Multi-Access Gateway – controller

Releases up to 24.3.R1

Control Plane Function Advanced Configuration Guide

3HE 21092 AAAA TQZZA
Edition: 01
October 2024

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.

Table of contents

List of tables

List of figures

Preface

About This Guide

Each Advanced Configuration Guide is organized alphabetically and provides feature and configuration explanations, CLI descriptions, and overall solutions. The Advanced Configuration Guide chapters in this guide are written for and based on MAG-c Release 24.3.R1.

The Advanced Configuration Guides supplement the user configuration guides listed in the MAG-c Guide to Documentation. This guide supplements the MAG-c Control Plane Function Guide .

Audience

This manual is intended for network administrators who are responsible for configuring the routers. It is assumed that the network administrators have a detailed understanding of networking principles and configurations.

Multi-Access Gateway Lawful Intercept - Fixed Wireless Access

This chapter provides information about Multi-Access Gateway (MAG) Lawful Intercept (LI) - Fixed Wireless Access (FWA).

Topics in this chapter include:

- Applicability
- Overview
- Configuration
- Conclusion

Applicability

The information and the configuration in this chapter are based on Multi-Access Gateway (MAG) controller (MAG-c) and SR OS Release 24.3.R1.

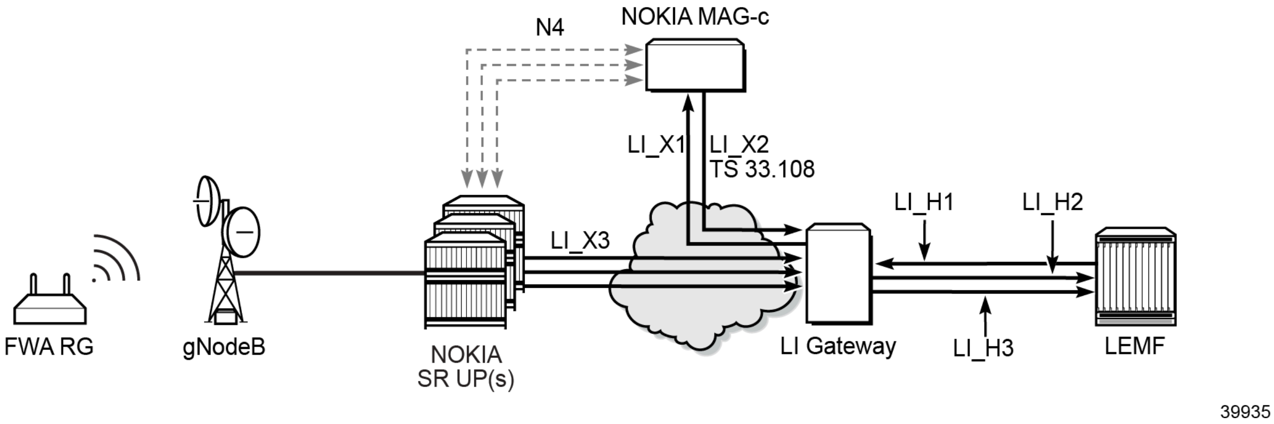
Overview

This chapter provides basic Lawful Intercept (LI) configurations for Fixed Wireless Access (FWA) broadband subscribers in a non-redundant MAG setup.

The LI target is the target to be monitored within the MAG LI system.

This chapter provides a MAG configuration example for the 3GPP X1, X2, and X3 interfaces. These X interfaces are based on 3GPP TS 33.107 and TS 33.108 for 4G and on 3GPP TS 33.127 and RS 33.128 for 5G. Figure 1: X interfaces for the MAG shows the X1, X2, and X3 interfaces for the MAG.

Figure 1: X interfaces for the MAG



The preceding figure lists the X interfaces for the MAG:

- The X1 interface in this document refers to 4G X1_1 and 5G LI_X1 interface. The X1 interface connects the MAG-c and the LI Gateway (LIG) and is used for configuration: setting up LI targets and the MAG-c LI infrastructure.
- The X2 interface in this document refers to 4G X2_1 and 5G LI_X2. It is also known as the Intercept Relation Information (IRI) interface. The X2 interface is used for transporting IRI LI target related events to the LIG. In 4G, the X2 interface to the LIG is often referred to as the delivery function (DF) 2 peer (DF2 peer).
- The X3 interface in this document refers to the Communication Content (CC) interface for both 4G and 5G. The CC interface is used to transport the mirrored packets from each User Plane (UP) to the LIG. In 4G, the LIG often is often referred to as the DF3 peer.

Characteristics

- The MAG-c supports 4G X1_1 CLI over the SSH interface. This interface is Nokia proprietary.
- The Supported Surveillance Target identifiers on the LI_X1 interface are: IMSI and MSISDN.
- The MAG-c supports multiple DF2 peers for processing IRI.
- The MAG-c supports one CC destination per FWA LI target.
- All IRI messages for a single target are sent to one DF. All CC messages for a single target are sent to one DF. The LIG, if configured, can perform any required fan-out and deliver the IRI messages to multiple Law Enforcement Agencies (LEAs). Activating a target using more than one identity (for example, IMSI and MSISDN) results in a single stream of IRI sent to the LIG. When multiple identities are activated for a target, it is expected that the LIG peer is the same for a given target.
- For 4G, the X2 interface uses TCP/IP as its transport protocol with TPKT encapsulation as per TS 33.108 section G2.1.2.2. The MAG-c 4G X2 IRI messages are ASN.1-encoded as per Annex B.9 of 3GPP Specification 33.108 [1]. Both IPv4 and IPv6 are supported.
- The 4G Lawful Intercept ID (LIID) is relevant only to LIG and the LEA. If a LIID is provisioned at the time of target activation, its value is populated in IRI messages. If a LIID is not provisioned at the time of

target activation, a default value is populated in the IRI message because it is a mandatory parameter in the ASN.1 (this default value can be safely ignored by the LIG).

- IRI messages are uni-directional and do not have a response message. A MAG-c includes at least one target ID when sending an IRI message to the LIG-DF. Additional target IDs, such as MSISDN, can be included in the X2 message, if available.
- The X3 interface utilizes UDP as transport to the LIG and the mirrored packets are encapsulated with an IP-UDP shim header. Only IPv4 IP/UDP shim is supported.

Configuration

The sequence to activate LI on MAG FWA is as follows:

- MAG-c and user plane FWA LI infrastructure setup through SSH CLI:
  - MAG-c FWA LI infrastructure setup provisioned through SSH CLI
  - User plane (UP) LI infrastructure setup provisioned through SSH CLI
- LI target provisioning:
  - 4G LI target provisioning for 4G IRI events through SSH CLI
  - 5G LI target provisioning for 5G IRI events through TCP/TLS based on ETSI 103.221-1
  - 4G and 5G LI target provisioning for CC through SSH CLI

The MAG-c and UP LI infrastructure setup is typically performed once at commissioning and rarely requires any additional configuration after commissioning.

It is expected that the operator repeats the three LI target provisioning steps for each FWA LI target. The reason for provisioning both 4G and 5G LI is because the operator may not be able to determine if the FWA subscriber is a 4G or a 5G Residential Gateway (RG). Therefore, to cover all bases, each FWA LI target is provisioned as both a 4G and a 5G LI FWA target. If the operator is certain that the end subscriber is only 4G capable, then only steps 1 and 3 are required. And if the operator is certain that the end customer has a 5G RG capable of falling back to 4G access then only steps 2 and 3 are required.

MAG-c and user plane FWA LI infrastructure setup through SSH CLI

The X1 interface on the MAG-c is a CLI interface over SSH. It is used for provisioning both the LI infrastructure and the LI targets. The LI X1_1 interface can only be accessed by CLI users with LI permission. CLI users without LI permission cannot view or manage LI configuration on the node. On MAG-c, a user with administrative access is required to create a user with LI permission first. For more information on LI user setup, see the 7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide. For more information on separating LI management from regular management, see the 7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide.

The X1 interface utilizes the common SSH IP address for generic MAG-c management. The user access rights determine the region the user can log into: regular management or LI management. It is possible to configure dedicated in-band SSH IP interfaces for LI management. For more information on SSH management, see the 7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide.

By default, the MAG-c denies the LI configuration file save. The saving of the LI configuration file locally is determined by the Boot Option File (BOF) setting. Any change on the BOF requires a reboot of the MAG-c. If the LI configuration is saved locally, the configuration is encrypted and the encryption key is unique per system. Saving the LI configuration allows the system to survive node failures and node reboots without the need for re-provisioning. The command **configure li save** is used to save the LI configuration.

It is assumed that the LIG periodically executes the target retrieval command for audits to maintain data integrity.

LI infrastructure setup: Setting up the 4G X2_1 interface

MAG-c supports one local X2_1 interface and maximum 16 DF2 peers.

The following command is used to configure the X2_1 local interface:

```
config>li>mobile-gateway ?
[no] local-interface <ip-address> [router <router-instance>]
[over-ride x2-interface <x2-ip-address> [x2-router <x2-router-instance>]]
```

The **configure li mobile-gateway local-interface** command is used to provision the source IP address used by the MAG-c for the LI X2 interface for both 4G and 5G (described in later sections). The **no** form of the command reverts to the default: **no local-interface**. The **over-ride x2-interface** option is an extension to the existing CLI used to specify a different IP address and/or VPRN for the 4G X2 interface. The 5G interface always takes the local interface IP address.

Table 1: Information elements for the 4G X2_1 local interface

Information Element (IE)	Description
local-interface	Source IP address used by xGW for LI interface
ip-address	IPv4 or IPv6 address of the xGW
router-instance	VPRN routing context identifier. Defaults to base routing context, when not specified.
x2-ip-address	Source IP address (IPv4 or IPv6) for the X2 interface.
x2-router-instance	VPRN routing context identifier for X2 interface.

Note:
By default, when the **over-ride x2-interface** option is not used, X2 utilizes the local interface. The X2 override command overrides both the 4G and 5G X2 interface.

Note:
The **local-interface** cannot be modified when targets/peers are configured/in service.

Some examples:

- Example 1:

  ```
  local-interface 1.1.1.1 router 1
  ```

  [X2-IP = 1.1.1.1] [X2-VPRN = 1]

- Example 2:

  ```
  local-interface 1.1.1.1 router 1 over-ride x2-interface 1.1.1.1 x2-router 2
  ```

  [X2-IP = 1.1.1.1] [X2-VPRN = 2]

- Example 3:

  ```
  local-interface 1.1.1.1 router 1 over-ride x2-interface 10.0.0.1 x2-router 2
  ```

  [X2-IP = 10.0.0.1] [X2-VPRN = 2]

The following command is used to configure the DF peer ID:

```
config>li>mobile-gateway ?
[no] df-peer <df-peer-Id> df2-addr <iri-addr> df2-port <port-num>
                        [df2-tls-profile <client-tls-profile-name>]
```

The **configure li mobile-gateway** command is used to provision a DF peer, which includes DF2 used for IRI of a Lawful Intercept Gateway.

Table 2: IEs for the DF peer ID

Information element (IE)	Comment
Delivery function peer ID	1-16
IRI DF address	IP address of the DF where the IRI is to be sent
IRI port number	TCP port of the DF where the IRI is to be sent
Client TLS profile	The client TLS profile used for the TLS connection between MAG-c and DF peer. Creation of a client TLS profile is covered in Appendix: Transport Layer Security.

LI infrastructure setup: Setting up the 5G X1 interface

The LI_X1 interface supports only mutual TLS. The interface encoding is specified in ETSI 130 221-1. The TLS version 1.2 and above is supported. For more information on TLS configuration, see Appendix: Transport Layer Security.

In mutual TLS, the LIG verifies the MAG-c certificates, and in return the MAG-c verifies the LIG certificates.

LI_X1 mutual TLS configuration

In this example, the files names are the same ones used in Appendix: Transport Layer Security for cohesiveness.

It is assumed that following Appendix: Transport Layer Security the keys, certificates, and certification revoking list (CRL) have already been generated. The next step is to import them on the MAG-c and configure the router to use them for TLS authentication and encryption.

Note:
The Appendix: Transport Layer Security only covers one set of certificates for MAG-c. For mutual TLS, the client (in this case, the LIG) is expected to have its own set of certificate files. To generate the client certs, the same process in Appendix can be repeated for the client application (in this case, the LIG).

Import certificates on the MAG-c

First, transfer the MAG-c private key and certificate (as well as the certification authority (CA) certificate and CRL), these are certs that are generated on a Linux system on behalf of MAG-c from Appendix Appendix: Transport Layer Security. The MAG-c then utilizes the certificates, keys, and CRL for authentication. LI_X1 requires mutual TLS, therefore the LIG is expected to also provide the client set of files to be installed on the MAG-c. It is expected that the LIG has the same set of files for the MAG-c to install for client authentication. The following example uses the **scp** (secure copy) command for only the MAG-c key and certication files. The same **scp** is used again to transfer the LIG set of files, the prefix "lig-" is pre-pended to the files to highlight the differences. Although the example uses scp for file transfer, other file transfer mechanism can be used, such as FTP. The certificates, keys, and CRL must be stored in cf1.

Transfer the MAG-c certificates for server authentication:

```
[root@centos8-dot32 telemetry]# scp pe3-cert.pem private/pe3-key.pem CAcert.pem CAcrl.pem
 admin@192.0.2.3:/

The authenticity of host '192.0.2.3 (192.0.2.3)' can't be established.
RSA key fingerprint is SHA256:HLc2D3INqxEzAdGc7ZkylD7O9VK0LT0nc0RWMCiG/MA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.0.2.3' (RSA) to the list of known hosts.

admin@192.0.2.3's password:
pe3-cert.pem                                                                               100%
 4168    51.8KB/s   00:00
pe3-key.pem                                                                                100%
 1675    19.0KB/s   00:00
CAcert.pem                                                                                 100%
 4386    74.7KB/s   00:00
CAcrl.pem                                                                                  100%
  658     7.4KB/s   00:00
```

Transfer the LIG certificates for client authentication:

```
[root@centos8-dot32 telemetry]# scp lig-pe3-cert.pem private/lig-pe3-key.pem lig-CAcert.pem
 lig-CAcrl.pem admin@192.0.2.3:/

The authenticity of host '192.0.2.3 (192.0.2.3)' can't be established.
RSA key fingerprint is SHA256:HLc2D3INqxEzAdGc7ZkylD7O9VK0LT0nc0RWMCiG/MA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.0.2.3' (RSA) to the list of known hosts.

admin@192.0.2.3's password:
lig-pe3-cert.pem
 100% 4168    51.8KB/s   00:00
lig-pe3-key.pem
 100% 1675    19.0KB/s   00:00
lig-CAcert.pem
 100% 4386    74.7KB/s   00:00
lig-CAcrl.pem
 100%  658     7.4KB/s   00:00
```

To utilize transferred keys, certificates, and CRL files, they must be converted to MAG-c system format file. When the following commands are executed, the system automatically creates the directory system-pki/ and stores the output files there for subsequent use. The process of importing certificates and keys only generates binary files in the cf1:/system/pki directory. These files are not loaded into memory at this point.

Import the MAG certificates:

```
A:pe-3# admin certificate import type cert input cf1:/pe3-cert.pem output cert.crt format pem
A:pe-3# admin certificate import type key input cf1:/pe3-key.pem output key.crt format pem
A:pe-3# admin certificate import type cert input cf1:/CAcert.pem output cacert.crt format pem
A:pe-3# admin certificate import type crl input cf1:/CAcrl.pem output cacrl.crt format pem
```

Import the LIG clients certificates:

```
A:pe-3# admin certificate import type cert input cf1:/lig-pe3-cert.pem output lig-cert.crt
 format pem
A:pe-3# admin certificate import type key input cf1:/lig-pe3-key.pem output lig-key.crt format
 pem
A:pe-3# admin certificate import type cert input cf1:/lig-CAcert.pem output lig-cacert.crt
 format pem
A:pe-3# admin certificate import type crl input cf1:/lig-CAcrl.pem output lig-cacrl.crt format
 pem
```

Confirm that the files have been correctly imported:

```
A:pe-3# file dir cf1:/system-pki/

Volume in drive cf1 on slot A is SROS VM.

Volume in drive cf1 on slot A is formatted as FAT32

Directory of cf1:\system-pki\

11/24/2020  10:07a      <DIR>          ./
11/24/2020  10:07a      <DIR>          ../
11/24/2020  10:08a                 989 cacert.crt
11/24/2020  10:09a                 433 cacrl.crt
11/24/2020  10:07a                 960 cert.crt
11/24/2020  10:08a                1255 key.crt
11/24/2020  10:18a                 992 lig-cacert.crt
11/24/2020  10:19a                 443 lig-cacrl.crt
11/24/2020  10:17a                 962 lig-cert.crt
11/24/2020  10:18a                1335 lig-key.crt
               8 File(s)                   7369 bytes.
               2 Dir(s)               786743296 bytes free.
```

MAG-c nodal configuration

The first step is to configure a PKI **ca-profile** which references both the CA root certificate and the CA certificate revocation list. There is no requirement to give a specific directory reference because the system always looks for the relevant certificates and keys in cf1:/system-pki/. The following example shows two ca-profiles:

- "Server-ca" is the MAG-c server certificate
- "LIG-ca" is the LIG client set of certificates

Because the server never sends its CA certificate, the ca-profile "Server-ca" is not used by the system, it is configured here only for reference.

Note:
The following utilizes the CRL file, but it is possible to make it optional with command **config>system>security>pki>ca-profile>revocation-check crl-optional**.

```
configure
    system
        security
            pki
                ca-profile "Server-ca" create
                    cert-file "cacert.crt"
                    crl-file "cacrl.crt"
                    no shutdown
                exit
                ca-profile "LIG-ca" create
                    cert-file "lig-cacert.crt"
                    revocation-check crl-optional
                    no shutdown
                exit
```

The next step is to configure the necessary components under the TLS context. This includes the following:

- A **cert-profile** that references the gRPC server certificate and private key.
- A **server-cipher-list** containing a list of acceptable (and negotiable) ciphers and authentication algorithms.
- A **server-tls-profile** that references both the **cert-profile** and the **cipher-list**. Client authentication is mandatory for mutual TLS. The client certificate is compared with the LIG root CA certificate, configured under trust-anchor.

```
configure
    system
        security
            tls
                cert-profile "MAG-c-tls-certificates" create
                    entry 1
                        certificate-file "cert.crt"
                        key-file "key.crt"
                    exit
                    no shutdown
                exit
                trust-anchor-profile "LIG-anchor-profile" create
                    trust-anchor "LIG-ca"
                exit
                server-cipher-list "cipher-list" create
                    cipher 4
                        name tls-rsa-with3des-ede-cbc-sha
                    exit
                    cipher 5
                        name tls-rsa-with-aes128-cbc-sha
                    exit
                    cipher 6
                        name tls-rsa-with-aes256-cbc-sha
                    exit
                    cipher 7
                        name tls-rsa-with-aes128-cbc-sha256
                    exit
                    cipher 8
                        name tls-rsa-with-aes256-cbc-sha256
                    exit
                exit
                server-tls-profile "MAG-c-tls-server-profile" create
                    cert-profile "MAG-c-tls-certificates"
                    cipher-list "cipher-list"
                    authenticate-client
                        trust-anchor-profile "LIG-anchor-profile"
                    exit
                    no shutdown
                    exit
```

The final step is to associate the server TLS profile to the LI application.

```
*A:SMF-DMZ>config>li>mobile# info
----------------------------------------------
            server-tls-profile  "MAG-c-tls-server-profile"
```

The interface for LI_X1 to listen to the TCP/TLS request for the LI_X1 connection is configured as follows:

```
*A:SMF-DMZ>config>li>mobile# info
----------------------------------------------
            li-x1
                li-x1-local-interface 208.184.70.164 router Base local-port 443
            exit
```

LI infrastructure setup: 5G LI _X2 interface

As per TS 33.128, the LI_X2 interface used for communicating IRI information must be TLS based. In this case, the MAG-c is a TLS client. In this example, it is assumed that LI_X1 and LI_X2 are connected to the same LIG. In the previous steps, the client certificates are already installed on the system for LI_X1, therefore, the following configuration reuses the trust-anchor for the client TLS profile. The client cert-profile is only configured for mutual TLS authentication.

```
configure
    system
        security
            tls
                cert-profile "client-tls-certificates" create
                    entry 1
                        certificate-file "client-cert.crt"
                        key-file "client-key.crt"
                    exit
                    no shutdown
                exit
                trust-anchor-profile "LIG-anchor-profile" create
                    trust-anchor "LIG-ca"
                exit
                server-cipher-list "cipher-list" create
                    cipher 4
                        name tls-rsa-with3des-ede-cbc-sha
                    exit
                    cipher 5
                        name tls-rsa-with-aes128-cbc-sha
                    exit
                    cipher 6
                        name tls-rsa-with-aes256-cbc-sha
                    exit
                    cipher 7
                        name tls-rsa-with-aes128-cbc-sha256
                    exit
                    cipher 8
                        name tls-rsa-with-aes256-cbc-sha256
                    exit
                exit
                client-tls-profile "LIG-tls-server-profile" create
                    cert-profile "client-tls-certificates"
                    cipher-list "cipher-list"
                    trust-anchor-profile "LIG-anchor-profile"
                    no shutdown
```

The 5G LI_X2 IP interface follows the same configuration as the following 4G X2 interface. See LI infrastructure setup: Setting up the 4G X2_1 interface section for more information.

For the local interface:

```
config>li>mobile-gateway ?
[no] local-interface <ip-address> [router <router-instance>]
[over-ride x2-interface <x2-ip-address> [x2-router <x2-router-instance>]]
```

LI infrastructure setup: 4G and 5G MAG-c PFCP (N4) interface

MAG-c reuses the Packet Forwarding Control Protocol (PFCP) interface to provision the LI target on the user plane. The LI attributes are sent with the subscriber session creation. Unlike regular PFCP IEs, the LI PFCP IEs are encrypted utilizing a secret key. The PFCP secret key is as follows:

```
config>li>
[no] pfcp-li-shared-key
```

The **configure li pfcp-li-shared-key** command is used to configure the shared key used between MAG-c and the user plane over N4 for LI PFCP IEs sent from MAG-c to the user plane function. This shared key is used to encrypt the LI PFCP IE at the MAG-c and decrypt the LI container IE at the UPF. The **no** form of the command reverts to default, which is null.

LI infrastructure setup: 4G and 5G service router user plane

The SR requires the secret key to be provisioned to decrypt the PFCP LI IEs.

```
A:sros1>config>li# info
        sci
            pfcp-li-shared-key "K7gNU3sdo+OL0wNhqoVWhuiT+uvppg==" hash2
        exit
```

In addition, each SR supports the CC interface. All CC messages are sent using an IP-UDP-shim header. The following describes the steps for provisioning the mirror destination service "1" utilizing the base routing instance for the LI mirrored packets.

```
A:sros1>config>mirror# info
----------------------------------------------
        mirror-dest 1 name "1" create
            encap
                layer-3-encap ip-udp-shim create
                    direction-bit
                    router Base
                    gateway create
                        ip src 1.1.1.1 dest 1.1.1.2
                        udp src 65111 dest 65111
                    exit
                exit
            no shutdown
            exit
```

In the LI context, this mirror destination requires reference:

```
A:sros1>config>li# info
        li-source 1
        no shutdown
```

LI target provisioning

FWA LI target provisioning typically consists of three steps:

- Provisioning of 4G IRI targets
- Provisioning of 5G IRI targets
- Provisioning of 4G and 5G CC targets

The reason for provisioning the target as both a 4G and a 5G target is because the service provider might not know if the FWA RG is 4G or 5G capable. However, in the case where the service provider can predetermine the client type, it is possible to only perform step 1 and 3 if the RG is only 4G capable and only step 2 and 3 if the RG is 5G capable with the ability to fall back to 4G.

Provisioning of 4G IRI targets

To provision 4G IRI, the following command set is used:

```
A:sros1>config>li# info
----------------------------------------------
        mobile-gateway
            local-interface 10.195.160.181 router vprn100 override-x2-interface 10.195.160.182
 x2-router vprn100
            custom-correlation-id-format disable
            server-tls-profile  "li-server-tls-profile"
            client-tls-profile  "li-client-tls-profile"
            3gpp-5g-release rel-base
            li-x1
                li-x1-local-interface 10.195.160.181 router 100 local-port 50001
            exit
            df-peer 2 df2-addr 10.178.229.137 df2-port 10047 df2-tls-profile li-client-tls-
profile
            target imsi id 310310995002222 intercept iri peer 2 liid 17097478
            target imsi id 310310995003362 intercept iri peer 2 liid 310310995003362
        exit
        pfcp-li-shared-key "YHTJfusmNsAtfdCMSBvb2qQMUwzSiefunPs=" hash2
```

Provisioning of 5G IRI targets

To provision 5G IRI, the ETSI 103.221-1 protocol is used. The steps include:

- CreateDestination to create the destination for IRI message, which is called the destination ID.
- ActivateTask to create the LI target and specify the DID for the IRI message.

Note: the LIG should only create x2-only DID.

Provisioning of 4G and 5G CC targets

To provision the CC for both 4G and 5G, the following command set is used:

```
sros1>config>li# info
----------------------------------------------
        mobile-gateway
            local-interface 10.195.160.181 router vprn100 override-x2-interface 10.195.160.182
 x2-router vprn100
            operator-id TMBL
            tls
            custom-correlation-id-format disable
            server-tls-profile  "li-server-tls-profile"
            client-tls-profile  "li-client-tls-profile"
            3gpp-5g-release rel-base
            nf-id-value uuid
            li-x1
                li-x1-local-interface 10.195.160.181 router 100 local-port 50001
                admf-peer 1 admf-addr 10.178.229.136 x1-port 10443
            exit
            df-peer 2 df2-addr 10.178.229.137 df2-port 10047 df2-tls-profile li-client-tls-
profile
            target imsi id 310310995002222 intercept iri peer 2 liid 17097478
            target imsi id 310310995003362 intercept iri peer 2 liid 310310995003362
        exit
        pfcp-li-shared-key "YHTJfusmNsAtfdCMSBvb2qQMUwzSiefunPs=" hash2
        target "310310995003362"
            source 1 imsi 310310995003362 egress ingress  intercept-id 17097489 mirror-
destination "8000"
        target "310310995003444"
            source 1 imsi 310310995003444 egress ingress  intercept-id 17097487 mirror-
destination "8000"
        exit
```

Conclusion

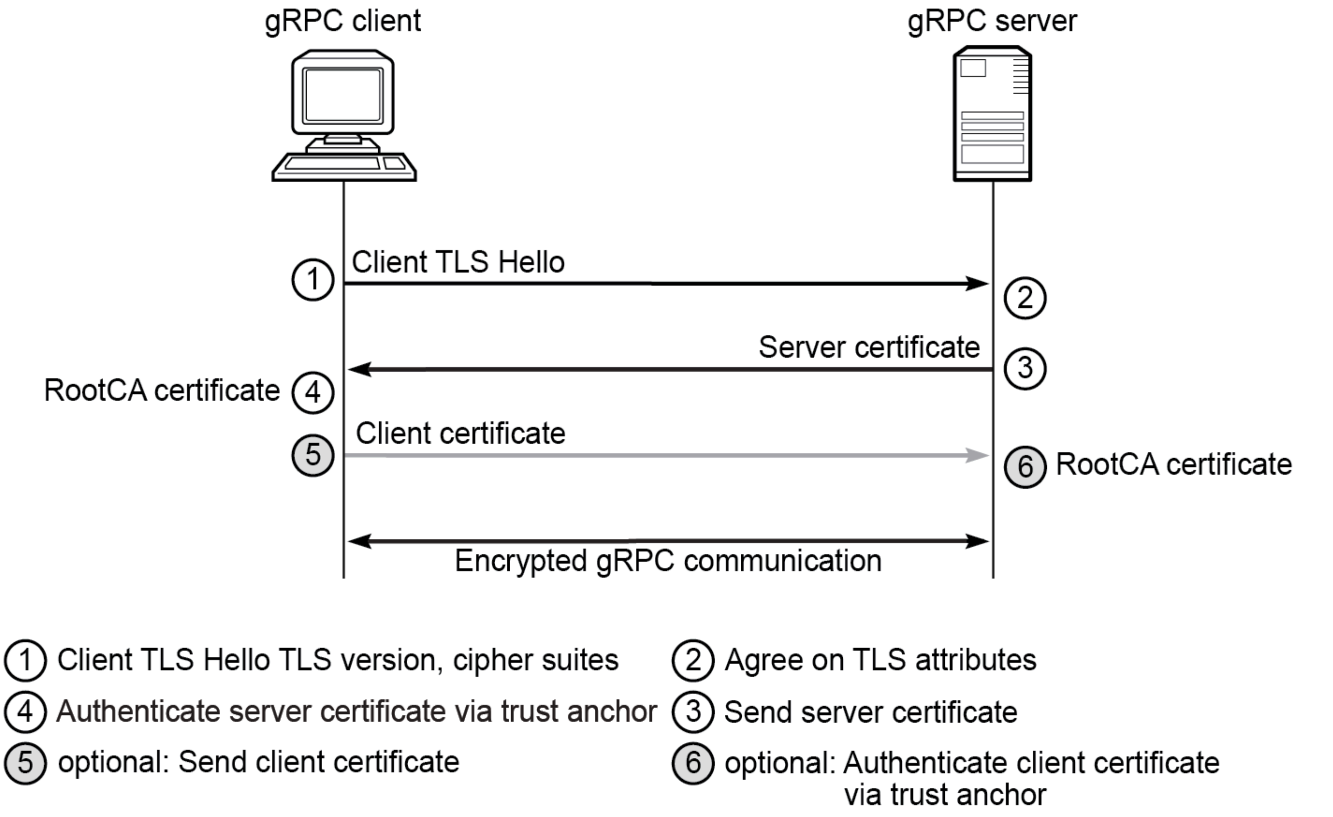
This chapter provides a configuration guidance to set up the MAG for FWA LI. The infrastructure for LI is typically set up once during commissioning. Afterward, the LIG utilizes both SSH CLI and ETSI-based 103.221-1 to provision FWA LI targets on the system.

Appendix: Transport Layer Security

This section provides a quick start guidance to generate TLS for the LI interface. For more detail information on TLS, see the 7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide.

5G LI_X1 and LI_X2 mandates TLS as the transport where TLS on 4G X2_1 is optional. The use of TLS requires an exchange of X.509 certificates to provide authentication, integrity, and encryption keying material. While the TLS handshake itself uses asymmetric keys for encryption, it allows for confidential generation of a shared key to allow for subsequent symmetric encryption. In general, only server-side authentication is used. However, TLS also supports two-way authentication where both the server certificate and the client certificate are authenticated: mutual TLS. MAG-c 5G LI_X1 mandates mutual TLS. Both 4G X2_1 (if used) and 5G LI_X2 only require server TLS authentication.

Figure 2: Transport layer security


gRPC client
gRPC server
1 Client TLS Hello
2
Server certificate 3
RootCA certificate 4
5 Client certificate
6 RootCA certificate
Encrypted gRPC communication
1 Client TLS Hello TLS version, cipher suites
2 Agree on TLS attributes
4 Authenticate server certificate via trust anchor
3 Send server certificate
5 optional: Send client certificate
6 optional: Authenticate client certificate via trust anchor
39936a

The use of X.509 certificates mandates the use of a Public Key Infrastructure (PKI), but because this is not commonly available in many test environments, the following section describes the use of self-signed certificates using OpenSSL.

Create a directory structure to store certificates and keys:

```
[root@centos8-dot32 ~]# mkdir /home/ftpuser/certs/telemetry
[root@centos8-dot32 ~]# cd /home/ftpuser/certs/telemetry
```

```
[root@centos8-dot32 telemetry]# mkdir private
```

Generate a CA certificate

Generating a self-signed CA certificate is a one-time activity. It is subsequently used to sign all certificate signing requests from network elements serving as LI_X1 servers.

Firstly, generate a private RSA key that forms part of the certificate request, and store it in the private sub-directory.

```
[root@centos8-dot32 telemetry]# openssl genrsa -out private/CAkey.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.............................+++++
.......+++++
e is 65537 (0x010001)
```

Generate a certificate signing request and reference the generated key generated.

```
[root@centos8-dot32 telemetry]#
          openssl req -out CAreq.pem -key private/CAkey.pem -new -passin "pass:" -subj
          "/C=UK/ST=SU/L=Guildford/O=IPD/OU=CE/CN=CA/emailAddress=nobody@nokia.com"
```

Create the following file if it does not exist already:

```
[root@centos8-dot32 telemetry]# touch /etc/pki/CA/index.txt
```

Self-sign the CA certificate request using the previously generated private key and certificate request.

```
[root@centos8-dot32 telemetry]# openssl ca -out CAcert.pem -keyfile private/CAkey.pem
 -batch -days 3650 -selfsign -create_serial -passin "pass:" -extensions v3_ca
 -infiles CAreq.pem
```

Create the following file if it does not exist already:

```
[root@centos8-dot32 telemetry]# echo 01 > /etc/pki/CA/crlnumber
```

Generate an empty certificate revocation list (CRL):

```
[root@centos8-dot32 telemetry]# openssl ca -out CAcrl.pem -keyfile private/CAkey.pem
 -batch -gencrl -cert CAcert.pem -passin "pass:"
```

Generate a server certificate

This section provides an example of how to generate a server certificate (for example LI_X1). Because a server certificate is needed for every MAG-c instance supporting LI, it requires some unique identification. The following example utilizes a lab environment, so it does not have a DNS and this example uses the hostname "pe3"; therefore, the name of the private key is pe3-key.pem and the name of the certificate is pe3-cert.pem.

Generate a private key for the MAG-c server certificate, as follows:

```
[root@centos8-dot32 telemetry]#  openssl genrsa -out private/pe3-key.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
```

```
.............................+++++
.......+++++
e is 65537 (0x010001)
```

Note:
Although the preceding example uses OpenSSL on a Centos 8 server to generate the key, it is equally possible to generate the key on an MAG-c server using the **admin certificate gen-keypair** command.

Generate a certificate signing request and reference the generated key. Note that the preferred value for the common name (CN) is a fully qualified domain name (FQDN), but a simple hostname can be used if DNS is not used.

```
[root@centos8-dot32 telemetry]#
          openssl req -out pe3-certreq.pem -key private/pe3-key.pem -new -passin "pass:" -subj
          "/C=UK/ST=SU/L=Guildford/O=IPD/OU=CE/CN=pe3"
```

Note:
Once again, although the example uses OpenSSL to generate the certificate request, it is possible to generate the request from an MAG-c server using the **admin certificate gen-local-cert-req** command.

Sign the certificate request using the CA's certificate. Note that, if a FQDN is not used as a CN in the certificate request, the certificate must include the IP address of the gRPC server in the subjectAltName (in this case the system address of PE3).

```
[root@centos8-dot32 telemetry]# openssl ca -out pe3-cert.pem -keyfile private/CAkey.pem -batch
 -passin "pass:" -days 3650 -cert CAcert.pem -policy policy_anything -extensions SAN -extfile
 <(printf "[SAN]\nsubjectAltName=IP:192.0.2.3") -infiles pe3-certreq.pem
Using configuration from /etc/pki/tls/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            32:af:0d:bb:56:f9:f4:6f:47:8c:17:a8:0c:36:8c:d9:f3:74:6a:53
        Validity
            Not Before: Nov 24 09:39:13 2020 GMT
            Not After : Nov 22 09:39:13 2030 GMT
        Subject:
            countryName               = UK
            stateOrProvinceName       = SU
            localityName              = Guildford
            organizationName          = IPD
            organizationalUnitName    = CE
            commonName                = pe3
            emailAddress              = nobody@nokia.com
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:192.0.2.3
Certificate is to be certified until Nov 22 09:39:13 2030 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
```

Verify that the server certificate has been correctly generated and view the certificate.

```
[root@centos8-dot32 telemetry]# openssl verify -verbose -CAfile CAcert.pem pe3-cert.pem
pe3-cert.pem: OK
```

```
[root@centos8-dot32 telemetry]# openssl x509 -text -in pe3-cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            32:af:0d:bb:56:f9:f4:6f:47:8c:17:a8:0c:36:8c:d9:f3:74:6a:53
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = UK, ST = SU, O = IPD, OU = CE, CN = CA, emailAddress = nobody@nokia.com
        Validity
            Not Before: Nov 24 09:39:13 2020 GMT
            Not After : Nov 22 09:39:13 2030 GMT
        Subject: C = UK, ST = SU, L = Guildford, O = IPD, OU = CE, CN = pe3, emailAddress =
 nobody@nokia.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d7:2c:ce:a7:10:29:fe:28:a7:bb:02:b5:01:1b:
                    30:2a:8d:12:21:3e:51:ab:bd:63:93:ee:c9:3e:dc:
                    1c:85:a2:a6:62:06:c7:aa:fe:15:d3:2e:fd:11:7c:
                    59:c5:c0:69:42:05:af:a1:e7:16:42:56:b6:66:53:
                    0a:d2:be:3f:13:fe:a6:6c:2d:86:43:71:f5:31:29:
                    fd:37:ab:ff:00:13:31:63:f7:f1:ff:c1:5a:9d:3c:
                    13:62:82:82:eb:10:f2:06:71:8e:f0:89:9e:af:b3:
                    68:45:30:91:81:43:61:6f:9e:4f:eb:b2:e8:bd:a1:
                    01:df:c5:32:64:5a:30:c7:8c:9f:a3:02:de:0a:68:
                    86:36:59:ea:43:6a:1d:23:7c:8b:cf:36:8d:36:33:
                    c0:49:c4:34:94:e9:8c:c7:6b:2c:3d:62:23:ad:a6:
                    55:92:7c:26:a0:60:e9:3c:6c:5d:ba:9b:e7:75:7a:
                    c1:da:05:f1:73:8e:23:9f:4c:c0:0e:c9:3c:23:bb:
                    49:69:d2:d2:d6:6d:b0:ec:5a:05:d3:0a:4c:96:17:
                    7c:69:38:08:6c:58:b7:0d:a6:ce:7a:5c:0d:f9:0e:
                    1d:bc:04:78:93:a6:81:3a:2f:80:e6:65:09:e3:22:
                    e9:1c:13:16:7d:d7:e8:0e:ba:bc:38:c5:10:ec:e6:
                    8a:c3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:192.0.2.3
    Signature Algorithm: sha256WithRSAEncryption
         0f:ac:16:75:2a:98:75:8b:7d:f0:ac:d2:fb:ba:01:12:a9:e7:
         f8:7a:34:59:e8:39:44:b3:16:98:26:f5:3a:eb:d5:91:bb:07:
         b0:6d:e1:08:07:6c:71:cd:36:51:2f:40:b7:e0:30:1c:3e:d4:
         6d:31:1a:ac:00:04:01:f1:2d:bc:38:1d:1b:e0:18:8e:cc:d3:
         67:69:23:b5:71:3d:2a:e3:0a:94:1f:ef:63:11:be:16:42:61:
         5d:78:95:9b:82:ea:dc:43:31:a4:2b:6f:27:e3:00:17:9d:97:
         3c:6d:96:4b:09:87:33:08:00:51:eb:ad:10:86:0f:4f:d9:35:
         18:d4:b5:d6:32:2e:cf:b5:33:85:cc:93:a9:dd:12:53:80:71:
         db:e0:48:7d:1f:d7:3d:04:21:fe:6d:76:47:ed:61:ff:7b:3b:
         a6:6e:75:74:ae:1e:62:7b:5d:28:43:73:09:dc:0f:f0:ac:80:
         65:02:60:31:95:54:24:61:17:a2:38:ec:4f:90:47:7c:a4:38:
         4d:ff:eb:b2:29:fe:26:c6:32:47:01:81:e2:ab:cf:85:42:f6:
         76:2d:46:9f:4a:d3:6d:55:5e:2d:3e:05:2e:77:8b:46:72:a6:
         0e:58:23:45:dc:bf:46:dc:b3:c4:3c:b3:ac:77:75:1b:49:e3:
         48:a2:d1:44
-----BEGIN CERTIFICATE-----
MIIDfDCCAmSgAwIBAgIUMq8Nu1b59G9HjBeoDDaM2fN0alMwDQYJKoZIhvcNAQEL
BQAwYzELMAkGA1UEBhMCVUsxCzAJBgNVBAgMAlNVMQwwCgYDVQQKDANJUEQxCzAJ
BgNVBAsMAkNFMQswCQYDVQQDDAJDQTEfMB0GCSqGSIb3DQEJARYQbm9ib2R5QG5v
a2lhLmNvbTAeFw0yMDExMjQwOTM5MTNaFw0zMDExMjIwOTM5MTNaMHgxCzAJBgNV
BAYTAlVLMQswCQYDVQQIDAJTVTESMBAGA1UEBwwJR3VpbGRmb3JkMQwwCgYDVQQK
DANJUEQxCzAJBgNVBAsMAkNFMQwwCgYDVQQDDANwZTMxHzAdBgkqhkiG9w0BCQEW
EG5vYm9keUBub2tpYS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
```

```
AQDXLM6nECn+KKe7ArUBGzAqjRIhPlGrvWOT7sk+3ByFoqZiBseq/hXTLv0RfFnF
wGlCBa+h5xZCVrZmUwrSvj8T/qZsLYZDcfUxKf03q/8AEzFj9/H/wVqdPBNigoLr
EPIGcY7wiZ6vs2hFMJGBQ2Fvnk/rsui9oQHfxTJkWjDHjJ+jAt4KaIY2WepDah0j
fIvPNo02M8BJxDSU6YzHayw9YiOtplWSfCagYOk8bF26m+d1esHaBfFzjiOfTMAO
yTwju0lp0tLWbbDsWgXTCkyWF3xpOAhsWLcNps56XA35Dh28BHiTpoE6L4DmZQnj
IukcExZ91+gOurw4xRDs5orDAgMBAAGjEzARMA8GA1UdEQQIMAaHBMAAAgMwDQYJ
KoZIhvcNAQELBQADggEBAA+sFnUqmHWLffCs0vu6ARKp5/h6NFnoOUSzFpgm9Trr
1ZG7B7Bt4QgHbHHNNlEvQLfgMBw+1G0xGqwABAHxLbw4HRvgGI7M02dpI7VxPSrj
CpQf72MRvhZCYV14lZuC6txDMaQrbyfjABedlzxtlksJhzMIAFHrrRCGD0/ZNRjU
tdYyLs+1M4XMk6ndElOAcdvgSH0f1z0EIf5tdkftYf97O6ZudXSuHmJ7XShDcwnc
D/CsgGUCYDGVVCRhF6I47E+QR3ykOE3/67Ip/ibGMkcBgeKrz4VC9nYtRp9K021V
Xi0+BS53i0Zypg5YI0Xcv0bcs8Q8s6x3dRtJ40ii0UQ=
-----END CERTIFICATE-----
```

Multi-Access Gateway Lawful Intercept - Fixed Wireless Access with Geo-redundancy

This chapter provides information about MAG-c LI - FWA with geo-redundancy.

Topics in this chapter include:

- Applicability
- Overview
- Configuration
- Conclusion

Applicability

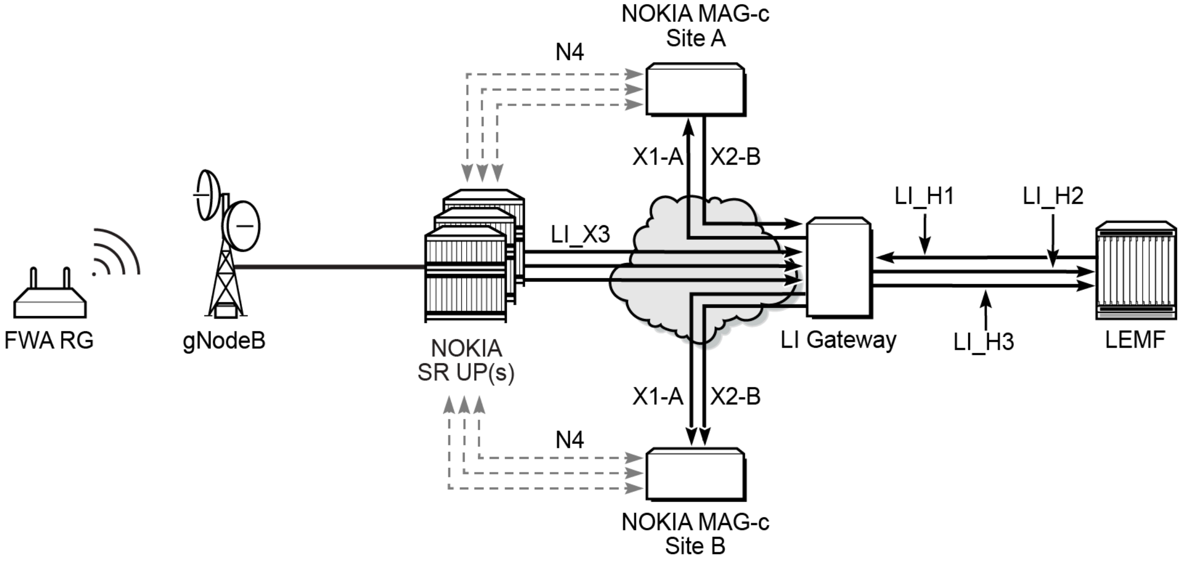
The information and the configuration in this chapter are based on Multi-Access Gateway (MAG) controller (MAG-c) and SR OS Release 24.3.R1.

Overview

This chapter provides Lawful Intercept (LI) configurations for geo-redundant Fixed Wireless Access (FWA) MAG setup. For the FWA LI basics, see the Multi-Access Gateway Lawful Intercept - Fixed Wireless Access chapter.

This chapter provides a configuration example for the 3GPP X1, X2, and X3 interfaces. Figure 3: Interfaces for the MAG shows the X interfaces which are based on 3GPP TS 33.107 and TS 33.108 for 4G and on 3GPP TS 33.127 and RS 33.128 for 5G.

Figure 3: Interfaces for the MAG



The X interfaces for the MAG are the following:

- The X1 interface in this document refers to the 4G X1_1 and the 5G LI_X1 interface. The X1-A interface connects from MAG-c site A (MAG-c A) to the LI Gateway (LIG) and the X1-B interface connects from MAG-c site B (MAG-c B) to the LIG. It is assumed that the X1 traverses through an IP routing network in between the MAG-c and the LIG. The X1 interface is used for configuration: setting up LI targets and the MAG-c LI infrastructure.
- The X2 interface in this document refers to the 4G X2_1 and the 5G LI_X2. It is also known as the Intercept Relation Information (IRI) interface. The X2-A interface connects from MAG-c site A (MAG-c A) to the LI Gateway (LIG) and the X2-B interface connects from MAG-c site B (MAG-c B) to the LIG. It is assumed that the X2 traverses through an IP routing network in between the MAG-c and the LIG. The X2 interface is used for transporting IRI LI target related events to the LIG. In 4G, the X2 interface to the LIG is often referred to as delivery function (DF) 2 peer (DF2 peer).
- The X3 interface in this example refers to the Communication Content (CC) interface for both 4G and 5G. The CC interface is used to transport the mirrored packets from each User Plane (UP) to the LIG. In 4G, the LIG often is often referred to as the DF3 peer.

Configuration

This section is separated into two parts:

- LI geo-redundant infrastructure setup
- 4G and 5G LI target provisioning on a geo-redundant setup

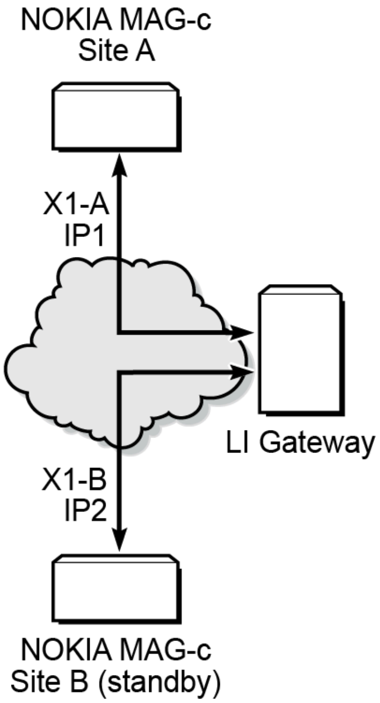
LI geo-redundant infrastructure setup

The infrastructure for LI is typically set up during commissioning. This section is separated into two parts: one for 4G and the other for 5G.

4G LI geo-redundant infrastructure setup for X1 interface

The 4G X1 interface on the MAG-c is a CLI interface over SSH. For geo-redundancy, it is expected that MAG-c site A and MAG-c site B have two different SSH IP addresses. The SSH address can be the local SSH address used for main management login. The 4G LI X1 interfaces on both MAG-c systems are always active, as shown in Figure 4: 4G X1 interfaces in geo-redundant MAG-c systems (solid lines between MAG-c systems and LIG).

Figure 4: 4G X1 interfaces in geo-redundant MAG-c systems

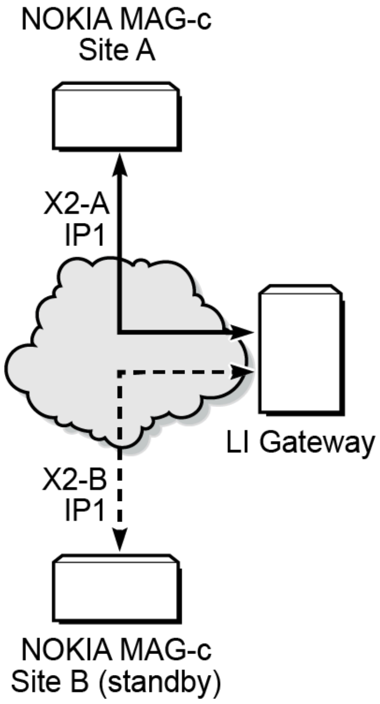


39938

4G LI geo-redundant infrastructure setup for X2 interface

The 4G X2 interface on the MAG-c is a TCP interface where TLS is optional. The LIG X2 interface known DF2-peer is required to be configured via SSH. For geo-redundancy, both MAG-c site A and MAG-c site B must share the same local IP address. Only one X2 interface is active. Both MAG-c IP1 interfaces are tracking the mc-mobile active/standby state. The IP1 interfaces on both MAG-c systems are also utilizing a routing protocol for advertisement. Therefore, only the active MAG-c announces the IP1 to the LIG via the routing protocol. Figure 5: 4G X2 interfaces in geo-redundant MAG-c systems shows that both X2 interfaces have IP address IP1, but only the X2 interface on MAG-c site A is active (solid line) while the X2 interface on MAG-c site B is standby (dashed line).

Figure 5: 4G X2 interfaces in geo-redundant MAG-c systems



39939

Step 1: Configure the IP1 interface identically on MAG-c-A and MAG-c-B and ensure the interface tracks the mc-mobile state. The CLI output only shows a MAG-c-A, but the configuration on MAG-c-B is identical.

```
*A:MAG-c-A>config>router#
            interface "Loopback interface for LI X2" create
                description "Loopback interface for LI X2"
                address 30.0.0.6/32
                loopback
                track-mobile
            exit
```

Step 2: Attach the routing interface to a routing protocol of your choice or within a routing policy for route export.

Step 3: Configure the LI X2 address.

```
*A:MAG-c-A>config>li# info
----------------------------------------------
        mobile-gateway
            local-interface 30.0.0.7 router vprn4 override-x2-interface 30.0.0.6 x2-router
 vprn4
```

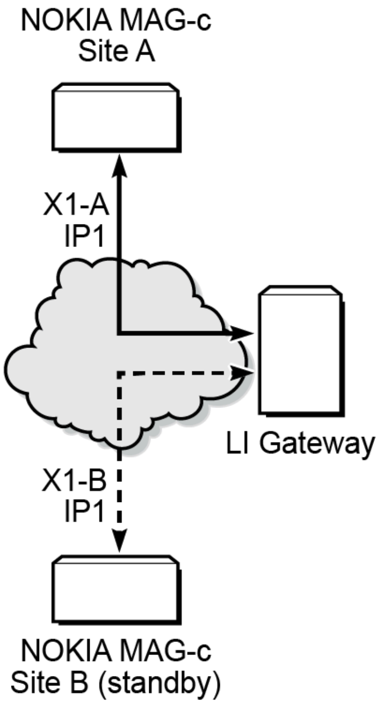
Note:
The local interface configured, in this example 30.0.0.7, must be the same on both MAG-c systems.

For 4G, the LI X2 interface utilizes the local-interface IP address but the override X2 address will override the local-interface IP address. Therefore, the override command for 4G X2 looks redundant. The override command is targeted for 5G LI X2. With this, the 5G X1 interface will utilize the local interface while the 5G X2 interface will utilize the override IP address.

5G LI geo-redundant infrastructure setup for X1 interface

The 5G X1 interface on the MAG-c is a TCP/TLS interface. For geo-redundancy, both MAG-c site A and MAG-c site B must share the same IP address. Only one X1 interface will be active. Both MAG-c IP1 interfaces are tracking the mc-mobile active/standby state. The IP1 interface on both MAG-c systems are also utilizing a routing protocol for advertisement. Therefore, only the active MAG-c announces the IP1 to the LIG via the routing protocol, as shown in Figure 6: 5G X1 interfaces in geo-redundant MAG-c systems.

Figure 6: 5G X1 interfaces in geo-redundant MAG-c systems



Step 1: Configure the IP1 interface on MAG-c-A and MAG-c-B and ensure that the interface tracks the mc-mobile state.

```
*A:MAG-c-A>config>router#
            interface "Loopback interface for 5G LI X1" create
                description "Loopback interface for 5G LI X1"
                address 30.0.0.5/32
                loopback
                track-mobile
            exit
```

Step 2: Attach the routing interface to a routing protocol of your choice or within a routing policy for route export.

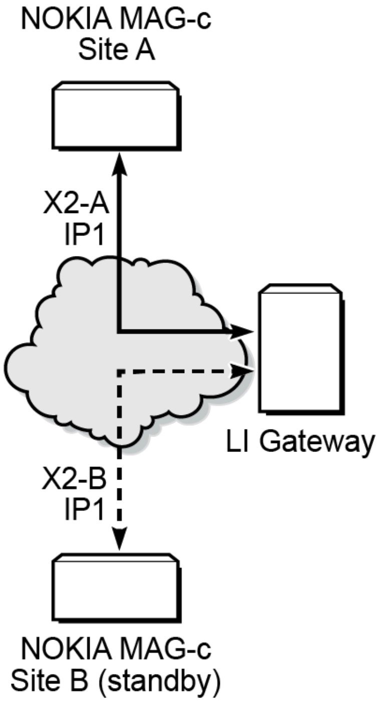
Step 3: Configure the local LI X1 address on MAG-c-A and MAG-c-B.

```
*A:MAG-c-A>config>li# info
----------------------------------------------
        mobile-gateway
            li-x1
                li-x1-local-interface 30.0.0.5 router Base local-port 443
```

5G LI geo-redundant infrastructure setup for X2 interface

The 5G X2 interface on the MAG-c is a TCP/TLS interface and it follows the same configuration as 4G X2 interface.

Figure 7: 5G X2 interfaces in geo-redundant MAG-c systems



In a similar way as for 4G X2, only the active MAG-c announces IP1 to the LIG. If the X2 interface is already configured for 4G, no additional configuration is required for 5G. Both 4G X2 and 5G X2 utilize the same interface and source IP address to communicate with the LIG.

The configuration is exactly the same as 4G X2 and the routing interface will be associated to a routing protocol or a routing policy for route export. Only the configuration on MAG-c-A is shown; the configuration on MAG-c-B is identical.

```
*A:MAG-c-A>config>router# info
----------------------------------------------
            interface "Loopback interface for LI X2" create
                description "Loopback interface for LI X2"
                address 30.0.0.6/32
                loopback
                track-mobile
            exit


*A:MAG-c-A>config>li# info
----------------------------------------------
        mobile-gateway
            local-interface 30.0.0.7 router vprn4 override-x2-interface 30.0.0.6 x2-router
 vprn4
```

LI geo-redundant infrastructure setup for N4

The SR requires the secret key to be provisioned to decrypt the PFCP LI IEs. Therefore, both MAG-c-A and MAG-c-B share the same PFCP LI shared key.

```
A:MAG-c-A>config>li# info
        sci
            pfcp-li-shared-key "Secretkey”
        exit
```

User plane configuration

In this application, the UP is non-redundant and is managed by the geo-redundant CP. The configuration is as described in the 7450 ESS, 7750 SR, 7950 XRS, and VSR System Management Guide.

```
A:sros1>config>mirror# info
----------------------------------------------
        mirror-dest 1 name "1" create
            encap
                layer-3-encap ip-udp-shim create
                    direction-bit
                    router Base
                    gateway create
                        ip src 1.1.1.1 dest 1.1.1.2
                        udp src 65111 dest 65111
                    exit
                exit
                no shutdown
```

In the LI context, this mirror destination requires reference.

```
A:sros1>config>li# info
        li-source 1
        no shutdown
```

4G and 5G LI target provisioning on a geo-redundant setup

FWA LI target provisioning typically consists of three steps.

- Provisioning of 4G IRI targets
- Provisioning of 5G IRI targets
- Provisioning of 4G and 5G CC targets

The reason for provisioning the target as both a 4G and 5G target is because the service provider might not know if the FWA RG is 4G or 5G capable. However, in the case where the service provider can predetermine the client type, then it is possible to only perform step 1 and 3 if the RG is only 4G capable and only step 2 and 3 if the RG is 5G capable with the ability to fall back to 4G.

Note:
It is highly recommended that provisioning of LI targets via SSH takes place on the standby MAG-c first before the active MAG-c. This is applicable to creation, modification, and deletion of LI targets.

Provisioning of 4G IRI targets

The provisioning of 4G IRI is identical on both MAG-c site A and MAG-c site B:

```
A:MAG-c-A>config>li# info
----------------------------------------------
        mobile-gateway
            local-interface 10.195.160.181 router vprn100 override-x2-interface 10.195.160.182
 x2-router vprn100
            custom-correlation-id-format disable
            server-tls-profile  "li-server-tls-profile"
            client-tls-profile  "li-client-tls-profile"
            3gpp-5g-release rel-base
            li-x1
                li-x1-local-interface 10.195.160.181 router 100 local-port 50001
            exit
            df-peer 2 df2-addr 10.178.229.137 df2-port 10047 df2-tls-profile li-client-tls-
profile
            target imsi id 310310995002222 intercept iri peer 2 liid 17097478
            target imsi id 310310995003362 intercept iri peer 2 liid 310310995003362
        exit
        pfcp-li-shared-key "YHTJfusmNsAtfdCMSBvb2qQMUwzSiefunPs=" hash2
```

Provisioning of 5G IRI targets

To provision 5G IRI, the ETSI 103.221-1 protocol is used. The steps include:

- CreateDestination to create the destination for IRI message, which is called the destination ID (DID).
- ActivateTask to create the LI target and specify the DID for the IRI message.

Note: The DID for IRI must be configured as X2-only.

Provisioning of 4G and 5G CC targets

The provisioning of CC for both 4G and 5G is identical on both MAG-c site A and MAG-c site B:

```
A:MAG-c-A>config>li# info
----------------------------------------------
        mobile-gateway
            local-interface 10.195.160.181 router vprn100 override-x2-interface 10.195.160.182
 x2-router vprn100
            operator-id TMBL
            tls
            custom-correlation-id-format disable
            server-tls-profile  "li-server-tls-profile"
            client-tls-profile  "li-client-tls-profile"
            3gpp-5g-release rel-base
            nf-id-value uuid
            li-x1
                li-x1-local-interface 10.195.160.181 router 100 local-port 50001
                admf-peer 1 admf-addr 10.178.229.136 x1-port 10443
            exit
            df-peer 2 df2-addr 10.178.229.137 df2-port 10047 df2-tls-profile li-client-tls-
profile
            target imsi id 310310995002222 intercept iri peer 2 liid 17097478
            target imsi id 310310995003362 intercept iri peer 2 liid 310310995003362
        exit
        pfcp-li-shared-key "YHTJfusmNsAtfdCMSBvb2qQMUwzSiefunPs=" hash2
        target "310310995003362"
            source 1 imsi 310310995003362 egress ingress intercept-id 17097489 mirror-
destination "1"
        target "310310995003444"
            source 1 imsi 310310995003444 egress ingress intercept-id 17097487 mirror-
destination "1"
        exit
```

For all bootup scenarios on a geo-redundant setup where the LI configuration is locally saved, the active MAG-c node will load the LI configuration and apply the configuration to both active and standby MAG-c.

Conclusion

This chapter provides a configuration example for FWA LI for a pair of geo-redundant MAG-c. The infrastructure for LI is typically set up once during commissioning. Afterward, depending on whether the UE is a 4G UE or a 5G UE, the LIG may be required to provision the LI target on both active and standby MAG-c.

Customer document and product support

Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback