **heart-beat** context.

message retransmit timeout > **interval** + **retry-count** × **timeout**

When headless mode is enabled, the sessions are not removed when there is a heartbeat failure. Instead, the configured timer starts and heartbeats continue to be sent. Subsequently, one of the following events occurs:

- The timer expires and all sessions are removed. The association remains in place.
- The path is restored (a successful heartbeat is completed) but a MAG-u restart is detected and all sessions are removed.
- The path is restored (a successful heartbeat is completed), the sessions are kept, and a PFCP audit procedure is started to ensure that the MAG-u and cMAG-c states are synchronized.

Note:

- To prevent the cMAG-c or MAG-u from deleting all sessions while the other node keeps all the sessions, Nokia recommends that the path restoration time is at least twice as large as the sum of the **heart-beat interval** plus the total heartbeat timeout.

  path restoration time ≥ 2 × (**heart-beat interval** + total heartbeat timeout)

  total heartbeat timeout = **heart-beat retry-count** N1 × **heart-beat timeout** T1

  This ensures that the cMAG-c and MAG-u nodes each run an audit or delete all the sessions in their respective nodes.
- All parameter configurations must be identical between the cMAG-c and MAG-u.

To avoid hanging resources on a MAG-u, the cMAG-c only removes a session after it receives confirmation that the MAG-u has removed the session. The cMAG-c may receive confirmation in the following messages:

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

- PFCP Session Deletion Response message (most common case)
- PFCP message including a Cause IE that indicates an error (the MAG-u lost the session)
- an indication that the MAG-u restarted and lost all its sessions; for example, a new PFCP Association Setup Request

If no confirmation is received, the cMAG-c retries the deletion of the session for up to 15 minutes. After this time, the cMAG-c removes the session without waiting for the MAG-u confirmation. To expedite the removal of a session, use the **local-only** keyword with the following command to manually remove the session.

```
tools subscriber-management session clear
```

This removes operational sessions on the cMAG-c without synchronization with any external server or the client.

Related topics

Operational commands and debugging

3.2.2.2 Session timer alignment

Nokia recommends aligning the session timers (signaled to the BNG RG) with the path restoration time. If the session timers are not aligned with the path restoration time, a session may time out autonomously before the headless mode could restore the path.

The following configurations for the session timers guarantee that the headless mode kicks in as expected.

- For DHCP, the DHCP lease time must at least equal the renew time plus the path restoration time. In the default case, where the renew time is half of the lease time, the lease time must be at least twice the path restoration time.
- For all IPv6 enabled sessions, the router lifetime included in RA messages must be at least equal to the maximum advertisement interval plus the path restoration time. In the default case, where the router lifetime is three times the maximum advertisement interval, the maximum advertisement interval must be equal to at least twice the path restoration time.
- For SLAAC, the IPv6 preferred lifetime must be at least equal to the maximum router advertisement interval plus the path restoration time.
- For DHCPv6, the IPv6 preferred lifetime must be at least equal to the renew timer (T1 timer) plus the path restoration time. In the default case, where the renew timer is half of the preferred lifetime, the preferred lifetime must be equal to at least twice the path restoration time.

The parameters can be locally configured or received from an external AAA server.

To configure or display information locally, use the following commands:

- **path restoration time**

  ```
  subscriber-management profiles pfcp-profile path-restoration
  ```

- **DHCP lease time**

  ```
  subscriber-management authentication-database entry address-assignment dhcpv4-lease-times
   lease-time
  ```


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

- **renew time**

```
subscriber-management authentication-database entry address-assignment dhcpv4-lease-times
 renew-time
```

- **router lifetime in RA messages**

```
subscriber-management profiles ra-profile options router-lifetime
```

- **maximum advertisement interval**

```
subscriber-management profiles ra-profile advertisement-interval max
```

- **IPv6 preferred lifetime**

```
subscriber-management authentication-database entry address-assignment ipv6-lifetimes
 preferred-lifetime
```

3.2.3 Subscribers

The cMAG-c supports bundling a group of sessions for a single subscriber.

Grouping of sessions is useful in cases where a subscription consists of multiple directly connected devices. For example, a subscription may consist of a routed residential gateway for Internet access, VoIP phones, and set-top boxes. The residential gateway bridges traffic for voice and video services to the VoIP phones and to the set-top boxes. The cMAG-c automatically creates a subscriber based on keys it derives from the session types, and allocates an auto-generated subscriber ID to the sessions.

See Subscriber identification for fixed access sessions and for more information about how the subscriber ID is generated.

A subscriber ID alias can be provided via AAA interfaces, but this alias cannot change the scope of a subscriber. For example, if the key of a subscriber contains a Layer 2 circuit (l2-circuit), the AAA subscriber ID alias cannot group two sessions with two different l2-circuit values.

3.2.4 QoS

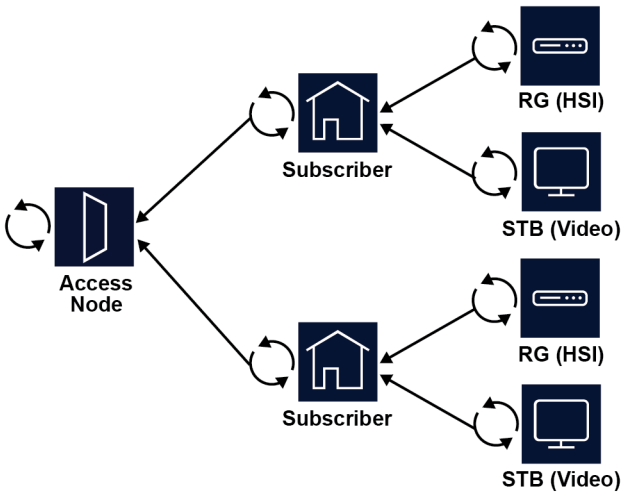
The cMAG-c enables the appropriate HQoS configuration by sending subscriber profiles and SLA profiles to the MAG-u.

A BNG connection uses HQoS structures, in which there are multiple levels of rate limiting and scheduling. For example, one structure has an aggregate rate per MSAN, a second structure has an aggregate rate per subscriber level, and a third structure has an aggregate rate per session.

The following figure shows an example of an HQoS model.

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

Figure 1: HQoS example



HQoS models can be complex and very hardware specific, the cMAG-c signals the MAG-u profiles to enable the appropriate HQoS configuration. The Nokia cMAG-c signals a subscriber profile and an SLA profile in the PFCP message. The profiles are provisioned during authentication.

The subscriber profile should be kept consistent for all sessions of a subscriber, but the cMAG-c does not enforce consistency. Short-lived inconsistencies are allowed while changing a subscriber profile; for example, when sending a CoA message to all sessions of the subscribers. However, long-lived inconsistencies may lead to unexpected behavior, including reverting to an old subscriber profile.

3.2.5 Service selection

The cMAG-c service model is based on a locally significant service and a network instance.

The cMAG-c service model is based on two concepts:

- A locally significant service defines the service to be delivered; for example, high speed Internet (HSI), video, or voice services. Each service can be associated with service-specific parameters, including a default set of IP pool names for address management. Use the following command to configure services.

  ```
  subscriber-management services service
  ```

- A network instance defines the forwarding context in which the session is installed on the MAG-u, typically a routing instance. The network instance also serves as the context for provisioning IP pool details. Use the following command to configure network instances.

  ```
  subscriber-management services network-instance
  ```

Each service must be associated with a network instance, and network instances can be shared across multiple services. The following example shows three services ("hsi", "voice", and "video"), all using the same network instance "base" but with distinct default IPv4 pools for address assignment.

```
# info from running with-context /subscriber-management services
```


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

```
    subscriber-management {
        services {
            network-instance base {
                pool hsi {
                    ipv4 {
                        micro-net-length 28
                        prefix 192.168.0.0/24 {
                        }
                    }
                }
                pool video {
                    ipv4 {
                        micro-net-length 28
                        prefix 192.168.1.0/24 {
                        }
                    }
                }
                pool voice {
                    ipv4 {
                        micro-net-length 28
                        prefix 192.168.2.0/24 {
                        }
                    }
                }
            }
            service hsi {
                network-instance base
                address-assignment-defaults {
                    local-dynamic {
                        ipv4-pool hsi
                    }
                }
            }
            service video {
                network-instance base
                address-assignment-defaults {
                    local-dynamic {
                        ipv4-pool video
                    }
                }
            }
            service voice {
                network-instance base
                address-assignment-defaults {
                    local-dynamic {
                        ipv4-pool voice
                    }
                }
            }
        }
    }
```


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

3.2.6 Operational commands and debugging

*Use the commands in the **show**, **clear**, and **tools** contexts to display cMAG-c sessions and subscribers, remove a session, and debug a failing session setup. Use the call trace feature for advanced debugging.*

Removing, debugging, and displaying session information

Use the following command to display information about cMAG-c sessions and subscribers.

```
show subscriber-management session
```

- The **session** command displays basic data related to all sessions on the cMAG-c.
- The supported filter options for the **session** command display the data for specific sets of sessions.
- The **detail** keyword displays all data relevant to a session in a structured fashion.

Use the following state tree to get session counts in various scopes; for example, total sessions on cMAG-c or per MAG-u.

```
subscriber-management statistics
```

The following example displays the session counters for the entire cMAG-c system.

```
# info depth 0 detail from state /subscriber-management statistics
    subscriber-management {
        statistics {
            active-sessions 1
            standby-sessions 0
            ipoe-sessions 1
            pppoe-sessions 0
            ipv4-stacks 1
            ipv6-stacks 0
            ipv6-slaac 0
            ipv6-na 0
            ipv6-pd 0
        }
    }
```

Use the following command to display an overview of the operational data related to a subscriber. The command has similar options as the session command.

```
show subscriber-management subscriber
```

Use the following state tree to get IBCP statistics .

```
subscriber-management ref-points up statistics ibcp
```

Use the following command to remove a session from the cMAG-c. When you issue this command, the cMAG-c sends a PFCP Session Deletion Request to the MAG-u.

```
tools subscriber-management session clear
```

Use the **local-only** keyword to delete an operational session on the cMAG-c without synchronization with any external server or the client session. This also bypasses the headless mode mechanism.

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

Tip: Always add filters to the **clear** command in the **tools subscriber-management session** context to avoid accidentally clearing all sessions.

Use the following command to display the session manager log for debugging a failing setup session.

```
show subscriber-management log subsystem session-manager
```

Related topics

In-band control plane and MAG-u selection

PFCP connectivity failure

3.2.7 Session state storage

For scalability and redundancy, the Nokia cMAG-c distributes the session state functionality across multiple pods. This section provides a high-level overview of how the cMAG-c handles session state in a distributed environment. See cMAG-c Overview Guide for a high-level view of the architecture.

To efficiently handle a distributed system where multiple pods operate on the same session state, the cMAG-c employs a stateless model, storing all session state in a database. This database serves as the sole stable state for a session and is maintained in a consistent manner. Multiple types of pods use the database state in different ways:

- **session management pods**
  Session management pods are the only pods that can update (write) session state in the database. They use transactions, including session setup, DHCP lease renewal, charging update, or session removal, to update the session state. At the start of each transaction, a session management pod retrieves the necessary session state from the database and locks the session. At the end of the transaction, the session management pod writes to the database, releases the lock, and removes all local in-memory session state. The lock guarantees that no other session management pod can start transactions for the same session, thereby preventing conflicting state. Because a session management pod removes all local session state at the end of a transaction, any subsequent transaction can be handled by any session management pod in the cMAG-c, without requiring it to be the same pod.
- **session orchestration pods**
  Session orchestration pods guarantee that the shared resources are correctly managed by the cMAG-c, primarily to prevent duplicate resource assignments to sessions. Examples of orchestration pods include the following:
  - **gatekeeper pod**
    The gatekeeper pod assigns a session to a new or existing subscriber and allocates a unique session and subscriber ID. It also applies session limits, such as per-subscriber, per-UP, or per-Layer 2 access ID limits.
  - **ODSA pod**
    The ODSA pod assigns addresses to sessions for local address assignment.

  These pods maintain partial session state in memory to track allocations. For example, the ODSA pod retains in-memory records of allocated addresses to avoid overlap when assigning new addresses. When these pods need to restart (for example, because of upgrade or pod relocation), they retrieve the necessary session state from the database records.
- **other pods**
  A lot of other pods interact with session state in a read-only fashion. Similar to session management pods, these pods do not maintain any session state in long-lived memory, but remove any local state upon completion of a specific work item. Examples include:

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

- **session state pod**
  The session state pod collects session state directly from the database and reflects it back to the requesting application. This is used, for example, to retrieve data when executing the **info from state subscriber-management subscriber** command, or its equivalent through external interfaces (Netconf or gNMI).
- **timer pod**
  The timer pod scans the database for expired timers (for example, lease timeout, RADIUS interim update interval) and triggers a session management pod to start a transaction to handle the timer.

3.2.8 Prefix delegation as a framed route

When configured properly, the cMAG-c can signal a PD prefix as a framed route to the MAG-u.

When a PD prefix is allocated to a session, the cMAG-c can be configured to signal the PD prefix as a framed route instead of as an explicit session address to the MAG-u. When the PD prefix is signaled as a framed route, the MAG-u cannot identify that the signaled prefix originated from a DHCPv6 PD lease, and treats it as any other IPv6 framed route.

To have the PD prefix signaled as a framed route, enable the following command (set to **true**).

```
subscriber-management authentication-database entry address-assignment pd-as-framed-route
```

To optimize host resource consumption on a Nokia MAG-u, the framed route is signaled with a :: next-hop address. As with regular framed routes, it is a requirement that the following command is set to **false**.

```
subscriber-management authentication-database entry ip-anti-spoof
```

When no other IPv6 stack is available, the cMAG-c automatically installs the PD prefix as a regular IP address and not as a framed route on the MAG-u.

Related topics
AAA-based address assignment

3.3 Fixed access sessions

Learn about the key identifiers for fixed access sessions, IBCP tunnels, MAG-u selection, limits on the number of sessions, and the PPPoE and IPoE setup flows.

3.3.1 Layer 2 circuit

The Layer 2 circuit (l2-circuit) is the combination of the Layer 2 access ID and the VLAN parameters.

Fixed access sessions have direct Ethernet connectivity from the client device to the BNG. The cMAG-c assumes that the Ethernet connectivity is configured and makes an abstraction of the underlying technology and topology. The cMAG-c only needs the opaque Layer 2 access ID (l2-access-id) that uniquely identifies the access context of a session. The access context can be a port, a LAG, a pseudowire, an EVPN service, or anything that provides Ethernet connectivity. The MAG-u defines the content of the l2-access-id. The cMAG-c does not interpret it.

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

The l2-access-id is called the logical port in BBF TR-459. The cMAG-c is aware of all Ethernet parameters such as MAC address, S-VLAN, and C-VLAN. Nokia uses the l2-circuit for the combination of the l2-access-id and VLAN parameters.

For resilient sessions set up in the context of a UP group, the Layer 2 circuit can also refer to the unique combination of a UP group name and the VLAN parameters. This definition is used in contexts where a consistent Layer 2 circuit is required over the set of resilient MAG-u nodes; for example, for the enforcement of session limits.

3.3.2 In-band control plane and MAG-u selection

The cMAG-c creates IBCP tunnels per Layer 2 access ID for messages between the MAG-u and cMAG-c. Initial packets use these per-Layer 2 access ID tunnels. At session creation, the cMAG-c sets up a per-session tunnel. The MAG-u selection is based on the per-Layer 2 access ID tunnel used for the triggering packet.

Fixed access sessions send in-band cMAG-c messages over the connection to the MAG-u. As defined in BBF TR-459, the cMAG-c creates GTP-U tunnels (called IBCP tunnels) between the MAG-u and the cMAG-c to forward in-band cMAG-c messages.

The initial cMAG-c packets of a fixed access session are sent over the per-Layer 2 access ID IBCP tunnel associated with the Layer 2 access ID where that packet is received by the MAG-u. The cMAG-c automatically sets up the per-Layer 2 access ID IBCP tunnels for all learned Layer 2 access IDs of an existing PFCP association. Layer 2 access IDs are learned in the following way:

- From the **l2-access-id** configuration in the following context.

  ```
  subscriber-management ref-points up group
  ```

- From health reports sent by the MAG-u. See MAG-u health determination for more information.

When a Layer 2 access ID is no longer configured and not seen in consecutive health reports, the per-Layer 2 access ID tunnel is automatically removed by the cMAG-c.

Packets sent over the per-Layer 2 access ID tunnel signal metadata like the Layer 2 access ID itself, the local MAG-u MAC address, and the MAG-u node ID to the cMAG-c in an NSH header (as defined in BBF TR-459). The cMAG-c matches packets coming in over the per-Layer 2 access ID tunnel against a UP group and subsequently to an entry point (EP). The following applies:

- The UP group identifies interconnected UPs on which resiliency is available. This step is optional and if no UP group is matched, the session is set up only in the context of the UP associated with the incoming IBCP tunnel.
- The EP acts as a gateway mechanism and provides basic setup parameters. It is mandatory for a packet to match an EP.

The cMAG-c can instruct the MAG-u to forward only specified packet triggers over the IBCP tunnels and to ignore other triggers. For example, ignore IPoE triggers if only PPPoE is deployed or the other way around.

Configure the EP and triggers using the following commands.

```
subscriber-management ref-points up fixed-access entry-point
subscriber-management ref-points up fixed-access ibcp-triggers
```

The following example shows IBCP configuration that matches only IPoE control plane packets and matches them against an EP named fixed-access.

```
# info from running with-context /subscriber-management ref-points up fixed-access
```


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

```
    subscriber-management {
        ref-points {
            up {
                fixed-access {
                    entry-point fixed-access
                    ibcp-triggers {
                        ipoe-dhcp true
                        ipoe-dhcpv6 true
                        ipoe-router-solicit true
                    }
                }
            }
        }
    }
```

The cMAG-c sets up a per-session tunnel at session creation.

To get IBCP statistics for both the per-Layer 2 access ID tunnel and the per-session tunnel, use the following state tree.

```
subscriber-management ref-points up statistics ibcp
```

To clear the IBCP statistics, use the following command.

```
tools subscriber-management statistics clear ref-points up ibcp
```

When multiple MAG-u devices are managed by the same cMAG-c, each MAG-u has its own set of per-Layer 2 access ID tunnels. At session creation, the MAG-u selection is based on the triggering packet, as follows:

- If the triggering packet matches a UP group, the session is tied to an FSG of that UP group. The cMAG-c creates the session on the active (and optionally standby) MAG-u of the FSG.
- If the triggering packet does not match a UP group, the cMAG-c installs the session on the MAG-u that corresponds with the per-Layer 2 access ID tunnel on which the packet was received.

Related topics

BNG entry point

Modeling a resilient MAG-u deployment using UP groups

3.3.3 Session keys and anti-spoofing

Session keys identify and match data traffic to specific sessions, using different keys for IPoE and PPPoE sessions. The cMAG-c creates sessions and maps keys to ensure packets from different MAG-u nodes match the same session.

The cMAG-c creates a session when receiving the initial triggering packet for a specific session type. Fixed access sessions are, by default, identified by the key <MAG-u, Layer 2 circuit, MAC address>, for IPoE and PPPoE. If a session is set up in the context of a resilient UP group, the MAG-u and Layer 2 circuit keys are internally mapped to a common key based on the UP group configuration. This guarantees that packets coming from different MAG-u nodes within the same UP group match the same session.

When multiple PPPoE sessions share the same key, the remote ID or circuit ID attributes can be used to differentiate between the sessions. This is useful in scenarios where multiple devices behind a residential gateway need separate PPPoE sessions while sharing the same MAC address.

The circuit ID and the remote ID are derived from BBF vendor-specific tags 1 (circuit ID) and 2 (remote ID) as defined in TR 101.

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

To enable multiple PPPoE sessions per MAC address, use the following command.

```
subscriber-management entry-point entry pppoe multiple-sessions-per-mac
```

To configure the attribute to differentiate between multiple PPPoE sessions sharing the MAC address, use the following command.

```
subscriber-management entry-point entry pppoe multiple-sessions-per-mac discriminator
```

Example: Configuration example to enable multiple PPPoE sessions per MAC address

```
# info from running with-context /subscriber-management entry-point entry pppoe multiple-
sessions-per-mac
    subscriber-management {
        entry-point residential {
            entry default {
                pppoe {
                    multiple-sessions-per-mac {
                        discriminator circuit-id
                        limit 4
                    }
                }
            }
        }
    }
```

If multiple PPPoE sessions per MAC address are enabled, and no remote ID or circuit ID can be found, the cMAG-c sets up the session anyway and no other sessions for the same <UP, l2-circuit, MAC address> key can be set up.

Data plane rules on the MAG-u use the following keys to match data traffic to a specific session:

- IPoE: <l2-circuit, source MAC address> or <l2-circuit, source MAC address, source IP address>
- PPPoE: <l2-circuit, source MAC address, session ID> or <l2-circuit, source MAC address, session ID, source IP address>

To add the source IP address to the key, configure the following command to **true**.

```
subscriber-management authentication-database entry ip-anti-spoof
```

If not explicitly specified, the **ip-anti-spoof** command is enabled for all sessions.

3.3.4 Subscriber identification

The subscriber identification is by default equal to the session key, but you can define alternative subscriber keys..

For fixed access sessions, the subscriber key is by default equal to the session key, that is, there is a single session per subscriber.

The cMAG-c groups sessions under the same subscriber when the sessions share a common subscriber key. The following alternative subscriber keys can be used individually or in combination to identify sessions for the same subscriber:

- Layer 2 access ID
- MAC address
- S-VLAN

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

- C-VLAN
- circuit ID with optional string masking
- remote ID with optional string masking

To enable multiple sessions per subscriber and define alternative subscriber keys, use the commands in the following context.

```
subscriber-management entry-point entry multi-session-subscriber
```

Example: Multiple-sessions subscriber configuration with S-VLAN subscriber key

```
# info from running with-context /subscriber-management entry-point entry pppoe multiple-
sessions-per-mac
    subscriber-management {
        entry-point residential {
            entry default {
                multi-session-subscriber {
                    session-limit 8
                    multiple-session-key {
                        s-vlan true
                    }
                }
            }
        }
    }
```

Related topics

Subscribers

Session limits

3.3.5 Session limits

The cMAG-c enforces limits on the number of sessions. These limits can be configured within a specific scope; for example, per Layer 2 access ID.

Session limits are applied when the session is created, before authentication. Changing a session limit only affects new sessions. Existing sessions are not removed to align with new session limits.

Use the commands in the following context to configure the session limits.

```
subscriber-management entry-point entry
```

The cMAG-c applies the following session limits if they are enabled:

- **per MAC address**
  When enabled, multiple PPPoE sessions for the same MAC address are supported. By default, the support for multiple sessions per MAC is disabled. Use the **pppoe multiple-sessions-per-mac limit** command to limit the maximum number of sessions per MAC address.

  Note: See Session keys and anti-spoofing for more information about multiple sessions per MAC address.

- **per subscriber**

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

When enabled, multiple fixed access sessions for the same subscriber are supported. By default, the support for multiple sessions per subscriber is disabled. Use the **multi-session-subscriber session-limit** command to limit the maximum number of sessions per subscriber.

Note: See Subscriber identification for more information about enabling multiple sessions per subscriber.

- **per Layer 2 access ID**
  Use the **session-limits per-l2-access-id** command to set a limit for the maximum number of sessions per Layer 2 access ID (l2-access-id). The system limits the maximum number of sessions per Layer 2 access ID (for example, port) and the associated MAG-u. By default, two sessions with the same Layer 2 access ID on two different MAG-u nodes do not count for the same session limit. However, if sessions are set up in the context of a UP group, the system maintains the limit per UP group instead. In this case, two sessions with the same Layer 2 access ID on different MAG-u nodes in the same UP group count for the same session limit.
- **per Layer 2 circuit**
  Use the **session-limits per-l2-circuit** command to set a limit for the maximum number of sessions per Layer 2 circuit (l2-circuit). For sessions not set up in context of a UP group, the cMAG-c enforces the maximum number of sessions per Layer 2 circuit and the associated MAG-u. In this case , two sessions with the same Layer 2 circuit on two different MAG-u nodes do not count for the same session limit. For resilient session set up in context of a UP group, the cMAG-c enforces the limit on the UP group-based Layer 2 circuit as defined in Layer 2 circuit. In this case, the MAG-u via which the session is set up is not taken into account.
- **per UP**
  Use the **session-limits per-up** command to set a limit for the maximum number of sessions per MAG-u. When the sessions are set up in the context of a UP group, this limit applies to the UP group instead because sessions can dynamically move between MAG-u nodes in one UP group.

It is possible to configure conflicting limits for the same context. For example, two sessions with the same Layer 2 access ID can match two different BNG EP entries. Each entry can have a different per Layer 2 access ID limit. Both sessions count toward the Layer 2 access ID limit of each entry, but the enforced limit at session creation is the per Layer 2 access ID limit of the matching BNG EP entry for the session.

Limits enforced for nonresilient contexts and resilient UP group contexts are never mixed. For example, if a BNG EP is configured with a per-UP session limit of 100, the system allows up to 100 nonresilient sessions on that MAG-u, and another 100 resilient sessions on any UP group linked to that MAG-u.

Related topics

Session keys and anti-spoofing
Subscriber identification
Subscribers

3.3.6 IBCP rate limiting

For every IBCP packet that the cMAG-c receives, it applies a session rate limiter that drops the messages that exceed the token limit and removes the corresponding session. Consecutive deletions can trigger session lockout, as usual. See Session lockout for more information.

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

The rate limiter uses a basic token bucket algorithm where each IBCP packet represents a token. Each session has a maximum budget (burst size) of 100 IBCP packets and a refresh rate of one packet per second. To see the current remaining budget, use the state in the following context.

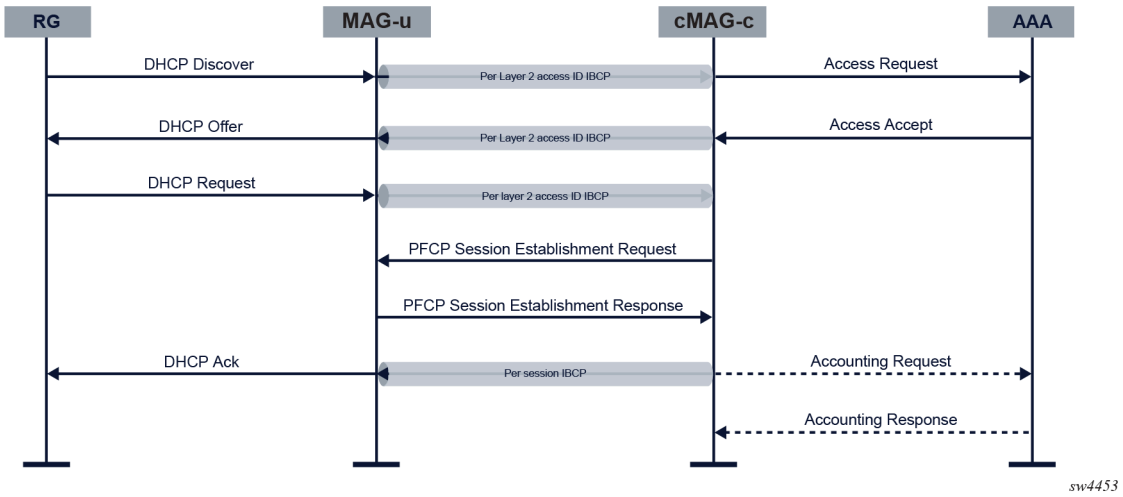
```
subscriber-management subscriber session ibcp-rate-limit
```

3.3.7 IPoE

IPoE does not involve a lower-layer connectivity protocol. Address assignment protocols and upstream data packets directly trigger IPoE sessions. The cMAG-c supports DHCP, DHCPv6, and ICMPv6 RS as triggering protocols.

The following figure shows an example of an IPoE session setup flow with DHCP as triggering protocol.

Figure 2: IPoE session setup with RADIUS authentication



When the cMAG-c receives the initial triggering packet over the per-Layer 2 access ID IBCP tunnel, the following actions are executed:

1. The cMAG-c matches the triggering packet with an EP, and creates an IPoE session using the configured keys. The cMAG-c assigns the EP and an IPoE profile. The IPoE profile defines the following behavior of the cMAG-c:
   - The cMAG-c sets dot1p and DSCP values in Ethernet and IP headers of CP messages to the IPoE client.
   - For packets that trigger session creation, the cMAG-c verifies the DHCP client Ethernet address (chaddr field). If the DHCP client Ethernet address does not equal the Ethernet source MAC address, the packet is dropped and no session is created.

   Use the following command to create an IPoE profile.

   ```
   subscriber-management profiles ipoe-profile
   ```


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

Use the following command to assign an IPoE profile to a session matching an EP entry.

```
subscriber-management entry-point entry ipoe profile
```

Note: If no IPoE profile is provisioned for a session, setup continues as if an IPoE profile with default values was provisioned.

2. The cMAG-c assigns a single authentication flow to the session and starts the authentication. Subsequent triggers for the same IPoE session do not trigger re-authentication.
3. The cMAG-c allocates addresses for the session.
4. The cMAG-c creates data plane rules and per-session IBCP tunnels on the MAG-u.
5. The cMAG-c assigns addresses over the per-session IBCP tunnel.
6. If accounting is provisioned, the cMAG-c starts accounting for the session.

The events in the following non-exhaustive list cause deletion of an IPoE session:

- The AAA triggers a failure; for example, RADIUS-initiated disconnect.
- An operator gives an explicit clear command for the session.
- No more DHCP or DHCPv6 lease is running; for example, because of a lease timeout or an explicit release message. Because of the lack of client-generated messages, SLAAC-assigned addresses are not tracked independently and require an active DHCP or DHCPv6 lease in the IPoE session.
- A session timeout has occurred.

Related topics

Session keys and anti-spoofing
Authentication
Address assignment
Accounting and charging

3.3.7.1 SHCV

Subscriber Host Connectivity Verification (SHCV) monitors the connection status of IPoE sessions and removes the appropriate stacks if a session is no longer connected while generating a log event.

The cMAG-c performs SHCV by instructing the user plane function (UPF) at the start of an IPoE session to periodically send ARP requests or Neighbor Solicitations (NS) to end devices. In the case of an IPv4 stack, an ARP request is sent to the device's assigned IPv4 address, whereas for IPv6 stack, an NS is sent to the device's link-local address. If there is no response and all retries fail, SHCV removes the appropriate stack and generates a log event in the syslog server.

Note: SHCV does not anticipate the IPv6 link-local address of end devices to change during an IPoE session. In case of such a change, the session must be re-established for SHCV to target the new address.

To configure how often (in minutes) SHCV checks for disconnected IPoE sessions, use the following command.

```
subscriber-management profiles shcv-profile periodic interval
```


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

The default is 30 minutes.

To configure how many times SHCV retries to get a response from an end device, use the following command.

```
subscriber-management profiles shcv-profile periodic retries
```

The default is two retries, in addition to the initial ARP request or NS.

Note: Because the initial ARP request or NS does not count as retrying, two retries means that an end device must fail to respond three times before the appropriate session is considered disconnected.

To configure how long (in seconds) SHCV waits for an end device's response to an ARP request or NS, use the following command.

```
subscriber-management profiles shcv-profile periodic timeout
```

The default is 10 seconds.

Changes in the SHCV configuration do not affect existing IPoE sessions.

3.3.8 PPPoE

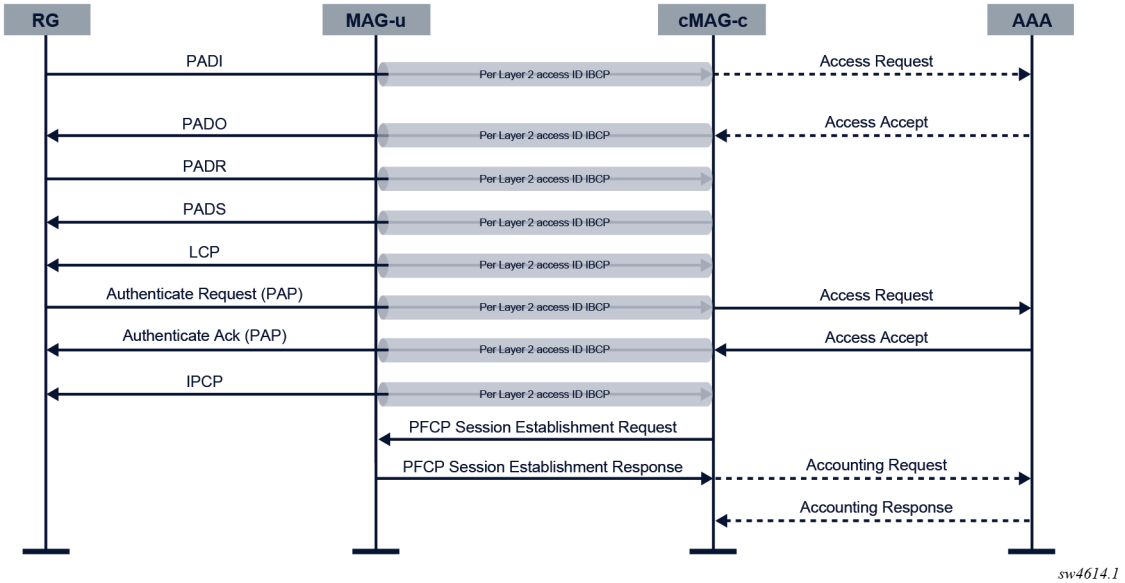
PPPoE session setup is linked with the PPPoE discovery protocol as defined in RFC 2516. PPPoE session setup consists of the following phases:

1. PPPoE discovery to enable PPP over Ethernet
2. PPP LCP negotiation to negotiate the PPP link connection
3. authentication
4. IP network connectivity using NCPs, such as Internet Protocol Control Protocol (IPCP) and IPv6CP; for IPv6 followed by IP assignment protocols, such as SLAAC or DHCPv6

The following figure shows an example PPPoE session setup flow for IPv4 network connectivity on a cMAG-c, using PAP as the authentication protocol.

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

Figure 3: PPPoE session setup flow



To initiate a PPPoE session, the residential gateway (RG) sends a PPPoE PADI discovery packet. The packet is sent over the default IBCP tunnel because no session context is known yet.

When the cMAG-c receives the initial triggering packet over the default IBCP tunnel, the following actions are executed:

1. The cMAG-c matches the triggering packet with an entry point. The entry point provides the PPPoE properties shown in the following table.

Table 3: PPPoE entry-point properties

Property	Description	Mandatory or Optional
pppoe-profile	The PPPoE profile contains properties for each phase in the PPPoE setup. It also specifies the dot1p value for all PPPoE control plane packets that the cMAG-c sends. If not provisioned the cMAG-c uses the default profile values.	O
authentication-flow	The authentication flow configuration contains PADI and PAP/CHAP authentication	
	PADI authentication	O
	PAP/CHAP authentication	M
allocation-scope	By default, the cMAG-c allocates a unique PPPoE session ID per combination of Layer 2 circuit ID and MAC address. When an aggregation device ignores MAC addresses and forwards based on PPPoE	—

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

Property	Description	Mandatory or Optional
	session ID only, the cMAG-c allocates a unique session ID per Layer 2 circuit.	
random	By default, the cMAG-c allocates the first free session ID within the allocation scope, starting with one. However, when randomization is configured, the cMAG-c allocates a random unique session ID within the scope.	—

Example: PPPoE entry point configuration

```
# info detail from running with-context /subscriber-management entry-point fixed-access
 entry default pppoe
    subscriber-management {
        entry-point fixed-access {
            entry default {
                pppoe {
                    profile example
                    authentication-flow {
                        pap-chap-adb [
                            basic-adb
                        ]
                    }
                    session-id {
                        allocation-scope l2-circuit-mac
                        random false
                    }
                }
            }
        }
    }
```

2. The cMAG-c allocates the PPPoE session ID. If a PPPoE session with the same key exists, the configuration of the PPPoE profile defines whether to delete or keep the existing PPPoE session. By default, the existing session is kept and the initial triggering PADI packet is ignored.

   To define the behavior in case of conflicts, use the following CLI.

   ```
   subscriber-management profiles pppoe-profile padi-removes-existing-session
   ```

3. If the authentication-flow configuration in the entry point requires PADI authentication, the cMAG-c performs the authentication and sends out the PADO. The following properties in the PPPoE profile apply:

   - **ac-name**

     By default, the AC name is the system name configured using the following CLI.

     ```
     subscriber-management system name
     ```

   - **generate-ac-cookie**

     By default, the generation of an AC cookie is enabled.

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

Example: Discovery configuration of a PPPoE profile

```
# info detail with-context from running /subscriber-management profiles pppoe-profile
 example discovery
    subscriber-management {
        profiles {
            pppoe-profile example {
                discovery {
                    generate-ac-cookie true
                    reply-on-padt false
                }
            }
        }
    }
```

4. The cMAG-c performs LCP negotiation as defined in RFC 1661 and RFC 4638. The following table describes the properties in the PPPoE profile.

Table 4: PPPoE profile LCP negotiation properties

Property	Description
max-mtu	The cMAG-c derives a downstream PPPoE MTU based on the maximum MTU value and the MRU the PPPoE client signals. If the MRU is smaller than the maximum MTU, the cMAG-c uses the MRU, otherwise the cMAG-c uses the maximum MTU. The cMAG-c sends the derived downstream PPPoE MTU to the MAG-u. The MAG-u applies the MTU on the downstream data path. **Note:** The MAG-u may enforce a lower MTU than the derived downstream PPPoE MTU; for example, because of port limitations. The cMAG-c does not learn this lower MTU and cannot send it as the MRU to the PPPoE client; therefore, Nokia recommends aligning the MAG-u and cMAG-c MTU configuration.
mru	To prevent the PPPoE client from sending packets that the MAG-u dropped, Nokia recommends aligning the MRU with the maximum packet size that a MAG-u can receive.
require-max-payload-tag	The **require-max-payload-tag** command defines whether an MRU above 1492 is negotiated. When enabled, the cMAG-c uses the PPP-Max-Payload tag, optionally received from the PPPoE client during PPPoE discovery, for MRU negotiations. See RFC 4638 for more information. When **require-max-payload-tag** is disabled, the cMAG-c sends the MRU as configured and accepts any MRU value. When **require-max-payload-tag** is enabled, the cMAG-c uses the value of the PPP-Max-Payload tag as a limit to MRU values. If the PPP-Max-Payload tag is not present, or if it is lower than 1492, the limit for MRU values is set to 1492. If the configured MRU is bigger than the limit, the limit is sent as the MRU. If the

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

Property	Description
	received MRU is bigger than the limit, the limit is used for the MTU calculations.
keep-alive	The **keep-alive** configuration options include an interval, a maximum number of tries, and a choice to ignore the value of received magic numbers. If no response is received after the configured number of tries, the session is considered disconnected and the cMAG-c terminates the PPPoE session.

Example: LCP negotiation properties in the PPPoE profile configuration

```
# info detail with-context from running /subscriber-management profiles pppoe-profile
 example lcp
    subscriber-management {
        profiles {
            pppoe-profile example {
                lcp {
                    max-mtu 1492
                    mru 1492
                    require-max-payload-tag true
                    keep-alive {
                        ignore-magic-numbers false
                        interval 30
                        tries 3
                    }
                }
            }
        }
    }
```

LCP renegotiation is not supported. After LCP negotiation completes and LCP enters the Opened state, the cMAG-c does the following when receiving an LCP Configuration Request message:

a. If the cMAG-c receives a message within a short interval after the LCP enters the Opened state, the cMAG-c assumes the message is a duplicate and drops it.

b. If the cMAG-c receives a message after a short interval, the message triggers the termination of the PPPoE session and subsequently restarts the full session.

5. The cMAG-c continues with authentication when the LCP stack is in the Opened state. Either PAP or CHAP authentication is required. The cMAG-c supports both the PAP (RFC 1334) and CHAP (RFC 1994) authentications. The cMAG-c negotiates the authentication protocol with the PPPoE client during the LCP link negotiation. The following **authentication method** parameters in the PPPoE profile define the priority in which PAP and CHAP are negotiated:

- **pap**

  The cMAG-c only requests PAP authentication during LCP link negotiation.

- **chap**

  The cMAG-c only requests CHAP authentication during LCP link negotiation.

- **pref-pap**

  During LCP link negotiation, the cMAG-c initially requests PAP authentication from the PPPoE client in an LCP Configure Request message. If the PPPoE client rejects PAP authentication with a

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

Configure Nak message and suggests using CHAP authentication instead, the cMAG-c sends a new LCP Configure Request message indicating to use CHAP authentication.

- **pref-chap**

  During LCP link negotiation, the cMAG-c initially requests CHAP authentication from the PPPoE client in an LCP Configure Request message. If the PPPoE client rejects CHAP authentication with a Configure Nak message and suggests using PAP authentication instead, the cMAG-c sends a new LCP Configure Request message indicating to use PAP authentication.

In the case of CHAP authentication, the cMAG-c generates a challenge with a random length within the range defined in the **chap-challenge-length** parameter of the PPPoE profile.

Example: Authentication properties in the PPPoE profile configuration

```
# info detail with-context from running /subscriber-management profiles pppoe-profile
 example authentication
    subscriber-management {
        profiles {
            pppoe-profile example {
                authentication {
                    method pref-chap
                    chap-challenge-length {
                        min 32
                        max 64
                    }
                }
            }
        }
    }
```

Both PAP and CHAP authentication are linked to the authentication flow.

6. After successful authentication, the cMAG-c starts the NCP stacks for the allocated addresses. PPPoE sessions support basic NCP renegotiation with the following limitations:

   - The cMAG-c never triggers renegotiation.
   - If the cMAG-c receives an NCP Configuration Request message within a short interval after the NCP enters the Opened state, the cMAG-c assumes the message is a duplicate and drops it.
   - Configuration Request messages received while the NCP stack is in the Opened state (beyond the short interval in which duplicates are dropped) are handled as per the RFC, and do not lead to a new IP address in the case of IPCP. Full IP renegotiation for IPCP requires an IPCP Terminate Request from the RG, followed by an IPCP Configuration Request.
   - When the only remaining NCP stack changes from the Opened to the Closed state, LCP termination is triggered.

   After successful IP allocation and negotiation, the cMAG-c installs the PFCP session on the MAG-u, and the MAG-u begins forwarding data-plane packets and handling LCP keepalive packets. Accounting starts if a charging profile has been provisioned during authentication.

Session termination

When it's necessary to terminate a PPPoE session, the cMAG-c fetches the final counters from the MAG-u and tears down the session by sending an LCP Terminate Request to the PPPoE client. The following non-exhaustive list of events cause the PPPoE session to terminate:

- reception of a LCP Terminate Request from the PPPoE client

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

- reception of a conflicting PADI if the configuration of the PPPoE profile defines the deletion of the existing PPPoE session in case of conflicts (**padi-removes-existing-session**)
- reception of a new LCP Configuration Request
- detection of an LCP keep-alive failure
- administrative removal; for example, RADIUS-initiated disconnect or clear commands
- charging quota exhaustion
- all NCP stacks changed from the Opened to the Closed state
- PFCP association loss between the MAG-u and the cMAG-c
- reception of a PADT from the PPPoE client

Note:
In this case, the **reply-on-padt** property in the PPPoE profile applies.

By default, the cMAG-c does not reply with a PADT.

LCP keep-alive offload

The cMAG-c offloads the LCP keep-alive function to the MAG-u, if the MAG-u signals the LCP keep-alive offload capability during the PFCP association.

Until the data plane session is created on the MAG-u, the cMAG-c typically responds to all LCP keep-alive requests. During the data plane session creation, the cMAG-c signals the LCP keep-alive offload to the MAG-u. After the LCP echo-session is installed on the MAG-u, the MAG-u starts answering incoming LCP keep-alive messages, and sends LCP keep-alive messages of its own, as needed. If a keep-alive message reaches the cMAG-c, the cMAG-c still answers it. This can happen, for example, in race conditions where the cMAG-c has already signaled the offload to the MAG-u, but the MAG-u has not yet fully installed it. The MAG-u forwards keep-alive packets until it has fully installed and enabled the offload.

Detection of an LCP keep-alive failure terminates the PPPoE session.

Resiliency based on PADO delay

PADO delay is a method to provision basic but deterministic (that is, determined from first use) MAG-u dual homing. A PADO delay value is provisioned during PADI authentication.

In MAG-u dual homing, a PPPoE client is connected to two MAG-u devices. The cMAG-c sends the PADO packet via one MAG-u device without delay and via the other MAG-u device with delay. The PPPoE client chooses the first received PADO and ignores the second received PADO. In stable conditions, the PADO delay determines a primary MAG-u choice with the option to fall back to a secondary MAG-u. The session setup continues on the primary MAG-u device. The feature is supported regardless of whether there is one cMAG-c device for both MAG-u devices or a different cMAG-c device per MAG-u device.

A prerequisite for deterministic MAG-u dual homing based on PADO delay is PADI authentication. If PADI authentication is not configured, the delay value is not known.

Note: PADI authentication is configured in the authentication-flow parameter of a PPPoE entry point.

```
subscriber-management entry-point entry pppoe authentication-flow padi-adb
```

To configure a delay for PADO packets, you can use one of the following options:

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

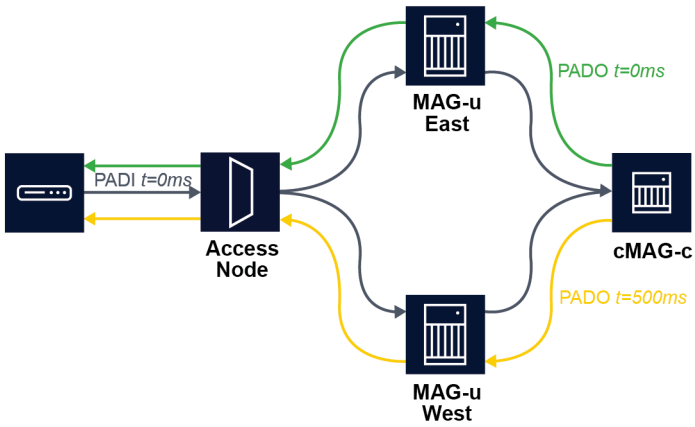
- Use the following CLI.

```
subscriber-management authentication-database entry pppoe pado-delay
```

- Provide the delay via the Alc-PPPoE-PADO-Delay VSA during RADIUS authentication.

The following figure shows an example of deterministic MAG-u dual homing. A PPPoE connection is dual homed to two MAG-u devices, called East and West. East and West share a common cMAG-c. The PPPoE client broadcasts the initial PADI to both MAG-u devices. The cMAG-c handles both PADIs and creates two sessions for it because they have different session keys. The session on East has no delay while the session on West has a 500 ms delay. The PPPoE client chooses the first received PADO sent via East. The session is established on East while the session on West times out. If the setup on East fails, the PPPoE client only gets the (delayed) PADO sent via West and the session is established on West.

Figure 4: Resiliency based on PADO



delay

IPCP subnet negotiation

IPCP subnet negotiation allows a BNG to assign an IPv4 subnet to a PPPoE session without the need for out-of-band provisioning (for example, using TR-69 signaling).

A prerequisite for IPCP subnet negotiation is to disable the IP address-based anti-spoofing functionality. To explicitly disable IP address-based anti-spoofing, set the **ip-anti-spoof** command to **false** in the following context.

```
subscriber-management authentication-database entry
```

The user can provision an IPCP subnet via an external AAA server, or use local address assignment through ODSA. To provision the subnet using local address assignment, configure an ODSA pool prefix with a target subnet-allocation length in the following context.

```
subscriber-management services network-instance pool ipv4
```

If the client signals support for IPCP subnet allocation, the cMAG-c signals the subnet using the non-standard IPCP sub-option 0x90. The cMAG-c selects the main session IP address from the subnet and signals it as the regular IPv4 address in IPCP option 0x03. The cMAG-c selects the main session IP address depending on the address-assignment type:

- the address in the Framed-IP-Address attribute, in the case of an AAA-assigned address

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

- the first address of the subnet, in the case of a local address assignment

On the MAG-u, the session is installed with the main session IP address as the session address and the remainder of the subnet as a framed route toward the main session IP address.

To include the main session IP address and the subnet mask in the Framed-IP-Address and Framed-IP-Netmask attributes of RADIUS accounting messages, respectively, enable the **address-information** command in the following context.

```
subscriber-management profiles charging-profile radius session include-attributes address-information
```

3.3.9 Application assurance for fixed subscriber sessions

The cMAG-c can assign an application assurance (AA) application profile to fixed IPoE and PPPoE sessions and send the profile to the MAG-u.

The cMAG-c supports dynamic assignment of an AA application profile (**app-profile**) for fixed IPoE and PPPoE subscriber sessions. The cMAG-c associates the application profile with the subscriber session on the cMAG-c, and sends it to the MAG-u. The MAG-u enforces AA for the session. The application profile must exist on the MAG-u.

The cMAG-c can receive the application profile in the following ways:

- During initial authentication, the cMAG-c can receive the application profile via RADIUS authentication, in the `Alc-App-Prof-Str` VSA in the Access-Accept message. The VSA is defined in the *7450 ESS, 7750 SR, and VSR RADIUS Attributes Reference Guide*.
- The cMAG-c can select an application profile when a configured ADB entry matches. Use the following command to configure the AA application profile in the ADB entry.

  ```
  subscriber-management authentication-database entry up-parameters app-profile
  ```

In a multi-ADB authentication flow, you can configure **app-profile discard** in a later ADB to discard a profile returned by an earlier ADB.

If an application profile is available from both RADIUS and the ADB, the profile received from RADIUS takes precedence.

The cMAG-c sends the assigned application profile to the MAG-u in the Nokia UP Profiles IE of the PFCP Session Establishment Request message, together with the subscriber profile and SLA profile.

The assigned application profile can be dynamically updated or removed for an existing session using RADIUS CoA. If the cMAG-c receives the `Alc-App-Prof-Str` VSA in a RADIUS CoA message with a value different from the current profile, it sends a PFCP Session Modification Request message with an updated UP Profiles IE containing the new application profile.

If the `Alc-App-Prof-Str` VSA contains the custom string `_tmnx_delete`, the cMAG-c sends a PFCP Session Modification Request message whose UP Profiles IE omits the application profile. This signals the MAG-u to remove AA for the corresponding hosts.

Dynamic updates or removal of the application profile in the ADB do not affect active sessions. The change takes effect only when the session is cleared and subsequently reconnects, or when the profile is changed with RADIUS CoA.

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

3.4 Address assignment protocols

A cMAG-c solution supports various address assignment protocols per session type.

Some address assignment protocols are specific to a session type (for example, IPCP for PPPoE) while other protocols are common for multiple session types (for example, SLAAC for IPoE and PPPoE).

The following table lists the supported address assignment protocols per session type.

Table 5: Address assignment protocols per session type

Address assignment protocol	IPoE session	PPPoE session
DHCP	✓	
DHCPv6 NA	✓	✓
DHCPv6 PD	✓	✓
SLAAC (see ICMPv6 Router Advertisements and SLAAC)	✓	✓

3.4.1 DHCP

The DHCP protocol, as defined in RFCs 2131, 2132, 3046, 4679, and 6842, is supported for IPv4 address assignment. The address allocation provides the address and the associated default gateway address. The subnet mask, as signaled in DHCP, is based on the micro-net subnet as provided by ODSA.

For messages sent by the cMAG-c, the source IP, the DHCP server IP option, and the siaddr option are by default equal to the default gateway. To override the default per service, use the following command.

```
subscriber-management services network-instance local-server-ip
```

The cMAG-c maintains a DHCP lease for every successfully negotiated DHCP transaction and extends the lease on renew or rebind. If a lease expires, the cMAG-c considers the IPv4 address for the session down and takes appropriate actions for the corresponding session (for example, bring the session down).

The following sources define the DHCP options sent in messages to the client:

- explicit option values provided by authentication sources
- bulk options signaled during authentication; for example, via the RADIUS Alc-ToClient-Dhcp-Options VSA
- bulk options derived from a locally configured DHCP profile using the following command

  ```
  subscriber-management profiles dhcp-option-profile
  ```

- DNS options from local address assignment (used in ODSA)

DHCP Offer and Ack messages to the client are constructed using the explicit option values. The option values of the two bulk sources (authentication and DHCP profile) are appended after the explicit option values.

The following rules apply to the options:

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

- Only one source can provide DNS or NBNS. If a source with higher priority provides DNS or NBNS, DNS or NBNS are filtered out of lower-priority bulk options if present. The sources have the following priority:
  1. explicit options
  2. authentication bulk options
  3. DHCP profile options
  4. local address assignment options
- Lease time, renew, and rebind timers are only provided by explicit per-session authentication sources and are filtered out of bulk options if present.
- Specific options cannot be configured in the message and are filtered out of authentication bulk options. Overriding these options leads to incorrect DHCP behavior. Examples of these options are subnet mask, router, and DHCP message type.

Related topics

Address assignment

3.4.2 ICMPv6 Router Advertisements and SLAAC

The cMAG-c periodically generates ICMPv6 Router Advertisements (RA) messages when an IPv6 address is allocated for the session. A client can trigger the generation of an ICMPv6 RA message by sending an ICMPv6 Router Solicitation (RS) message, but this is not mandatory.

Note: RFC 4861 and RFC 4443 define the ICMPv6 RA messages.

The client uses the source address of the ICMPv6 RA message as its default gateway address. By default, this source address is a link-local address derived from a hash of the cMAG-c system name. The cMAG-c installs the link-local address on the MAG-u via PFCP so the MAG-u can answer any ND request for it.

In some cases, this may lead to address conflicts; for example, when two MAG-u nodes are connected to the same Layer 2 aggregation. To solve this, you can override the link-local address using the following command.

```
subscriber-management authentication-database entry up-parameters link-local-address
```

The cMAG-c installs the override on the MAG-u via PFCP. While this allows very granular overrides, a Nokia MAG-u can only have one unique link-local address per network instance.

ICMPv6 RA messages use an RA profile. The RA profile is assigned to a session during authentication. To configure the RA profile in the ADB, use the following command.

```
subscriber-management authentication-database entry ra-profile
```

If no RA profile is retrieved during authentication, the session behaves as if it is using an RA profile with all default values.

Use the following command to configure the RA profile locally.

```
subscriber-management profiles ra-profile
```


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

The RA profile defines the following parameters:

- **advertisement-interval min** and **advertisement-interval max**

  These parameters define the interval between periodical unsolicited ICMPv6 RA messages. The cMAG-c sends periodical unsolicited ICMPv6 RA messages with a random interval between the configured **min** and **max**. The random interval is regenerated after every unsolicited RA message.

  By default, the maximum advertisement interval is 600s and the minimum advertisement interval is 33% of the maximum interval.

- **force-unicast-mac**

  This parameter defines which MAC address to use.

  If **force-unicast-mac** is enabled, the cMAG-c sends ICMPv6 RA messages to the unicast MAC address of the session, otherwise the cMAG-c sends the ICMPv6 RA messages to the all-nodes multicast MAC address (33:33:00:00:00:01).

  To avoid sending ICMPv6 RA messages to the wrong client, the **force-unicast-mac** parameter is enabled by default.

  Note: The destination IP address is always the all-nodes multicast IP address (FF02::1).

- **router-lifetime**

  This parameter defines the validity period of the default router after receipt of the ICMPv6 RA message. By default, the **router-lifetime** is equal to (**advertisement-interval max** × 3).

- **reachable-time** and **retransmit-timer**

  The **reachable-time** parameter defines the period that a neighbor can be reached after receiving a reachability confirmation.

  The **retransmit-timer** parameter defines the interval between retransmitted NS messages.

  By default, both parameters are set to zero, that is, the cMAG-c does not specify a value, and the client can choose a value based on local configurations.

- **hop-limit**

  This parameter defines the value of the Hop Limit field in the outgoing ICMPv6 RA messages.

  By default, the **hop-limit** value equals 255 hops.

- **mtu**

  This parameter defines whether the MTU option is included in the ICMPv6 RA messages and, if included, what value the MTU option contains. By default, the MTU option equals **not-included**.

- **other-configuration**

  This parameter defines whether the O flag (other configuration) in the ICMPv6 RA message is enabled. If the O flag is enabled, a client can receive options via DHCPv6 without acquiring an address via DHCPv6; for example, in combination with SLAAC based address assignment. By default, the **other-configuration** parameter is disabled. To indicate whether address assignment via DHCPv6 is available, the related M flag (managed address configuration) is automatically set if a DHCPv6 IA-NA or an IA-PD prefix was allocated to the session.

- **on-link**

  This parameter defines whether the L (on-link) flag is set in the SLAAC prefixes that are present in the ICMPv6 RA messages.

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

By default, this flag is set.

When an SLAAC address is allocated to the client, each ICMPv6 RA message includes the SLAAC prefix with the A (autonomous address-configuration) flag enabled. With the A flag enabled, the client can autonomously allocate an IPv6 address from the signaled SLAAC prefix (as defined in RFC 4862).

The SLAAC prefix contains the preferred and valid lifetime that is learned during authentication. The default values of the preferred and valid lifetime are equal to 7 and 30 days respectively.

Note: Nokia recommends that the preferred lifetime is at least double or more than the configured maximum advertisement interval. This avoids the expiration of the preferred lifetime on the client side because of the loss of a single ICMPv6 RA message.

The ICMPv6 RA messages do not contain any other prefixes. A prefix that is derived from either DHCPv6 IA-PD or IA-NA, is not present.

The ICMPv6 RA messages include all IPv6 DNS servers that are discovered during session authentication (as defined in RFC 8106).

3.4.3 DHCPv6

The cMAG-c supports the DHCPv6 protocol, as defined in RFC 8415, with additional support for a lightweight DHCPv6 relay agent (LDRA) between the DHCPv6 client and the MAG-u/cMAG-c as defined in RFC 6221.

Within the DHCPv6 lease, the following is signaled to the client:

- an allocated IA-NA address, an IA-PD prefix, or both
- preferred and valid lifetimes
- IPv6 DNS servers
- DUID of the server

Preferred and valid lifetimes can be locally configured or received from an external AAA server in the Alc-v6-Preferred-Lifetime and Alc-v6-Valid-Lifetime VSAs. To locally configure the lifetimes, use the **valid-lifetime** and **preferred-lifetime** commands in the following context.

```
subscriber-management authentication-database entry address-assignment ipv6-lifetimes
```

Valid and preferred lifetimes are common for all IPv6 addresses of a session.

The server DUID is by default based on the cMAG-c system name. To override the default server DUID per service, use the following command.

```
subscriber-management services service dhcpv6-server-duid
```

The cMAG-c maintains a DHCP6 lease for every successfully negotiated DHCPv6 transaction and extends the lease on renew or rebind. The lease time is based on the IPv6 valid lifetime. If a lease expires, the cMAG-c considers the IA-NA address or IA-PD prefix for the session down and takes appropriate actions for the corresponding session (for example, remove dataplane state, bring the session down, or bring IPv6CP down).

DHCPv6 options can come from multiple sources. The following sources define the DHCPv6 options sent in messages to the client:

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

- explicit option values provided by authentication sources
- bulk options signaled during authentication; for example, via the RADIUS Alc-ToClient-Dhcp6-Options VSA
- bulk options derived from a locally configured DHCP profile using the following command

```
subscriber-management profiles dhcpv6-option-profile
```

- DNS options from local address assignment (ODSA)

DHCPv6 Advertise and Reply messages to the client are constructed using the explicit option values. The option values of the two bulk sources (authentication and DHCPv6 profile) are appended after the explicit options.

The following rules apply to the options:

- Only one source can provide DNS. If a source with higher priority provides DNS options, they are filtered out of lower priority bulk options if present. The sources have the following priority:
  1. explicit options
  2. authentication bulk options
  3. DHCPv6 profile options
  4. local address assignment options
- Identity association (IA) options, server DUID, server unicast, relay message, status code, interface ID, and other similar options are filtered out of the bulk options because these must be in full control of the cMAG-c.
- In case of LDRA, all options are included in the relayed message.

If an IA-PD prefix or IA-NA address is allocated, the cMAG-c sends ICMPv6 RA messages so the client can learn its default gateway address. For consistency, the cMAG-c sends DHCPv6 messages with a link-local address that is the same as the source address in ICMPv6 RA messages.

Related topics

DHCP

ICMPv6 Router Advertisements and SLAAC

3.5 Call trace

The cMAG-c supports call trace, an advanced debugging feature that supports tracing of CP packets and events during the lifetime of a session.

Call trace is an advanced debugging tool that provides detailed inspection of all the transactions of single sessions. It correlates multiple protocols and internal events in a single interface. All the pods that process call trace sessions decide whether a specific packet or event is traced. At a high-level, call trace consists of the following major elements:

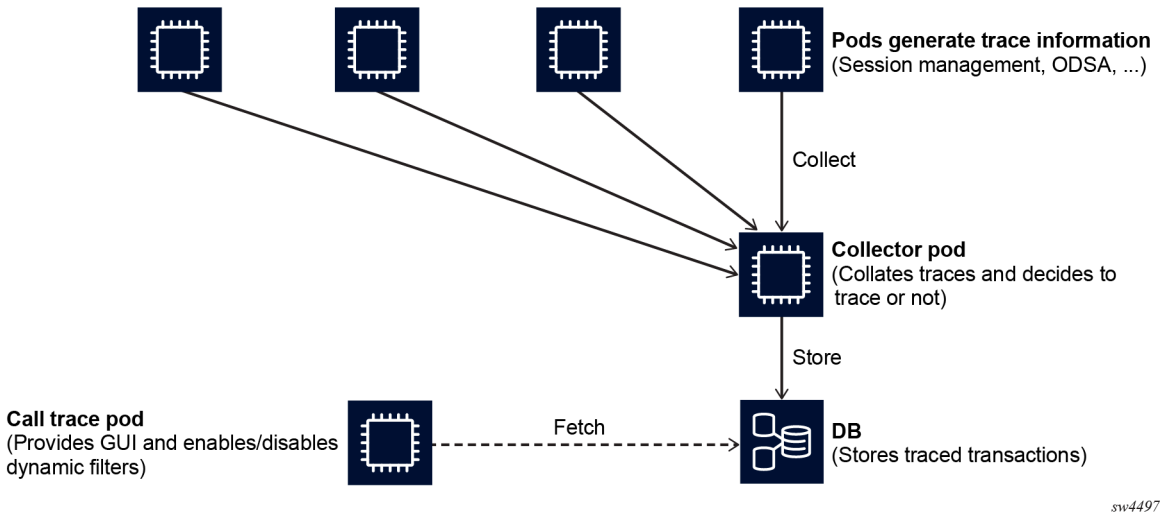
- Pods, including the session management, ODSA, and so on, generate trace information.
- One or more collector pods collect the individual trace candidates and correlate them to a single transaction and session. When a transaction finishes, the pod makes the final decision about whether to trace or discard the transaction.
- The cMAG-c database stores all the traced transactions. See "cMAG-c high level architecture" in the *cMAG-c Overview Guide* for more information about the cMAG-c state retention architecture.

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

- The call trace pod provides a GUI to inspect the traced transactions and manage the capture filters.

The following figure shows the high-level elements for call tracing.

Figure 5: High-level call trace elements



3.5.1 Always-on tracing

All the pods that participate in the processing of session transactions assess each transaction to determine whether it is subject to tracing. To ensure that every transaction is automatically subject to tracing, the always-on tracing mode is enabled by default. The user can change the configuration of this mode to conserve resources, as needed.

Every pod that participates in processing a session transaction must decide whether the transaction is potentially subject to tracing. The easiest way to accomplish this is to use the default **always-on enabled** tracing mode. This mode automatically assumes that every transaction is potentially subject to tracing.

Example: Always-on tracing enabled

```
# info from running /subscriber-management call-trace always-on
    enabled {
    }
```

The benefit of always-on tracing is the traces are only evaluated upon finalizing a transaction. This allows advanced tracing capabilities such as the following:

- Trace transactions based on parameters that are not available in each packet, such as a username or subscriber name. See Managing session tracing filters for more information.
- Trace any transaction that is considered failed, regardless of the point at which the failure occurs. See Enabling automatic tracing based on error conditions for more information.

The disadvantage of always-on tracing is it consumes resources to send transactions to the collector pods. If enough resources are available, Nokia recommends to keep always-on tracing enabled. However, if insufficient resources are available, you can completely disable always-on tracing.

Use the following CLI to disable always-on tracing. With this option, only the always-available filters are subject to tracing; see Managing session tracing filters.

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

Example: Always-on tracing disabled

```
# info from running /subscriber-management call-trace always-on
    disabled
```

The **always-on disable** option only has an effect if a transaction does not match an always-available filter, as described in Managing session tracing filters. If a transaction matches an always-available filter, it is traced regardless of the enabled or disabled state of the always-on configuration.

3.5.2 Packet tracing

You can use the cMAG-c CLI to manage the configuration of the default call trace packet-tracing options.

By default, the cMAG-c captures packets as part of all the traced transactions. You can use the commands in the following context to change the packet-tracing properties.

```
subscriber-management call-trace packet-tracing
```

The following are examples of reasons you may want to disable packet capturing for traced transactions, and the properties to use to do so:

- If you need to lower the resource impact of always-on tracing, use the **packet-tracing default-off** property. This disables the default packet-tracing functionality, while allowing session filters to explicitly enable packet tracing using the CLI or the GUI tool.

  ```
  subscriber-management call-trace packet-tracing default-off
  ```

  See Managing session tracing filters for information about how to configure call trace filters for specific sessions.
- If you need to fully disable packet tracing to manage privacy or regulatory requirements, use the **packet-tracing disallowed** property. This disables all packet tracing, and prevents individual session filters from enabling it.

  ```
  subscriber-management call-trace packet-tracing disallowed
  ```

3.5.3 Enabling automatic tracing based on error conditions

The cMAG-c provides the ability to configure automatic tracing based on error conditions, when always-on tracing is enabled. For example, it is possible to automatically trace any session transaction that leads to a failure, and to manage the duration of tracing transactions.

Enabling automatic tracing based on any error

When always-on tracing is enabled, it is possible to configure the tracing functionality to automatically trace any session transaction that leads to a failure. To enable tracing based on any error condition, set the **any-error** property to **true**.

```
subscriber-management call-trace any-error true
```


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

When **any-error** is enabled, the system traces any transaction that does not lead to an expected result, as internally determined by the cMAG-c; for example, a PFCP or RADIUS communication times out or is rejected.

Example: Any-error tracing configuration

```
# info from running /subscriber-management call-trace
    any-error true
    always-on {
        enabled {
        }
    }
```

Configuring automatic tracing based on maximum duration

When always-on tracing is enabled, it is possible to configure a maximum duration for packet tracing. When a maximum duration is specified, the system traces any transaction that takes longer than the configured value. This is useful for debugging transactions that incur timeouts or very high latency but cannot be associated with specific sessions. To use automatic tracing based on a maximum duration, configure the **max-duration** property to the required value (in milliseconds).



WARNING: Nokia cautions against permanently enabling duration-based tracing. Only use duration-based tracing to debug specific issues, and then disable it immediately afterwards. Because high-latency transactions can naturally occur in a network, for example, in the case of routing updates, a majority of transactions are fully traced when duration-based tracing is enabled, which is not recommended.

Example: Maximum transaction duration configuration

```
# info from running /subscriber-management call-trace
    max-duration 5000
    always-on {
        enabled {
        }
    }
```

3.5.4 Accessing the call trace GUI

About this task

Use this procedure to open the Call Trace GUI.

Procedure

Step 1. Open a browser and go to the web UI domain name.

The domain name is the value of the `domain` field under the `webUI` node in the preset file. See "Preset file" in the *cMAG-c Installation Guide* for more information. If you did not install the cMAG-c, obtain the domain name from the administrator who performed the installation.

Step 2. Log in using credentials that are authorized to access the Call Trace GUI.

See Accessing the cMAG-c GUI for more information about how to provision an authorized user.

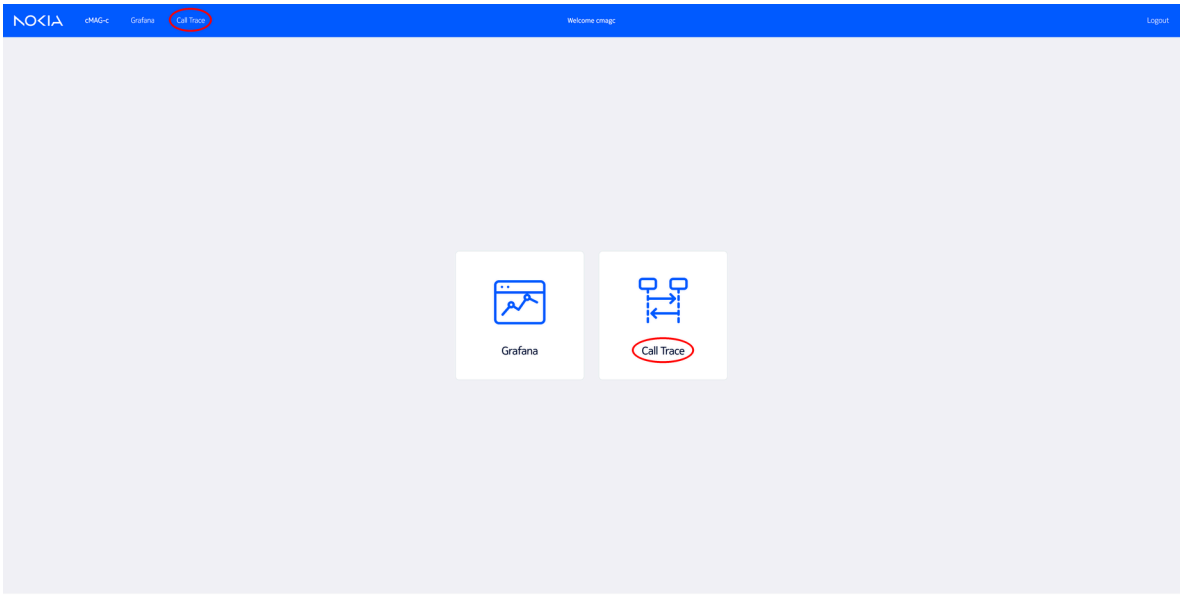
Step 3. Navigate to the Call Trace GUI by clicking any of the call trace links.

The following figure shows the Call Trace links on the GUI landing page.

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

Note: If you do not see Call Trace in the GUI, verify that you have access to the call trace role. See Accessing the cMAG-c GUI for more information about that role. Then log out and log in again.

Example



3.5.5 Managing session tracing filters

The cMAG-c provides session filters with configurable options for matching the sessions to trace. You can use the CLI or the cMAG-c Call Trace GUI tool to manage filters for session tracing.

It is possible to always trace specific sessions, whether they fail or not. To do this, use the CLI or the GUI tool to enable the applicable filters. Filters provisioned using the CLI are referred to as static filters, while filters provisioned using the GUI tool are referred to as dynamic filters. Static filters cannot be modified using the GUI and dynamic filters cannot be modified using the CLI.

A filter provides the following configurable properties for matching the sessions to trace:

- options that are always available:
  - MAC address
  - UP node ID
  - Layer 2 access ID
  - C-VLAN
  - S-VLAN
- options that are only available when the **always-on** property is enabled:
  - subscriber name
  - username

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

The configuration may include multiple options that must all match (logical AND) for a transaction to match the filter. A filter is considered always available only if all its configured options are always available. If even one option requires always-on tracing, the entire filter requires always-on tracing.

To administratively disable a static filter entry without removing it, specify the **disable** option for the **admin-state** command.

```
subscriber-management call-trace filter admin-state disable
```

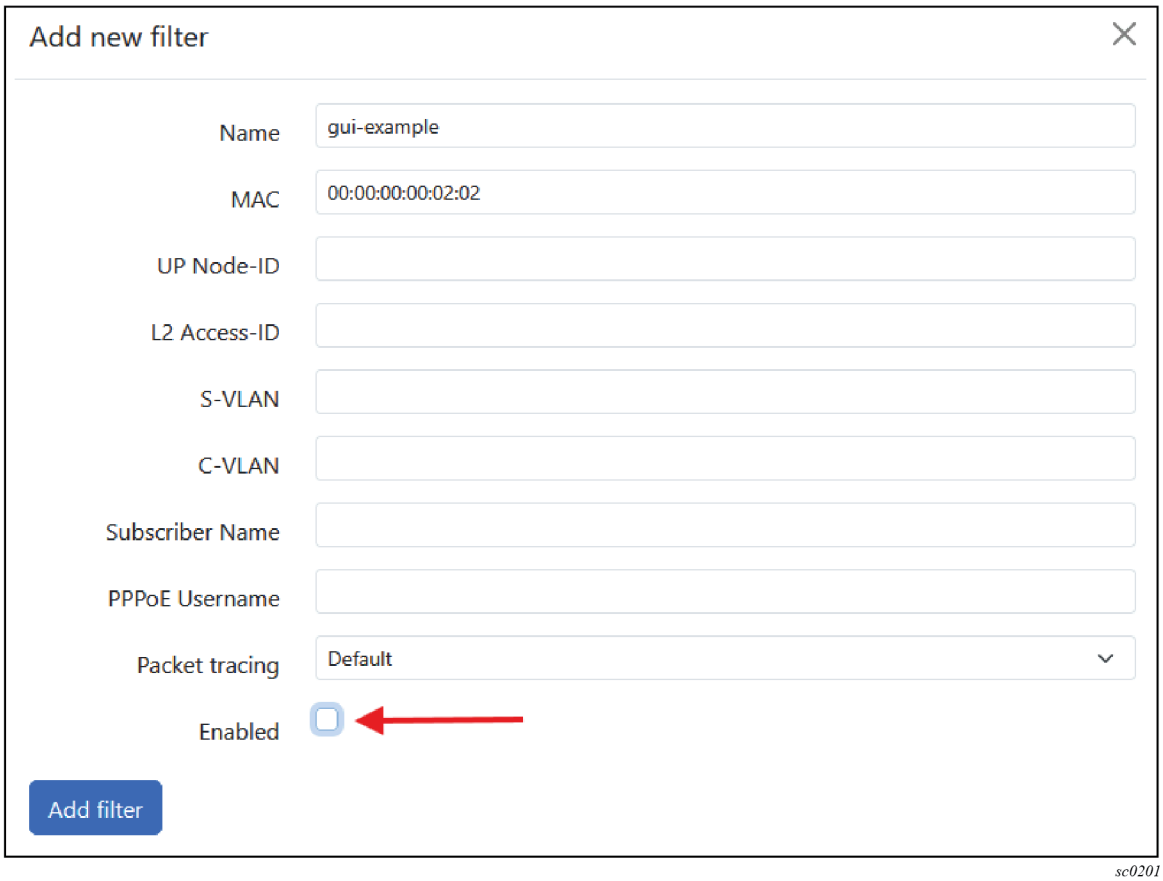
You can use the GUI tool to administratively disable dynamic filters.

1. Navigate to the **cMAG-c Call Trace Configuration** window in the GUI tool.
2. Under **Dynamic filters**, select the edit icon beside the filter.
3. Uncheck the **Enabled** check box in the **Add new filter** window; see the following figure.

See Managing dynamic filters using the Call Trace GUI tool for more information about using the GUI tool to manage filters.

Note: When debugging is complete, Nokia recommends fully removing the filter entry. Do not leave the entry permanently in the administratively-disabled state.

Figure 6: Administratively disabling a filter using the Call Trace GUI tool



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

3.5.5.1 Managing static filters using the CLI

Prerequisites

See Managing session tracing filters to learn about managing specific session filters, if needed.

About this task

You can enable, modify, or delete a static call trace filter using the CLI.

Procedure

Step 1. Create or navigate to a filter entry.

```
subscriber-management call-trace filter name
```

Example

```
subscriber-management call-trace filter example
```

Step 2. Specify the match options under the new filter entry.

The following example shows a configuration to capture transactions for sessions with a specific MAC address.

Example

```
# info from running /subscriber-management call-trace filter example
    mac 00:00:00:00:01:01
```

Step 3. Commit the configuration.

Step 4. Optional: To delete a specific filter entry, use the following CLI command to remove it from the configuration, and then commit the changes.

```
subscriber-management call-trace delete filter example
```

3.5.5.2 Managing dynamic filters using the Call Trace GUI tool

Prerequisites

See Managing session tracing filters to learn about managing specific session filters.

About this task

You can use the cMAG-c Call Trace GUI tool to create, modify, or delete dynamic call trace session filters.

Procedure

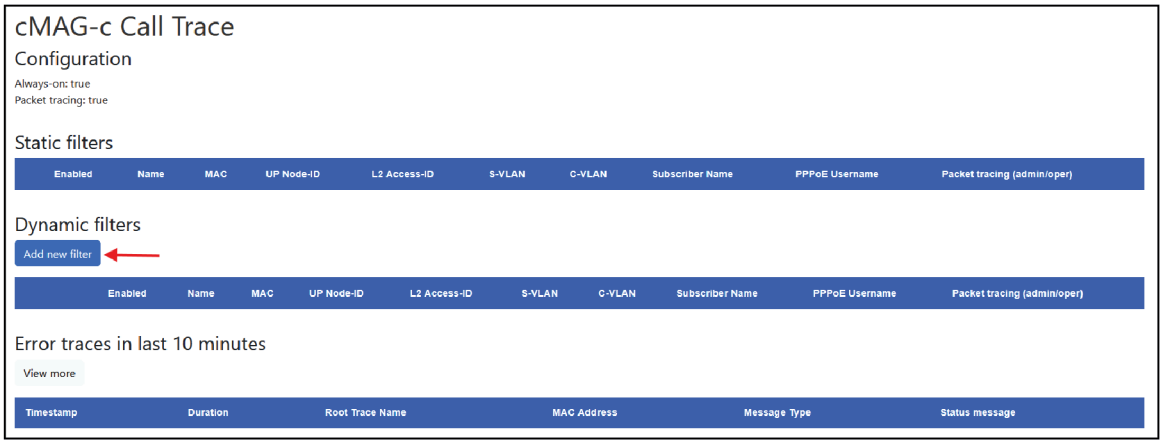
Step 1. Navigate to the **cMAG-c Call Trace Configuration** window in the GUI tool.

Step 2. To add a new filter, use the following steps.

a. Under **Dynamic filters**, click the **Add new filter** button.

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

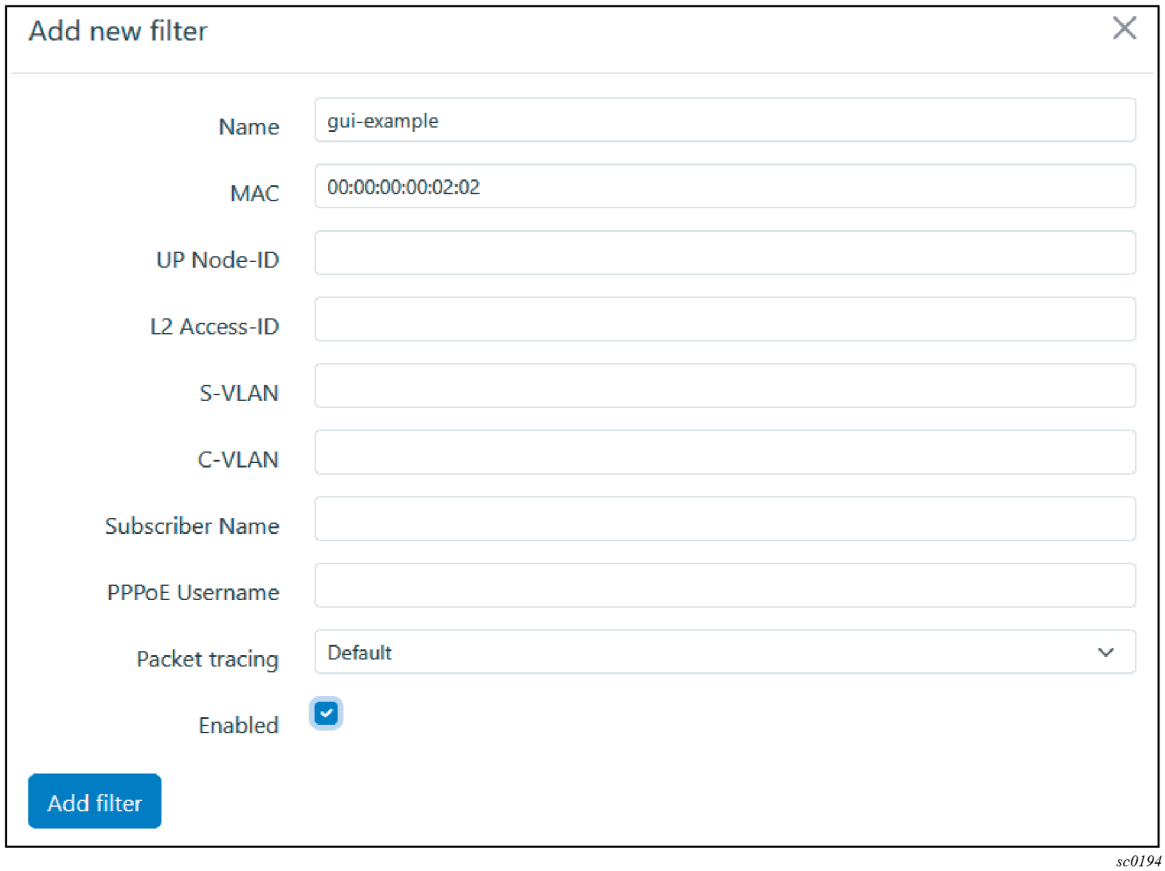
Example



sc0187

b. Enter the filter name in the form and at least one filter parameter.
The subscriber name and username can only be entered if the always-on mode is enabled.

Example



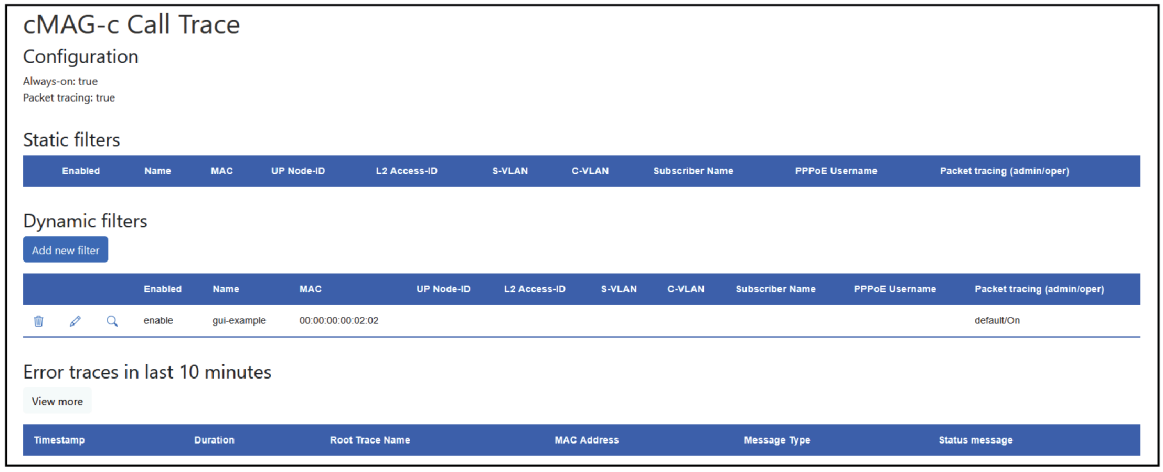
sc0194

c. Click the **Add filter** button to create the new filter entry.

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

The dynamic filter becomes visible in the list of filter entries.

Example

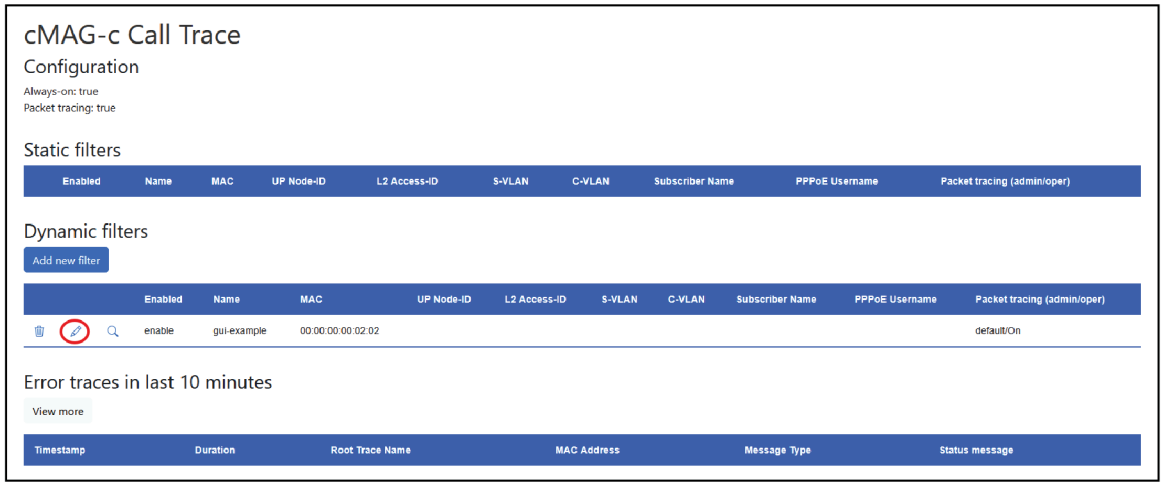


sc0192

Step 3. To modify an existing filter, use the following steps:

a. Select the edit icon next to the filter entry.

Example



sc0195

b. Change the filter information as needed (see 2.b for information about the parameters) and click the **Modify filter** button.

Step 4. To delete a filter, do the following steps:

a. Select the delete icon beside the filter entry.

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

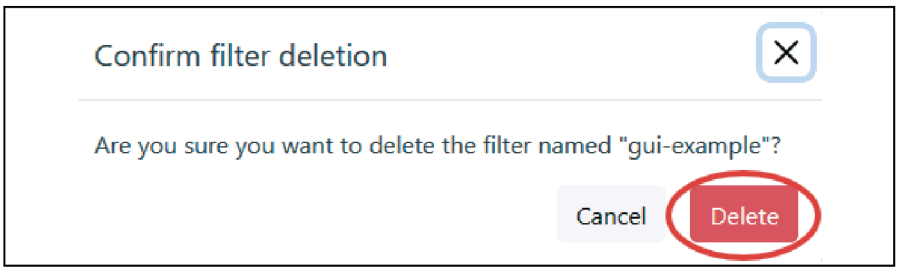
Example



sc0193

b. Select **Delete** to confirm that you want to proceed with the deletion.

Example



sc0191

Troubleshooting

The following are examples of the conditions when an existing dynamic filter could become inconsistent with the base call trace configuration in CLI:

- The dynamic filter in the GUI is set to enable packet capture, while the CLI configuration is changed to always disallow packet capture.
- The dynamic filter in the GUI specifies a match criterion that requires always-on tracing, while the CLI configuration is changed to disable always-on tracing.

In cases such as these, the cMAG-c automatically disables the filters and no longer captures new transactions. However, the filters are not removed from the system and you can still inspect the previously-captured transactions.

3.5.6 Inspecting call trace captures

Use the Nokia Call Trace GUI tool to inspect the details of call trace captures.

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

3.5.6.1 Searching for session traces

About this task

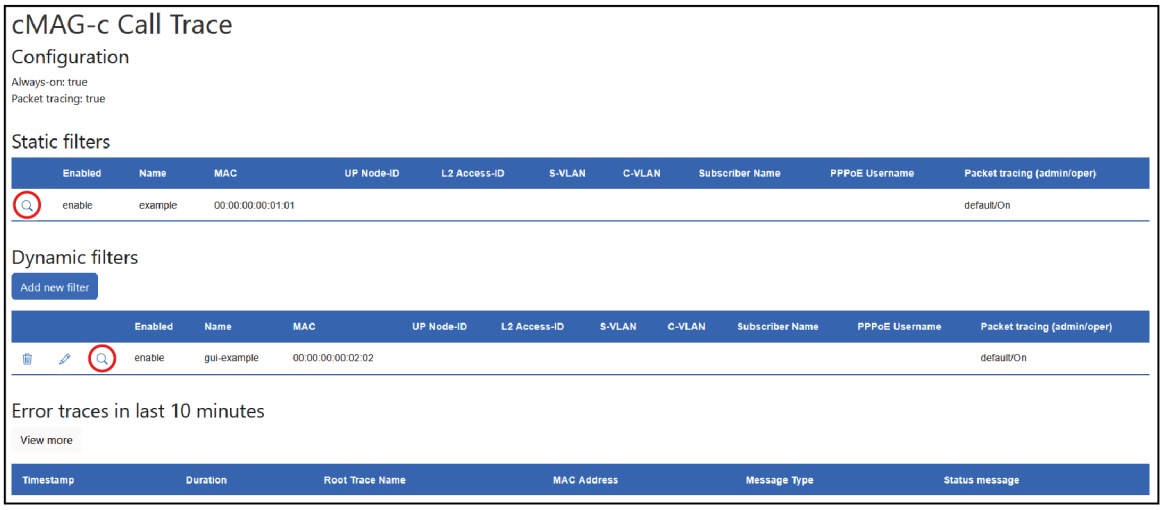
Use the cMAG-c Call Trace GUI tool to locate and perform analysis of the call-trace captures for a session.

Procedure

Step 1. Navigate to the Call Trace GUI tool.

Step 2. Select the magnifying glass icon next to the filter to see all traces for the filter.

Example



sc0202

Expected outcome

The GUI tool displays a list of captured transactions for the session with the following information:

- capture timestamp
- duration of the captured transaction
- incoming service that started the capture
- name of the captured procedure
- message type that initiated the transaction
- if the transaction was faulty or not, with an applicable error message if faulty

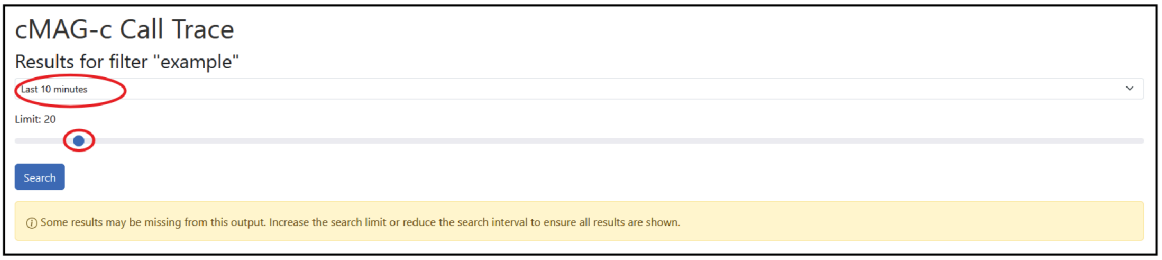
Step 3. Optional: If you want to display more traces, do one of the following:

- Use the drop-down menu to change the maximum-trace age.
- Use the slider to change the maximum number of traces.

Note: By default, the tool only shows a limited number of recent traces.

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

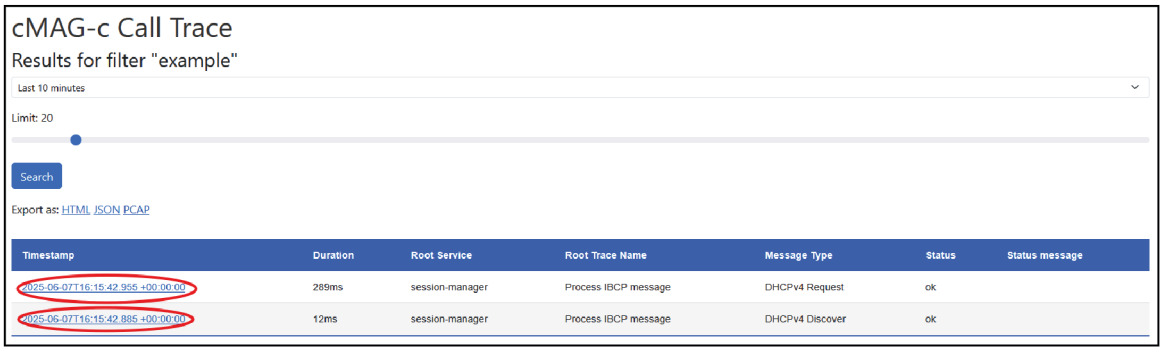
Example



sc0200

Step 4. From the list of traces, select the timestamp for a specific trace to display detailed information about it.

Example



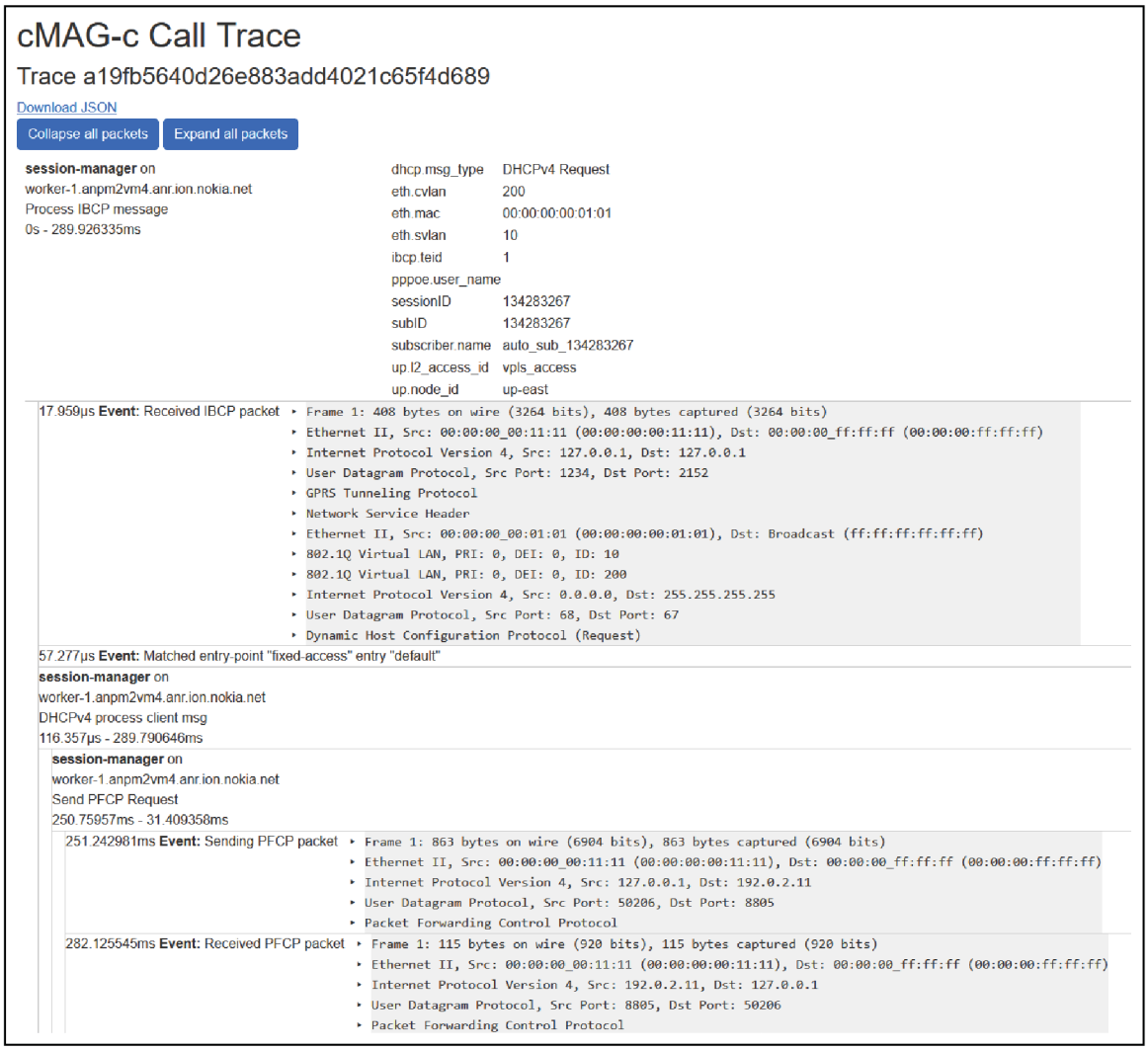
sc0188

Expected outcome

The following example shows the details of a specific traced transaction, including packet captures, if enabled; see Enabling automatic tracing based on error conditions.

See Reviewing the details of a trace for more information about the trace details.

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



sc0198

3.5.6.2 Reviewing the details of a trace

After navigating to a detailed trace as described in Searching for session traces, the detailed view of the trace events is displayed.

The trace details include relevant information for each captured event, such as the following:

- event timestamp within the trace and the optional duration
- the relevant packets for the event
- the pods handling the event

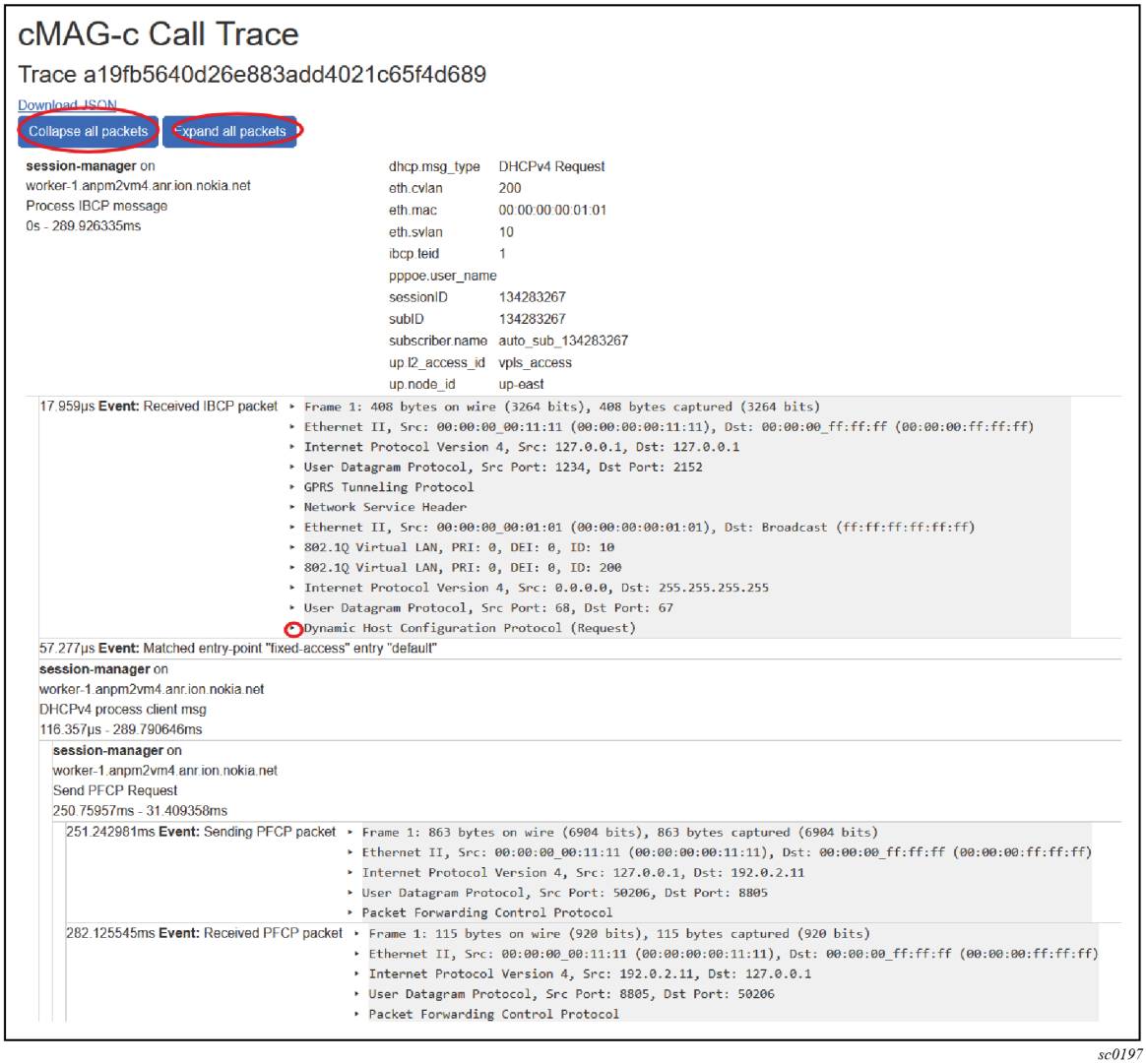
Each trace usually consists of one initial event with a series of sub-events. For example, the trace shown in the following figure has one main event, traced by the session manager, detailing the session data and the captured procedure (IBCP processing). The trace in the figure further consists of multiple sub-events:

- The first event shows the details of a received IBCP packet (DHCP Request).

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

- The second event shows an entry point lookup was done for an entry named “default”.
- The third event shows further processing of the DHCP request within the session management pod. For illustration purposes, the event shows the first of multiple sub-events. The first sub-event shows handling of a PFCP Session Establishment transaction that also consists of two sub-events, one for sending the outgoing PFCP request message, and one for handling the incoming PFCP response message. Both sub-events also show the PFCP packet details.

Figure 7: Viewing event details in the Call Trace tool



sc0197

By default, only a summary of each protocol layer in a traced packet is displayed. To expand the details for all the traced packets:

- For a specific layer, select the arrow next to it.
- For all layers of all packets, click the **Expand all packets** button.

To collapse the details of all layers of all packets, click the **Collapse all packets** button.

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

3.5.7 Trace retention

When the collector pod traces a transaction, it stores the traced transaction record in the cMAG-c database. Traces can contain sensitive, user-identifying information such as IP addresses or subscriber names. To comply with various privacy regulations, it is important to apply correct retention policies. The cMAG-c offers multiple options for configuring the trace transaction retention policy.

- Configure the **timeout** value to specify how long traces are retained before they are automatically removed. By default, a timeout of 72 hours is configured. It is not possible to disable the **timeout** option.

  ```
  subscriber-management call-trace trace-retention
  ```

- When a trace filter is removed, the cMAG-c removes all traces that match the removed filter. If two filters match the same trace, removing one filter also makes the trace unavailable for the other filter. Use the **clear-with-filter** command in the following context to disable automatic trace removal when a filter is deleted.

  ```
  subscriber-management call-trace trace-retention
  ```

- Use the **filter** command in the following context to remove all traces that match an existing filter. Unlike the previous option, this command does not remove the filter itself.

  ```
  tools subscriber-management call-trace clear
  ```

- Use the **older-than** command in the following context to remove all traces older than a specified time.

  ```
  tools subscriber-management call-trace clear
  ```

In addition to automatic trace retention management, the cMAG-c enforces a limit on the size of trace data that can be stored. You can monitor the current trace storage parameters using the **used-bytes**, **maximum-bytes**, and **used-percent** options in the following context. The start page of the GUI also displays this information. See Accessing the call trace GUI for more information about the GUI start page.

```
subscriber-management call-trace trace-storage
```

When no more trace storage is available, the cMAG-c no longer stores new traces. Existing traces must be removed using one of the preceding options.

3.6 Session lockout

To prevent exhausting its computing resources because of DOS attacks or incorrect configuration, the cMAG-c uses the session-lockout feature.

The cMAG-c locks out a client if the sum of the number of session setup failures and the number of session disconnects reaches a specific threshold within a specific time window. If a client is in the locked-out state, the cMAG-c drops all packets coming from the client for a specific duration of time. The specific duration is calculated using a minimum and maximum duration.

The threshold, time window, and the minimum and maximum duration have default values or can be configured in the session-lockout profile.

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

For a specific client, the initial lockout duration is the minimum duration. When this duration ends, the cMAG-c puts the client in the suspect state for a duration equal to the time window. While the client is in the suspect state, the cMAG-c acts as follows:

- The cMAG-c processes packets from the client.
- If a setup failure or disconnect occurs, the cMAG-c locks out the client for a duration of twice the previous lockout duration, capped at the maximum duration.
- If there is no setup failure or disconnect, the client recovers from the suspect state. The next lockout duration is reset to the minimum duration and the number of allowed session failures and disconnects is reset to the configured threshold.

To remove the locked-out or suspect state from a client, use the following command.

```
tools subscriber-management session-lockout clear
```

Session lockout is enabled by default using the default configuration values of the session-lockout profile. For more information, see *cMAG-c CLI and Data Model Explorer*. See Configuring and applying a session-lockout profile to configure customer-specific values in a session-lockout profile.

Note: Nokia recommends to keep the session-lockout feature enabled.

See Disable session lockout to disable session lockout.

3.6.1 Configuring and applying a session-lockout profile

To enable the session-lockout feature with customer-defined values, configure a session-lockout profile in the BNG EP.

About this task

Session lockout is enabled by default using default values. See the *cMAG-c CLI and Data Model Explorer* for more information about CLI syntax and default values.

To configure customer-specific values, use the following steps.

Procedure

Step 1. Define a session-lockout profile.

```
subscriber-management profiles session-lockout-profile
```

The profile includes:

- **failure-count** – threshold
- **window** – time window
- **min-block-duration** – minimum lockout duration
- **max-block-duration** – maximum lockout duration

Example

```
# info from running with-context /subscriber-management profiles session-lockout-
profile slp
    subscriber-management {
        profiles {
            session-lockout-profile slp {
```


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

```
                attempts {
                    window 600
                    failure-count 10
                }
                min-block-duration 30
                max-block-duration 90
            }
        }
    }
```

Step 2. In the BNG EP entry, reference the session-lockout profile that you configured in the preceding step. The referenced session-lockout profile is applicable for sessions that match this BNG EP entry.

```
subscriber-management entry-point entry session-lockout-profile
```

Example

```
# info from running with-context /subscriber-management entry-point ep entry e
 session-lockout-profile
    subscriber-management {
        entry-point ep {
            entry e {
                session-lockout-profile {
                    profile slp
                }
            }
        }
    }
```

3.6.2 Disable session lockout

Procedure

Note: Nokia recommends to keep the session-lockout feature enabled.

To disable the session-lockout feature, use the following command.

```
subscriber-management entry-point entry session-lockout-profile disabled
```

Example

```
# info from running with-context /subscriber-management entry-point ep entry e session-
lockout-profile
    subscriber-management {
        entry-point ep {
            entry e {
                session-lockout-profile {
                    disabled
                }
            }
        }
    }
```


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

4 Address assignment

The cMAG-c supports various address assignment options, including local address assignment via ODSA, local static address assignment via authentication database, AAA-based address assignment, non-provisioned address assignment, and external DHCPv4 and DHCPv6 server address assignment.

4.1 Overview of address assignment

For sessions that require direct connectivity to a Layer 3 network, the cMAG-c supports the following address assignment options:

- local address assignment via ODSA
- local static address assignment via authentication database
- AAA-based address assignment
- non-provisioned address assignment
- external DHCPv4 and DHCPv6 server address assignment

Additionally, the cMAG-c allocates corresponding prefixes (micro-nets) for the MAG-u, to allow a MAG-u device to send aggregate routes without announcing the per-session routes. For IPv4, the cMAG-c assigns a dedicated gateway address per prefix. It is possible to select different address allocation methods for different address types of the same session. For example, IPv4 can use AAA-based address assignment while IPv6 PD can use a local pool. However, all allocation methods should be known after session authentication.

After session authentication, an address is allocated based on the local address assignment or the AAA-based address assignment.

4.2 ODSA and local address assignment

ODSA can be used to assign a local address, to assign an aggregate prefix per MAG-u, and to derive the default gateway.

4.2.1 ODSA

On demand subnet allocation (ODSA) is a dedicated CUPS address assignment system.

ODSA is a dedicated CUPS address assignment system that can automatically split a common subnet into smaller subnets (micro-nets). The micro-nets are automatically installed on the associated MAG-u. The MAG-u announces the micro-nets in routing. ODSA can either assign an address itself (local address assignment) or work in combination with external address assignment systems (for example, AAA-based).

ODSA pools are configured on a per-network instance basis. A network instance represents a single IP routing context and maps to an IP service on the MAG-u (for example, to a VPRN). See Service selection

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

for more information. ODSA guarantees that there is no overlap between addresses within one network instance.

The main function of ODSA is to assign subnets to an allocation context. The default allocation context is a single MAG-u. In resilient environments, the allocation context is a single fate sharing group (FSG). Each ODSA pool consists of one or more prefixes and is either configured in dedicated mode or with a target micro-net length.

- **dedicated mode**
  In dedicated mode, a prefix is assigned directly to an allocation context. It is not divided into smaller micro-nets.

  To enable the dedicated mode, use the following command.

  ```
  subscriber-management services network-instance pool dedicated
  ```

  Note: The term micro-net in the documentation, state output, or show commands refers to the full prefix when using dedicated mode.

- **target micro-net length**
  With a target micro-net length, all prefixes are divided into smaller, equally sized, micro-nets. Those smaller micro-nets are assigned to an allocation context.

  Note:
  In case of DHCPv6 prefix delegation, you can allocate a variable prefix length per session and a variable micro-net size.

  The following example shows the configuration of an ODSA pool with a target micro-net length.

  ```
  # info from running with-context /subscriber-management services network-instance hsi pool
   hsi
      subscriber-management {
          services {
              network-instance hsi {
                  pool hsi {
                      hold-time 300
                      ipv4 {
                          micro-net-length 28
                          prefix 192.0.2.0/24 {
                          }
                      }
                      ipv6 {
                          na {
                              micro-net-length 120
                              prefix 2001:db8:a00::/116 {
                              }
                          }
                          pd {
                              micro-net {
                                  length 48
                              }
                              prefix 2001:db8:b00::/40 {
                              }
                          }
                          slaac {
                              micro-net-length 56
                              prefix 2001:db8:c00::/48 {
                              }
                          }
  ```


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

```
                    }
                }
            }
        }
    }
```

A subnet (either micro-net or dedicated prefix) can be assigned to only one context. When the first address of a subnet is assigned to a session, the subnet is assigned to the context of the session (for example, to a MAG-u). To guarantee that the full subnet can always be announced in routing without introducing routing conflicts, the following applies:

- The subnet is only unlinked from the context after the last address of the subnet is released.
- While a subnet is linked to a context, no address of the subnet can be assigned to another context, even if ODSA does not do the address assignment for the other context.

To generate a log event when the number of available free micro-nets is minimal, set a threshold using the following command.

```
subscriber-management services network-instance pool minimum-free
```

For IPv4 subnets, ODSA also assigns a default gateway address. To define whether the first or the last address in the subnet is selected for the default gateway address, set the **default-gateway** command to respectively **first-address** or **last-address** in the following context.

```
subscriber-management services network-instance pool ipv4
```

To associate default DNS servers with the ODSA pool, use the following commands.

```
subscriber-management services network-instance pool ipv4 dns primary
subscriber-management services network-instance pool ipv4 dns secondary
subscriber-management services network-instance pool ipv6 dns primary
subscriber-management services network-instance pool ipv6 dns secondary
```

Default DNS servers can be reflected in protocols such as IPCP, DHCP, ICMPv6, and DHCPv6, but sessions can get more specific individual DNS servers.

4.2.2 Variable prefix and micro-net lengths

For DHCPv6 prefix delegation, you can allocate a variable prefix length per session and a variable micro-net length.

You can allocate a variable prefix length per session instead of a fixed prefix length for the whole pool in case of DHCPv6 prefix delegation. The following steps enable a variable prefix length per session:

1. Configure a **minimum** and **maximum** prefix length for ODSA in the following context.

   ```
   subscriber-management services network-instance pool ipv6 pd delegated-prefix variable
   ```

   Example:

   ```
   # info from running with-context /subscriber-management services network-instance ni pool
    pni ipv6 pd delegated-prefix variable
       subscriber-management {
           services {
               network-instance ni {
                   pool pni {
                       ipv6 {
   ```


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

```
                        pd {
                            delegated-prefix {
                                variable {
                                    minimum 56
                                    maximum 64
                                }
                            }
                        }
                    }
                }
            }
        }
    }
```

2. Provision different prefix lengths per session during session setup.

ODSA allocates a micro-net per prefix length. For example, consider the following sequence of session setups, all within the same ODSA pool and MAG-u:

1. For the setup of session 1 with prefix length 56, ODSA allocates micro-net A.
2. For the setup of session 2 with prefix length 64, ODSA allocates a new micro-net B.
3. For the setup of session 3 with prefix length 64, ODSA reuses micro-net B.
4. For the setup of session 4 with prefix length 56. ODSA reuses micro-net A.
5. For the setup of session 5 with prefix length 60, ODSA allocates a new micro-net C.

The combination of variable prefix length with a single fixed micro-net length leads to unequally loaded micro-nets. Consider the following examples:

- Micro-nets with length /52 serving variable prefix lengths 64 and 56, can hold up to 4096 /64 prefixes, but only 16 /56 prefixes.
- Micro-nets with length /44 serving variable prefix lengths 64 and 48, can hold up to 1048576 /64 prefixes, but only 16 /48 prefixes.

This difference leads to over-provisioning and inefficiency if only a few large prefixes are delegated.

To solve this, provision a variable micro-net length using the **minimum** and **maximum** commands in the following context.

```
subscriber-management services network-instance pool ipv6 pd micro-net variable
```

Example:

```
# info from running with-context /subscriber-management services network-instance hsi pool hsi
 ipv6 pd
    subscriber-management {
        services {
            network-instance hsi {
                pool hsi {
                    ipv6 {
                        pd {
                            delegated-prefix {
                                variable {
                                    minimum 52
                                    maximum 60
                                }
                            }
                            micro-net {
                                variable {
                                    minimum 44
```


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

```
                                    maximum 48
                                }
                            }
                            prefix 2001:db8:b00::/40 {
                            }
                        }
                    }
                }
            }
        }
    }
```

With a variable micro-net length, the system automatically chooses the micro-net length that best fits the corresponding prefix length. The following examples illustrate that the configuration must be done carefully considering both the micro-net length and prefix length ranges.

- For a variable micro-net length between 42 and 50, and a variable prefix-length between 56 and 64, the system allocates a /50 micro-net for a /64 prefix, a /42 micro-net for a /56 prefix, and a /46 micro-net for a /60 prefix. Each micro-net holds up to 16384 prefixes, independent of its length.
- For a variable micro-net length between 48 and 50, and a variable prefix-length between 54 and 64, the system allocates a /50 micro-net for a /64 prefix which holds 16384 prefixes, and a /48 micro-net for a /54 prefix which holds 64 prefixes.

Threshold configuration can be used with variable micro-net lengths. To configure thresholds for the pool, use the commands in the following context.

```
subscriber-management services network-instance pool minimum-free
```

Example:

```
# info from running with-context /subscriber-management services network-instance hsi pool hsi
 minimum-free
    subscriber-management {
        services {
            network-instance hsi {
                pool hsi {
                    minimum-free {
                        low 5
                        rising-threshold 5
                        percent
                    }
                }
            }
        }
    }
```

When using variable micro-net lengths, the number of free micro-nets is not deterministic. A micro-net with a small length uses a bigger chunk of the pool than a micro-net with a large length. Therefore the threshold mechanism is different from the one using a fixed micro-net length. It works as follows:

- When the threshold configuration values are absolute values (the **percent** option is not set), the threshold takes into account the smallest micro-net length. The cMAG-c generates a log event in the following cases:
  - The number of free micro-nets (with the smallest length) that can be allocated in the pool drops below the **low** threshold.
  - The number of free micro-nets (with the smallest length) that can be allocated in the pool exceeds the high threshold (sum of the **low** and the **rising-threshold** values).

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

- When the threshold configuration values are a percentage (the **percent** option is set), the threshold takes into account the biggest micro-net length. The cMAG-c generates a log event in the following cases:
  - The percentage of free micro-nets (with the biggest length) that can be allocated in the pool drops below the **low** threshold.
  - The percentage of free micro-nets (with the biggest length) that can be allocated in the pool exceeds the high threshold (sum of the **low** and the **rising-threshold** values).

4.2.3 Local address assignment

ODSA can act as a stand-alone subnet allocation mechanism for MAG-u devices, but it can also assign addresses to individual sessions, without the need for additional configuration.

To allocate an address for a session, ODSA performs the following checks:

- Are there subnets already linked to the allocation context of the session?
- Do any of the linked subnets have available addresses?

If the answer to both questions is yes, an address from any of the linked subnets is allocated to the session.

If the answer to one of the questions is no, a new address is allocated from any subnet that is not yet linked to an allocation context. The subnet is automatically linked to the allocation context of the session. If no subnets are available, the address allocation fails.

To exclude one or more address ranges in a prefix from address allocation, use the following commands.

```
subscriber-management services network-instance pool ipv4 prefix exclude-address
subscriber-management services network-instance pool ipv6 slaac prefix exclude-prefix
subscriber-management services network-instance pool ipv6 na prefix exclude-address
subscriber-management services network-instance pool ipv6 pd prefix exclude-prefix
```

Excluded address ranges can be assigned with other allocation methods (for example, via AAA). In case of IPv4, excluded address ranges are not used for default gateway selection.

When a prefix or entire pool is removed while allocations still exist, the prefix or pool is retained internally and enters automatic drain mode. Existing address allocations from the prefix remain allocated until the corresponding sessions are terminated.

Use the **auto-drain** state indicator in the following contexts to check whether a prefix is in automatic drain mode:

```
subscriber-management services network-instance pool ipv4 prefix
subscriber-management services network-instance pool ipv6 slaac prefix
subscriber-management services network-instance pool ipv6 na prefix
subscriber-management services network-instance pool ipv6 pd prefix
```

When the prefix is in automatic drain mode, the output includes `auto-drain`. When the prefix is not in automatic drain mode, `auto-drain` is absent from the output.

Example: Prefix in automatic drain mode

```
# info from state subscriber-management services network-instance hsi pool radius-ipoe-
pool1 ipv4 prefix 11.0.0.0/16
    apply-state to-be-removed
```


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

```
    auto-drain
    available-micro-nets 16
    micro-nets-in-use 1
    ip-addresses-usable 65488
    ip-addresses-excluded 0
    ip-addresses-active-in-use-non-excl 1
    ip-addresses-active-in-use-excl 0
    ip-addresses-hold-off-non-excl 0
    ip-addresses-hold-off-excl 0
    ip-addresses-free-local-dynamic 65487
    ip-addresses-reserved 48
```

To expedite the cleanup of these pools, sessions must be manually removed, for example, by using the following command with the **ip-prefix** parameter set.

```
tools subscriber-management session clear
```

Local address assignment can be combined with AAA-based address assignment for different address types. For example, IPv4 and IPv6 PD can use local address assignment while IPv6 NA can use AAA-based assignment.

Related topics

AAA-based address assignment

4.3 AAA-based address assignment

AAA services such as RADIUS can provide an address during authentication. The cMAG-c marks the AAA-based address as in use in the ODSA pools and allocates the micro-net to the corresponding context (for example, the MAG-u). In the case of IPv4, the default gateway is assigned using ODSA.

AAA-based addresses can fall within an exclude-addresses range.

Setup of the new session fails in specific situations including the following:

- The address is already allocated to another session.
- The corresponding micro-net is allocated to a context (for example, UP or FSG) that does not match the context of the session.

The prefix pool on which ODSA operates can be used in the following ways:

- If the AAA service provisions both an address pool and an explicit IP address for the same address type (for example, IPv4 or IPv6 PD), ODSA uses the explicit IP address for assignment and the pool for marking the address and allocating MAG-u prefixes and IPv4 gateway addresses.
- In the absence of a pool signaled by AAA itself, pools can be provisioned using the following commands.

```
subscriber-management authentication-database entry address-assignment unmanaged ipv4-pool
subscriber-management authentication-database entry address-assignment unmanaged ipv6-slaac-
pool
subscriber-management authentication-database entry address-assignment unmanaged ipv6-na-
pool
subscriber-management authentication-database entry address-assignment unmanaged ipv6-pd-
pool
```


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

- In the absence of any pool during authentication, a default fallback pool can be provisioned per service using the following commands.

```
subscriber-management services service address-assignment-defaults unmanaged ipv4-pool
subscriber-management services service address-assignment-defaults unmanaged ipv6-slaac-pool
subscriber-management services service address-assignment-defaults unmanaged ipv6-na-pool
subscriber-management services service address-assignment-defaults unmanaged ipv6-pd-pool
```

When no dedicated pools are available, ODSA assigns micro-nets to a context. It is important that the AAA service is aware of the micro-net sizes and that addresses are allocated per context within the scope of a micro-net.

For example, the prefix 192.168.0.0/16 is available, to which addresses are allocated per MAG-u in the AAA. All sessions of MAG-u "east" fall within 192.168.1.0/24 and all sessions of MAG-u "west" fall within 192.168.2.0/24. In this case, it is not necessary to provision these per-MAG-u prefixes on the cMAG-c. The cMAG-c has provisioned a non-dedicated pool with prefix 192.168.0.0/16 and micro-net length 24 and automatically derives the /24 prefixes based on the AAA-based addresses.

The following requirements apply when using ODSA pools for a mix of AAA-based addresses and locally assigned addresses:

- The AAA-based addresses must fall within the configured exclude-addresses ranges to avoid conflicts with local assigned addresses.
- If a pool is not dedicated to a specific context (for example, the MAG-u), the exclude-addresses ranges should align with a micro-net size. This is required to avoid the case where a locally-assigned address allocates the corresponding micro-net to a different context.

Because of the complexity of the requirements, Nokia recommends having a non-dedicated pool for AAA-based address assignment and a separate non-dedicated pool for local address assignment.

4.4 AAA framed routes

The cMAG-c supports AAA provisioned framed routes for sessions with **ip-anti-spoof** disabled (set to **false**); for example, using the Framed-Route and Framed-IPv6-Route RADIUS attributes. The cMAG-c installs these routes on the MAG-u using the PFCP protocol. The cMAG-c does not check these routes for overlap with other framed routes or session allocated addresses. Framed routes are supported for all address assignment types, and not restricted to AAA-based address allocation.

4.5 Managed routes from the ADB

The ADB may return managed routes (Framed-Route RADIUS attribute), in a similar way to the routes AAA returns. The managed routes are installed on the MAG-u via the PFCP protocol. To configure managed routes from the ADB, including the route address, metric, preference, and tag, use the CLI in the ADB context.



Note: If both AAA and ADB return managed routes, the cMAG-c uses the routes from AAA.

The following example shows the configuration of ADB managed routes.

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

Example

```
# info from running with-context /subscriber-management authentication-database adb1 entry
 default address-assignment managed-routes
    subscriber-management {
        authentication-database adb1 {
            entry default {
                address-assignment {
                    managed-routes {
                        managed-route 1.1.1.0/24 {
                            metric 65535
                            preference 255
                            tag 4294967295
                        }
                        managed-route 1.1.2.0/24 {
                            metric 65535
                            preference 255
                            tag 4294967295
                        }
                        managed-route 1.1.3.0/24 {
                            metric 65535
                            preference 255
                            tag 4294967295
                        }
                        managed-route 1.1.4.0/24 {
                            metric 65535
                            preference 255
                            tag 4294967295
                        }
                    }
                }
            }
        }
    }
```

4.6 Unmatching prefixes

Configuring the ADB to support unmatching prefixes enables external entities to assign session addresses without knowledge of the overarching subnet or prefix.

When an external entity managed by a third party assigns a session address, the user is not aware of which overarching subnet or prefix is used to assign the address. Therefore, the user cannot provision such an unknown subnet or prefix on the cMAG-c. To support this use case, the user can configure the ADB to allow unmatching prefixes for one or multiple address types. An externally assigned address (for example, AAA-based) is unmatching if one of the following conditions applies:

- No ODSA pool is provisioned during session authentication.
- An ODSA pool is provisioned, but the address is not within any subnet or prefix of the provisioned pool.

To support unmatching prefixes for specific address types, use the CLI in the following context.

```
subscriber-management authentication-database entry address-assignment unmatching-prefix
```

The cMAG-c cannot send the subnet or prefix information to the MAG-u because the subnet or prefix for the unmatching address is not provisioned on the BNG system. Therefore, the MAG-u installs /32 or /128 routes for each unmatching address, or the exact prefix route for an IPv6 SLAAC or Delegated Prefix.

The following applies to an unmatching address via DHCPv4:

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

- If the external source does not return a subnet mask, the cMAG-c automatically generates one and returns it in the DHCP reply. To generate the subnet mask, the cMAG-c searches for the biggest prefix length for which not all bits in the assigned address are equal to 0, with a maximum prefix length of /30. The following examples illustrate the generation of the subnet mask:
  - The assigned address is 192.0.2.32, 32 equals the binary number 0b00100000. The last non-zero bit is found at position 3 in this byte, or position 27 in the whole IPv4 address. To include this bit, the cMAG-c assigns a prefix length of /26.
  - The assigned address is 192.0.2.1, 1 equals the binary number 0b00000001. The last non-zero bit is found at position 8 in this byte, or position 32 in the whole IPv4 address. To include this bit and leave room for an additional IP address to represent the IP gateway, the cMAG-c assigns a prefix length of /30.
- The cMAG-c automatically generates a default router address and returns it in the DHCP reply. This auto-generated default router address is not passed to the MAG-u. Instead the MAG-u uses the ARP proxy to answer all the client's ARP requests.

  To generate the default router address, the host address part of the assigned address within the assigned subnet mask is set to one, or to two if the host address part already equals one. The following examples illustrate the generation of the default router address:
  - The assigned address is 192.0.2.139 and the subnet mask is /28, so the host bits are the last 4 bits. 139 equals the binary number 0b10001011. The value of the host bits does not equal 1. When setting the value of the last 4 bits to 1, it becomes 0b10000001 or 129. The default router address is 192.0.2.129.
  - The assigned address is 192.0.2.129 and the subnet mask is /28, so the host bits are the last 4 bits. 129 equals the binary number 0b10000001. The value of the host bits already equals 1. When setting the value of the last 4 bits to 2, it becomes 0b10000010 or 130. The default router address is 192.0.2.130.

For PPPoE sessions with unmatching IPv4 addresses, use the following CLI to configure the IPv4 loopback address used as the BNG address in the IPCP negotiation for the corresponding network instance.

```
subscriber-management services network-instance local-server-ip
```

The cMAG-c sends the loopback address to the MAG-u in the PFCP Session Establishment Request message.

Related topics
BNG EP and ADB lookup

4.7 Local static address assignment via authentication database

To return the same configured address to a specific client, the cMAG-c supports the following static address options:

- IPv4 address
- IPv6 NA address
- IPv6 PD prefix
- IPv6 SLAAC prefix

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

Configure the address using the following commands.

```
subscriber-management authentication-database entry address-assignment unmanaged ipv4-address
subscriber-management authentication-database entry address-assignment unmanaged ipv6-slaac-
prefix
subscriber-management authentication-database entry address-assignment unmanaged ipv6-na-
address
subscriber-management authentication-database entry address-assignment unmanaged ipv6-pd-prefix
```

These addresses interact with ODSA micro-nets in the same manner as AAA-based address assignment, as described in AAA-based address assignment.

4.8 External DHCPv4 and DHCPv6 server address assignment

An external DHCPv4 or DHCPv6 server can assign a session address via cMAG-c acting as a DHCPv4 or DHCPv6 relay agent, which relays DHCP messages between the client and the external server.

During authentication, only the ADB (and not RADIUS) can return DHCP relay configuration, including an external server address, a tracking pool, a DHCPv4 giaddr, and a DHCPv6 link address. The cMAG-c uses that ADB configuration to relay the DHCP messages.

Note: Relaying a DHCP server initiated exchange (such as DHCPv4 Force-renew or DHCPv6 Reconfigure) is not supported.

4.8.1 Local ODSA pool tracking

When DHCP relay is in use, the external DHCP server assigns the IP address and the cMAG-c tracks the address assignment, including the subnet and default gateway, to ensure there is no conflict.

To track the DHCP relay address assignments, specify a local ODSA tracking pool under the DHCP relay configuration in the ADB. The subnets and prefixes configured in the tracking pool must be the same as in the external server. The tracking pool is not used to allocate micro-nets; it is a dedicated pool that is only used to track the DHCP relay assignments. The cMAG-c ignores any configuration within the tracking pool with the exception of the prefix.

Use the following command to create a tracking pool.

```
subscriber-management services network-instance pool tracking dhcp-relay
```

Use the commands in the following context to configure the tracking pool.

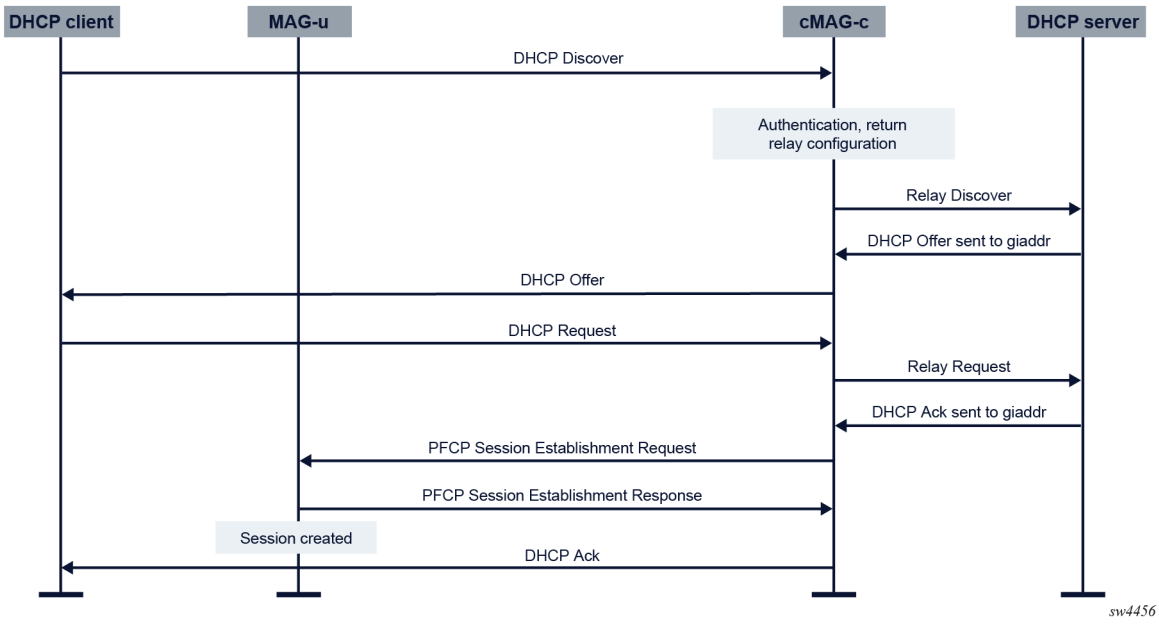
```
subscriber-management services network-instance pool
```

4.8.2 DHCPv4 relay

The following figure shows the DHCPv4 call flow.

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

Figure 8: DHCPv4 call flow



Because the DHCPv4 server sends responses to the giaddr, the giaddr must be provisioned via the Kubernetes service. See the *cMAG-c Installation Guide* for more information. The dhcp-proxy pod is the giaddr service endpoint. It receives the response from the server and forwards that response to the corresponding session-manager pod.

Multiple servers can be configured in the ADB configuration. The cMAG-c sends broadcast requests such as DHCP Discover to all configured servers.

Example: ADB configuration for DHCPv4 relay

```
# info from running /subscriber-management authentication-database adb1 entry 10 address-
assignment
    dhcp-relay {
        ipv4 {
            gi-address 172.100.100.101
            pool relay-pool
            server-list {
                server [
                    10.96.212.90
                ]
            }
        }
    }
```

4.8.3 DHCPv6 relay

The cMAG-c as a DHCPv6 relay server supports the following cases:

- The DHCPv6 client starts the call flow with a Router Solicit (RS) message.
- The DHCPv6 client does not send the RS message.

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

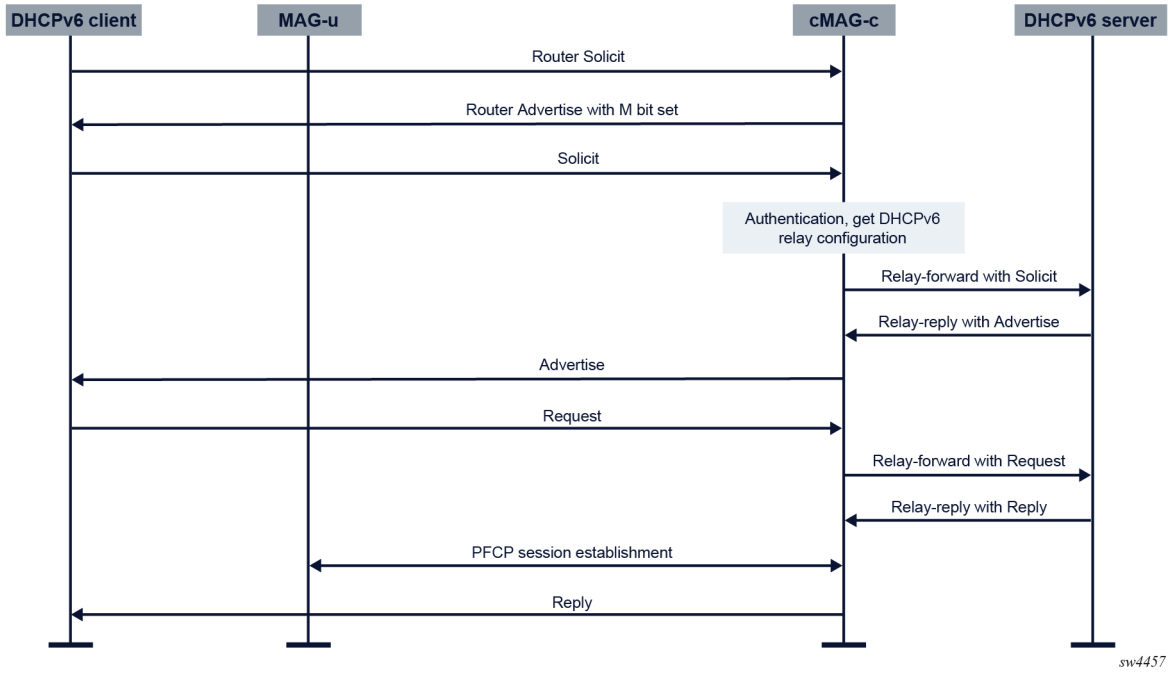
- The DHCPv6 client is behind a lightweight DHCPv6 relay agent (LDRA).

Call flow with RS message

The DHCPv6 client first sends an RS message. When the M bit in the Router Advertisement (RA) message is set, the client starts the DHCPv6 message exchange.

The following figure shows the DHCPv6 call flow for a client sending the RS.

Figure 9: DHCPv6 call flow with RS message

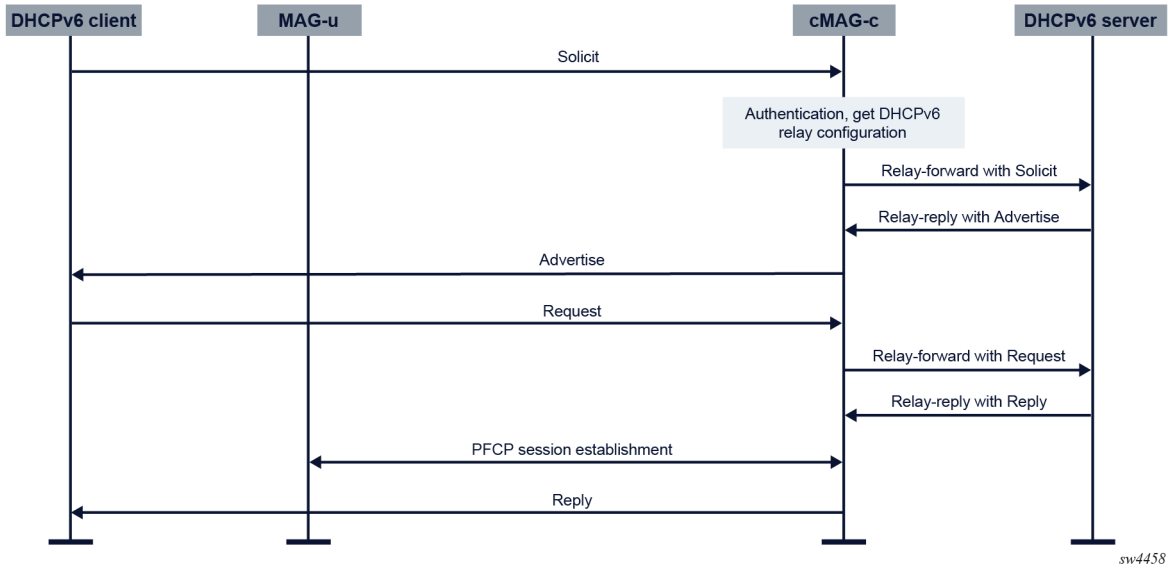


Call flow without RS message

The following figure shows the DHCPv6 call flow when a DHCPv6 client starts the DHCPv6 message exchange without first sending an RS message. It also applies when the cMAG-c starts the flow with an unsolicited RA.

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

Figure 10: DHCPv6 call flow without RS message



Call flow behind an LDRA

The DHCPv6 client is behind an LDRA. The LDRA sends a Relay-forward message to the cMAG-c and the cMAG-c replies with a Relay-reply message.

Configuration specifics

The configuration of an RA profile in the ADB customizes the content of the RA message. Use the following command to configure an RA profile.

```
subscriber-management profiles ra-profile
```

The source address of the Relay-forward message is typically the worker address, because the DHCPv6 proxy pod, which is deployed as a daemonset, handles the message forwarding between the cMAG-c and the DHCPv6 server.

Use the following command to configure a link address that the server can use to select a pool and prefix.

```
subscriber-management authentication-database entry address-assignment dhcp-relay ipv6 link-
address
```

Example: DHCPv6 relay configuration

```
# info from running /subscriber-management authentication-database adb1 entry 10 address-
assignment
    dhcp-relay {
        ipv6 {
            link-address 2001:9999::1
            pool p2
            server-list {
                server [
                    2001:beef::100
                ]
```


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

```
            }
        }
    }
```

4.8.4 DHCP options

DHCPv4

Use the following commands to configure a DHCPv4 option profile for the specified direction:

- **from the cMAG-c toward the DHCP server**

  ```
  subscriber-management authentication-database entry address-assignment dhcp-relay ipv4 to-server-dhcp-option-profile
  ```

  This profile references a DHCP option profile that specifies the DHCP options that are sent to the server, including the relay-agent options such as the circuit ID and remote ID. A drop or replace action can be configured for the received DHCPv4 Request message from the client.

- **from the cMAG-c toward the DHCP client**

  ```
  subscriber-management authentication-database entry to-client-dhcp-option-profile
  ```

  This profile specifies the DHCPv4 options that are sent to the client. Relay-agent options do not apply in this direction.

The following is an example of a DHCPv4 option profile in the direction toward the server (**to-server-dhcp-option-profile**).

Example: DHCPv4 option profile

```
# info from running /subscriber-management profiles dhcp-option-profile d4op
    relay-agent {
        action replace
        sub-option circuit-id {
            access-identifier
        }
        sub-option remote-id {
            mac
        }
    }
```

DHCPv6

Use the following CLI to configure a DHCPv6 profile that specifies the DHCPv6 options for the Relay-forward message.

```
subscriber-management authentication-database entry address-assignment dhcp-relay ipv6 to-server-dhcpv6-option-profile
```

Because a relay agent cannot modify the encapsulated message (per RFC 8415), the cMAG-c inserts the options at the top level of the generated Relay-forward message, and not in the encapsulated message.

This profile can include relay agent options, such as interface ID and remote ID.

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

The following is an example of a DHCPv6 option profile for the Relay-forward message (**to-server-dhcpv6-option-profile**).

Example: DHCPv6 option profile

```
# info from running /subscriber-management profiles dhcpv6-option-profile d6op
    append {
        option remote-id {
            client-id
        }
    }
```

4.8.5 DHCP relay and MAG-u redundancy

Note: The content of this chapter only applies if the following conditions are both met:

- MAG-u redundancy is enabled.
- The server relies on the cMAG-c insert option for pool or subnet, and client identification.

If the external server uses a DHCP option inserted by the access node, not configuring any **to-server-dhcp-option-profile** or **to-server-dhcpv6-option-profile** ensures that the option inserted by the access node is not changed during MAG-u switchover.

Access ports and VLANs on multiple MAG-u nodes can be part of the same UP group in case of MAG-u redundancy. Consequently, the same set of sessions may come from different ports, VLANs, or MAG-u nodes depending on the active MAG-u. Therefore, when the DHCP server assigns an address or prefix to a session with MAG-u redundancy enabled and while relying on an option inserted by the cMAG-c to select pool or subnet, it must take the UP group into consideration to avoid sharing subnets or prefixes between different UP groups.

Use one of the following options to prevent sharing subnets or prefixes between different UP groups:

- If the DHCP server uses the giaddr or link address to select a pool or subnet, configure one unique giaddr or link address per UP group on the cMAG-c and use one pool or subnet per UP group on the DHCP server.
- Use the following commands to configure the UP group ID as circuit ID, remote ID, or interface ID in the DHCPv4 or DHCPv6 profile for sessions with MAG-u redundancy enabled. The UP group does not change during MAG-u switchover.

```
subscriber-management profiles dhcp-option-profile relay-agent sub-option circuit-id
subscriber-management profiles dhcp-option-profile relay-agent sub-option remote-id
subscriber-management profiles dhcpv6-option-profile append option remote-id
subscriber-management profiles dhcpv6-option-profile append option interface-id
```

For the DHCP renew to work, the client identification as seen by the DHCP server must be the same during the MAG-u switchover; for example, in case of a MAG-u switchover to a different MAG-u, port, or VLAN, the client identification must be the same. When the DHCP server uses the circuit ID, remote ID, or interface ID as the client identification, and if the port ID is different on the MAG-u nodes for a specific UP group, configure the same Layer 2 access ID alias on all MAG-u nodes in the UP group to obtain the same client identification.

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

5 Authentication

Configure authentication for a new cMAG-c session, including the RADIUS authentication profile. Learn about the BNG EP and ADB lookup process.

5.1 Overview of the authentication process

The authentication process for a new session on cMAG-c performs a lookup in the following order:

1. BNG EP for sessions
2. authentication flow

The BNG EP lookup returns the following:

- basic configurations for the CP protocol negotiation (for example, the IPoE profile)
- basic session configuration (for example, subscriber identification)
- the authentication flow used to authenticate the session

The authentication flow contains an ordered list of authentication databases (ADBs). The cMAG-c performs a lookup in each ADB in the list, in the specified order. The lookup returns the following configurations required to create the session:

- session attributes (for example, the SLA profile and the subscriber profile)
- address assignment configuration (for example, the local address pool name)
- optional external AAA authentication (for example, RADIUS)

When both the BNG EP lookup and the authentication flow lookup complete successfully, the cMAG-c creates a full forwarding state on the MAG-u for the session using the session management procedures.

Related topics

Session management
QoS

5.2 BNG entry point

The BNG entry point (EP) provides information needed in the authentication flow.

Use the following command to create a BNG EP.

```
subscriber-management entry-point
```

To define the control packet types that trigger the BNG EP lookup, use the following command.

```
subscriber-management ref-points up fixed-access ibcp-triggers
```


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

To reference the entry-point for the triggers, use the following command.

```
subscriber-management ref-points up fixed-access entry-point
```

Example

The following example shows an EP configuration in the BNG profile.

```
# info from running /subscriber-management entry-point e1
    admin-state enable
    match 1 {
        attribute up-node-id
    }
    entry 10 {
        admin-state enable
        ipoe {
            authentication-flow {
                authentication-database [
                    adb1
                    adb2
                ]
            }
        }
    }
```

5.3 Authentication database

Each ADB entry contains three groups of configuration parameters:

- match criteria
- action parameters
- session creation parameters (for example, SLA profile)

After the cMAG-c chooses the best matched entry in the ADB, the cMAG-c executes the configured action. The action can be any of the following types:

- **reject**
  The session authentication fails and no subsequent ADB lookups are performed, even if they are configured as part of the authentication flow.
- **accept**
  The cMAG-c includes the session creation configuration parameters of the chosen ADB entry for the session creation.
- **radius**
  The cMAG-c performs the RADIUS authentication using the RADIUS authentication profile. Use the following command to configure the RADIUS authentication profile.

  ```
  subscriber-management profiles radius-authentication-profile
  ```

  If the RADIUS authentication succeeds, the cMAG-c includes the returned RADIUS authentication attributes and the session creation configuration parameters for the session creation.

  If all RADIUS servers in the RADIUS selection profile that is associated with the RADIUS authentication profile fail to respond, and RADIUS fallback is not configured or the configured triggers are not met, the session authentication fails. If fallback to a second ADB is configured and all RADIUS servers in the

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

profile match the enabled triggers (down or overload), the cMAG-c performs a normal ADB lookup in the fallback ADB instead. See RADIUS fallback to ADB for more information about configuring RADIUS fallback.

- **local-authentication**
  The cMAG-c performs a PAP/CHAP authentication using the configured username and password in the ADB entry for the PPPoE session. Configure the username using the **username** command in the following context.

  ```
  subscriber-management authentication-database entry match
  ```

  Configure the password using the **action local-authentication** command in the following context.

  ```
  subscriber-management authentication-database entry
  ```

The cMAG-c uses the session creation configuration parameters of all ADBs. The authentication flow contains an ordered list of ADBs. If ADBx comes before ADBy in the ordered list of ADBs, the values of the parameters in ADBy have priority over the values of the parameters in ADBx. For example, an authentication flow contains two ADBs, ADB1 and ADB2. If the matched entry in ADB1 returns **sla-profile** `foo`, and the matched entry in ADB2 returns **sla-profile** `bar`, a new session is created with **sla-profile** `bar`.

If the user does not explicitly configure a session creation configuration node (for example, the configuration node uses the default value), the ADB lookup returns no value for this configuration. For example, an authentication flow contains two ADBs, ADB1 and ADB2. If ADB1 returns **sla-profile** `bar`, and the matched entry in ADB2 does not contain an explicit configuration for **sla-profile** (the configuration uses the default value), the cMAG-c creates the new session with **sla-profile** `bar`.

Some session creation configuration nodes support a special **discard** keyword. The **discard** keyword means that the previously returned ADB value for the attribute must be discarded. For example, an authentication flow contains two ADBs, ADB1 and ADB2. If ADB1 returns a value for **to-client-dhcp-option-profile** and ADB2 configures **to-client-dhcp-option-profile discard**, the cMAG-c creates the session without **to-client-dhcp-option-profile**.

Related topics

BNG EP and ADB lookup

5.4 Authentication flow

An authentication flow contains the following configuration items:

- trigger packet type; for example, DHCPv4 discovery or PPPoE PADI packet
- ordered list of one or more ADBs for the specified trigger packet type

When the MAG-u sends a trigger packet, the cMAG-c performs a lookup in each ADB in the list, in the specified order. Each ADB can return session-related configurations. These session-related configurations can be locally configured or returned from an external AAA server.

An IPoE session has only one authentication flow. A PPPoE session requires at least one of the following independent authentication flows:

- PADI
- PAP/CHAP

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

If an ADB lookup fails, the session setup fails. The ADB lookup may fail, for example, if an entry is matched with the reject action or if there is an AAA authentication failure.

If all lookups complete successfully, the cMAG-c continues session setup using the combined configurations from all ADB lookups. For example, the BNG EP lookup returns two authentication flows for a new PPPoE session. The authentication flows return the following configuration:

- PADI authentication flow with 1 ADB: ADB1 returns PADO delay value
- PAP/CHAP authentication flow with 2 ADBs: ADB2 configures RADIUS authentication, ADB3 returns a local address pool

In this example, the cMAG-c uses the combined configuration result from the three ADB lookups to set up the PPPoE session.

Each session requires a service configuration, as described in Service selection. The service can also provide override for specific configurations. If different types of sources return the same type of configuration (for example, an address pool name), the cMAG-c uses the value of the source with the highest ranking. The sources are ranked as follows, with the highest ranked first:

1. AAA
2. Local ADB
3. Service

If different sources of the same type (for example, different ADBs) return the same type of configuration, the cMAG-c uses the last returned value. For example, if both ADB1 and ADBN return an SLA profile name, and ADB1 returns SLA profile name X and ADBN returns SLA profile name Y, the system uses SLA profile name Y because it is the last returned value.

Related topics

Authentication database

5.5 BNG EP and ADB lookup

Both the BNG EP entries and the ADB entries contain session configuration and one or more ordered match criteria. The match criteria are used in the lookup. The session configuration is used in the creation of the session.

Match criteria properties

Match criteria have the following properties:

- **match-id**
  The match ID defines the priority. The lower the ID, the higher the priority.
- **attribute**
  The attribute defines the name of the attribute that is used for the lookup. It is the name of a session attribute. The attribute can be a control protocol field (for example, DHCP option 82 **circuit-id**, **vendor-class**), data packet field (for example, **source-ip-prefix**), or metadata of the session (for example, **l2-access-id**).
- **value**
  The value defines the criteria value to which the session value must match for the specified attribute. If the attribute is optional, the value can be empty, meaning any session value matches with the criteria value.

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

- **optional**
  Match criteria can be optional or mandatory. The attribute of optional criteria does need to be present in the session data to match the entry. If the attribute of optional criteria is present in the session data, the session value must equal the criteria value to match the entry. An attribute that is not present in the entry can have any value in the session (including not available).
- **string-mask**
  A string mask is applied to the value of the session attribute before comparing it with the value of the criteria. It can be used for supported attributes (for example, **l2-access-id**).

The string mask can be length-based or string-based and can be a suffix or a prefix, as follows:

- **prefix**
  - **length-based**
    The cMAG-c removes the specified number of characters from the beginning of the session value.
  - **string-based**
    The cMAG-c removes the specified string from the beginning of the session value. An asterisk (*) can be used as a wild-card in the string mask.
- **suffix**
  - **length-based**
    The cMAG-c removes the specified number of characters from the end of the session value.
  - **string-based**
    The cMAG-c removes the specified string from the end of the session value. An asterisk (*) can be used as a wild-card in the string mask.

The following examples show the string that is used to compare the session value of **l2-access-id** with the criteria value for a specific string mask configuration. Assume that the session value of **l2-access-id** equals `1/2/3`.

- For **string-mask** equal to **prefix length 2**, the cMAG-c removes the first two characters of the session value. The resulting value `2/3` is used to match with the end of the criteria value; for example, the resulting value `2/3` matches with the criteria value `4/2/3`.
- For **string-mask** equal to **suffix string "/*"**, the cMAG-c removes the last slash (/) and everything after it at the end of the session value. The resulting value `1/2` is used to match with the beginning of the criteria value; for example, the resulting value `1/2` matches with the criteria value `1/2/4`.

Default entries

If a BNG EP entry or an ADB entry does not have any match criteria, this BNG EP entry or ADB entry is the default entry. The cMAG-c chooses the default entry when there is no other matched entry. Only one default entry is allowed for the BNG EPs and for the ADBs.

Entry matching

Entries of a BNG EP or of an ADB cannot have the same set of match criteria within the same BNG EP or ADB. In this case, the entry becomes operationally down. The system does allow entries with the same match criteria in different BNG EPs or ADBs.

During a BNG EP or ADB lookup, the cMAG-c compares the attributes of the session with the match criteria of all entries in the BNG EP or in the ADB and creates a list of all matched entries. A matched entry is one for which all mandatory match criteria are fulfilled.

At the end of the lookup, the cMAG-c chooses the best matched entry from the list of all matched entries for session creation. The cMAG-c chooses an entry from the list as follows:

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

- If the list of all matched entries contains only one entry, that entry is the best match.
- If the list of all matched entries contains more than one entry, the cMAG-c reduces the list to the entries with the highest number of match criteria. If this list contains only one entry, that entry is the best match.
- If the reduced list of entries with the highest number of match criteria contains more than one entry, the cMAG-c selects the entry with matches for the highest priority attributes.

Example mandatory and optional match criteria

As an example, the match criteria for an ADB entry contain the attribute **l2-access-id** (marked **optional**) and the attribute **up-node-id** (mandatory). To call the ADB entry a matched entry, one of the following must be true.

- Both **up-node-id** and **l2-access-id** are present in the session and both match the values in the ADB entry.
- Only **up-node-id** is present in the session and it matches the value in the ADB entry.

If both **l2-access-id** and **up-node-id** are present in the session, but only **l2-access-id** matches the value in the ADB entry, the ADB entry is not a matched entry.

Example entry matching and selection

The following output defines the configuration of four ADB entries.

```
# info from running /subscriber-management authentication-database testdb
    admin-state enable
    match 1 {
        !!! first match criteria is UP node id
        attribute up-node-id
        optional true
    }
    match 2 {
        !!! 2nd match criteria is layer2 access ID
        attribute l2-access-id
        optional true
    }
    match 3 {
        !!! 3rd match criteria is SVLAN
        attribute s-vlan
        optional true
    }
    entry 10 {
        admin-state enable
        match {
            up-node-id 172.16.10.50
            l2-access-id 1/1/2
            s-vlan-range {
                start 100
                end 200
            }
        }
        up-parameters {
            sla-profile entry10
            sub-profile entry10
        }
    }
    entry 20 {
        admin-state enable
        match {
            up-node-id 172.16.10.50
            l2-access-id 1/1/2
```


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

```
        }
        up-parameters {
            sla-profile entry20
            sub-profile entry20
        }
        charging {
            profiles [
                mybngcharging
            ]
        }
    }
    entry 30 {
        admin-state enable
        match {
            l2-access-id 1/1/2
            s-vlan-range {
                start 100
                end 200
            }
        }
        up-parameters {
            sla-profile entry30
            sub-profile entry30
        }
    }
    entry 40 {
        admin-state enable
        match {
            s-vlan-range {
                start 100
                end 200
            }
        }
        up-parameters {
            sla-profile entry40
            sub-profile entry40
        }
    }
```

A new session has the following attributes and values:

- **up-node-id** with value `172.16.10.50`
- **l2-access-id** with value `1/1/2`
- **s-vlan** with value `100`

The session matches with all ADB entries. The cMAG-c chooses the entry 10 because it has the highest number of matching criteria; that is, three matching criteria.

Assume entry 10 is shut down. Both entries 20 and 30 have the highest number of matching criteria; that is, two matching criteria. The cMAG-c chooses entry 20 because it has the matching criteria with the highest priority; that is, **up-node-id**.

Assume all entries except entry 40 are shutdown. The cMAG-c chooses the only matching entry; that is, entry 40.

Related topics

VLAN list-based lookups

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

5.6 VLAN list-based lookups

The cMAG-c supports list-based lookups for VLAN matching. The VLAN list-based lookup feature allows an entry point or ADB to match on a list of values that are not contiguous, instead of a single value; for example, a list of VLANs or VLAN ranges. A VLAN list keeps one entry for the whole set.

Lookup behavior

Before entry matching, the cMAG-c compares the incoming value (for example, an S-VLAN) with all values in all configured VLAN lists in the entry point or ADB. The comparison returns one matching list, which is then used as the regular match criterion. The attributes are **s-vlan-list** and **c-vlan-list**.



WARNING: Lists for the same tag type (for example, two S-VLAN lists) in the same ADB or entry point must not share a VLAN. For example, two S-VLAN lists in the same ADB cannot both contain VLAN 10.

VLAN list configuration

Configure VLAN lists in the following context.

```
subscriber-management lists vlan-list
```

Each list entry is one VLAN or one inclusive VLAN range. Use the following options for the list entry configuration:

- **value** – for one VLAN
- **vlan-range value**– for a VLAN range

Example: ADB match configuration on two S-VLAN lists

```
# info from running with-context /subscriber-management lists
    subscriber-management {
        lists {
            vlan-list example {
                entry 1 {
                    value 10
                }
                entry 2 {
                    vlan-range {
                        start 20
                        end 24
                    }
                }
            }
            vlan-list example_expedited {
                entry 1 {
                    value 15
                }
                entry 2 {
                    vlan-range {
                        start 25
                        end 29
                    }
                }
            }
        }
```


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

```
    }
```

```
# info from running with-context /subscriber-management authentication-database vlan-list-
example
    subscriber-management {
        authentication-database vlan-list-example {
            admin-state enable
            match 1 {
                attribute s-vlan-list
                optional true
            }
            entry list1 {
                admin-state enable
                service-name hsi
                match {
                    s-vlan-list example
                }
                action {
                    accept
                }
            }
            entry list2 {
                admin-state enable
                service-name hsi_expedited
                match {
                    s-vlan-list example_expedited
                }
                action {
                    accept
                }
            }
        }
    }
```

Combination of S-VLAN and C-VLAN lists

S-VLAN and C-VLAN lists are evaluated independently. Consider the following example, where an ADB matches both an S-VLAN and C-VLAN list. In this case, the entry "example1" matches all the following (`s-tag,c-tag`) range combinations.

- `(10-15, 500-550)`
- `(10-15, 600-650)`
- `(20-25, 500-550)`
- `(20-25, 600-650)`

Example: S-VLAN and C-VLAN list evaluation

```
# info from running with-context / subscriber-management lists
    subscriber-management {
        lists {
            vlan-list c-vlan-example {
                entry 1 {
                    vlan-range {
                        start 500
                        end 550
                    }
                }
                entry 2 {
                    vlan-range {
```


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

```
                        start 600
                        end 650
                    }
                }
            }
            vlan-list s-vlan-example {
                entry 1 {
                    vlan-range {
                        start 10
                        end 15
                    }
                }
                entry 2 {
                    vlan-range {
                        start 20
                        end 25
                    }
                }
            }
        }
    }
```

```
# info from running with-context / subscriber-management authentication-database combined-
list-example
    subscriber-management {
        authentication-database combined-list-example {
            admin-state enable
            match 1 {
                attribute s-vlan-list
            }
            match 2 {
                attribute c-vlan-list
            }
            entry example1 {
                admin-state enable
                match {
                    c-vlan-list c-vlan-example
                    s-vlan-list s-vlan-example
                }
                action {
                    accept
                }
            }
        }
    }
```

5.7 Required minimal configuration for a session creation

To create a session, the cMAG-c requires a minimal number of session creation configuration parameters. The table lists the parameters that are required for session creation, as well as the source that contains those parameters.

Table 6: Minimal configuration for a session creation

Configuration	Source
authentication-flow	BNG EP

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

Configuration	Source
service	ADB, RADIUS
address-assignment	ADB, RADIUS
sla-profile[1]	ADB, RADIUS
sub-profile[1]	ADB, RADIUS
group-interface-template[1]	ADB, RADIUS
sap-template[1]	ADB, RADIUS

5.8 RADIUS authentication profile

RADIUS authentication is performed when the **action** parameter in the best-matched ADB entry is set to **radius**. The RADIUS authentication profile defines the RADIUS authentication behavior. Use the following command to define the profile.

```
subscriber-management profiles radius-authentication-profile
```

RADIUS authentication is triggered by the ADB lookup. Consequently, it is possible to have multiple rounds of RADIUS authentication during the authentication flow lookup. If the same attributes are returned in the Access-Accept message during multiple authentication rounds, the last attribute received is used.

A RADIUS authentication profile contains the following configuration commands:

- **server-selection-profile**

  The **server-selection-profile** command references a RADIUS server selection profile that is defined using the following command.

  ```
  subscriber-management profiles radius-server-selection-profile
  ```

  The RADIUS server selection profile references one or multiple RADIUS servers configured in the **subscriber-management ref-points aaa radius** context.

  The RADIUS server configuration contains a server address, port, secret, and other server-specific configuration. The RADIUS server selection profile contains access-related configuration; for example the access algorithm for selecting a destination RADIUS server for a request from the list of servers.

- **user-name-format**

  The **user-name-format** command defines the username format for the RADIUS server.

  Use the **data-trigger-source-ip** option in the following command to send the source IP address of the data-trigger packet.

  ```
  subscriber-management profiles radius-authentication-profile username-format ipoe format
  ```

[1] If the MAG-u contains a template or a profile with the name `default`, the default template or profile is used when the authentication does not return a template or profile. If the MAG-u does not contain a specific template or profile with the name `default`, the configuration of the parameters is required.

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

- **password**

  The **password** command defines the password of the RADIUS user.

- **include-attributes**

  The **include-attributes** command defines the RADIUS attributes to be included in an Access-Request message. Use the commands in the following context to define the attributes to include.

  ```
  subscriber-management profiles radius-authentication-profile include-attributes
  ```

  See the *cMAG-c RADIUS Attributes and IU Triggers* for more information about the attributes and the messages they may appear in.

The username and password configuration are required for IPoE authentication and PPPoE PADI authentication.

For RADIUS authentication using point-to-point protocol (PPP) challenge handshake authentication protocol (CHAP), the value of the Request Authenticator field in the header of the Access-Request is the CHAP challenge value, if the challenge is 16 bytes long.

Optional fallback to another ADB when all RADIUS servers in the profile are unreachable or overloaded is configured on the ADB entry in the **subscriber-management authentication-database entry action radius fallback** context, not inside the RADIUS authentication profile. See RADIUS fallback to ADB for more information.

5.9 RADIUS fallback to ADB

When an ADB entry uses RADIUS authentication, the user can configure a fallback ADB. The cMAG-c uses the fallback ADB if all RADIUS servers in the referenced RADIUS authentication profile are unreachable or overloaded (according to the configured triggers). The cMAG-c performs a normal ADB lookup in the fallback ADB, which could return configurations needed to establish the session. This behavior provides operational continuity when all RADIUS servers in the profile are unable to respond.

To configure ADB fallback, use the commands in the following context.

```
subscriber-management authentication-database entry action radius fallback
```

ADB fallback is disabled by default. When fallback is enabled and all RADIUS servers in the RADIUS server selection profile that is associated with the RADIUS authentication profile fail to respond, the following events occur:

1. The cMAG-c evaluates the operational state of all RADIUS servers in the RADIUS server selection profile that is associated with the RADIUS authentication profile for that entry.
2. Fallback is triggered if the state of every evaluated RADIUS server matches one of the enabled triggers (down or overload).
3. The cMAG-c performs a normal ADB lookup in the configured fallback ADB.

The following are the available fallback triggers:

- **down** — all RADIUS servers down; **true** by default
- **overload** — all RADIUS servers in overload; **false** by default

Note:

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

- The fallback ADB must be a different ADB than the ADB that contains the entry (the cMAG-c rejects self-reference at commit).
- An entry in the fallback ADB may configure the **action radius** command with its own fallback configuration, forming a chain of up to three fallback ADB hops.

Example: Fallback configuration

```
# info from running /subscriber-management authentication-database primary-adb entry 1
    action
        radius {
            authentication-profile prof1
            fallback {
                adb fallbackdb1
                trigger {
                    down true
                }
            }
        }
```

5.10 RADIUS CoA and DM

A RADIUS Change of Authorization (CoA) message or a Disconnect Message (DM) asks for changes in the session or subscriber object.

To enable support for RADIUS CoA and DM messages, use the following command.

```
subscriber-management ref-points aaa radius dynamic-authorization
```

The listening address and port are provisioned via the Kubernetes service. See the *cMAG-c Installation Guide* for more information.

When the cMAG-c receives a CoA or DM message, it makes the requested change to the target object. The *cMAG-c RADIUS Attributes and IU Triggers* list defines the message attributes that can be used to identify one or multiple sessions as a target object. Filter on the value **True** for the CoA key column to find attributes that are used as an identifier, for example, Alc-Subsc-ID-Str. If a subscriber is specified in the request, the cMAG-c applies the requested changes to all sessions of the targeted subscriber.

The CoA message contains one or more attributes that define the requested changes; for example, the Alc-SLA-Prof-Str VSA defines a new SLA profile for the target object. For more information about the supported attributes, see the *cMAG-c RADIUS Attributes and IU Triggers*.

If the cMAG-c applies all requested changes successfully to all targeted objects, the cMAG-c sends a CoA-ACK message to the RADIUS server. If the cMAG-c can apply the requested changes only partially or only on a subset of the target objects, the cMAG-c sends a CoA-NAK message and rolls back the changes as follows:

- If the change request is for multiple attributes on a single session and only part of the attribute changes are successful, the cMAG-c sends a CoA-NAK message with ERROR-CAUSE code 404, and rolls back the already applied changes.
- If the change request is for multiple attributes on multiple sessions and the changes are successful only for a part of all the target sessions, the cMAG-c sends a CoA-NAK message with ERROR-CAUSE code 506 and rolls back the applied changes for the sessions that were only partially changed. For example, if a CoA message requests to change three attributes on five sessions, the cMAG-c successfully applies

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

all attribute changes on session 1, session 2, and session 3 but only one attribute change on session 4 and session 5. The cMAG-c sends a CoA-NAK message with ERROR-CAUSE code 506 and rolls back the attribute change on session 4 and session 5.

A DM message only contains target objects. The cMAG-c removes the sessions of the target objects and sends an ACK message. If the target objects do not exist, the cMAG-c sends a CoA-NAK message with ERROR-CAUSE code 503.

If a CoA or DM message contains an unsupported attribute, the cMAG-c rejects the request with a CoA-NAK message by default. To ignore unsupported attributes, use the following command.

```
subscriber-management ref-points aaa radius dynamic-authorization ignore-unknown-attributes
```

5.11 Example configuration

The example configurations in this section are for the following setup:

- IPoE session
- RADIUS authentication
- address pool `pool-up-1` for sessions from MAG-u `1.1.1.1`
- address pool `pool-up-2` for sessions from MAG-u `2.2.2.2`
- sla-profile `basic`, sub-profile `basic`, and authentication with `radius-auth-profile-1` for sessions with s-vlan `100`
- sla-profile `premium`, sub-profile `premium`, and authentication with `radius-auth-profile-2` for sessions with s-vlan `200`

This setup uses an authentication flow with three ADBs for which the following are returned:

- ADB `adb1` only returns the address pool.
- ADB `adb2` only returns the sla-profile and the sub-profile, and performs RADIUS authentication.
- ADB `adb3` returns the other configuration parameters.

Example: ADB configuration with three ADBs

```
# info from running /subscriber-management
  authentication-database adb1 {
        admin-state enable
        match 1 {
            attribute up-node-id
        }
        entry up-1 {
            admin-state enable
            match {
                up-node-id 1.1.1.1
            }
            address-assignment {
                local-dynamic {
                    ipv4-pool pool-up-1
                }
            }
        }
        entry up-2 {
            admin-state enable
```


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

```
            match {
                up-node-id 2.2.2.2
            }
            address-assignment {
                local-dynamic {
                    ipv4-pool pool-up-2
                }
            }
        }
    }
    authentication-database adb2 {
        admin-state enable
        match 1 {
            attribute s-vlan
        }
        entry basic {
            admin-state enable
            match {
                s-vlan 100
            }
            action {
                radius {
                    authentication-profile radius-auth-profile-1
                }
            }
            up-parameters {
                sla-profile basic
                sub-profile basic
            }
        }
        entry premium {
            admin-state enable
            match {
                s-vlan 200
            }
            action {
                radius {
                    authentication-profile radius-auth-profile-2
                }
            }
            up-parameters {
                sla-profile premium
                sub-profile premium
            }
        }
    }
    authentication-database adb3 {
        admin-state enable
        entry default {
            admin-state enable
            service-name mybng
            up-parameters {
                group-interface-template defaultgroup
                sap-template defaultsap
            }
        }
    }
```

The following example shows the configuration of the BNG EP.

Example: BNG EP configuration

```
# info from running /subscriber-management
```


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

```
    entry-point e1 {
        admin-state enable
        entry 10 {
            admin-state enable
            ipoe {
                authentication-flow {
                    authentication-database [
                        adb1
                        adb2
                        adb3
                    ]
                }
            }
        }
    }
```

The following example shows a reference to the BNG EP configured in the following context.

```
subscriber-management ref-points up fixed-access
```

Example: BNG EP reference configuration

```
# info from running /subscriber-management ref-points up fixed-access
    entry-point e1
    ibcp-triggers {
        ipoe-dhcp true
    }
```


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

6 Accounting and charging

Learn about the statistics collection from the MAG-u, time-based and volume-based charging, RADIUS accounting configuration, and buffering of the RADIUS accounting messages for later retransmission.

6.1 BNG charging profiles

BNG charging profiles define the charging interfaces for a session. A session can be associated with multiple BNG charging profiles.

BNG charging profiles contain the configuration of the charging interfaces for a session; for example, the RADIUS accounting interface. Charging profiles are assigned to sessions during authentication.

Multiple charging profiles can be provisioned per session. The following example use cases enable the same charging interface in different contexts.

- Two charging profiles support duplicate RADIUS accounting to a main and a backup accounting server. The two charging profiles are identical, except for the target servers.
- Two charging profiles support distinct logging systems using the same interface. For example, one profile is used for RADIUS packet and octet accounting and one is used for session create and delete logging.

To configure BNG charging profiles, use the following command.

```
subscriber-management profiles charging-profile
```

To use a BNG charging profile for a specific set of sessions, use the following command.

```
subscriber-management authentication-database entry charging profiles
```

Except for the communication with the MAG-u, there is no interaction between multiple charging profiles for the same session. Each charging profile uses the session data and the triggers (periodic interval or trigger events) to act according to its configuration. For example, a messaging failure for one profile does not affect retransmits in another profile.

The cMAG-c tries to optimize the number of messages sent in the communication with the MAG-u. For example, if the same event triggers multiple charging profiles to fetch MAG-u data, the cMAG-c attempts to send a single request to the MAG-u instead of a request per charging profile.



Caution: The cMAG-c guarantees unique charging identifiers (such as Acct-Session-Id) per session but not per profile and session. If the same servers are used in two profiles, the servers may not be able to distinguish between log events which leads to unpredictable behavior. Nokia recommends that you do not define multiple charging profiles with interfaces to the same set of servers; for example, two profiles using the same server selection profile.

Related topics

BNG EP and ADB lookup

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

6.2 Statistics collection from the MAG-u

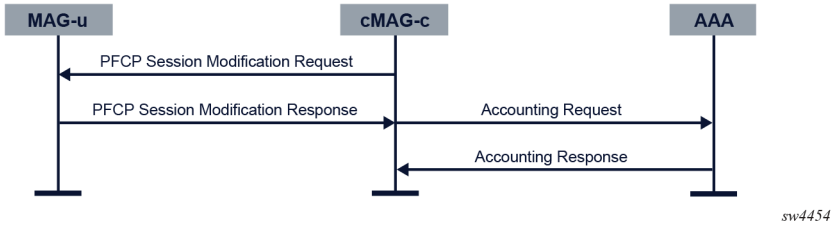
Configure the pull or push model to fetch mid-session PFCP usage reports from the MAG-u.

A PFCP Usage Report IE contains incremental MAG-u statistics per session. The usage report includes only statistics collected since the previous usage report. The cMAG-c aggregates the statistics for the session. This incremental method is robust and can handle a MAG-u failure. When a MAG-u failure occurs, statistics collected since the previous report are lost. However, the cMAG-c statistics remain correct and increase monotonically. Similarly, when MAG-u resiliency is used, the cMAG-c can add counters of both MAG-u nodes to calculate the correct aggregate.

The cMAG-c supports two models to fetch mid-session PFCP usage reports:

- **pull model**
  The cMAG-c explicitly requests a usage report in a PFCP Session Modification Request message when it needs up-to-date counters. The cMAG-c does not send periodic unsolicited pull requests. For example, it requests a Usage Report for a RADIUS Accounting Request Interim Update message.

  Figure 11: Statistics collection using the pull model

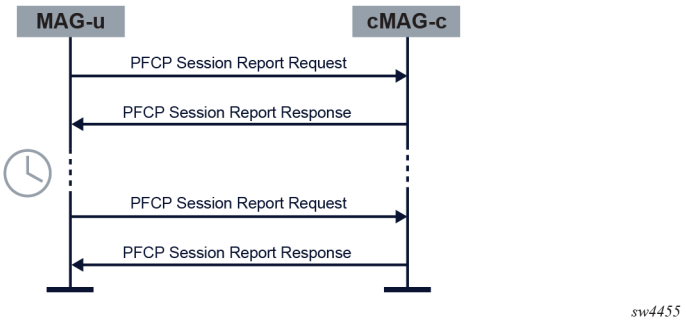


- **push model**
  The MAG-u sends an unsolicited PFCP Usage Report IE in a PFCP Session Report Request message. Upon receiving this message, the cMAG-c records and stores the statistics. The push message does not directly trigger an update (for example, Radius Accounting Interim Update). However, the statistics update may trigger any reporting limit, threshold, or quota; for example, Volume-based charging.

  The unsolicited usage report is periodic. The MAG-u sends a report within a fixed interval. If another report was generated (for example, pull-based), the interval is reset.

  The following figure shows the statistics collection using the push model.

  Figure 12: Statistics collection using the push model



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

To enable the periodic push model, configure the push interval using the following command.

```
subscriber-management authentication-database entry charging up-statistics-collection push-
interval
```

A small push interval can reduce counter loss in case of MAG-u failures but increases the load on the cMAG-c. The system must be dimensioned accordingly.

Push and pull modes can work in parallel. For example, the RADIUS accounting is enabled with an interval of 6 h (pull mode) and the MAG-u reporting is enabled with an interval of 15 min (push mode). Every six hours, the RADIUS accounting message triggers an explicit pull from the MAG-u to fetch the latest counters, while the MAG-u sends unsolicited usage reports every 15 min. This allows for a frequent counter update to avoid loss without overloading the AAA server and without the AAA server having outdated statistics.

Note:
If the pull interval is similar to the push interval, Nokia recommends disabling the push mode. Having similar intervals for the push and the pull mode increases the load without a direct benefit.

Note: The cMAG-c may optimize to not pull the stats if the current stats are very recent, for example, because of a push or other pull directly before the event that would cause a pull request. This optimization is however not guaranteed to occur in every instance.

For resilient sessions, the cMAG-c maintains one set of counters that are aggregated from all PFCP sessions that have been set up over the lifetime of the encompassing session. The incremental nature of the PFCP reports allow this without risking duplicate counters. The cMAG-c can present these aggregated counters monotonically increasing to other interfaces such as RADIUS accounting, cMAG-c charging, and **show** commands. Because of MAG-u resiliency, back-end systems, such as accounting servers, do not need to account for sudden counter resets resulting from MAG-u failure.

In case of hot standby MAG-u resiliency, there are two PFCP sessions. When performing pull requests, the cMAG-c pulls statistics from the active MAG-u in steady state, because it does not expect traffic from the standby MAG-u. During switchovers, the cMAG-c pulls from both MAG-u nodes to fetch the potentially still available final statistics from a degraded MAG-u. The cMAG-c installs the push mode on both MAG-u nodes. The Nokia MAG-u, however, is optimized to only send push reports if the reported statistics contain non-zero values. The statistics of a standby MAG-u in steady state normally contain only zero values.

Independent of mid-session statistics collection, final statistics are always fetched when the session is removed in a PFCP session deletion procedure.

The following statistics are supported:

- aggregate number of bytes upstream and downstream
- aggregate number of packets upstream and downstream, if the MAG-u signals the measurement of number of packets (MNOP) function feature in the PFCP association procedure
- detailed statistics as collected by the Nokia MAG-u

  Examples of detailed statistics are per queue statistics, per policer statistics, and separate IPv4 and IPv6 counters. The content of the detailed statistics depends on the MAG-u QoS **stat-mode** configuration.

Detailed statistics are collected and available for reporting if the **detailed-statistics** is enabled (set to **true**) in the ADB using the following command.

```
subscriber-management authentication-database entry charging up-statistics-collection detailed
```


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

When enabled, the cMAG-c requests the MAG-u to send detailed statistics.

If detailed statistics are collected and available for reporting, they can be included in the RADIUS accounting messages. Use the following command to send detailed statistics in the RADIUS accounting messages.

```
subscriber-management profiles charging-profile radius session include-attributes detailed-
statistics
```

When the cMAG-c detects a new **stat-mode** or SLA Profile, the detailed statistics are reset. The cMAG-c sends the final detailed statistics for the previous **stat-mode** or SLA profile in RADIUS accounting messages if enabled. Because aggregated statistics are not dependent on the **stat-mode** nor on the SLA profile, they are not reset.

Note:
On a Nokia MAG-u, both aggregate and detailed statistics are based on the QoS model. If multiple sessions of the same subscriber share QoS resources, the statistics are collected on a per-session basis, but they do not provide real usage of a specific session. The aggregate of the session statistics is correct for the shared QoS resource. If real usage of per-session statistics are required in a multiple sessions per-subscriber model, Nokia recommends enabling an SLA profile instance (SPI) per session model on the MAG-u.

Related topics
Authentication

6.3 cMAG-c-based charging

Learn about time-based and volume-based charging.

Time-based charging

The cMAG-c provides time-based charging using the session timeout mechanism. This session timeout starts after successful authentication. The cMAG-c deletes the session when the timer expires.

Volume-based charging

For basic volume-based charging, the cMAG-c compares the statistics to provisioned thresholds. The cMAG-c compares the statistics with the thresholds for every received usage report.

The following thresholds are supported:

- total number of upstream bytes
- total number of downstream bytes
- total number of upstream and downstream bytes

To configure the thresholds in the ADB, use the following commands.

```
subscriber-management authentication-database entry charging cp-volume-tracking total
subscriber-management authentication-database entry charging cp-volume-tracking uplink
subscriber-management authentication-database entry charging cp-volume-tracking downlink
```

The threshold values can also be provided via RADIUS. For more information, see *cMAG-c RADIUS Attributes and IU Triggers*.

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

As soon as one of the provisioned thresholds is reached, the cMAG-c deletes the session.

For deterministic behavior, Nokia recommends combining the volume-based charging with periodic statistics collection.

Related topics

Statistics collection from the MAG-u

6.4 RADIUS accounting

Learn about the RADIUS accounting configuration in the BNG charging profile and how to enable RADIUS accounting.

The cMAG-c supports RADIUS accounting as defined in RFC 2866.

To enable RADIUS accounting, perform the steps in Enabling RADIUS accounting.

The RADIUS accounting configuration in the BNG charging profile includes the following parameters:

- **RADIUS server selection profile**
  The RADIUS server selection profile provides the list of RADIUS servers and load-balancing parameters.

  Use the following command to reference the RADIUS server selection profile in the BNG charging profile.

  ```
  subscriber-management profiles charging-profile radius server-selection-profile
  ```

  Use the following command to define and configure the RADIUS server selection profile.

  ```
  subscriber-management profiles radius-server-selection-profile
  ```

- **session accounting parameters**
  The accounting parameters for sessions include configuration of attributes to include in accounting messages, and triggers to send the RADIUS Accounting Request Interim Update message.

  Use the commands in the following context for the session accounting parameters.

  ```
  subscriber-management profiles charging-profile radius session
  ```

For more information about the accounting attributes, their content, the associated include-attribute configuration, and the messages they can appear in, see the *cMAG-c RADIUS Attributes and IU Triggers* and the *cMAG-c Data Model Guide*.

6.4.1 Enabling RADIUS accounting

Procedure

Step 1. Define a charging profile.

```
subscriber-management profiles charging-profile
```

Step 2. Configure RADIUS accounting for the BNG charging profile.

```
subscriber-management profiles charging-profile radius
```


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

Step 3. Reference the BNG charging profile.

```
subscriber-management authentication-database entry charging profiles
```

Step 4. Define match criteria for the ADB so that the BNG charging profile gets assigned to a session during authentication.

Related topics

BNG EP and ADB lookup

6.4.2 Session accounting

The cMAG-c sends RADIUS accounting messages to start and stop session accounting. Interim update messages contain updates of the accounting data. The interim update messages can be periodic or triggered by an event.

Start and stop messages

When session accounting is enabled, the cMAG-c sends an Accounting Request Start message to the RADIUS accounting server. The exact time when the message is sent in the session setup procedure depends on the session type. Sending the Accounting Request Start message is linked to the data plane creation on the MAG-u and to the IP address assignment protocols.

The server selection for the Accounting Request Start message follows the generic load-balancing configured in the following context.

```
subscriber-management profiles radius-server-selection-profile
```

When the **stickiness** command in the preceding context is set to **true**, subsequent messages are sent to the same server. When the selected server fails, a new server is selected. When the **stickiness** command is set to **false**, load-balancing is applied to each accounting message.

After accounting is started, the cMAG-c sends Accounting Request Interim Update (IU) messages. The cMAG-c sends the IU messages periodically or based on triggers.

When the session is removed, the cMAG-c sends an Accounting Request Stop message, including the final counters.

Periodic interim updates

Periodic sending of Accounting Request IU messages is on by default and can be optionally disabled using the following command.

```
subscriber-management profiles charging-profile radius session update-triggers periodic
```

When the periodic sending is enabled, the interval for the Accounting Request IU messages can be provisioned as follows, in order of precedence:

1. during the session authentication; for example, using the RADIUS Acct-Interim-Interval attribute
2. using the following command

```
subscriber-management profiles charging-profile radius default-interim-update-interval
```

Note: Changing the value by using this command updates existing sessions after the next scheduled Accounting Request Interim Update message. This command does not establish

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

an interim update interval for sessions that do not already have one, because there is no scheduled IU message to trigger the change.

The interval can be changed during the lifetime of a session by sending a RADIUS CoA with the Acct-Interim-Interval attribute. In this case, a session sends an immediate Accounting Request IU message with the reason Interval-Changed and starts a timer with the new interval.

When multiple BNG charging profiles are configured, the periodic interim update interval can be provisioned or changed per BNG charging profile using the RADIUS Alc-Charging-Profile-Interim-Interval VSA.

Note: Nokia recommends provisioning the same interval for all charging profiles with periodic interim updates enabled. In this case, the cMAG-c runs a common interval timer, and sends only one message per periodic interim update interval to fetch the statistics from the MAG-u for all the periodic Accounting Request IU messages.

Triggered interim updates

The cMAG-c sends a triggered Accounting Request IU message when it detects changes in the session or subscriber data, or when an external system instructs to send an IU message.

The vendor-specific Alc-Acct-Triggered-Reason attribute in the IU message indicates the type of trigger.

See the *cMAG-c RADIUS Attributes and IU Triggers* for information about supported trigger events.

When several trigger events occur at the same time, the cMAG-c sends a single IU message with multiple Alc-Acct-Triggered-Reason attributes to include all trigger reasons.

In case one event triggers multiple IU messages, such as an SLA profile change, other simultaneous trigger events are included in the first IU message.

Related topics

IPoE

Message retransmission and buffering

BNG charging profiles

6.4.3 Message retransmission and buffering

RADIUS accounting messages are retried and also buffered for later retransmission. Learn how to configure and manage the buffering of the different RADIUS accounting messages.

The cMAG-c retries the transmission of RADIUS accounting messages based on the configuration of the following commands.

```
subscriber-management ref-points aaa radius server retry-count
subscriber-management ref-points aaa radius server retry-timeout
```

If no server responds after all the retries, the cMAG-c buffers messages for later retransmission. The cMAG-c uses a non-configurable timer to trigger periodic retransmission of the buffered messages and exponential back-off when servers remain unavailable.

When buffering is enabled, the cMAG-c can buffer the following messages per session:

- one Accounting Stop message
- one Accounting Start message

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

- Multiple Accounting IU messages

To enable buffering of RADIUS accounting messages, use the following commands:

- To enable buffering of Accounting Stop messages, use the following command.

```
subscriber-management profiles charging-profile radius buffering
```

- To additionally enable buffering of Accounting Start message, use the following command.

```
subscriber-management profiles charging-profile radius buffering start
```

- To additionally enable buffering of Accounting IU messages, use the following command.

```
subscriber-management profiles charging-profile radius buffering interim-update
```

The default lifetime of buffered accounting messages is 24 hours. To manage the final retransmission attempts, the cMAG-c can keep a message longer than the configured lifetime. To change the configured lifetime for the buffered accounting messages, use the following command.

```
subscriber-management profiles charging-profile radius buffering lifetime
```

The cMAG-c classifies Accounting IU messages as critical or non-critical depending on the trigger event:

- **Non-critical Accounting IU messages**

  Non-critical messages do not reflect a significant state change and contain data that is present either in the subsequent Accounting IU messages or in the Accounting Stop message. For example, a periodic IU message contains only updated cumulative counters that are also present in a subsequent IU or Stop message. The following rules apply for non-critical messages when IU buffering is enabled:

  – Buffering only applies to the last non-critical IU message for a session.

  – When the session terminates, a Stop message overwrites the optionally stored non-critical IU message for the session.

- **Critical Accounting IU messages**

  Critical messages reflect a significant state change, and may contain data that is lost if not sent; for example, a stop of service and the final statistics related to that service. Enabling IU-message buffering ensures the buffering of multiple critical IU messages per session, to prevent loss of data.

Periodic IU messages are non-critical messages. Triggered IU messages can be critical or non-critical depending on the trigger reason. See the *cMAG-c RADIUS Attributes and IU Triggers* searchable HTML reference for more information.

The cMAG-c also provides the following commands for clearing buffered accounting messages:

- To determine which messages are buffered and obtain information per message, use the following command.

```
info from state subscriber-management buffered-radius-accounting-session id
```

- To clear buffered messages for a specific session, use the following command.

```
tools subscriber-management buffered-radius-accounting-session clear id
```


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

- To clear all buffered messages, use the following command.

```
tools subscriber-management buffered-radius-accounting-session clear all
```

Related topics

Session accounting

6.4.4 Sending Accounting-On and Accounting-Off messages

cMAG-c supports sending Accounting-On and Accounting-Off messages to a RADIUS server based on the configuration.

About this task

Enable sending Accounting-On and Accounting-Off messages to mark the start and end of accounting toward the RADIUS server.

Note: Because the cMAG-c is a cloud-native solution and individual components can be restarted any time, there is no support for the traditional boot, reboot, and shutdown triggers for Accounting-On and Accounting-Off messages as mentioned in RFC 2866.

Procedure

Step 1. Create and configure a RADIUS server.

Note: Do not commit the configuration yet, because the cMAG-c does not generate Accounting-On messages for an already configured server.

Use the commands in the following context.

```
subscriber-management ref-points aaa radius server
```

Step 2. Enable Accounting-On and Accounting-Off messages.

```
subscriber-management ref-points aaa radius server accounting-on-off true
```

Step 3. Commit the configuration for the new server.

```
commit
```

Note: Setting the **accounting-on-off** configuration to **true** after the server is initially created does not result in the generation of an Accounting-On message.

Expected outcome

- The cMAG-c sends Accounting-On messages to the RADIUS server until the RADIUS server acknowledges the message.
- When the server is removed from the system, for example by deleting the `server` configuration, the cMAG-c sends a single Accounting-Off message to the deleted server.

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

7 Lawful intercept

The lawful intercept (LI) solution provides legally sanctioned, official access to private communications and is implemented on the cMAG-c and on the MAG-u.

The topics in this section address the LI solution implemented on the Nokia cMAG-c and on the MAG-u. For geo-redundant LI deployments, see the *cMAG-c Geo-redundancy Guide* for more information.

7.1 LI overview

LI is a legally sanctioned, official access to private communications. To provide intercepted private communications to law enforcement officials, a service provider or network operator collects communication of a private subscriber or organization using an LI security process.

LI typically consists of the following interfaces, irrespective of the access technology:

- administrative interface – supports LI target provisioning
- information-related interface (IRI) – provides event information related to subscribers
- contents-of-communications interface (CC) – sends mirrored packets to the LI gateway (LIG)

The Nokia CUPS architecture supports administrative and IRI interfaces on the cMAG-c and the CC interface on each MAG-u.

The cMAG-c provides a centralized location to provision all LI targets, and instructs the MAG-u to perform LI for specific target subscribers by sending encrypted LI PFCP IEs through the Sx interface. The cMAG-c and the MAG-u share a private key to allow decryption of LI PFCP IEs.

To allow the LI target to remain anonymous, every subscriber PFCP session includes encrypted LI PFCP IEs.

See the *cMAG-c Installation Guide* for more information about restoring LI management to its factory-default settings, for example, to restore the default password and regain access.

7.2 LI strict licensing

To activate the LI functionality, the cMAG-c requires an LI license. The cMAG-c uses a single license for all features, including LI. The cMAG-c license is installed on the main management pod, not on the LI session management pod. After installing a cMAG-c license including LI, the LI session management POD becomes available.

The cMAG-c license is a term-based license, the license is not tied to a particular release but expires when the term is over. In the expire state, the cMAG-c remains functional but sends continuously reminders to update the license as soon as possible.

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

If you cannot reach the LI session management pod, use the following command to ensure that the cMAG-c license includes LI.

```
info from state system license
```

See the *cMAG-c CLI and Data Model Explorer* for information about this CLI including its parameters.

Output example: cMAG-c license including the LI license

```
# info from state system license cmagc_0_0
    admin-state enable
    preferred true
    data "..."
    issued-date "YYYY-MM-DD time"
    expiration-date "YYYY-MM-DD time"
    rtuLawfulIntercept: true
    expired false
    valid true
    in-use true
```

When the cMAG-c license includes LI and is successfully installed, the wireline LI functionality becomes available. See LI solution for wireline application for information about the wireline LI.

If the cMAG-c license expires, the cMAG-c remains functional during a grace period and sends reminders to renew the license.

Caution:
Installing an invalid license results in factory defaults.

Nokia recommends to always back up the current configuration, so it is possible to reapply it to the cMAG-c after an upgrade.

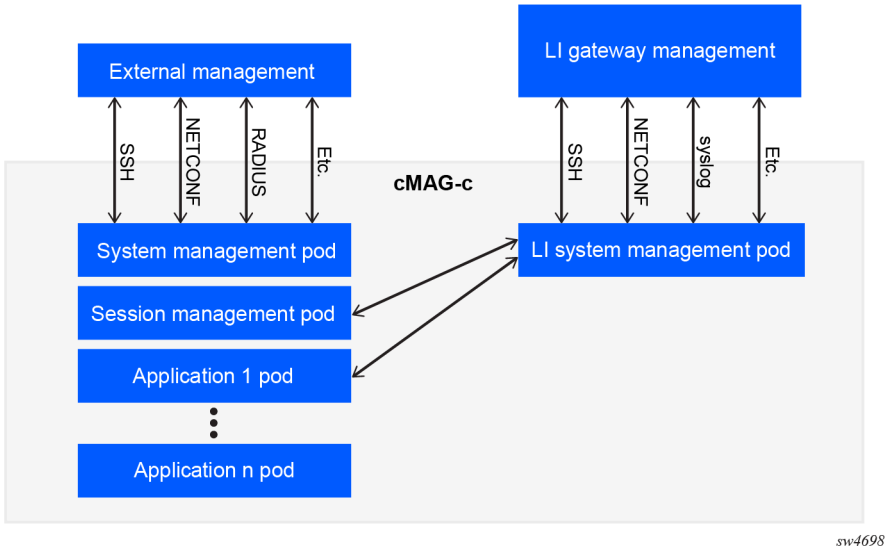
See the *cMAG-c Installation Guide* for more information about cMAG-c licensing.

7.3 LI architecture

The following figure provides a high-level overview of the cMAG-c LI functional architecture.

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

Figure 13: High-level cMAG-c LI architecture



The cMAG-c installs and manages the LI function on its own instance of the system management pod, separate from the rest of the system. The LI system management pod or LI pod has a separate user, Authentication, Authorization, and Accounting (AAA) functionality, management IP address, and ports.

To perform LI, the cMAG-c informs the LI pod of every new subscriber session created on the system. The LI pod compares the provisioned LI targets with the newly created subscribers. If a new subscriber matches a provisioned LI target, the cMAG-c activates LI for the new subscriber session. When a user provisions an LI target in real time, the LI pod queries the session management pod to check whether the target is online. If the subscriber is online, the cMAG-c activates LI for the subscriber session.

The cMAG-c encrypts all LI target information, including the following:

- LI information exchanged between pods
- PFCP LI instructions, which can only be decrypted by the MAG-u using a shared secret
- technical support files and crash dumps

7.4 LI administrative interface

LI management interfaces

LI supports the following management interfaces:

- SSH
- NETCONF
- syslog

The LI management is limited to local authorization and authentication of users, that is, remote authentication and authorization such as RADIUS and TACACS+ are not supported.

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

Mandatory configuration for LI

When the cMAG-c license including LI is installed and the LI session management pod becomes available for the first time, the LI admin user must reconfigure the password for both the admin and linuxadmin users; see Configuring passwords and seeds.

Following this, the LI admin user can set up the infrastructure for LI; see Setting up the LI infrastructure.

7.4.1 Configuring passwords and seeds

The passwords and the seeds must be configured when the LI session management pod comes up for the first time after installing a cMAG-c license including LI.

Prerequisites

The cMAG-c contains a valid license including LI.

Procedure

Step 1. Log in to the LI management function.

Step 2. Change the default password for the admin and the linuxadmin users.

```
system aaa authentication admin-user password
system aaa authentication linuxadmin-user password
```

Example

```
system aaa authentication admin-user password ditaup=8h6t
system aaa authentication linuxadmin-user password 6g7g=pultid
```

Step 3. Set up the root seed, a private encryption key for technical support file encryption. Use the following **kubectl** command on the admin host server to set up the root seed.

```
kubectl create secret generic secure-seed-secret -n cmag-c --from-file=seed=<(openssl
 rand 32)
```

Step 4. Add the following line with the secret seeds to the cMAG-c custom resource (CR) YAML file.

```
secrets:
   secureSeed: secure-seed-secret
```

What to do next

Setting up the LI infrastructure

7.4.2 Setting up the LI infrastructure

Configure a PFCP secret to allow LI on the cMAG-c and the MAG-u nodes.

Prerequisites

Passwords and seeds are configured; see Configuring passwords and seeds.

Procedure

Step 1. Optional: Configure a system name for the LI management function.

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

Note: Although this is an optional step, Nokia recommends to configure a system name for the LI management function

```
lawful-intercept system name
```

Example

```
# lawful-intercept system name li-management
```

Step 2. Configure a PFCP shared secret on both the cMAG-c and the MAG-u nodes, to allow LI on the MAG-u nodes.

Note: Nokia recommends to configure the same shared secret on all MAG-u nodes.

See the SR OS documentation for information about how to configure the secret on the MAG-u nodes. Use the following command to configure the secret on the cMAG-c.

```
lawful-intercept pfcp shared-secret
```

Example

```
# lawful-intercept pfcp shared-secret mySecret
```

What to do next

Setting up LI targets

7.5 LI solution for wireline application

Understand the tools to use and guidelines to follow when configuring cMAG-c LI for wireline applications.

7.5.1 Setting up LI targets

About this task

Setting up LI targets uses the X1 interface (LI_H1 is another common industry term). The cMAG-c X1 interface supports LI provisioning via SSH CLI and NETCONF.

Note: This guide only covers the LI architecture and provisioning requirements for the cMAG-c. To perform LI functionality, both the cMAG-c (CP) and the MAG-u (UP) require LI configuration. See section LI contents of communication for more information about the MAG-u configuration.

Prerequisites

Configure the LI infrastructure such as the PFCP shared secret; see Setting up the LI infrastructure.

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

Procedure

Configure the name of the subscriber being mirrored, the direction of the mirror, and the intercept and session ID when using Layer 3 IP UDP shim headers on the MAG-u nodes.

Use the CLI in the following context.

```
lawful-intercept targets subscriber
```

Note: See the *cMAG-c CLI and Data Model Explorer* for the full context of the commands including command parameters.

Example: LI target configuration

```
info from running /lawful-intercept targets
    subscriber subscr1 {
        intercept-id 1
        session-id 2
        direction ingress-egress
        mirror-instance-name mirror501
    }
```

7.5.2 LI information related interface

The cMAG-c IRI interface (X2 and LI_H2 are other common industry terms) delivers LI-related information via syslog and telemetry state information.

The IRI information includes the following:

- LI targets configured on the cMAG-c
- LI targets removed from the cMAG-c when a subscriber logs off

In rare circumstances, the cMAG-c fails to provision the LI target on the MAG-u. A reporting mechanism informs the LI gateway of the failed provisioning and that the provisioning must be re-attempted.

Each LI target has an operational state:

- up – LI target is online and the LI session is ongoing
- waiting – LI target is provisioned, but is offline; the system is ready for LI and waiting for the LI target to come online
- failed – MAG-u is unreachable; reprovision the LI target when the MAG-u is reachable again

When the provisioning is unsuccessful, use the following CLI to display the reason.

```
info from state /lawful-intercept targets subscriber oper-down-reason
```

7.5.3 LI contents of communication

The MAG-u provides the CC interface (X3, LI_H3 are other common industry terms).

To support cMAG-c LI, the MAG-u requires a minimal set of LI configurations including the following:

1. Within the main MAG-u configuration region, provision a designated mirror destination service for LI.

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

Note: The mirror destination ID is a key parameter that the cMAG-c sends to the MAG-u. The mirror destination IDs on the MAG-u and the cMAG-c must match.

2. Within the MAG-u LI configuration region, provision the LI source referencing the mirror destination.
3. Within the MAG-u LI configuration region, provision the PFCP shared secret that matches the provisioning on the cMAG-c.

See the *7450 ESS, 7750 SR, 7950 XRS, and VSR OAM and Diagnostics Guide* for more information and configuration guidelines.

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

8 Python support

Customize the cMAG-c behavior by applying user-defined Python scripts to inspect and modify control protocol packets.

Python scripts

Sending or receiving specific control protocol packets can trigger a user-defined Python script. Using the packet as input, the script applies a set of Nokia API calls to inspect and modify the packet. The script outputs the modified packet.

The direction of the triggering protocol message defines when the Python script runs:

- ingress – before the subscriber management processing
- egress – after the subscriber management processing

For example, when the cMAG-c receives a RADIUS Access-Accept message, a user-defined Python script can update the Alc-SLA-Prof-Str attribute in the message to a new SLA profile name. The system processes the modified packet and creates the session with the new SLA profile.

Python version and libraries

The cMAG-c Python support is based on Python version 3.11. The software includes the following libraries:

- Python standard libraries
- Nokia-provided TPSDA API
- Cryptodome package, see PyCryptodome

For more information about the Nokia-provided TPSDA APIs, see *cMAG-c TPSDA Python 3 API*.

Supported protocol messages

The following tables list the supported protocol message types and direction.

Table 7: Supported direction for RADIUS messages

Message type	Ingress	Egress
Access-Request		✓
Access-Accept	✓	
Access-Reject	✓	
Account-Request		✓
Account-Response	✓	
Access-Challenge	✓	

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

Table 8: Supported direction for RADIUS CoA messages

Message type	Ingress	Egress
CoA Request	✓	
DM Request	✓	
CoA or DM Reply		✓

Table 9: Supported direction for PPPoE messages

Message type	Ingress	Egress
PADI	✓	
PADO		✓
PADR	✓	
PADS		✓
PADT	✓	✓
LCP	✓	✓
PAP	✓	✓
CHAP	✓	✓
IPCP	✓	✓
IPv6CP	✓	✓

Table 10: Supported direction for DHCPv4 messages

Message type	Ingress	Egress
Discover	✓	✓ (relay)
Offer	✓ (relay)	✓
Request	✓	✓ (relay)
Ack	✓ (relay)	✓
Decline	✓	✓ (relay)
Nak	✓ (relay)	✓
Release	✓	✓ (relay)
Inform	✓	✓ (relay)
Lease-Query	✓	✓ (relay)

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

Table 11: Supported direction for DHCPv6 messages

Message type	Ingress	Egress
Solicit	✓	✓ (relay)
Advertise	✓ (relay)	✓
Request	✓	✓ (relay)
Confirm	✓	✓ (relay)
Renew	✓	✓ (relay)
Rebind	✓	✓ (relay)
Reply	✓ (relay)	✓
Release	✓	✓ (relay)
Decline	✓	✓ (relay)
Info-Request	✓	✓ (relay)
Relay-Forward	✓ (LDRA)	✓ (relay)
Relay-Reply	✓ (relay)	✓ (LDRA)

Note:

- (relay) means supported only for relayed messages
- (LDRA) means supported only for lightweight DHCPv6 relay agent (LDRA)

Operational commands

To check if a Python script is in service, use the following command.

```
info from state /subscriber-management python python-script <name> oper-state
```

To see the in-use source code of a Python script, use the following command.

```
info from state /subscriber-management python python-script <name> source-in-use
```

To bring a modified script in service, use the following command.

```
tools subscriber-management python python-script reload script
```


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

8.1 Configuring a Python script

You can customize the cMAG-c behavior with a Python script.

Procedure

Step 1. Create a Python script file, and either save it in the `/python` folder of the management pod or upload it to an HTTP or FTP server.



Note: When storing the script file in the `/python` folder of the management pod, it must be backed up on a Kubernetes cluster storage, so that the management pod can still access the file if the pod is rescheduled to a different worker.

Step 2. Configure the URL of the script file.

```
subscriber-management python python-script
```

Step 3. Specify the trigger packet type, the direction, and the corresponding Python script in a Python policy.

```
subscriber-management python python-policy
```

Step 4. Reference the Python policy in the corresponding protocol configuration; for example, inside the radius-authentication-profile for the RADIUS authentication messages.

Example

The following example configures to run the `/python/test.py` Python script file upon sending the RADIUS Access-Request message.

```
# info from running /subscriber-management python
   python-script test {
        admin-state enable
        code {
            path /python/test.py
        }
    }
    python-policy rad {
        radius access-request direction egress {
            script test
        }
    }

# info from running /subscriber-management profiles radius-authentication-profile auth1
    server-selection-profile sel1
    python-policy rad
    password $aes1$AWPJEozXM6/vxG8=$P6tGQqEKHwszh6LDBJ3e1w==
    username-format {
        ipoe {
            format mac-address
            mac-format ab:ab:ab:ab:ab:ab
        }
    }
```


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

9 MAG-u resiliency

The Nokia cMAG-c supports a cMAG-c-driven MAG-u resiliency scheme. Learn about this resiliency scheme, the resiliency handling, and deployment use cases.

9.1 Terminology for MAG-u resiliency

fate sharing group (FSG)	An FSG is a group of sessions that stay together when moved between MAG-u nodes. This guarantees that any associated resources, such as ODSA allocated prefixes, are moved together with the sessions. This maps to the TR-459 concept of a subscriber group (SGRP), where FSGs use the PFCP extensions for SGRPs defined in TR-459. In the context of the PFCP, the terms FSG and SGRP are interchangeable.
active MAG-u	In the scope of a single FSG, the active MAG-u is the MAG-u on which the sessions are created and which actively forwards traffic for those sessions. The active MAG-u also answers incoming ARP requests for fixed access sessions.
standby MAG-u	In the scope of a single FSG, the standby MAG-u is the MAG-u that is ready to install sessions and forward traffic upon failure of the active MAG-u. Whether sessions are proactively created on this MAG-u depends on the chosen resiliency model.
hot standby	In the hot standby resiliency model, sessions are proactively created on a standby MAG-u. The standby MAG-u does not attract traffic but is ready to start forwarding as soon as the cMAG-c instructs it to do so.
warm standby	In the warm standby resiliency model, sessions are created solely on the active MAG-u. Sessions on the standby (new active) MAG-u are created only after the active MAG-u fails.
force hot standby	In some cases warm standby sessions are automatically converted to hot standby sessions. In these cases, any behavior related to the hot standby session applies, not the behavior related to the warm standby session. See Make before break for warm standby.

Note:

9.2 Introduction to cMAG-c-driven MAG-u resiliency

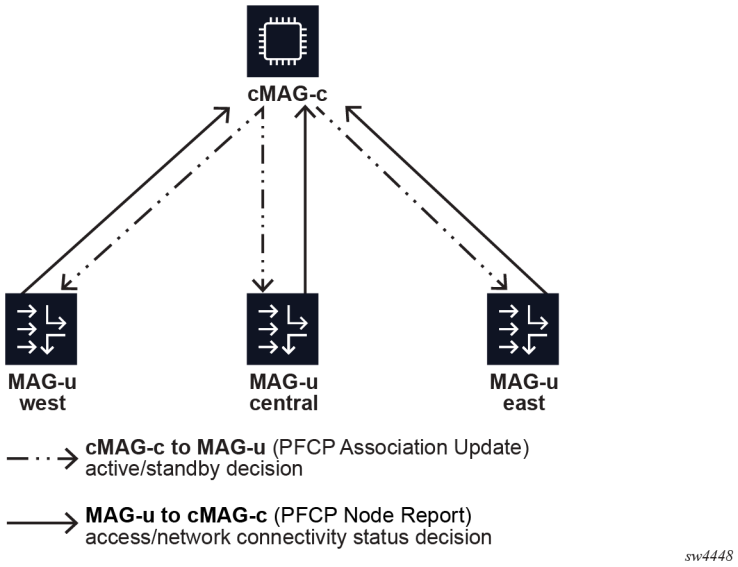
The Nokia cMAG-c supports a cMAG-c-driven MAG-u resiliency scheme. In this scheme, the cMAG-c selects the active and standby MAG-u nodes and the MAG-u nodes must follow this decision. The MAG-u nodes do not communicate directly to negotiate the active or standby role or to synchronize session

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

state. Instead, each MAG-u sends its local status indicators to the cMAG-c; for example, whether it has full connectivity to the access network. The cMAG-c aggregates these status indicators from all MAG-u nodes and makes an informed decision that is sent to the MAG-u nodes. The PFCP node messages of the PFCP association between the MAG-u and cMAG-c that are already in place for session management carry the status indicators and informed decisions.

The following figure shows a high-level overview of communication for MAG-u resiliency.

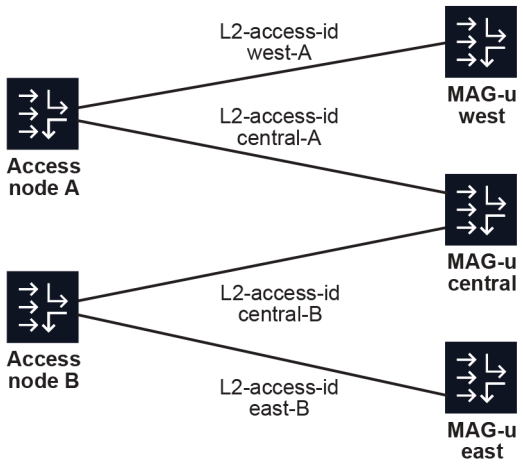
Figure 14: High-level overview of communication for MAG-u resiliency



It is possible, and often preferred, that a MAG-u is active for a subset of the sessions and standby for another subset of the sessions. For example, when two MAG-u nodes are fully available, making both MAG-u nodes active for half of the sessions and standby for the other half of the sessions may be preferred. Similarly, two Layer 2 access IDs (ports) on the same MAG-u can be backed up by two different MAG-u nodes. The following figure shows the use case where the MAG-u "central" is backed up by both the MAG-u nodes "west" and "east" for two different Layer 2 access IDs.

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

Figure 15: Multiple MAG-u backup nodes



To support all use cases, the cMAG-c assigns sessions to an FSG. The cMAG-c assigns the active or standby state to each FSG. The state applies to all sessions of the FSG, but not to any other session on the same MAG-u nodes. ODSA is also FSG-aware and allocates micro-nets on an FSG basis, instead of a MAG-u basis, to account for FSGs moving between MAG-u nodes.

9.3 Modeling a resilient MAG-u deployment using UP groups

The UP group configuration is a key component of the CUPS MAG-u resiliency. This configuration serves as a high-level description of the MAG-u access network so that the cMAG-c knows which MAG-u nodes are interconnected for MAG-u resiliency. Based on the UP group configuration, the cMAG-c automatically generates FSGs for the resiliency functionality.

Use the following command to configure the UP group.

```
subscriber-management ref-points up group
```

Note: See the *cMAG-c CLI and Data Model Explorer* for more information about the full CLI syntax, including variable options.

At the core of the UP group configuration is a list of MAG-u nodes. The PFCP Node ID IE as signaled during the PFCP association setup procedure identifies each MAG-u. The identifier can be either a name or an IP address. The MAG-u nodes that form the UP group are interconnected and MAG-u resiliency can occur between them.

See Modifying UP groups for information about modifying and managing UP groups.

Related topics

Fate sharing groups

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

9.3.1 Modifying UP groups

The cMAG-c supports modifications to existing UP groups. Following an intent-based mechanism, the cMAG-c automatically makes a best-effort attempt to modify any of the FSGs to accommodate the changes to the UP groups. However, it does not execute any UP group changes that result in the deletion of sessions. This includes, but is not limited to, the following changes:

- deleting a UP group with active sessions
- deleting an L2-Access-ID from a UP group while there are sessions attached to that Layer 2 access ID
- removing a VLAN range or part of a VLAN range, either directly or via a VLAN list that the UP group references, while there are active sessions on that UP group

Note: This also applies if no sessions are active on the removed VLANs.

In these cases, the cMAG-c keeps working with the previous configuration but no longer accepts new sessions within that UP group. The new configuration is stored as the intended configuration and is periodically retried. This is made clear using an apply state field; see Apply state for more information.

Note: If using a VLAN list, verify the apply state of the VLAN list. This is required because changing only a VLAN or VLAN range in a list without changing the UP group configuration itself may cause a conflict. In this case, the apply state of the UP group does not show a conflict but the apply state of the VLAN list does. Additionally, the following state is set to error.

```
subscriber-management ref-points up group s-tag-list-oper-state
subscriber-management ref-points up group c-tag-list-oper-state
```

In advanced cases, configuration changes to multiple UP groups can block each other. For example, attempting to move a Layer 2 access ID from a UP group A to a UP group B is not applied on either UP group. Instead, the following occurs:

- On UP group A, this acts as a delete that is not applied until all sessions are removed (as described previously).
- On UP group B, a Layer 2 access ID addition is allowed, but it now overlaps with the still applied configuration on UP group A, and is therefore also rejected.

After making changes, execute the procedure in Validating UP group changes to verify that a change did not result in a blocked scenario.

To avoid configurations not being applied and to avoid unnecessary FSG changes, Nokia recommends following these guidelines.

- Before and after implementing any change, verify that all FSGs of the targeted UP groups are stable. Execute step 1 from Performing maintenance on a Nokia MAG-u. For simplicity skip step 1a and replace the *fsg-id* in step 1b by the wildcard identifier *.

  Note: This does not apply when adding a UP group.

- Never remove or replace more than one MAG-u in a single commit. Additionally, before removing the MAG-u, execute steps 1 to 3 in Performing maintenance on a Nokia MAG-u to make sure that the standby MAG-u is first in the targeted UP groups.

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

- Avoid temporarily removing a MAG-u from a UP group, and if you do, consider the advice in Blocking the setup of non-resilient sessions.
- When moving any combination of MAG-u, Layer 2 access ID, and VLAN from one UP group to another, do the full move in a single commit. Immediately check the apply state of both UP groups, and be prepared that you may have to remove all sessions from the first UP group for the commit to be fully applied.

  Note: If a move is not done in a single commit, unintended non-resilient sessions may be set up. See Blocking the setup of non-resilient sessions for more information.

- Limit the number of changes to one per commit, for example, one addition, one removal, one replacement, or one move.

9.3.1.1 Validating UP group changes

Prerequisites

See Modifying UP groups for background information about modifying and validating UP groups after making changes.

About this task

Use these steps to validate the state of the UP groups after making changes.

Procedure

Step 1. Check the state output using the following command.

```
info depth 0 from state /subscriber-management ref-points up group * | eql "apply-
state != 'applied'" | filter fields apply-state
```

Expected outcome

If the command returns no output, all configuration is applied and no further action is required. If the command returns output, continue to step 2.

Step 2. Wait one minute and execute the command again. In some cases multiple valid changes are not applied simultaneously but the cMAG-c rectifies this automatically.

Step 3. Find more information about the cause using the following command to display and check the output of log messages for the ConfigurationApplyFailed and ConfigurationDeleteFailed events.

```
show system logging buffer messages apply-state
```

Step 4. If the apply-state is blocked because of a delete case and the change is required, clear the sessions of the UP group. For example, use the following command:

```
tools subscriber-management session clear up-group
```

Expected outcome

The cMAG-c automatically applies the new configuration.

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

What to do next

To further validate whether the applied UP group configuration matches your intended design, use the following command.

```
show subscriber-management ref-points up group
```

See Operational commands for more information.

9.3.2 Fate sharing group creation

The cMAG-c creates a single FSG per configured UP group. The following configuration for the FSG is provisioned via the UP group:

- **reference to an FSG profile**
  Use the following command to configure a reference to an FSG profile.

  ```
  subscriber-management ref-points up group fsg-profile
  ```

  The profile contains detailed parameters on the resiliency behavior; for example, health calculation for each MAG-u. If no profile is provided in the UP group, the UP group behaves as if a profile with default parameters was applied.
- **preferred indicator**
  Per MAG-u, a flag indicates whether the MAG-u is active by preference. When the flag is set for a MAG-u, the FSG prefers this MAG-u to be active if all other parameters are equal. This flag requires the **active-change-without-failure** property in the following context to be set to a value other than **never**.

  ```
  subscriber-management profiles fsg-profile active-standby-selection
  ```
- **drain indicator**
  Per MAG-u, a flag indicates whether the MAG-u is in drain mode. When the flag is set for a MAG-u, the FSG avoids selecting this MAG-u as active. For example, this flag can be used before upgrading a MAG-u to achieve a graceful switchover.

  Note: Changing the drain flag for an active MAG-u acts as a MAG-u reselection trigger for the linked FSGs. The cMAG-c moves the sessions after changing the configuration.

To see the FSGs created for a UP group, use either of following commands.

```
info from state / subscriber-management ref-points up group fsg
show subscriber-management ref-points up group
```

See Operational commands for examples and more information about these commands.

Related topics

Fate sharing groups

9.3.3 Fixed access with active/standby pseudowire access

MAG-u resiliency is possible with active/standby pseudowire (A/S PW) access. The access network selects the active and standby PW of an A/S PW, and the MAG-u nodes must follow this decision.

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

The configuration of the FSG-based resiliency mechanism ensures that the FSG state follows the A/S state determined by the access node. This mechanism is modeled using UP groups as follows:

- The A/S PW pair is covered by a single UP group, that is, the Layer 2 access IDs representing the A/S PW cannot be present in any other UP group.
- The UP group covering the A/S PW pair cannot contain any other Layer 2 access IDs.
- The MAG-u signals to the cMAG-c, a Layer 2 access ID health that indicates the status of the PW on that MAG-u:
  - standby (0%)
  - active (100%)

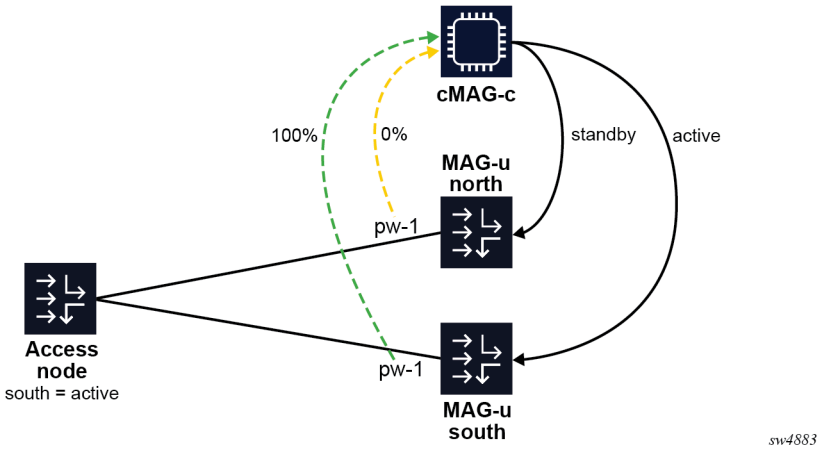
  See Configuring health reporting for an A/S PW port on the Nokia MAG-u to configure this on a Nokia MAG-u.
- The UP group covering the A/S PW pair must not contain any configuration that triggers the cMAG-c to enforce an A/S state in the access network; for example, the configurations of the following commands.

```
subscriber-management ref-points up group peer drain
subscriber-management ref-points up group peer preferred
```

- The linked FSG profile cannot monitor network health because that may lead to the cMAG-c enforcing an A/S decision that does not correspond to the pseudowire's A/S state.

The following figure and configuration example show a PW and the associated UP group configuration.

Figure 16: A/S PW deployment



Example

```
# info from running with-context / subscriber-management ref-points up group north-south-
pw
    subscriber-management {
        ref-points {
            up {
                group north-south-pw {
                    l2-access-id [
                        pw-1
                    ]
                    peer up-north {
```


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

```
                    }
                    peer up-south {
                    }
                }
            }
        }
    }
```

Note:
Because the **drain** command is not supported in this setup, Nokia recommends performing the following procedure when maintenance on a MAG-u is required: Maintenance on a Nokia MAG-u in an A/S PW setup.

When the headless PFCP mode is enabled, exercise care to avoid active/active scenarios. When PFCP path management to one node fails, the cMAG-c forces a switchover independent of the signaled Layer 2 access ID health. This can occur in the following indistinguishable cases:

- The entire MAG-u fails. The decision to switch over is correct. The A/S PW also performs a switchover.
- Only the PFCP path fails (headless). The decision to switch over may be incorrect because the A/S PW state is independent of the PFCP path.

The following configuration is required to handle the preceding cases:

- When in headless mode, the MAG-u must fully bring down the PW. This forces the access node to also switch over because it perceives a failed MAG-u. See Bringing down the PW in headless conditions to configure this.

  Caution: If both MAG-u nodes of an A/S PW pair become headless, forwarding stops but the session state is retained.

- The MAG-u must be configured to move an FSG to standby whenever headless operations occur. To configure this, see Moving an FSG to standby in headless mode.

9.3.3.1 Configuring health reporting for an A/S PW port on the Nokia MAG-u

Prerequisites

Ensure the basic SDP, PW port, and capture SAP configuration are present.

About this task

Perform this task to configure an A/S PW port on the MAG-u and enable the NokiaMAG-u to signal a health value of 0% (standby) or 100% (active) to the cMAG-c. See Fixed access with active/standby pseudowire access for more information.

Note: The commands shown in this task are MAG-u MD-CLI commands. The equivalent MAG-uclassic CLI commands may have slightly different syntax.
See the *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Command Reference Guide*, the 7450 ESS, 7750 SR, 7950 XRS, and VSR Classic CLI Command Reference Guide, or the corresponding CLI Explorer Tools delivered with the *7450 ESS, 7750 SR, 7950 XRS, and VSR* WebHelp, for more information about the MAG-u CLI syntax.

Procedure

Step 1. Configure an operational group to monitor the PW port.

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

Example

```
configure service oper-group myopergroup
```

Step 2. Apply the operational group to the PW port.

Example

```
configure pw-port 1 oper-group myopergroup
```

Step 3. Apply the operational group for health monitoring on the capture SAP created for the PW port.

Example

```
configure service vpls 10 capture-sap 10 pfcp up-resiliency monitor-oper-group
 myopergroup
```

Step 4. Set the drop in health value to 100 in the context created in step 3. This causes the reported health of the Layer 2 access ID to go from 100% to 0% when the PW becomes standby on the MAG-u.

Example

```
configure service vpls 10 capture-sap 10 pfcp up-resiliency monitor-oper-group
 myopergroup health-drop 100
```

Step 5. Optional: Define a Layer 2 access ID alias to simplify the correlation of the A/S PWs on two different MAG-u nodes when provisioning UP groups on the cMAG-c.

Example

```
configure service vpls 10 capture-sap 10 l2-acces-id-alias l2alias1
```

9.3.3.2 Maintenance on a Nokia MAG-u in an A/S PW setup

About this task

Because the **drain** command is not supported in a MAG-u resiliency setup with A/S PW access, Nokia recommends performing the following procedure for MAG-u maintenance. For example, perform this procedure for upgrading the MAG-u or restarting the PFCP association.

Avoid performing maintenance on multiple MAG-u nodes in parallel. If multiple MAG-u nodes require maintenance, execute the procedure for each MAG-u one at a time.

Note: Some steps in this procedure contain MD-CLI commands that you must execute on the MAG-u in MD-CLI mode.
See the *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Command Reference Guide*, the MD-CLI online help, or the MD-CLI Explorer Tool included with the 7450 ESS, 7750 SR, 7950 XRS, and VSR WebHelp for more information about the MAG-u CLI syntax.

Procedure

Step 1. Verify that no FSG changes are ongoing for FSGs related to the MAG-u; for example, changes as a result of finalizing a maintenance procedure for another MAG-u.

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

a. Use the following CLI to display the UP groups and FSGs related to the MAG-u.

The asterisk (*) indicates all UP groups and FSGs, and the *peer-id* variable must be the node ID of the UP that requires maintenance.

```
info flat from state /subscriber-management ref-points up group * fsg * peer peer-id
 | filter keys-only
```

The following output example shows statistics for the following UP groups:

- domain 1 with FSG ID 4 and UP peer east
- domain 2 with FSG ID 5 and UP peer east

Example

```
# info flat from state /subscriber-management ref-points up group * fsg * peer up-
east | filter keys-only
/ subscriber-management ref-points up group domain_1 fsg 4 peer up-east statistics
 sgrp-messages
/ subscriber-management ref-points up group domain_2 fsg 5 peer up-east statistics
 sgrp-messages
```

b. Execute the following command for each FSG listed in the output of the previous substep.

Replace the *up-group* and *fsg-id* variables with the values from the output in the previous substep.

```
info detail depth 0 flat from state /subscriber-management ref-points up group up-
group fsg fsg-id | eql "standby-up-ready = 'false' or standby-up-changing = 'true'
 or active-up-changing = 'true' or current-hold-off-delay is set" | filter fields
 standby-up-ready standby-up-changing active-up-changing current-hold-off-delay
```

This command checks the value of the following fields of each FSG:

- **standby-up-ready** – boolean value that indicates whether a standby MAG-u is available, is not failed, and has all hot standby sessions installed
- **standby-up-changing**– boolean value that indicates whether the standby MAG-u is currently being changed
- **active-up-changing** – boolean value that indicates whether the active MAG-u is currently being updated
- **current-hold-off-delay** – time duration value that indicates an FSG reselection is scheduled (even if one is not currently ongoing) or no value indicates no scheduled reselection

c. If output is generated for the FSG fields, this indicates a change is in process that must complete; execute the preceding command to check the progress.

If no output is generated, no changes are required.

If only **standby-up-ready** indicates **false**, and there is no **hold-off-delay** set and no active or standby changing indicator, an issue may be present on the current standby MAG-u that is preventing it from becoming ready. For example, the MAG-u may be set to drain mode or may have completely failed.

Step 2. On the MAG-u, disable the PW port.

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

Example

```
configure pw-port 1 sdp 1 admin-state disable
```

Example

```
configure pw-port 2 epipe 2 admin-state disable
```

Step 3. If a PFCP association restart is required as part of the maintenance operations, disable the PFCP association on the MAG-u.

Example

```
configure subscriber-mgmt pfcp association association1 admin-state disable
```

Step 4. Execute the required maintenance operations on the MAG-u.

Step 5. If a PFCP association restart was required in step 3, enable the PFCP association on the MAG-u.

Example

```
configure subscriber-mgmt pfcp association association1 admin-state enable
```

Step 6. After the MAG-u maintenance operations fully complete, perform step 1 again to verify that the FSGs are stable and the cMAG-c synchronizes all the sessions.

Step 7. On the MAG-u, enable the PW port that you disabled in step 2.

Example

```
configure pw-port 1 sdp 1 admin-state enable
```

Example

```
configure pw-port 2 epipe 2 admin-state enable
```

9.3.3.3 Bringing down the PW in headless conditions

About this task

The MAG-u must fully bring down the PW when operating in headless mode. This forces the access node to also switch over because it perceives a failed MAG-u. To bring down the PW on a Nokia MAG-u in headless conditions, perform the following steps on the NokiaMAG-u. See Fixed access with active/standby pseudowire access for more information.

Note: You must execute the commands in this procedure on the MAG-u in the MD-CLI mode. The equivalent MAG-uclassic CLI commands are available but may have slightly different syntax. See the *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Command Reference Guide*, the MD-CLI online help, or the MD-CLI Explorer Tool delivered with the *7450 ESS, 7750 SR, 7950 XRS, and VSR WebHelp Library* for more information about the MAG-u CLI syntax.

Procedure

Step 1. Configure an operational group to monitor the path between the MAG-u and the cMAG-c.

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

Example

```
configure service oper-group myopergroup
```

Step 2. Apply the operational group under the PFCP association.

Example

```
configure subscriber-mgmt pfcp association association1 oper-group myopergroup
```

Step 3. Set up the configured operational group for monitoring under the SDP linked to the PW port. This causes the system to bring down the SDP and PW port when in headless mode.

```
configure pw-port number sdp reference monitor-oper-group reference
```

9.3.3.4 Moving an FSG to standby in headless mode

About this task

Perform the following steps on the Nokia MAG-u to automatically move an FSG to standby when headless operations occur. See Fixed access with active/standby pseudowire access for more information.

Note: You must execute some of the commands in this procedure on the MAG-u in the MD-CLI mode.
See the *7450 ESS, 7750 SR, 7950 XRS, and VSR MD-CLI Command Reference Guide*, the MD-CLI online help, or the MD-CLI explorer tool delivered with the *7450 ESS, 7750 SR, 7950 XRS, and VSR WebHelp Library* for more information about the MAG-u CLI syntax.

Procedure

Step 1. Create an FSG template on the MAG-u.

Example

```
configure subscriber-mgmt up-resiliency fate-sharing-group-template fsg1
```

Step 2. In the configured FSG template on the MAG-u, set the path restoration state to **standby**.

Example

```
configure subscriber-mgmt up-resiliency fate-sharing-group-template fsg1 path-
restoration-state standby
```

Step 3. Apply the FSG template to the FSG on the cMAG-c.

- If the configured FSG template name is "default" and the cMAG-c does not specify any template, the template is automatically applied and no further configuration is needed.
- If the configured FSG template name is different from "default", perform the following substeps.

a. Create an FSG template on the cMAG-c.

```
subscriber-management profiles fsg-profile
```


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

b. In the configured FSG profile on the cMAG-c, set the MAG-u FSG template name to the FSG template name configured in step 1.

```
subscriber-management profiles fsg-profile up-fsg-template
```

c. Apply the cMAG-c FSG template to the UP group for the A/S PW port on the cMAG-c.

```
subscriber-management ref-points up group fsg-profile
```

Example

The following example shows a full configuration to apply a MAG-u FSG template named "force_standby"

```
# info from running with-context / subscriber-management profiles fsg-profile up-pw-
template
    subscriber-management {
        profiles {
            fsg-profile up-pw-template {
                up-fsg-template force_standby
            }
        }
    }

# info from running with-context / subscriber-management ref-points up group north-south-
pw
    subscriber-management {
        ref-points {
            up {
                group north-south-pw {
                    fsg-profile up-pw-template
                    l2-access-id [
                        pw-1
                    ]
                    peer up-north {
                    }
                    peer up-south {
                    }
                }
            }
        }
    }
```

9.3.4 Fixed access with broadcast access

Fixed access sessions require the Layer 2 circuit (Layer 2 access ID and VLAN parameters) that is learned from incoming IBCP packets. In a resilient setting, the Layer 2 circuits can differ between the MAG-u nodes. For example, in Figure 15: Multiple MAG-u backup nodes, Layer 2 access ID "central-A" on MAG-u "central" is backed up by Layer 2 access ID "west-A" on MAG-u "west". Because the cMAG-c cannot rely on the initial IBCP messages to learn all the Layer 2 access IDs, the IDs must be configured manually.

Layer 2 circuits with Layer 2 access ID configuration

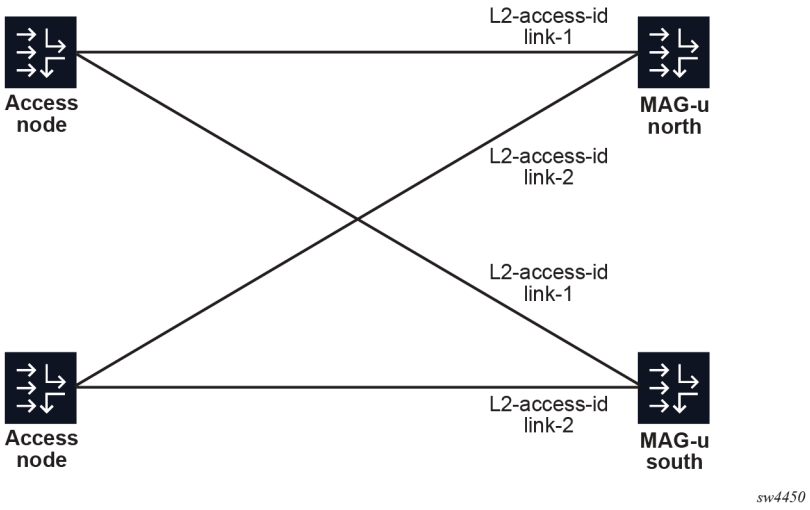
A single Layer 2 access ID can be configured per MAG-u in a UP group. When setting up a new session for this UP group, the cMAG-c learns the initial Layer 2 access ID from the incoming IBCP packet, but derives the Layer 2 access IDs for the other MAG-u nodes from the configuration. A UP group-level default

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

can be configured to simplify cases where the Layer 2 access IDs are identically named. See the example 1:1 hot standby resiliency example with two connected MAG-u nodes in Hot-standby resiliency examples for this use case.

When all MAG-u nodes use identical Layer 2 access IDs, it is possible to list multiple Layer 2 access IDs per UP group at the group level to avoid creating multiple UP groups for each Layer 2 access ID. When this is configured, the MAG-u assumes that each Layer 2 access ID is backed up by the identically named Layer 2 access ID on other MAG-u nodes. The cMAG-c does not assume that there is one big broadcast domain shared between all ports and does not move sessions between differently named Layer 2 access IDs. The following figure shows a UP group that covers two Layer 2 access IDs, named "link-1" and "link2". The sessions on "link-1" cannot be backed up on "link-2" because "link-2" connects to another access node.

Figure 17: Multiple Layer 2 access IDs per UP group



Example: UP group configuration with two Layer 2 access IDs

```
# info from running with-context /subscriber-management ref-points up group demo
    subscriber-management {
        ref-points {
            up {
                group demo {
                    l2-access-id [
                        link-1
                        link-2
                    ]
                    peer north {
                    }
                    peer south {
                    }
                }
            }
        }
    }
```


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

Layer 2 circuit with VLAN range configuration

Similarly, a VLAN range can be configured per MAG-u for both S-tags and C-tags. A UP group level default is also available. The VLAN range configuration serves the following purposes:

- Split a single Layer 2 access ID in multiple FSGs and set a different preferred status on different MAG-u nodes. In stable conditions, this achieves active/active behavior where some sessions are active on one MAG-u while others are active on another MAG-u. See 1:1 hot standby resiliency example with two connected MAG-u nodes in Hot-standby resiliency examples for this use case.
- Set different VLAN ranges on several MAG-u nodes in more complex aggregation requirements. The cMAG-c automatically adjusts the VLANs learned from IBCP for each MAG-u based on the difference between the start values of the VLAN ranges of each MAG-u. For example, if MAG-u A is configured with range 100 to 200, and MAG-u B with range 500 to 600, a session with VLAN 150 on MAG-u A automatically uses VLAN 550 on MAG-u B. While the start values of the VLAN range can be different, all ranges must have an equal size. For example, it is not possible to configure a range of 100 to 200 on one MAG-u, and 100 to 300 on another MAG-u in the same UP group.



WARNING: VLAN ranges with a different offset over more MAG-u nodes are an advanced use case and should be carefully validated against the deployed aggregation network. To avoid accidentally enabling different offsets when this functionality is not required, Nokia recommends only configuring a VLAN range on the UP group level.

A UP group can reference a VLAN list instead of one contiguous range. To do so, use the **s-tag-list** or **c-tag-list** option in the following context.

```
subscriber-management ref-points up group
```

Related topics

In-band control plane and MAG-u selection

Session keys and anti-spoofing

9.3.4.1 Blocking the setup of non-resilient sessions

About this task

If a packet is received that does not match a configured UP group, the cMAG-c always sets up the packet as a non-resilient session. However, consider the following examples where this may occur although it is not intended:

- A newly-provisioned MAG-u is not yet added to a UP group because the PFCP connection must first be validated.
- A MAG-u is temporarily excluded from a UP group to identify potential resiliency issues with that specific MAG-u.



Note: For this case Nokia recommends enabling the drain mode (**true** option) using the following command to avoid this issue.

```
subscriber-management ref-points up group peer drain
```

- Multiple MAG-u nodes are part of the same broadcast domain, but are split in multiple smaller 1:1 UP groups, such as shown in 1:1 hot standby resiliency example with four MAG-u nodes sharing a

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

broadcast domain. In this specific example, if a session setup packet (for example, DHCP discover) comes in with s-tag1 on MAG-u nodes "west" or "south", it is set up as a non-resilient session if no further action is taken.

To avoid setup of unintentional, non-resilient sessions, Nokia recommends to configure the ADB to reject non-resilient sessions in these contexts.

Note: This procedure shows matching on a node ID. By matching on MAG-u node ID only, non-resilient sessions are matched because resilient sessions only match a group ID. If required, the user can further restrict this to only match non-resilient sessions on a specific Layer 2 access ID or VLAN range. See Authentication database for more information about combining ADB match criteria.

Procedure

Step 1. Reuse an existing ADB or create a new ADB using the following command.

```
subscriber-management authentication-database
```

Step 2. Configure a match criterion for the ADB to match on the MAG-u node ID using the following command.

```
subscriber-management authentication-database match attribute up-node-id
```

Step 3. Block non-resilient ADB packets, by using the following commands to configure node ID matching and action reject for the ADB entries.

```
subscriber-management authentication-database entry match up-node-id
subscriber-management authentication-database entry action reject
```

Output example: Block non-resilient traffic

The following output example shows a configuration that blocks non-resilient traffic (using node ID and reject action matching) for the example shown in 1:1 hot standby resiliency example with four MAG-u nodes sharing a broadcast domain.

```
# info from running with-context /subscriber-management authentication-database basic-adb
    subscriber-management {
        authentication-database block-non-resilient {
            match 1 {
                attribute up-node-id
            }
            entry block-east-non-resilient {
                match {
                    up-node-id up-east
                }
                action {
                    reject
                }
            }
            entry block-north-non-resilient {
                match {
                    up-node-id up-north
                }
                action {
                    reject
                }
            }
```


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

```
            entry block-south-non-resilient {
                match {
                    up-node-id up-south
                }
                action {
                    reject
                }
            }
            entry block-west-non-resilient {
                match {
                    up-node-id up-west
                }
                action {
                    reject
                }
            }
        }
    }
```

9.3.4.2 Hot-standby resiliency examples

Find deployment use cases and example UP group configurations for the MAG-u hot standby resiliency concepts.

1:1 hot standby resiliency example with two connected MAG-u nodes

Four access nodes are connected to a pair of MAG-u nodes using a shared broadcast domain. This illustrates how to model the common model of direct 1:1 MAG-u resiliency where two MAG-u nodes only back up each other. To simplify Layer 2 forwarding, each access node is assigned a unique S-tag. The broadcast domain is connected to each MAG-u through an identically-named Layer 2 access ID on both MAG-u nodes. The cMAG-c makes abstraction of whether this connection is a port, LAG, BGP-VPLS, EVPN, or any similar construct.

Note: To achieve identical naming on a Nokia MAG-u, provision a Layer 2 access ID alias using the following command on the MAG-u:

- **MD-CLI**

  ```
  configure service vpls capture-sap pfcp l2-access-id-alias
  ```

- **classic CLI**

  ```
  configure service vpls sap pfcp l2-access-id-alias
  ```

  See the *7750 SR and VSR BNG CUPS User Plane Function Guide* for more information about configuring the MAG-u.

The goal is to have hot standby resiliency, in stable conditions (both MAG-u nodes are healthy), such that the active sessions are split between the two MAG-u nodes. The following configurations achieve this goal:

- Split the Layer 2 access IDs based on S-tag ranges in two UP groups, each serving half of the access nodes.
- Configure a different MAG-u as preferred in each group to make the associated FSG active on the preferred MAG-u as long as that MAG-u is healthy.

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

Note: The configuration of an FSG profile is not required because the default mode is hot standby and applied automatically.

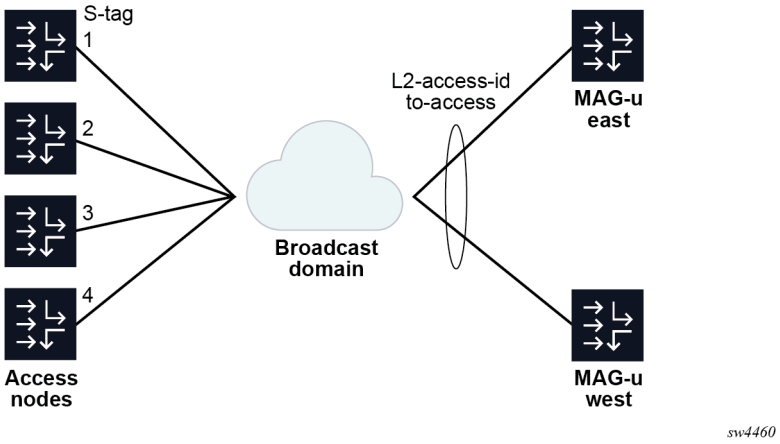
Example

```
# info from running with-context /subscriber-management ref-points up group prefer-east
    subscriber-management {
        ref-points {
            up {
                group prefer-east {
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 1
                        end 2
                    }
                    peer up-east {
                        preferred true
                    }
                    peer up-west {
                        preferred false
                    }
                }
            }
        }
    }
# info from running /subscriber-management ref-points up group prefer-west
    subscriber-management {
        ref-points {
            up {
                group prefer-west {
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 3
                        end 4
                    }
                    peer up-east {
                        preferred false
                    }
                    peer up-west {
                        preferred true
                    }
                }
            }
        }
    }
```

The following figure shows an example for a 1:1 hot standby resiliency with an S-tag per access node.

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

Figure 18: 1:1 hot standby resiliency example



1:1 hot standby resiliency example with four MAG-u nodes sharing a broadcast domain

This example extends the previous model with two access nodes and two MAG-u nodes to illustrate how a shared broadcast domain with more than two MAG-us can be modeled.

Instead of splitting the MAG-u nodes such that there are two pairs of 1:1 MAG-u nodes, each S-tag range gets a different pair of standby MAG-u nodes as follows:

- S-tag 1 is backed by MAG-u "north" and "east"
- S-tag 2 is backed by MAG-u "east" and "west"
- S-tag 3 is backed by MAG-u "west" and "south"
- S-tag 4 is backed by MAG-u "south" and "north"
- S-tag 5 is backed by MAG-u "north" and "west"
- S-tag 6 is backed by MAG-u "east" and "south"

Example

```
# info from running with-context /subscriber-management ref-points up group s-tag-*
    subscriber-management {
        ref-points {
            up {
                group s-tag-1 {
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 1
                        end 1
                    }
                    peer up-east {
                    }
                    peer up-north {
                    }
                }
                group s-tag-2 {
                    l2-access-id [
                        to-access
                    ]
```

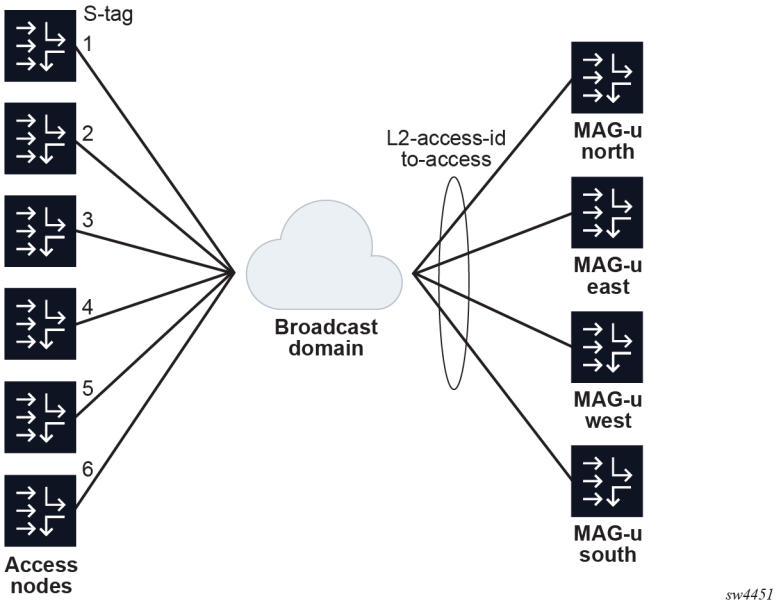

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
                    s-tag-range {
                        start 2
                        end 2
                    }
                    peer up-east {
                    }
                    peer up-west {
                    }
                }
                group s-tag-3 {
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 3
                        end 3
                    }
                    peer up-south {
                    }
                    peer up-west {
                    }
                }
                group s-tag-4 {
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 4
                        end 4
                    }
                    peer up-north {
                    }
                    peer up-south {
                    }
                }
                group s-tag-5 {
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 5
                        end 5
                    }
                    peer up-north {
                    }
                    peer up-west {
                    }
                }
                group s-tag-6 {
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 6
                        end 6
                    }
                    peer up-east {
                    }
                    peer up-south {
                    }
                }
            }
        }
    }
```


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

The following figure shows an example of a per S-tag 1:1 hot standby resiliency.

Figure 19: Per S-tag 1:1 hot standby resiliency example



When using default FSGs, the cMAG-c distributes the FSGs and sessions as equal as possible by default:

- Two MAG-u nodes have two active FSGs.
- Two MAG-u nodes have one active FSG.

To improve the balance, you can add more S-tags or more MAG-u nodes or both. For example, using 12 S-tags with a UP group each leads to a balance where each MAG-u has three active FSGs.

The difference between a MAG-u-level 1:1 model and an S-tag-level 1:1 model lies in the impact of multiple MAG-u failures. For example, compare the deployment where "north" and "south" back up each other and "east" and "west" back up each other without overlap. We assume each S-tag range is responsible for about 1/6th of the traffic. The following are conditions of node failures:

- When two MAG-u nodes fail in the per-S-tag mode, it always impacts 1/6th of the traffic because each pair of MAG-u nodes is always uniquely responsible for one S-tag out of six. For example, if "north" and "south" fail, S-tag 4 completely fails.
- When two MAG-u nodes fail in the per-MAG-u mode, the impact depends on which nodes fail and that can either impact 0% or 50% of the traffic. For example, if both "north" and "west" fail, there is no lasting traffic impact because they do not back up each other. If both "south" and "north" fail, all traffic of the two S-tags covered by these MAG-u nodes fails.

This effect becomes stronger with more MAG-u nodes and S-tags to distribute. For example, in a model with 10 MAG-u nodes, the configuration can limit a failure of two MAG-u nodes to only affect about 2% of the traffic versus potentially 20% of the traffic if five 1:1 pairs are used.

This model makes the following assumptions on the aggregation model:

- A shared L2 broadcast domain must be available for all MAG-u nodes.
- A suitable granularity to differentiate UP groups must be available, such as S-tags in the example above.

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

- The MAG-u failures are unrelated. If the MAG-u failures happen in bulk (for example, because they are co-located), it can be better to make sure no co-located MAG-u nodes back up each other instead of to distribute resiliency as much as possible.

Attention: This model requires additional configuration to avoid setting up non-resilient sessions on VLANs on a MAG-u that is part of the broadcast domain, but not part of the UP group for that VLAN. See Blocking the setup of non-resilient sessions for more information.

9.3.4.3 Warm-standby resiliency examples

Find deployment use cases and example UP group configurations for the MAG-u warm standby resiliency concepts.

N:1 warm standby resiliency example with three connected MAG-u nodes

This example is a variant of the model described in 1:1 hot standby resiliency example with two connected MAG-u nodes:

- Instead of the two MAG-us ("east" and "west") backing up each other, each MAG-u is backed up by a dedicated third MAG-u ("backup").
- Four access nodes are connected using a shared broadcast domain with each access node defined by its own S-tag.

Note: This example shows a 2:1 resiliency setup and is kept minimal for clarity. It is possible to configure higher oversubscribed resiliency ratios such as 4:1 or 10:1, or even an N:K model as illustrated in N:K warm standby resiliency example with six connected MAG-u nodes.

When both active MAG-u nodes are healthy, the active sessions are split between MAG-u "east" and MAG-u "west" based on the S-tag. S-tags 1 and 2 go to MAG-u "east" while S-tags 3 and 4 go to MAG-u "west". All sessions have the third MAG-u ("backup") as a standby, but no sessions are preinstalled on this MAG-u. MAG-u "backup" is oversubscribed and preinstalling all sessions would exhaust its resources.

The cMAG-c only creates sessions on MAG-u "backup" when either MAG-u "east" or MAG-u "west" fails. To enable this form of redundancy, link the UP group to an FSG profile that has a default standby mode set to warm. See Standby modes for more information about warm standby resiliency.

Because MAG-u "backup" is oversubscribed, it must only be used during failure conditions or when one of the other MAG-u nodes is being drained. To achieve this, configure "east" and "west" as **preferred** in each UP group. See Fate sharing group creation for more information about the **preferred** indicator. For illustrative purposes, the **active-change-without-failure** property in the FSG profile is explicitly set to its default of **always**, which forces a revert to the preferred MAG-u as soon as it recovers. See Active/standby selection for more information about the **active-change-without-failure** property.

Caution: Enabling reverting behavior and setting a **preferred** MAG-u is crucial in any N:1 or N:K deployment.Not doing so may result in session loss because sessions are not actively moved away from the oversubscribed standby MAG-u nodes which leads to resource exhaustion.

Example

```
# info from running with-context / subscriber-management profiles fsg-profile warm
    subscriber-management {
        profiles {
            fsg-profile warm {
                default-standby-mode warm
                active-standby-selection {
```

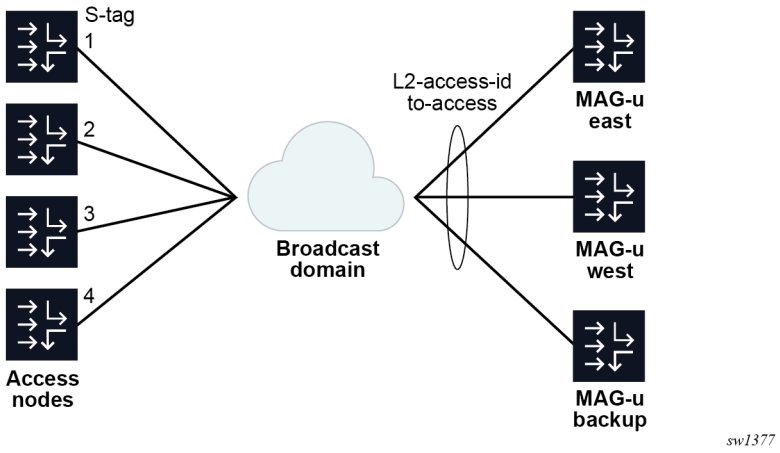

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
                    active-change-without-failure {
                        always
                    }
                }
            }
        }
    }
# info from running with-context / subscriber-management ref-points up group s-tag-*
    subscriber-management {
        ref-points {
            up {
                group s-tag-1-2 {
                    fsg-profile warm
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 1
                        end 2
                    }
                    peer up-backup {
                    }
                    peer up-east {
                        preferred true
                    }
                }
                group s-tag-3-4 {
                    fsg-profile warm
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 3
                        end 4
                    }
                    peer up-backup {
                    }
                    peer up-west {
                        preferred true
                    }
                }
            }
        }
    }
```

The following figure shows the example topology used for N:1 warm standby resiliency.

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

Figure 20: N:1 warm standby resiliency example



N:K warm standby resiliency example with six connected MAG-u nodes

This example extends the Hot-standby resiliency examples by adding two active nodes and a backup node. This essentially achieves a 4:2 redundancy setup with the following properties:

- MAG-u nodes are linked in pairs of active and backup. There is no concept of a redundant backup. For example, if MAG-u "backup-one" fails, all sessions connected to the pairs <"east", "backup-one">, <"west", "backup-one">, <"north", "backup-one">, < "south", "backup-one"> continue without a backup until that MAG-u recovers.
- Sessions are assigned to a pair based on the S-tag. For example, S-tags 1 and 2 are still assigned to MAG-u "east" but are now split over two different backups.

The main advantage of this model over modeling 2x2:1 groups is better recovery times and more flexibility. After failure of a single MAG-u, the installation of warm standby sessions is now spread over two backup MAG-u nodes instead of a single backup MAG-u. This also allows combinations like 7:3 that are harder to split into separate N:1 setups.

```
# info from running with-context / subscriber-management profiles fsg-profile warm
    subscriber-management {
        profiles {
            fsg-profile warm {
                default-standby-mode warm
                active-standby-selection {
                    active-change-without-failure {
                        always
                    }
                }
            }
        }
    }
# info from running with-context / subscriber-management ref-points up group s-tag-*
    subscriber-management {
        ref-points {
            up {
                group s-tag-1 {
                    fsg-profile warm
                    l2-access-id [
                        to-access
                    ]
```


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

```
                    s-tag-range {
                        start 1
                        end 1
                    }
                    peer up-backup-one {
                    }
                    peer up-east {
                        preferred true
                    }
                }
                group s-tag-2 {
                    fsg-profile warm
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 2
                        end 2
                    }
                    peer up-backup-two {
                    }
                    peer up-east {
                        preferred true
                    }
                }
                group s-tag-3 {
                    fsg-profile warm
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 3
                        end 3
                    }
                    peer up-backup-one {
                    }
                    peer up-west {
                        preferred true
                    }
                }
                group s-tag-4 {
                    fsg-profile warm
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 4
                        end 4
                    }
                    peer up-backup-two {
                    }
                    peer up-west {
                        preferred true
                    }
                }
                group s-tag-5 {
                    fsg-profile warm
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 5
                        end 5
                    }
```

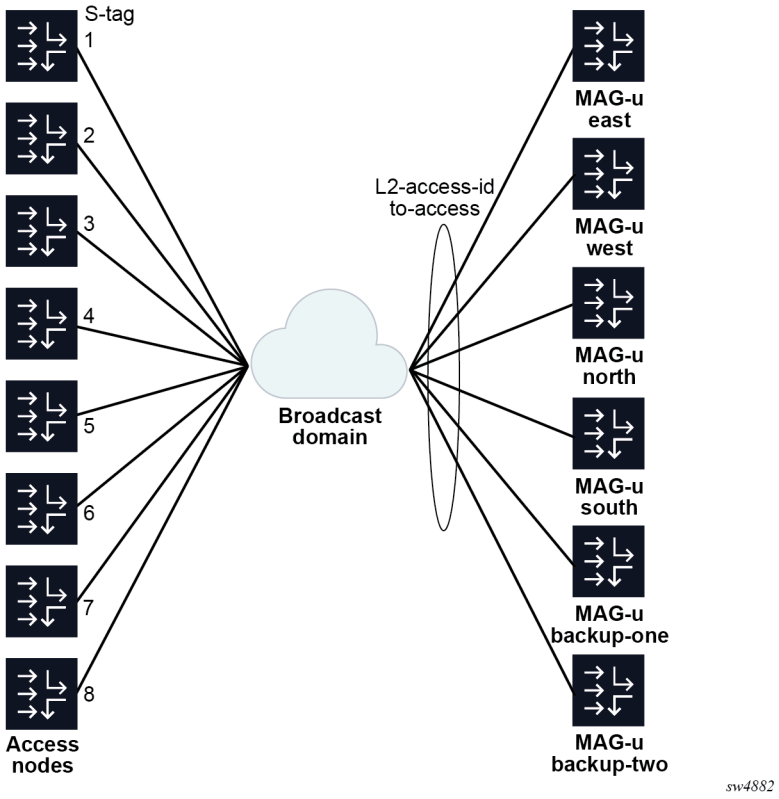

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms.

```
                    peer up-backup-one {
                    }
                    peer up-north {
                        preferred true
                    }
                }
                group s-tag-6 {
                    fsg-profile warm
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 6
                        end 6
                    }
                    peer up-backup-two {
                    }
                    peer up-north {
                        preferred true
                    }
                }
                group s-tag-7 {
                    fsg-profile warm
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 7
                        end 7
                    }
                    peer up-backup-one {
                    }
                    peer up-south {
                        preferred true
                    }
                }
                group s-tag-8 {
                    fsg-profile warm
                    l2-access-id [
                        to-access
                    ]
                    s-tag-range {
                        start 8
                        end 8
                    }
                    peer up-backup-two {
                    }
                    peer up-south {
                        preferred true
                    }
                }
            }
        }
    }
```

The following figure shows the example topology used for N:K warm standby resiliency.

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

Figure 21: N:K warm standby resiliency example



Mixing hot and warm standby

N:1 and N:K solutions are primarily aimed at warm standby sessions, but it is possible to make a subset of sessions hot standby on a per FSG or per session basis. See Standby modes for more information about how to configure this. This can be useful to give expedited recovery times to a small number of sessions while maintaining a generic oversubscribed resiliency architecture. In such deployments, the following applies:

- The oversubscribed resiliency architecture must take into account that hot standby sessions are always present on the backup MAG-u. For example, consider a 4:1 setup where each active MAG-u handles 100 000 sessions and there is an overall maximum of 225 000 sessions per MAG-u:
  - **only warm standby resiliency**
    Up to two active MAG-u nodes can fail. The standby MAG-u has 200 000 sessions when two MAG-u nodes fail.
  - **10% of the sessions are in hot standby resiliency**
    Up to two active MAG-u nodes can fail. The standby MAG-u has a persistent load of 40 000 hot standby sessions. When two MAG-u nodes fail, the standby MAG-u has 220 000 sessions: 200 000 from the two failed MAG-u nodes and 20 000 hot standby sessions from the two non-failed MAG-u nodes.
  - **20% of the sessions are in hot standby resiliency**
    Only one active MAG-u can fail. The standby MAG-u has a persistent load of 80 000 sessions. When one MAG-u fails, the standby MAG-u has 160 000 sessions: 100 000 from the failed MAG-u

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

and 60 000 hot standby sessions from the three non-failed MAG-u nodes. A second MAG-u failure would require capacity for 240 000 sessions.

Note: The numbers in this example are purely illustrative. Real capacity numbers depend on MAG-u hardware and session resource consumption.

- When a standby MAG-u recovers after failure, there is no priority between installing hot or warm sessions in force-hot mode as described in Standby modes. Therefore, if there is a second failure during the recovery period, hot standby sessions are as vulnerable as warm standby sessions and state may be lost.

9.3.5 Performing maintenance on a Nokia MAG-u

About this task

Nokia recommends performing the following procedure for MAG-u maintenance where session stability cannot be guaranteed; for example, for upgrading the MAG-u or restarting the PFCP association.

Note:
If multiple MAG-u nodes require maintenance, execute the procedure on each MAG-u sequentially. Avoid performing maintenance on multiple MAG-u nodes in parallel.

Commit the configuration after each step.

Procedure

Step 1. Verify that no FSG changes are ongoing for FSGs related to the MAG-u; for example, changes as a result of finalizing a maintenance procedure for another MAG-u.

a. Use the following CLI to display the UP groups and FSGs related to the MAG-u.

The asterisk (*) indicates all UP groups and FSGs, and the *peer-id* variable must be the node ID of the UP that requires maintenance.

```
info flat from state /subscriber-management ref-points up group * fsg * peer peer-id
 | filter keys-only
```

The following output example shows statistics for the following UP groups:

- domain 1 with FSG ID 4 and UP peer east
- domain 2 with FSG ID 5 and UP peer east

Example

```
# info flat from state /subscriber-management ref-points up group * fsg * peer up-
east | filter keys-only
/ subscriber-management ref-points up group domain_1 fsg 4 peer up-east statistics
 sgrp-messages
/ subscriber-management ref-points up group domain_2 fsg 5 peer up-east statistics
 sgrp-messages
```

b. Execute the following command for each FSG listed in the output of the previous substep.

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

Replace the *up-group* and *fsg-id* variables with the values from the output in the previous substep.

```
info detail depth 0 flat from state /subscriber-management ref-points up group up-
group fsg fsg-id | eql "standby-up-ready = 'false' or standby-up-changing = 'true'
 or active-up-changing = 'true' or current-hold-off-delay is set" | filter fields
 standby-up-ready standby-up-changing active-up-changing current-hold-off-delay
```

This command checks the value of the following fields of each FSG:

- **standby-up-ready** – boolean value that indicates whether a standby MAG-u is available, is not failed, and has all hot standby sessions installed
- **standby-up-changing**– boolean value that indicates whether the standby MAG-u is currently being changed
- **active-up-changing** – boolean value that indicates whether the active MAG-u is currently being updated
- **current-hold-off-delay** – time duration value that indicates an FSG reselection is scheduled (even if one is not currently ongoing) or no value indicates no scheduled reselection

c. If output is generated for the FSG fields, this indicates a change is in process that must complete; execute the preceding command to check the progress.

If no output is generated, no changes are required.

If only **standby-up-ready** indicates **false**, and there is no **hold-off-delay** set and no active or standby changing indicator, an issue may be present on the current standby MAG-u that is preventing it from becoming ready. For example, the MAG-u may be set to drain mode or may have completely failed.

Step 2. Enable the drain mode (**true** option) for the MAG-u using the following CLI.

- for all UP groups

```
subscriber-management ref-points up peer drain
```

- for a single UP group (if maintenance is limited to a single group)

```
subscriber-management ref-points up group peer drain
```

Example

Enable drain mode for all UP groups

```
# info from running with-context subscriber-management ref-points up peer up-east
    subscriber-management {
        ref-points {
            up {
                peer up-east {
                    admin-state enable
                    drain true
                    address-resolution {
                        static-ip [
                            192.0.2.11
                        ]
                    }
                }
            }
        }
```


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

```
    }
```

Example

Enable drain mode for a single UP group

```
# info from running with-context / subscriber-management ref-points up group prefer-
east peer up-east
    subscriber-management {
        ref-points {
            up {
                group prefer-east {
                    peer up-east {
                        preferred true
                        drain true
                    }
                }
            }
        }
    }
```

Step 3. Verify that the MAG-u is no longer active in any FSG and that the FSGs are stable.

a. List the MAG-u state in all FSGs and filter by role.

The asterisk (*) indicates all UP groups and FSGs, and the *peer-id* variable must be the node ID of the MAG-u that requires maintenance.

```
info depth 0 flat from state /subscriber-management ref-points up group * fsg *
 peer peer-id | eql "role = 'active'" | filter fields role
```

The MAG-u is no longer active if the output of the **info** command does not return any data. If this is not the case, wait until no entries are returned. Periodically execute the preceding command to check this information.

b. Execute the following command for the FSGs identified in step 1.

This command is similar to the command in step 1, except it does not check the **standby-up-ready** option. That is because the MAG-u being drained is often the standby MAG-u, and a drained MAG-u can never be ready.

```
info detail depth 0 flat from state /subscriber-management ref-points up group up-
group fsg fsg-id | eql "standby-up-changing = 'true' or active-up-changing = 'true'
 or current-hold-off-delay is set" | filter fields standby-up-changing active-up-
changing current-hold-off-delay
```

c. Do one of the following, depending on the output for the FSG fields.

- If no output is returned, no changes are ongoing; proceed to the next step.
- If any output is returned, a change is in process that must complete; periodically execute the preceding command to check the progress.

Step 4. Execute the required maintenance operations (for example, an upgrade or PFCP Association restart) on the MAG-u.

Step 5. After the MAG-u maintenance operations fully complete, perform step 3 to verify that the FSGs are stable.

Step 6. Disable the **drain** mode for the MAG-u using the following CLI.

```
delete subscriber-management ref-points up peer drain
```


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

```
delete subscriber-management ref-points up group peer drain
```

Example

Disable drain mode for all UP groups

```
--{ candidate shared-exclusive default }--[  ]--
A:cmagc@cmag-c# delete /subscriber-management ref-points up peer up-east drain

--{ * candidate shared-exclusive default }--[  ]--
A:cmagc@cmag-c# commit stay
/system:
    Saved current running configuration as initial (startup) configuration '/etc/opt/
srlinux/config.json'

All changes have been committed. Starting new transaction.

--{ candidate shared-exclusive default }--[  ]--
A:cmagc@cmag-c# info from running / subscriber-management ref-points up peer up-east
    admin-state enable
    address-resolution {
        static-ip [
            192.0.2.11
        ]
    }
```

Example

Disable drain mode for a single UP group

```
--{ candidate shared-exclusive default }--[  ]--
A:cmagc@cmag-c# delete / subscriber-management ref-points up group prefer-east peer
 up-east drain

--{ * candidate shared-exclusive default }--[  ]--
A:cmagc@cmag-c# commit stay
/system:
    Saved current running configuration as initial (startup) configuration '/etc/opt/
srlinux/config.json'

All changes have been committed. Starting new transaction.

--{ candidate shared-exclusive default }--[  ]--
A:cmagc@cmag-c# info from running with-context / subscriber-management ref-points up
 group prefer-east peer up-east
    subscriber-management {
        ref-points {
            up {
                group prefer-east {
                    peer up-east {
                        preferred true
                    }
                }
            }
        }
    }
```

Step 7. Optionally, use the following command to get a global overview of the MAG-u and its current state in all UP groups after the maintenance procedure is completed.

```
show subscriber-management ref-points up peer
```


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

See Operational commands for more information.

Note: This command is intended to provide an easy-to-access overview. It can be used to assist in the previous steps, but it does not replace the checks imposed on the commands in the **info from state** context.

Example

State of a MAG-u after maintenance

```
# show subscriber-management ref-points up peer up-east
===============================================================================
Peer up-east
  Type                   : fqdn
  Admin-state            : enable
  Up-state               : active
  Association-state      : up
  Apply-state            : applied
  Number-of-hot-sessions : 0
  Number-of-warm-sessions: 0
-------------------------------------------------------------------------------
Group prefer-east
  Fsg-profile            : demo
  Number-of-hot-sessions : 0
  Number-of-warm-sessions: 0
  L2-access-id           : vpls_access
  Active-in-fsg          : 3
```

9.3.6 Operational commands

To fetch all the operational data for the UP groups, use the following command.

```
info from state / subscriber-management ref-points up group fsg
```

Example: state information for the FSG associated with the group "prefer-east"

```
# info depth 0 from state / subscriber-management ref-points up group prefer-east fsg *
    fsg 3 {
        fsg-state active
        active-up-peer up-east
        standby-up-peer up-west
        number-of-hot-sessions 0
        number-of-warm-sessions 0
        active-up-changing false
        standby-up-changing false
        standby-up-ready true
        virtual-mac-address 02:00:5E:00:00:03
    }
```

In addition, the cMAG-c provides the following built-in show commands. These commands give a high-level summary of the UP groups and FSGs, without needing to build complex queries for the **info from state** command.

To display an overview of the UP group information, use the following command.

```
show subscriber-management ref-points up group
```


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

This overview includes:

- information per UP group about whether the group is active and which FSG profile parameters are applied
- list of FSGs relevant to the UP group, with information about which MAG-u nodes are active and standby, as well as how many sessions are linked to that FSG
- all MAG-u nodes that are part of the group, as well as all health values for each MAG-u

Example: information for the group "prefer-east"

```
# show subscriber-management ref-points up group prefer-east
===============================================================================================
Group prefer-east
  Oper-state  : up
  Apply-state : applied
-----------------------------------------------------------------------------------------------
Fsg-profile demo
  Apply-state                  : applied
  Hold-off-on-recovery         : 300000
  Hold-off-on-degradation      : 0
  Failure-lockout              : 60
  Failure-threshold            : 1
  Aggregation-mode             : lowest
  Include-l2-access-ids        : true
  Default-standby-mode         : hot
  Mac-prefix                   : 02:00:5e:00
  Network-instance             : hsi
-----------------------------------------------------------------------------------------------
Fsg 3
  Active-up-peer         : up-east
  Active-up-peer-health  : 100
  Standby-up-peer        : up-west
  Standby-up-peer-health : 100
  Virtual-mac-address    : 02:00:5E:00:00:01
  Number-of-hot-sessions : 0
  Number-of-warm-sessions: 0
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
Peer up-east
  Role               : active
  Preferred          : true
  Drain              : false
+-----------------------------------------------------------------------------------------+
|                       Instance                                      Health              |
+=========================================================================================+
| hsi                                                         100                         |
+-----------------------------------------------------------------------------------------+
+-----------------------------------------------------------------------------------------+
|                      Access-id                                      Health              |
+=========================================================================================+
| vpls_access                                                 100                         |
+-----------------------------------------------------------------------------------------+
-----------------------------------------------------------------------------------------------
Peer up-west
  Standby-in-fsg     : 3
  Preferred          : false
  Drain              : false
+-----------------------------------------------------------------------------------------+
|                       Instance                                      Health              |
+=========================================================================================+
| hsi                                                         100                         |
```


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

```
+-------------------------------------------------------------------------------+
+-------------------------------------------------------------------------------+
|                     Access-id                                  Health         |
+===============================================================================+
| vpls_access                                            100                    |
+-------------------------------------------------------------------------------+
```

To display an overview of MAG-u peer information, use the following command.

```
show subscriber-management ref-points up peer
```

This overview includes:

- peer state and how many sessions are connected to that MAG-u
- list of all groups the MAG-u is part of and basic group parameters per group, as well the active and standby FSGs for this MAG-u

Example: information for the peer "up-east"

```
# show subscriber-management ref-points up peer up-east
===============================================================================
Peer up-east
  Type                   : fqdn
  Admin-state            : enable
  Up-state               : active
  Association-state      : up
  Apply-state            : applied
  Number-of-hot-sessions : 0
  Number-of-warm-sessions: 0
-------------------------------------------------------------------------------
Group prefer-east
  Fsg-profile            : demo
  Number-of-hot-sessions : 0
  Number-of-warm-sessions: 0
  L2-access-id           : vpls_access
  Active-in-fsg          : 3
```

9.4 Fate sharing groups

Fate sharing groups (FSGs) are groups of sessions on which resiliency operations are performed. FSGs are automatically created based on configured UP groups. The FSGs are provisioned via the UP group.

When an FSG is created, the cMAG-c performs the following operations:

- Map new sessions to the FSG (see Session-to-FSG mapping).
- Determine traffic management parameters to attract traffic only to the MAG-u that serves the specific FSG (see Traffic steering parameters).
- Determine an aggregated health value for each MAG-u in the FSG.
- Upon MAG-u state and health changes, reselect an active and standby MAG-u for the FSG. Any change triggers this reselection, which guarantees that no state change is lost. In many cases, the cMAG-c selects the same active and standby MAG-u as before.
- Upon any active/standby change, update the FSG state on the MAG-u and, if necessary, update the session state on the MAG-u.

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

FSGs follow an intent-based processing model. The configuration specifies the conditions of resiliency behavior, expressing its intent. For example, the configuration specifies whether switchovers should be revertive and whether there is a preferred MAG-u. The cMAG-c monitors multiple parameters and, if necessary, changes active/standby decisions to better match the intent. The cMAG-c may execute multiple subsequent FSG changes to accomplish this.

Related topics

Fate sharing group creation

9.4.1 Session-to-FSG mapping

When setting up a fixed access session, the cMAG-c uses the MAG-u ID, the Layer 2 access ID, and the VLAN ranges of the triggering IBCP packet to look up a UP group. If a UP group contains this set of parameters, the cMAG-c links the session automatically to the FSG created for that UP group.

9.4.2 Traffic steering parameters

FSGs specify the granularity for the session switchover from one MAG-u to another. A MAG-u must uniquely attract traffic for a specific FSG in both the uplink and downlink direction without affecting other FSGs. To achieve this, the cMAG-c:

- associates unique uplink and downlink parameters with each FSG
- signals those parameters to the MAG-u as part of creating the FSG when that MAG-u is selected as active or standby MAG-u for that specific FSG

ODSA allocates a unique set of per-FSG subnets (micro-nets). Because the subnets are unique per FSG, the active MAG-u can announce these subnets. To achieve the uniqueness, a session that is linked to an FSG passes the FSG as an allocation context to ODSA. ODSA automatically makes the micro-nets unique in that context.

Note: A standby MAG-u can also announce the subnet in routing messages but it should make sure that the subnet has lower priority. To achieve this, the standby MAG-u appropriately sets metrics or preference values in the used routing protocol.

For fixed access sessions, the cMAG-c generates a unique MAC address per FSG. When receiving ARP or ND requests in the scope of sessions or subnets linked to a specific FSG, only the active MAG-u can respond to the requests with the unique MAC address. This makes sure that any MAC forwarding databases in the Layer 2 aggregation point to the correct active gateway. Each time the cMAG-c signals a MAG-u to become active, the MAG-u can generate GARPs with the unique MAC address to expedite traffic convergence to the new active MAG-u. The cMAG-c bases the generation of the MAC addresses on a /32 prefix configuration. Use the following command to configure the prefix.

```
subscriber-management profiles fsg-profile mac-prefix
```

The default 02-00-5e-00 prefix is based on the MAC prefix used for VRRP, with the L bit flipped to remove its globally unique significance.

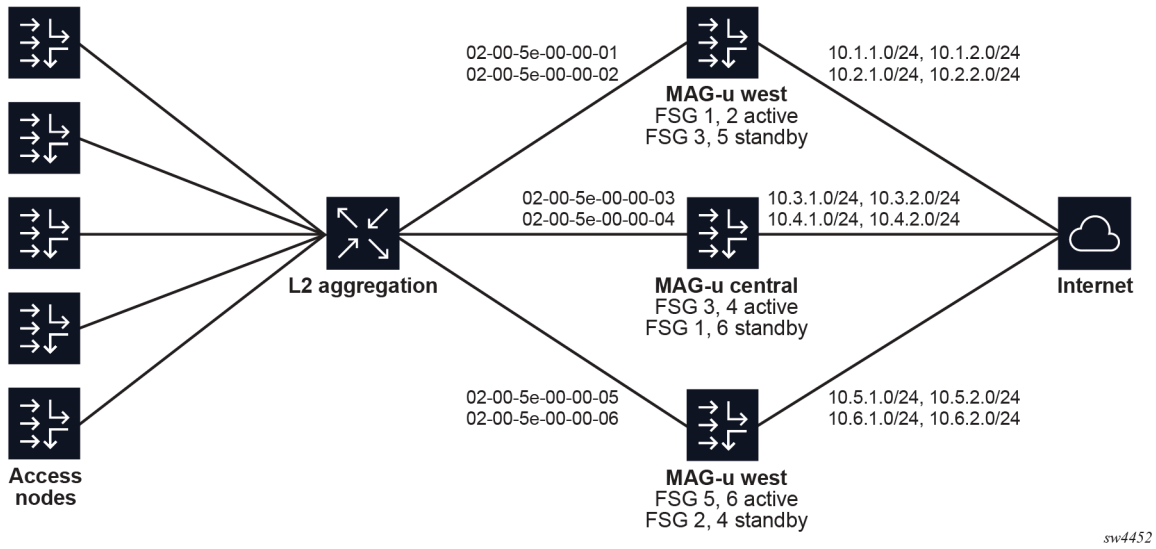
Example of the relationship between FSGs, MAC addresses, and subnets shows the MAC addressing for 6 FSGs with 2 subnets each, distributed over 3 MAG-u nodes. The relationship between the FSGs, MAC addresses, and subnets is as follows:

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

- FSG 1
  MAC 02-00-5e-00-00-01
  session subnet 10.1.1.0/24
  session subnet 10.1.2.0/24
- FSG 2
  MAC 02-00-5e-00-00-02
  session subnet 10.2.1.0/24
  session subnet 10.2.2.0/24
- FSG 3
  MAC 02-00-5e-00-00-03
  session subnet 10.3.1.0/24
  session subnet 10.3.2.0/24
- FSG 4
  MAC 02-00-5e-00-00-04
  session subnet 10.4.1.0/24
  session subnet 10.4.2.0/24
- FSG 5
  MAC 02-00-5e-00-00-05
  session subnet 10.5.1.0/24
  session subnet 10.5.2.0/24
- FSG 6
  MAC 02-00-5e-00-00-06
  session subnet 10.6.1.0/24
  session subnet 10.6.2.0/24

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

Figure 22: Example of the relationship between FSGs, MAC addresses, and subnets



Related topics

ODSA

9.4.3 MAG-u health determination

The MAG-u health is the main criterion that the cMAG-c uses to determine the active and standby MAG-u. Health is a value between 0% and 100%; the -1 value indicates the MAG-u is unavailable. The following rules determine the MAG-u health per UP group:

- When the PFCP path between the cMAG-c and the MAG-u is in headless mode, the health value is -1 (unavailable).

  Note: If a PFCP association is not set up (for example, because the path is down), the MAG-u is operationally not part of the UP group and has no health.

- When either of the following are configured to true, the health value is -1 (unavailable).

```
subscriber-management ref-points up group peer drain
subscriber-management ref-points up peer drain
```

- In all other cases, the health value is based on an aggregation of the operational statuses received from the MAG-u.

  Note: See the *cMAG-c CLI and Data Model Explorer* for more information about the CLI syntax, including variable options.

The MAG-u can signal the following operational status values to the cMAG-c:

- **per Layer 2 access ID**

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

A percentage value per Layer 2 access ID indicates the current forwarding capacity compared to the full forwarding capacity. For example, if the Layer 2 access ID represents a LAG with five members where one member failed, the expected capacity is 80%.

- **per Layer 3 service (also known as network instance)**
  A binary connectivity status per Layer 3 service indicates whether the Layer 3 core network is reachable or not (connected or isolated). A Nokia MAG-u additionally augments this value with a percentage value to cover partial failures. The cMAG-c uses the more detailed percentage value if available; otherwise, the cMAG-c interprets the binary connectivity status as 100% for the connected state and 0% for the isolated state.

Not all status values of a single MAG-u apply to a specific FSG. For example, a UP group that only covers a single Layer 2 access ID is not impacted by the status of any other Layer 2 access ID. The cMAG-c determines the applicable status values as follows:

- By default, the cMAG-c uses for the aggregation all the Layer 2 access IDs configured for the MAG-u in the UP group. The following commands configure the Layer 2 access IDs.

```
subscriber-management ref-points up group peer l2-access-id
subscriber-management ref-points up group l2-access-id
```

- The cMAG-c can exclude configured Layer 2 access IDs from the health calculation if the user prefers not to track access health. The following command specifies whether to include Layer 2 access IDs and is **true** by default.

```
subscriber-management profiles fsg-profile health-calculation include-l2-access-ids
```

- The cMAG-c tracks a list of configured network instances for health aggregation. The following command configures the tracked network instances.

```
subscriber-management profiles fsg-profile health-calculation network-instance
```

To calculate a single health value from the set of status values, the cMAG-c applies an aggregation calculation that is configured using the following command.

```
subscriber-management profiles fsg-profile health-calculation aggregation-mode
```

The options for the aggregation mode are:

- **lowest**
  This mode sets the per-MAG-u health to the lowest value of any Layer 2 access ID and network instance value. A single failure aggressively decreases the health.
- **average**
  This option sets the per-MAG-u health to the arithmetic mean of all Layer 2 access ID and network instance values. A single failure less aggressively impacts the health.

If the MAG-u does not signal a status value for a Layer 2 access ID or a network instance that is configured to be tracked, the cMAG-c does not include it in the aggregate calculation. If the cMAG-c does not receive a status value for any Layer 2 access ID or network instance for the MAG-u, the cMAG-c uses a default health value of 100%.

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

In addition to the MAG-u health ranging from 0% to 100%, the cMAG-c maintains a simplified MAG-u failure state. A MAG-u is considered failed if its health is below the configured failure threshold. You can configure the failure threshold using the following command.

```
subscriber-management profiles fsg-profile health-calculation failure-threshold
```

By default, the failure threshold is set to 1% , meaning that only a MAG-u with a health value equal to 0% or unavailable (-1) is considered failed.

The cMAG-c maintains a special not-ready indicator for the current standby MAG-u. This indicator is set in the following conditions:

- The MAG-u changes to standby, independent of its previous state or health.
- The MAG-u health becomes unavailable (-1).

The cMAG-c removes the not-ready indicator each time an FSG change successfully completes (see Active/standby change or switchover) and the health of the MAG-u at that time is 0% or higher.

The cMAG-c avoids making a standby MAG-u that has the "not-ready" indicator active, unless it has no other choice; for example. when the PFCP association for the active MAG-u is released. This mechanism gives a failed or new standby MAG-u a chance to go through one FSG change sequence to reinstall all the hot standby sessions before it can be made active.

The cMAG-c can put a MAG-u in a lockout state for an FSG. When a MAG-u is in the lockout state, it cannot be made active or standby. Contrary to the other health values, the lockout state is intended to recover from hard failures where it is important that all FSG and related session state is removed from the MAG-u before it is considered active or standby again. See MAG-u lockout for more information.

The following table provides an overview of the states that are kept for MAG-u nodes that have an active association and that are linked to at least one FSG.

Table 12: Summary of MAG-u states

State	Description	Sources
health	Value between 0% and 100% or the special value -1 (unavailable) Indicates the health of the MAG-u	• Aggregation of the per-logical-port and per-network-instance health reports from the MAG-u. • PFCP path management state (for example, headless). • Drain mode configured with the following command. `subscriber-management ref-points up group peer drain`
failed indicator	Indicator that considers the MAG-u failed if its health is less than the failure threshold	Based on the health state and the threshold configured with the following command. `subscriber-management profiles fsg-profile`

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

State	Description	Sources
	Enables switchovers in more restrictive (for example, non-revertive) scenarios	`health-calculation failure-threshold`
not-ready indicator	Indicator on the standby MAG-u that does not have all hot standby sessions installed Kept until the standby MAG-u has installed the hot standby sessions	Set for each new standby MAG-u or a standby MAG-u whose health becomes unavailable (-1). Removed after the first successful FSG change when the health is 0% or higher.
lockout	Failure state in which the MAG-u cannot be made active or standby Kept until the MAG-u is no longer active or standby and a lockout timer has expired	Applied automatically for multiple failure scenarios, see MAG-u lockout for more information.

9.4.4 Active/standby selection triggers

The cMAG-c monitors multiple triggers that can impact the active/standby selection and trigger a potential switchover. Most events are classified as one of the following:

- recovery (for example, health up)
- degradation (for example, health down)

When a trigger occurs, the cMAG-c performs the following:

- starts a hold timer
- waits for the hold timer expiry
- triggers the active/standby selection

A different hold timer can be set for recovery and degradation using the following commands respectively.

```
subscriber-management profiles fsg-profile active-standby-selection hold-off-on-recovery
subscriber-management profiles fsg-profile active-standby-selection hold-off-on-degradation
```

Note: See the *cMAG-c CLI and Data Model Explorer* for more information about the full CLI syntax, including variable options that may apply.

By default, the degradation hold timer is disabled (0 ms) to immediately execute potential switchovers because of failure.

When a trigger occurs while the hold timer is running, the new hold timer is only applied if it is shorter than the one already running. For example, suppose the following events occur with 2 s in between:

- A health increase triggers a recovery hold timer of 5 s.
- A health decrease triggers the default degradation hold timer of 0 ms.

Because the second hold timer is shorter than the first one, the cMAG-c immediately triggers the active/standby selection for the degradation.

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

When a trigger occurs while an active/standby change is in progress, the cMAG-c ignores the hold timer of the new trigger and re-evaluates the active/standby selection as soon as the in-progress change completes.

The cMAG-c treats the following events as a recovery trigger:

- health increase; the cause of the health increase is irrelevant and may be because of headless recovery, change of the **drain** configuration of the MAG-u, or a MAG-u health report
- PFCP association setup, except if it is the first MAG-u set up for the FSG
- UP lockout removal
- intended FSG state not matching the current FSG state after an FSG event (see Active/standby change or switchover).

The cMAG-c treats the following events as a degradation trigger:

- health decrease
- PFCP association release, except if it is already the active or standby MAG-u
- UP lockout acts as a degradation trigger

The following exceptional triggers bypass the normal reselection mechanism because of their big impact:

- The setup of the first PFCP association for an FSG triggers an immediate reselection. The cMAG-c does not wait for the expiry of the recovery hold timer. If the PFCP association being set up is not the first association, it acts as a health increase and the cMAG-c starts the recovery hold timer.
- A PFCP association release for the active or standby MAG-u triggers an immediate reselection, bypassing any hold timers. If an active/standby change is already in progress, the ongoing change is completed first. A PFCP association release for any other MAG-u acts as a health decrease and the cMAG-c starts the degradation hold timer.
- If all MAG-u nodes become headless, the cMAG-c does not trigger any reselection. As soon as the first MAG-u recovers from headless, the cMAG-c ignores the recovery hold timer but starts a timer based on the configured path-management heartbeat intervals. The cMAG-c triggers reselection of all MAG-u nodes when one of the following occurs:
  - The timer based on the configured path-management heartbeat intervals expires.
  - Five seconds have passed after the last MAG-u recovered.



Note: This mechanism ensures that after a full connectivity failure, all MAG-u nodes have time to recover the PFCP communication. It makes sure that the cMAG-c makes decisions based on the full set of recovered MAG-u nodes and not on the first recovered MAG-u nodes.

9.4.5 Active/standby selection

When an active/standby selection trigger occurs, the cMAG-c re-evaluates the selection of the active and standby MAG-u nodes for an FSG. If only one MAG-u with an active association is available, that specific MAG-u is always selected as the active MAG-u. Otherwise, both the active and standby MAG-u can be reselected.

Replacing the active MAG-u with the current standby MAG-u works in one of the following basic modes:

- **revertive**

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

The current standby MAG-u can be selected as the active MAG-u even if the active MAG-u did not fail. The conditions in which the standby MAG-u can become the active MAG-u are the same as the conditions to select the standby MAG-u. Additionally, the standby MAG-u cannot have the not-ready indicator set. To configure which MAG-u to revert to when health is equal, use the **preferred** command in the following context.

```
subscriber-management ref-points up group peer
```

- **non-revertive**
  The current standby MAG-u can only be selected as the active MAG-u if the PFCP association of the current active MAG-u is removed or if the MAG-u is considered failed (see MAG-u health determination), or if the MAG-u is in lockout state (see MAG-u lockout). Otherwise, the current active MAG-u is always reselected as the active MAG-u.

To configure the mode, use the following CLI command.

```
subscriber-management profiles fsg-profile active-standby-selection active-change-without-failure
```

Note: See the *cMAG-c CLI and Data Model Explorer* for more information about the full CLI syntax, including variable options that may apply.

The following command options are available:

- **always**
  The cMAG-c always uses the revertive mode.
- **never**
  The cMAG-c always uses the non-revertive mode.

If the standby MAG-u becomes active, the active MAG-u automatically becomes standby. The cMAG-c takes no further action.

The cMAG-c selects a standby MAG-u independent of the revertive mode configuration.

Both the revertive active MAG-u and the standby MAG-u are selected using the following criteria. This is a fall-through list that stops as soon as there is only one MAG-u that meets all the criteria. Any MAG-u that is in lockout or for which the PFCP association is down is not considered.

1. MAG-u with the highest health (see MAG-u health determination)
2. **preferred** MAG-u
3. MAG-u with the lowest number of sessions, simulated as if the FSG would move to that MAG-u

   Note: To avoid unnecessary FSG changes when the number of sessions on several MAG-u nodes is very similar, the cMAG-c applies a weight multiplier to the FSG session count when it simulates a move to a different MAG-u than the current one.

4. MAG-u with the lowest amount of FSGs, excluding the current FSG, with the goal to provide initial load balancing when no sessions are set up
5. current state of the MAG-u, where the current active MAG-u has priority over the current standby MAG-u that has priority over any backup MAG-u to avoid any unnecessary active or standby changes if all else is equal
6. MAG-u with the lowest IP used in PFCP signaling, with no specific goal other than to have a deterministic tiebreaker when all else is equal

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

If the result of the active/standby selection differs from the current active/standby selection, the cMAG-c initiates an active/standby change.

If the result of the active/standby selection is the same as the current active/standby selection, but the health of any MAG-u has changed from unavailable (-1) to 0% or higher, the cMAG-c also initiates an active/standby change.

Otherwise, the cMAG-c takes no further action.

Note: The trigger to change the FSG for a recovered MAG-u (even without an active/standby change) is to guarantee that a MAG-u has all the PFCP state information after a potential communication failure between the MAG-u and the cMAG-c. The FSG change procedure guarantees that all the FSG states and PFCP session states are correctly downloaded if necessary. For example, when a standby MAG-u becomes headless, it may miss the FSG updates and session installations and modifications for hot standby sessions. When the MAG-u is recovered from headless, it becomes not ready (see section MAG-u health determination). The active/standby state does not change, but the cMAG-c triggers an FSG change procedure so that the latest FSG and session state are installed on the MAG-u. After the FSG change, the cMAG-c removes the not-ready indicator from the MAG-u and the standby MAG-u is again ready to fully take over.

9.4.6 Active/standby change or switchover

If the active/standby selection results in a new active or new standby MAG-u, the cMAG-c executes the change on the MAG-u nodes as follows:

1. The cMAG-c updates the PFCP FSG state on all involved MAG-u nodes.

   The change procedure ends if the active MAG-u does not positively confirm. If the active MAG-u change times out or explicitly returns an error, the cMAG-c rolls back the changed FSG states and stops the active/standby change procedure.

   Changes to other MAG-u nodes (for example, standby MAG-u nodes) may fail. This is even expected in some cases; for example, in 1:1 deployments where the previously active MAG-u has failed and becomes standby, the failed MAG-u is not expected to respond.

   A MAG-u that explicitly rejects an explicit FSG update is put into lockout. This triggers a degradation reselection, which is handled as soon as the change is completed. See MAG-u lockout for more information.

2. When the active MAG-u confirms the FSG change, the cMAG-c starts updating the PFCP session states. The exact update for each session depends on the change and the session resiliency model as follows:

   - **warm standby, active/standby switch**
     The cMAG-c establishes the session on the new active MAG-u and deletes it from the previous active MAG-u.
   - **warm standby, new standby MAG-u**
     No updates to the MAG-u nodes are needed.
   - **warm standby, health change only**
     No updates to the MAG-u nodes are needed.
   - **hot standby, active/standby switch**
     No updates to the MAG-u nodes are needed.

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

- **hot standby, new standby MAG-u**
  The cMAG-c establishes the session on the new standby MAG-u and deletes it from the previous standby MAG-u if there was one.
- **hot standby, health change only**
  This acts as a trigger to reinstall missing standby sessions on the standby MAG-u.

Note: When a warm standby session is in force hot standby mode, the hot standby behavior applies and not the warm standby behavior. See Make before break for warm standby for more information.

3. When the standby MAG-u confirms the FSG change, the cMAG-c sends a second FSG update message to the active MAG-u without changing anything. This can be done in parallel with the previous step. See GARP/ARP race conditions for more details on this step.
4. When the session change procedure is completed, the cMAG-c signals any required FSG deletions to the MAG-u.
5. When the change is completed, the cMAG-c evaluates whether the current active/standby state matches the expected active/standby state by running the selection logic again (see Active/standby selection). If the states do not match, the cMAG-c automatically triggers a recovery reselection and starts the recovery hold timer (see Active/standby selection triggers).

GARP/ARP race conditions

Fixed access connections use per-FSG MAC addresses to attract traffic (see Traffic steering parameters). Most Layer 2 aggregation switches keep a forwarding database (FDB) that points each gateway MAC address to the correct MAG-u to avoid broadcasting traffic. The FDBs are (amongst others) populated by snooping ARP and ND messages. To expedite updates of the FDBs during active/standby switchovers, the Nokia MAG-u generates a gratuitous ARP (GARP) message with the FSG MAC address when the FSG is signaled to become active. However, in a very exceptional case, a single GARP is not enough when the following conditions apply:

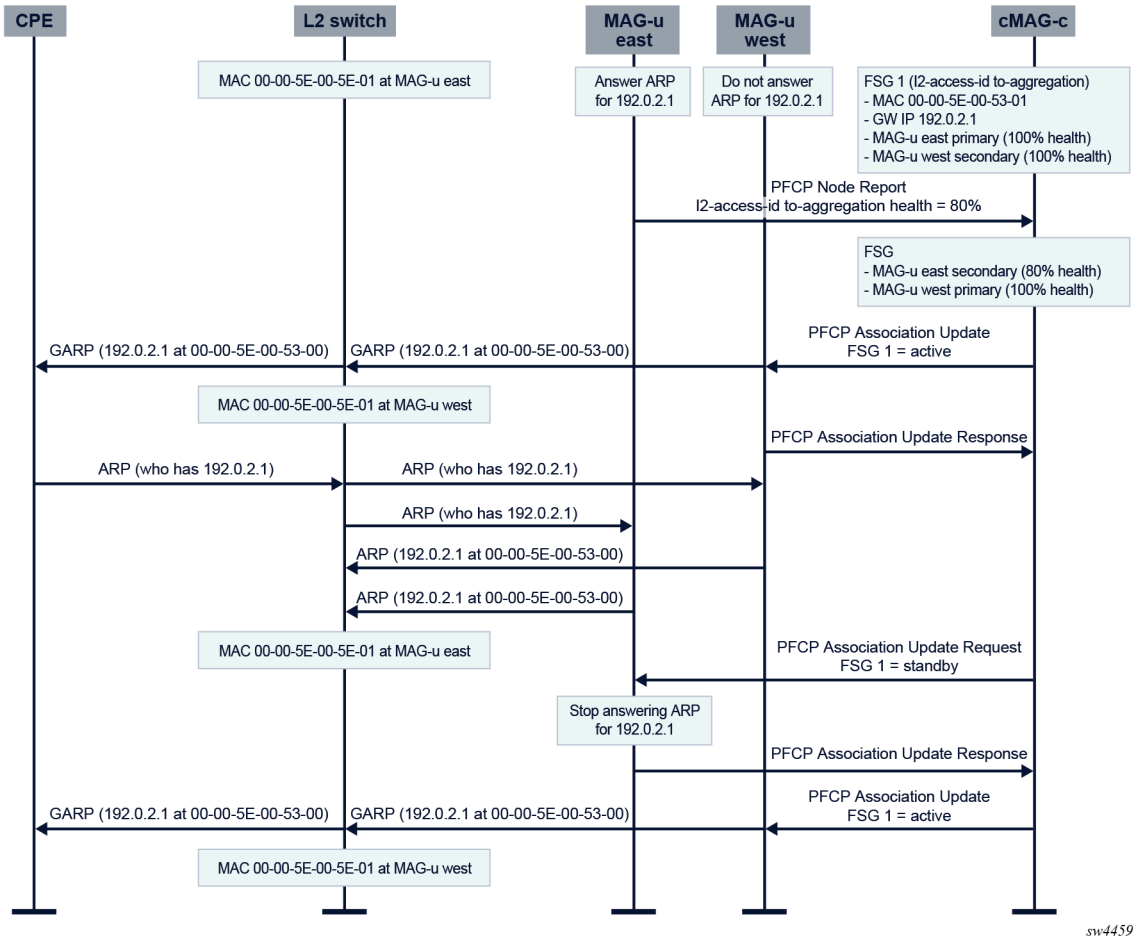
- The new standby MAG-u has not yet processed the message that asks it to become standby.
- A regular ARP is sent and broadcast as normal.
- Both MAG-u nodes answer, and the ARP response from the new standby MAG-u comes later than the ARP response of the new active MAG-u.

If the preceding conditions apply, the Layer 2 aggregation switch has a wrong FDB entry. Sending a second update to the new active MAG-u can act as a new GARP trigger to correct the situation. The following figure shows this case.

Note: The second update is a very lightweight operation as no actual FSG changes need to occur. It only acts as a GARP trigger. The MAG-u may not have any action to perform if it does not need to send GARPs; for example, on aggregation networks where the FDBs are populated out-of-band such as EVPN networks.

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

Figure 23: GARP race conditions



9.4.7 MAG-u lockout

To handle FSG failure scenarios, the cMAG-c can put a specific MAG-u in lockout for the failed FSG. The following example scenarios trigger lockout:

- an explicit FSG error from the MAG-u when signaling an FSG create, modify, or delete operation
- the path or association of a MAG-u goes down, in addition to setting its health to -1 (unavailable); see MAG-u health determination

Note: This applies only to a full PFCP path down, and not to headless mode. See Headless mode for more information about the differences. See Interaction with headless mode for more information about the interaction of MAG-u resiliency with headless mode.

The cMAG-c treats a MAG-u going in lockout as a degradation trigger for the FSG (see Active/standby selection triggers). The cMAG-c attempts to remove the locked out MAG-u from being selected as either active or standby (see Active/standby selection).

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

Because many failure scenarios do not have an automatic recovery signal, the lockout is subject to a timer. For explicit FSG errors, use the following command to configure the lockout timer.

```
subscriber-management profiles fsg-profile active-standby-selection failure-lockout
```

For other scenarios, the lockout timer is set to a fixed value, typically equal to the minimal configurable value. When the lockout timer expires, the cMAG-c performs one of the following actions:

- If the MAG-u is not active or standby for the FSG, the cMAG-c removes the lockout state and triggers a recovery reselection for the FSG.
- Otherwise, the cMAG-c restarts the lockout timer with a fixed value and takes no further action. This guarantees that the MAG-u is removed from the FSG at least one time and starts from a clean slate before it can be made active or standby again.

9.5 Standby modes

Warm and hot standby in MAG-u resiliency are a per-session concept that defines how a session is handled on the standby MAG-u:

- Warm standby sessions are created on the standby MAG-u when the MAG-u becomes active. The sessions are not created in advance on the standby MAG-u. This saves resources on the standby MAG-u, but it takes significantly longer before there is forwarding capability for those sessions after a switchover.
- Hot standby sessions are created in advance on the standby MAG-u. As soon as the MAG-u becomes active, it can start forwarding traffic for those sessions. While this consumes more resources on the standby MAG-u, it offers significantly reduced forwarding loss during a switchover. Depending on the capabilities of the aggregation network, it may even be possible to achieve a non-loss planned switchover; for example, to seamlessly handle MAG-u upgrades.

For hot standby, any procedure that interacts with a MAG-u change (for example, a CoA with a QoS update) first applies the change on the active MAG-u. If the change succeeds, the procedure updates the standby MAG-u . In the unlikely event that only the standby MAG-u update fails, the cMAG-c does not fail the triggering procedure. Instead, it tries to reapply the update periodically in the background until the standby MAG-u is realigned with the active MAG-u.

By default, the cMAG-c creates sessions in an FSG always in hot standby mode. Use the following command to change the default at a per-FSG level,

```
subscriber-management profiles fsg-profile default-standby-mode
```

Use the following command to change the mode on a per-session level.

```
subscriber-management authentication-database entry resiliency standby-mode
```

WARNING: On a large scale and depending on the install rate of the involved MAG-u nodes, it can take a long time for warm standby sessions to switch over. If timers such as the PPP keepalive, DHCP lease times, and RA lifetimes are set too short, they may time out before the switchover is completed.

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

Make before break for warm standby

When an FSG switchover is planned and not because of failure, the cMAG-c creates sessions on the standby MAG-u before the switchover occurs when specific conditions apply. This makes the window where traffic is impacted during the switchover much smaller and comparable to hot standby. The specific conditions are:

- **drain** is enabled for the active MAG-u in an FSG.
  This allows optimized behavior during MAG-u maintenance procedures such as upgrades. See Performing maintenance on a Nokia MAG-u for more information.
- The standby MAG-u is the **preferred** MAG-u in an FSG.

While these conditions apply, the cMAG-c enforces all affected sessions to temporarily act as hot standby sessions and creates them on the standby MAG-u. This proactive establishment of sessions on the standby MAG-u, embodying the make before break principle, is what the cMAG-c knows as force hot standby. As soon as the conditions no longer apply, the sessions act as warm standby sessions again and the cMAG-c removes any session state on the standby MAG-u.

Use the following state fields to verify whether the force hot standby mode is enabled for a specific FSG or session:

```
subscriber-management ref-points up group fsg force-hot-standby
subscriber-management subscriber session up force-hot-standby
```

9.6 Interaction with headless mode

MAG-u resiliency is supported in combination with the MAG-u headless mode (see Headless mode). When a MAG-u becomes headless, its health becomes unavailable (-1) because the cMAG-c cannot differentiate between a MAG-u toward which communication failed (headless) or a MAG-u that completely failed. See MAG-u health determination for more information.

A MAG-u becoming headless acts as a trigger to perform a potential switchover from active to standby. A switchover cannot be signaled to the headless MAG-u, which operates on stale data. The Nokia MAG-u, by default, uses a heuristic process to determine whether to keep FSGs active or make them standby during headless operations. In rare cases, the MAG-u may keep an FSG active while the cMAG-c has successfully made another MAG-u active. As a result, there is an active/active forwarding situation in which both the headless and non-headless MAG-u nodes of an FSG have an active state. In this scenario, the following applies:

- Uplink QoS cannot always be guaranteed because traffic may switch from one MAG-u to the other at any time. After headless recovery, the active/standby situation stabilizes and traffic flows through only one MAG-u with normal QoS guarantees.

  Note: Downlink QoS can still be guaranteed when the non-headless MAG-u announces routes with a higher preference than the headless MAG-u to consistently forward downlink traffic through the non-headless MAG-u. Additionally, if the access network updates its uplink forwarding based on downlink traffic, uplink traffic is forwarded through the non-headless MAG-u.

- Accounting reports may be off because traffic on the headless MAG-u is not counted. After headless recovery, the cMAG-c can fetch the missing statistics and the accounting is corrected.

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

- If there is unicast replication in the access network, these packets may end up being replicated also in the data network. However, this is extremely unlikely as the FSG MAC is most likely known at any point in time.

For more information about the headless heuristics and the downlink routing differentiation, see the *7750 SR and VSR BNG CUPS User Plane Function Guide*.

To avoid the unwanted consequences of the active/active state, configure the Nokia MAG-u to always automatically make any FSG standby when the headless conditions occur. This configuration avoids an active/active state, and one of following scenarios occurs:

- When a single MAG-u is headless, that MAG-u makes its FSGs standby and the cMAG-c makes the other MAG-u active. This results in an active/standby state as expected.
- When both MAG-u nodes are headless, for example, because of a networking issue at the cMAG-c, the FSG becomes standby on all MAG-u nodes and all traffic is dropped.

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

10 cMAG-c management

The cMAG-c management features are built on top of SR Linux management with some exceptions and differences from SR Linux.

The cMAG-c management features are built on top of SR Linux management, implemented via the management pod. Key features include:

- CLI
- SSH server
- NETCONF using YANG
- user management with AAA

The cMAG-c management features are identical to those of SR Linux with the following exceptions:

- Not all SR Linux management features are supported on the cMAG-c. See the *cMAG-c Release Notes* for a detailed list of supported features.

  Note: See the *SR Linux Configuration Basics Guide* and the *SR Linux System Management Guide* for information about the supported SR Linux management features.

- Specific aspects of the cMAG-c management features differ from SR Linux. See cMAG-c-specific system management for descriptions of these differences.

10.1 cMAG-c-specific system management

Specific aspects of cMAG-c management features differ from SR Linux.

Persistent Storage

The cMAG-c management features are implemented in a management pod that is run in Kubernetes. Therefore, file changes in the pod are not persistent unless they are stored, for example, with a persistent volume claim (PVC). The following folders provide persistent storage:

- `/etc/opt/srlinux`
- `/etc/ssh`
- `/python`
- `/var/log/srlinux`

Note: This folder stores cMAG-c log files and can grow over time. Nokia recommends regular cleanup.

External client to reach the management server

The cMAG-c is a cloud-native application running on top of Kubernetes. As a result, SR Linux network instance and source address configurations do not apply to the cMAG-c. The external-facing listening

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

addresses and ports of all management servers, including SSH and gNMI servers, are provisioned through the Kubernetes services. See the *cMAG-c Installation Guide* for more information.

Apply state

The cMAG-c has the following data stores:

- running data store – contains the intended configuration
- state data store – contains the applied configuration

The system typically applies configuration changes immediately, resulting in the running and state data store being identical. However, specific cases may prevent immediate application, causing long-lasting discrepancies between the intended and applied configurations.

Use the **apply-state** state to display the current apply state of the configuration node.

Only specific parts of the cMAG-c configuration have an apply state; see the cMAG-c CLI and Data Model Explorer for more information.

Example: Discrepancy caused by the removal of an ODSA pool prefix

When an ODSA pool prefix is removed from the running data store, but existing sessions use addresses from that prefix, the prefix remains present in the state data store with **to-be-removed** as the **apply-state**. When there are no sessions anymore that use addresses from the prefix, the prefix is removed from the state data store.

Configuration

During configuration, state data is persistently stored in the cMAG-c database. If there is no running data stored in the cMAG-c database when the management pod starts up, the system reads the configurations in the `config.json` file in the `/etc/opt/srlinux` directory.

SSH server

The host keys of the cMAG-c SSH server persist across management pod restarts. To rotate the host key:

1. Delete the key files with the `ssh_host` prefix located in the `/etc/ssh` and `/data/ssh` folders.
2. Restart the management pod.

User type

SR Linux supports the following management user types:

- local user
- remote user
- Linux user

The cMAG-c does not support the Linux user type.

System time

The cMAG-c is a distributed system consisting of multiple pods that can run on multiple Kubernetes workers. To ensure correct operation, synchronized and consistent time is required across the Kubernetes nodes and pods.

Nokia recommends the following practices:

- Synchronize the time of all nodes in the Kubernetes cluster using NTP.

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

- Use the UTC time for nodes and pods.

System name

Use the following cMAG-c CLI to configure the system name for the cMAG-c, instead of the **system name** command for SR Linux.

```
subscriber-management system name
```

Events and logging

The cMAG-c logs events to the following locations:

- management pod
- stdout of a specific pod

The log messages can be processed via the management pod.

Use the following CLI to inspect the log messages on a specific pod.

```
kubectl -n cmag-c logs pod-name
```

Use CLI in the **/system/logging** context to configure logging on the management pod, similar to SR Linux.

The cMAG-c differs from SR Linux in that it supports:

- no local persistence logging
- only memory buffer and remote server for logging destinations
- no persistent leaf in the buffer node
- only RSYSLOG_FileFormat for the format of the memory buffer

10.2 Accessing the cMAG-c GUI

Prerequisites

The cMAG-c GUI must be accessible via a domain name and a corresponding TLS certificate.

About this task

The cMAG-c uses role-based authorization to control access to GUI applications. An administrator configures the GUI authorization roles and assigns the appropriate roles to individual user accounts. A user with a password can access the generic GUI landing page, but the user must have the appropriate role to access a specific GUI application.

Procedure

Step 1. Configure the required system authorization roles using the supported application role names.

The following GUI role names are supported:

- **grafana** – accesses the built-in Grafana dashboards
- **call-trace** – accesses the Call Trace GUI; see Accessing the call trace GUI for more information

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

Example

Access role configuration

```
# info from running with-context / system aaa authorization
    system {
        aaa {
            authorization {
                role call-trace {
                }
                role grafana {
                }
            }
        }
    }
```

Step 2. Use the following CLI to create a user.

```
system aaa authentication user name
```

Step 3. Provision the user configured in step 2 with a password and the roles configured in step 1.

In the following example, cmagc_gui is the username. Replace *pass* with your own password.

Example

User configuration for a user named 'cmagc_gui'

```
# info from running with-context / system aaa authentication user cmagc_gui
    system {
        aaa {
            authentication {
                user cmagc_gui {
                    password pass
                    role [
                        grafana
                        call-trace
                    ]
                }
            }
        }
    }
```

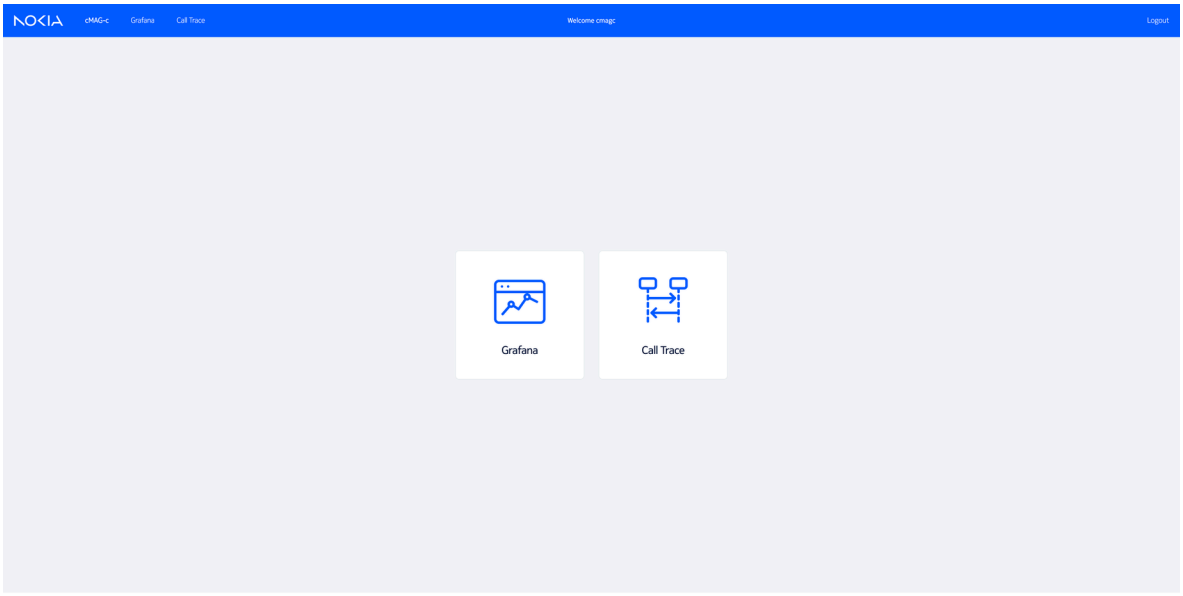
Repeat the user configuration for each user who requires access to a GUI application, assigning only the roles that the user requires.

Step 4. Log in to the GUI using the configured domain name and the credentials of a configured user.

The following figure shows the GUI after a successful login by a user with Grafana and Call Trace roles assigned.

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

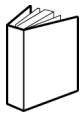
Example



Step 5. If the login fails, verify the user's password, and then log in again. If the login succeeds but the expected GUI applications are not available, verify the user's assigned roles. After correcting the configuration, select **Logout** in the upper-right corner of the page, and then log in again.

© 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