CHF Interworking Function microservice guide v1.2.1

1. About

The microservice implements an M3UA IPSP/ASP over SCTP, a DIAMETER server and perform the termination of CAMEL transactions and DIAMETER sessions. It implements common interworking call flows between IMS entities and CAMEL. Most typically it is used to charge IMS calls using a CAMEL-based Online Charging System or to charge circuit switched calls using a DIAMETER-based OCS. The service can also be use to mediate the charging interface for SMS and GPRS. REST APIs are exposed for the administation of the microservice.

2. System requirements

The software can be deployed in common linux distribution operations system. It requires network connectivity for the DIAMETER and SIGTRAN interfaces. A minimum least 2vCPUs and 4GB RAM and 50GB disk space for typical configurations.

3. Installation

A software is packaged for debian or redhat linux system. the correct software package must be acquired according to the hosting operating system. The package will automatically deploy sctp and java packages required for the execution of the service. The installation procedure will also disable the selinux of the operating system.

Installing on a redhat/centos OS system

```
sudo rpm -i chf-iwf-1.2.2-1.rpm
```

Installing on a debian OS system

```
sudo apt install chf-iwf-1.2.2-1.deb
```

Installing on a docker

```
docker pull gcr.io/mdl-repo/chf-iwf
docker container create -p 22950:22950 -p 2905:2905/sctp -p 3868:3868/sctp
-t -i \
-v ./workload/chf-iwf-1/config/:/config/ \
-v ./workload/chf-iwf-1/logs/:/logs/ --name chf-iwf-1 gcr.io/mdl-repo/chf-
iwf
```

NOTE If a firewall service is running on the host OS, it is required to properly configure and allow access to HTTP, DIAMETER and SIGTRAN signaling ports in the firewall service settings.

After the completion the installation, a systemctl script is deployed on the system. After configuration of the system, it is required to enable the service so it is automatically started at boot time.

```
sudo systemctl enable chf-iwf
```

For docker deployments, the service is started through docker environment.

```
sudo docker start chf-iwf-1
```

4. File system

Path	Content description
/opt/chf-iwf/	Software binaries
/var/log/chf-iwf/	Log files
/etc/chf-iwf/	Configuration files

4.1 Log files

File	Content description
app.log	Application log file
cdr.log	Call data record log file
audit.log	API Audit log file
error.log	Log only errors generated by the microservice
alarm.log	Log SNMP traps reported to the SNMP server

5. Configuration

5.1 Configuration files

File	Content description
appsettings.json	Main configuration
logger.json	Logger configuration
dictionary.xml	Diameter AVPs dictionary

5.2 Main configuration file

5.2.1 General settings

Setting	Format	Setting description
instanceName	String	Name of instance, used for identification but not for logic
licenseKey	String	License key
useURL	String	URL to be used for the HTTP interface, common for API and GUI
enableWriteCDR	Boolean	Enable write to CDR
enableWriteAUDIT	Boolean	Enable write AUDIT
hostName	String	HostName
configDir	String	Config dir
internationalPrefix	String	International prefix
firewallEnabled	Boolean	Enables/disables the application firewall function
overloadSendAlarmOnly	Boolean	Overload send alarm only
scriptReloadPeriod	Number	The time interval in seconds to reload cached data such as dp scenarios, normalization and formatting rules
overloadRecoveryThreshold	Number	Overload recovery Threshold
overloadDisoveryPeriod	Number	Overload Disovery Period
overloadRecoveryPeriod	Number	OverloadRecoveryPeriod
sessionCacheMaxSize	Number	The maximum number of sessions to maintain in this instance
sessionCacheMaxTime	Number	The maximum session time in seconds
sendContinueOnError	Boolean	Set to true/false to enable/disable send continue on error
overloadThreshold	Number	Set a number value as threshold to trigger an overload event (e.g. 80.0 for 80% utilization)
defaultChfUrl	String	Define a default CHF url to sent request to in case CAPIF is unavailable
callMaxDuration	Number	Define maximun duration for call (in seconds)

Setting	Format	Setting description
firewallReloadPeriod	Number	Time interval in seconds to reload the firewall settings from the file
defaultServiceKey	Number	Default service key for initalDP
routerReloadPeriod	Number	Time interval in seconds to reload the router settings from the file
routerEnabled	Booleam	Is router enable or not
idpResTimeout	Number	The maximum time in seconds to wait for idp response

5.2.2 HTTP2 settings

Setting	Format	Setting description
keyPath	String	relative path to the key to be used for TLS
secret	String	the TLS key secret
port	Number	the tcp port to be used for HTTP2 (default: 8443)
disabled	boolean	true to enable HTTP2, false to disable HTTP2

Example: Enable HTTP2 on any address and port 8443

```
"http2": {
    "keyPath": "keys/keystore.jks",
    "secret": "password",
    "port": 8443,
    "disabled": false
  }
```

Example: Disable HTTP2

```
"http2": {
  "disabled": true
}
```

5.2.3 Snmp settings

Allows to configure an SNMP server to send traps to.

Setting	Format	Setting description
serverAddress	String	The IPv4 address of the SNMP server
serverPort	Number	The destination port for SNMP traps (default: 162)

Below the list of traps:

Trap	OID	Trap description
Service state	.1.3.6.1.4.1.68560.1.1.2.1.1	Service status change (UP/DOWN)
Sctp link state	.1.3.6.1.4.1.68560.1.1.2.1.2	Link status change (UP/DOWN)
M3UA peer state	.1.3.6.1.4.1.68560.1.1.2.1.3	Peer status change (ACTIVE/INACTIVE)
CPU overload event	.1.3.6.1.4.1.68560.1.1.2.1.9	DB connection status change (SET/CLEAR)
Diameter peer state	.1.3.6.1.4.1.68560.1.1.2.1.11	Peer status change (UP/DOWN)

NOTE All traps should be considered as critical.

5.2.4 Ss7 configuration

Configure the ss7 settings.

Setting	Format	Description
sendContinueOnError	boolean	Set to true/false to enable/disable send continue on error
sctp	sctp	See response option table below
m3ua	m3ua	See response option table below
sccp	sccp	See response option table below
tcap	tcap	See response option table below
cap	cap	See response option table below

Sctp settings Configuration of the sctp associations. Each association must be set with the following:

Setting	Format	Description
servers	List	List of servers
associations	List	List of associations

Sctp servers settings

Setting	Format	Description
id	Number	Identifier of sctp associations
name	String	A unique identifier for the association (refered by M3UA layer)
primaryIP	String	IPv4 local primary IP address
secondaryIP	String	IPv4 local secondary IP address (optional)
serverPort	Number	The listening port of the server side

Setting	Format	Description
ipChannelType	String	Transport to be used, remains SCTP in most cases

Sctp associations settings

Setting	Format	Description
id	Number	Identifier of sctp associations
name	String	A unique identifier for the association (refered by M3UA layer)
primaryIP	String	IPv4 local primary IP address
secondaryIP	String	IPv4 local secondary IP address (optional)
serverPort	Number	The listening port of the server side
ipChannelType	String	Transport to be used, remains SCTP in most cases
clientIP	String	IP address of the client machine that is initiating an SCTP connection
clientPort	Number	The local port to use for the connection
serverIP	String	IPv4 primary address of the remote party (secondary IP is self configured)
serverName	String	Identifier used to specify the server in the network.

Example: 2 SCTP associations

```
"sctp": {
        "servers": [],
        "associations": [
          {
            "id": 1,
            "primaryIP": "172.20.169.59",
            "clientPort": 2905,
            "serverIP": "10.98.13.4",
            "serverPort": 2905,
            "name": "GTCEN1P",
            "ipChannelType": "SCTP"
          },
          {
            "id": 2,
            "primaryIP": "172.20.169.59",
            "clientPort": 2906,
            "serverIP": "10.98.13.68",
            "serverPort": 2905,
            "name": "GTGDV1P",
            "ipChannelType": "SCTP"
          },
          {
            "id": 3,
            "primaryIP": "172.20.169.59",
            "clientPort": 2936,
```

```
            "serverIP": "10.196.27.11",
            "serverPort": 2914,
            "name": "CRHER1P",
            "ipChannelType": "SCTP"
          },
          {
            "id": 4,
            "primaryIP": "172.20.169.59",
            "clientPort": 2937,
            "serverIP": "10.203.7.141",
            "serverPort": 2914,
            "name": "CRPOZ1P",
            "ipChannelType": "SCTP"
          },
          {
            "id": 5,
            "primaryIP": "172.20.169.59",
            "clientPort": 2913,
            "serverIP": "10.143.129.219",
            "serverPort": 2905,
            "name": "ESROM1P",
            "ipChannelType": "SCTP"
          },
          {
            "id": 6,
            "primaryIP": "172.20.169.59",
            "clientPort": 2914,
            "serverIP": "10.143.130.21",
            "serverPort": 2905,
            "name": "ESVEN1P",
            "ipChannelType": "SCTP"
          },
          {
            "id": 7,
            "primaryIP": "172.20.169.59",
            "clientPort": 2921,
            "serverIP": "10.10.1.13",
            "serverPort": 2905,
            "name": "HNTEG1P",
            "ipChannelType": "SCTP"
          },
          {
            "id": 8,
            "primaryIP": "172.20.169.59",
            "clientPort": 2922,
            "serverIP": "10.10.2.13",
            "serverPort": 2905,
            "name": "HNSPS1P",
            "ipChannelType": "SCTP"
          },
          {
            "id": 9,
            "primaryIP": "172.20.169.59",
            "clientPort": 2929,
```

```
            "serverIP": "10.15.38.9",
            "serverPort": 2905,
            "name": "NIVIF1P",
            "ipChannelType": "SCTP"
          },
          {
            "id": 10,
            "primaryIP": "172.20.169.59",
            "clientPort": 2930,
            "serverIP": "10.15.9.12",
            "serverPort": 2905,
            "name": "NIEST1P",
            "ipChannelType": "SCTP"
          }
        ]
      }
```

M3ua settings

Setting	Format	Description
stackId	Number	Identifier for the protocol stack instance associated with this M3ua
maxAsForRoute	Number	Controls the maximum number of AS that can be used to route the message to the same Destination Point Code

Configuration of the M3UA peers. Each peer must be set with the following:

Setting	Format	Description
id	Number	Identifier of M3UA peer
routingContext	Number	The routing context to be used for the peer
trafficModeType	Number	1 for Override, 2 for Loadsharing, 3 for Broadcast
associationName	String	Unique identifier of the underlayer sctp association
ipspType	String	Always CLIENT for typical use cases, can be occasionally SERVER
exchangeType	String	SE for Single exchange, DE for Double exchange
networkAppearance	Number	NEtwork appearance indicator for this peer
remotePointCode	Number	Decimal value of the peer point code
routes	List	See routes settings below

Example: 2 M3UA peers

```
"m3ua": {
        "stackId": 1,
        "maxAsForRoute": 2,
        "asps": [
```

```
            {
              "id": 1,
              "routingContext": 1,
              "trafficModeType": 2,
              "associationName": "GTCEN1P",
              "ipspType": "CLIENT",
              "exchangeType": "SE",
              "networkAppearance": null,
              "remotePointCode": 2406,
              "routes": []
            },
            {
              "id": 2,
              "routingContext": 1,
              "trafficModeType": 2,
              "associationName": "GTGDV1P",
              "ipspType": "CLIENT",
              "exchangeType": "SE",
              "networkAppearance": null,
              "remotePointCode": 2677,
              "routes": []
            },
            {
              "id": 3,
              "routingContext": 1,
              "trafficModeType": 2,
              "associationName": "CRHER1P",
              "ipspType": "CLIENT",
              "exchangeType": "SE",
              "networkAppearance": null,
              "remotePointCode": 1830,
              "routes": []
            },
            {
              "id": 4,
              "routingContext": 1,
              "trafficModeType": 2,
              "associationName": "CRPOZ1P",
              "ipspType": "CLIENT",
              "exchangeType": "SE",
              "networkAppearance": null,
              "remotePointCode": 1838,
              "routes": []
            },
            {
              "id": 5,
              "routingContext": 1,
              "trafficModeType": 2,
              "associationName": "ESROM1P",
              "ipspType": "CLIENT",
              "exchangeType": "SE",
              "networkAppearance": null,
              "remotePointCode": 810,
              "routes": []
```

```
            },
            {
              "id": 6,
              "routingContext": 1,
              "trafficModeType": 2,
              "associationName": "ESVEN1P",
              "ipspType": "CLIENT",
              "exchangeType": "SE",
              "networkAppearance": null,
              "remotePointCode": 811,
              "routes": []
            },
            {
              "id": 7,
              "routingContext": 1,
              "trafficModeType": 2,
              "associationName": "HNTEG1P",
              "ipspType": "CLIENT",
              "exchangeType": "SE",
              "networkAppearance": null,
              "remotePointCode": 10384,
              "routes": []
            },
            {
              "id": 8,
              "routingContext": 1,
              "trafficModeType": 2,
              "associationName": "HNSPS1P",
              "ipspType": "CLIENT",
              "exchangeType": "SE",
              "networkAppearance": null,
              "remotePointCode": 10397,
              "routes": []
            },
            {
              "id": 9,
              "routingContext": 1,
              "trafficModeType": 2,
              "associationName": "NIVIF1P",
              "ipspType": "CLIENT",
              "exchangeType": "SE",
              "networkAppearance": null,
              "remotePointCode": 1029,
              "routes": []
            },
            {
              "id": 10,
              "routingContext": 1,
              "trafficModeType": 2,
              "associationName": "NIEST1P",
              "ipspType": "CLIENT",
              "exchangeType": "SE",
              "networkAppearance": null,
              "remotePointCode": 785,
```

```
            "routes": []
          }
        ],
        "sgws": []
      }
```

M3ua routes settings

Setting	Format	Description
id	Number	Identifier of M3UA route
dpc	Number	Destination point code
opc	Number	Originating point code
si	Number	Service indicator
asName	String	Unique name of As
trafficModeType	Number	1 for Override, 2 for Loadsharing, 3 for Broadcast

Sccp general settings

Setting	Format	Description
version	String	This parameter is four octets with the MSB first and the LSB last.
routingIndicator	Number	Default 0 for GT routing, 1 for SSN/PC routing
numberingPlan	Number	Default 1 for ISDN Telephony, 2 for Generic, ... , 7 for ISDN Mobile
natureOfAddress	Number	Default 1 for Subscriber Number, 3 for National, 4 for International
translationType	Number	Default translation type for GT addressing (Default: 0)

Sccp resources settings

Setting	Format	Description
remotePointCode	Number	Decimal representation of the remote point code
ssn	Number	Decimal representation of the remote subsystem number

Example: 1 remote ssn

```
"resources": [
          {
            "id": 1,
            "remotePointCode": 2406,
            "ssn": 146
          },
          {
            "id": 2,
```

```
            "remotePointCode": 2677,
            "ssn": 146
          },
          {
            "id": 3,
            "remotePointCode": 1830,
            "ssn": 146
          },
          {
            "id": 4,
            "remotePointCode": 1838,
            "ssn": 146
          },
          {
            "id": 5,
            "remotePointCode": 810,
            "ssn": 146
          },
          {
            "id": 6,
            "remotePointCode": 811,
            "ssn": 146
          },
          {
            "id": 7,
            "remotePointCode": 10384,
            "ssn": 146
          },
          {
            "id": 8,
            "remotePointCode": 10897,
            "ssn": 146
          }
          ,{
            "id": 9,
            "remotePointCode": 1029,
            "ssn": 146
          },
          {
            "id": 10,
            "remotePointCode": 785,
            "ssn": 146
          }
        ]
```

Sccp saps settings

Setting	Format	Description
sapId	Number	Identifier for the Service Access Point (SAP).
stackId	Number	Identifier for the protocol stack instance associated with this SAP.

Setting	Format	Description
localPointCode	Number	Decimal representation of the remote point code
networkIndicator	Number	1 for Internatinal, 2 for National
networkid	Number	Identifier of the network
localGtDigits	String	SAPS specifies the local Global Title digits
destinations	List	List of destinations, see destination parameters below

#Saps destinations settings

Setting	Format	Description
remotePointCode	Number	Decimal representation of the remote subsystem number
firstSls	Number	The first Signaling Link Selection (SLS) value used for load sharing across multiple links.
lastSls	Number	The last Signaling Link Selection (SLS) value used for load sharing across multiple links.
slsMask	Number	A bitmask applied to the SLS value to determine the actual link to use for message routing.

Example: 1 SCCP saps

```
  "saps": [
           {
             "id": 1,
             "sapId": 1,
             "stackId": 1,
             "localPointCode": 2001,
             "networkIndicator": 3,
             "networkid": 0,
             "localGtDigits": "50255300501",
             "destinations": [
               {
                 "id": 1,
                 "remotePointCode": 2406,
                 "firstSls": 0,
                 "lastSls": 255,
                 "slsMask": 255
               },
               {
                 "id": 2,
                 "remotePointCode": 2677,
                 "firstSls": 0,
                 "lastSls": 255,
                 "slsMask": 255
               },
               {
```

```
      "id": 3,
      "remotePointCode": 1830,
      "firstSls": 0,
      "lastSls": 255,
      "slsMask": 255
    },
    {
      "id": 4,
      "remotePointCode": 1838,
      "firstSls": 0,
      "lastSls": 255,
      "slsMask": 255
    },
    {
      "id": 5,
      "remotePointCode": 810,
      "firstSls": 0,
      "lastSls": 255,
      "slsMask": 255
    },
    {
      "id": 6,
      "remotePointCode": 811,
      "firstSls": 0,
      "lastSls": 255,
      "slsMask": 255
    },
    {
      "id": 7,
      "remotePointCode": 10384,
      "firstSls": 0,
      "lastSls": 255,
      "slsMask": 255
    },
    {
      "id": 8,
      "remotePointCode": 10897,
      "firstSls": 0,
      "lastSls": 255,
      "slsMask": 255
    },
    {
      "id": 9,
      "remotePointCode": 1029,
      "firstSls": 0,
      "lastSls": 255,
      "slsMask": 255
    },
    {
      "id": 10,
      "remotePointCode": 785,
      "firstSls": 0,
      "lastSls": 255,
      "slsMask": 255
```

```
            }
          ]
        }
      ]
```

Sccp addresses settings

Setting	Format	Description
id	Number	Index and identifier of the address entry
description	String	Decription of routing endress
pc	Number	Decimal representation of the point code
ssn	Number	Decimal representation of the subsystem number
gt	GlobalTile	The local global title

GlobalTitle:

Setting	Format	Description
digits	String	Global title digits
translationType	Number	Translation type for GT addressing (Default: 0)
numberingPlan	Number	1 for ISDN Telephony, 2 for Generic, ... , 7 for ISDN Mobile
bcdEncoding	Number	1 for Odd, 2 for Even
natureOfAddress	Number	1 for Subscriber Number, 3 for National, 4 for International

Example: 2 SCCP addresses

```
"addresses": [
        {
          "id": 1,
          "description": "LOCAL",
          "pc": 2001,
          "ssn": 146,
          "gt": {
            "digits": "50255300501",
            "translationType": 0,
            "numberingPlan": 1,
            "bcdEncoding": 1,
            "natureOfAddress": 4
          }
        },
        {
          "id": 2,
          "description": "GTCEN1P",
          "pc": 2406,
          "ssn": 146,
```

```
      "gt": {
        "digits": "+/+",
        "translationType": 0,
        "numberingPlan": 1,
        "bcdEncoding": 1,
        "natureOfAddress": 4
      }
    },
    {
      "id": 3,
      "description": "GTGDV1P",
      "pc": 2677,
      "ssn": 146,
      "gt": {
        "digits": "+/+",
        "translationType": 0,
        "numberingPlan": 1,
        "bcdEncoding": 1,
        "natureOfAddress": 4
      }
    },
    {
      "id": 4,
      "description": "CRHER1P",
      "pc": 1830,
      "ssn": 146,
      "gt": {
        "digits": "+/+",
        "translationType": 0,
        "numberingPlan": 1,
        "bcdEncoding": 1,
        "natureOfAddress": 4
      }
    },
    {
      "id": 5,
      "description": "CRPOZ1P",
      "pc": 1838,
      "ssn": 146,
      "gt": {
        "digits": "+/+",
        "translationType": 0,
        "numberingPlan": 1,
        "bcdEncoding": 1,
        "natureOfAddress": 4
      }
    },
    {
      "id": 6,
      "description": "ESROM1P",
      "pc": 810,
      "ssn": 146,
      "gt": {
        "digits": "+/+",
```

```
        "translationType": 0,
        "numberingPlan": 1,
        "bcdEncoding": 1,
        "natureOfAddress": 4
      }
    },
    {
      "id": 7,
      "description": "ESVEN1P",
      "pc": 811,
      "ssn": 146,
      "gt": {
        "digits": "+/+",
        "translationType": 0,
        "numberingPlan": 1,
        "bcdEncoding": 1,
        "natureOfAddress": 4
      }
    },
    {
      "id": 8,
      "description": "HNTEG1P",
      "pc": 10384,
      "ssn": 146,
      "gt": {
        "digits": "+/+",
        "translationType": 0,
        "numberingPlan": 1,
        "bcdEncoding": 1,
        "natureOfAddress": 4
      }
    },
    {
      "id": 9,
      "description": "HNSPS1P",
      "pc": 10897,
      "ssn": 146,
      "gt": {
        "digits": "+/+",
        "translationType": 0,
        "numberingPlan": 1,
        "bcdEncoding": 1,
        "natureOfAddress": 4
      }
    },
    {
      "id": 10,
      "description": "NIVIF1P",
      "pc": 1029,
      "ssn": 146,
      "gt": {
        "digits": "+/+",
        "translationType": 0,
        "numberingPlan": 1,
```

```
            "bcdEncoding": 1,
            "natureOfAddress": 4
          }
        },
        {
          "id": 11,
          "description": "NIEST1P",
          "pc": 785,
          "ssn": 146,
          "gt": {
            "digits": "+/+",
            "translationType": 0,
            "numberingPlan": 1,
            "bcdEncoding": 1,
            "natureOfAddress": 4
          }
        }
      ]
```

Sccp rules settings

Setting	Format	Description
id	Number	Index and identifier of routing rule
networkId	Number	Identifier of the network
description	String	Sccp rule description
type	String	SOLITARY for single destination, DOMINANT for primary/secondary with primary dominant or LOADSHARE for load balancing between primary and secondary
lbAlgo	String	Specifies the load balancing to be used for distributing traffic across multiple signaling links.
originationType	String	LOCAL to apply on sccp message comming from local ASP or REMOTE to apply onsccp message comming from remote ASP
mask	string	R for replace, K for keep, - for padding and / to split
primaryAddress	Number	Id of the sccp address to be applied to this rule
secondaryAddress	Number	Id of the secondary sccp address to be applied to this rule
pattern	Pattern	The pattern to use to match the rule against
newCallingPartyAddress	Number	

Pattern

Setting	Format	Description
pc	Number	Decimal representation of the point code

Setting	Format	Description
ssn	Number	Decimal representation of the subsystem number
gt	GlobalTile	The local global title

GlobalTitle

Setting	Format	Description
digits	String	Global title digits
translationType	Number	Translation type for GT addressing (Default: 0)
numberingPlan	Number	1 for ISDN Telephony, 2 for Generic, ... , 7 for ISDN Mobile
bcdEncoding	Number	1 for Odd, 2 for Even
natureOfAddress	Number	1 for Subscriber Number, 3 for National, 4 for International

Example: SCCP rule

```
  "rules": [
           {
             "id": 1,
             "networkId": 0,
             "description": "LOCAL",
             "type": "SOLITARY",
             "lbAlgo": "Undefined",
             "originationType": "REMOTE",
             "pattern": {
               "pc": 0,
               "ssn": 0,
               "gt": {
                 "digits": "50255300501",
                 "translationType": 0,
                 "numberingPlan": 1,
                 "bcdEncoding": 1,
                 "natureOfAddress": 4
               }
             },
             "mask": "K",
             "primaryAddress": 1,
             "secondaryAddress": -1,
             "newCallingPartyAddress": 0
           },
           {
             "id": 2,
             "networkId": 0,
             "description": "REMOTE",
             "type": "LOADSHARED",
             "lbAlgo": "Bit0",
             "originationType": "LOCAL",
             "pattern": {
```

```
        "pc": 0,
        "ssn": 0,
        "gt": {
          "digits": "502/*",
          "translationType": 0,
          "numberingPlan": 1,
          "bcdEncoding": 1,
          "natureOfAddress": 4
        }
      },
      "mask": "K/K",
      "primaryAddress": 2,
      "secondaryAddress": 3,
      "newCallingPartyAddress": 0
    },
    {
      "id": 3,
      "networkId": 0,
      "description": "REMOTE",
      "type": "LOADSHARED",
      "lbAlgo": "Bit0",
      "originationType": "LOCAL",
      "pattern": {
        "pc": 0,
        "ssn": 0,
        "gt": {
          "digits": "506/*",
          "translationType": 0,
          "numberingPlan": 1,
          "bcdEncoding": 1,
          "natureOfAddress": 4
        }
      },
      "mask": "K/K",
      "primaryAddress": 4,
      "secondaryAddress": 5,
      "newCallingPartyAddress": 0
    },
    {
      "id": 4,
      "networkId": 0,
      "description": "REMOTE",
      "type": "LOADSHARED",
      "lbAlgo": "Bit0",
      "originationType": "LOCAL",
      "pattern": {
        "pc": 0,
        "ssn": 0,
        "gt": {
          "digits": "503/*",
          "translationType": 0,
          "numberingPlan": 1,
          "bcdEncoding": 1,
          "natureOfAddress": 4
```

```
        }
      },
      "mask": "K/K",
      "primaryAddress": 6,
      "secondaryAddress": 7,
      "newCallingPartyAddress": 0
    },
    {
      "id": 5,
      "networkId": 0,
      "description": "REMOTE",
      "type": "LOADSHARED",
      "lbAlgo": "Bit0",
      "originationType": "LOCAL",
      "pattern": {
        "pc": 0,
        "ssn": 0,
        "gt": {
          "digits": "504/*",
          "translationType": 0,
          "numberingPlan": 1,
          "bcdEncoding": 1,
          "natureOfAddress": 4
        }
      },
      "mask": "K/K",
      "primaryAddress": 8,
      "secondaryAddress": 9,
      "newCallingPartyAddress": 0
    },
    {
      "id": 6,
      "networkId": 0,
      "description": "REMOTE",
      "type": "LOADSHARED",
      "lbAlgo": "Bit0",
      "originationType": "LOCAL",
      "pattern": {
        "pc": 0,
        "ssn": 0,
        "gt": {
          "digits": "505/*",
          "translationType": 0,
          "numberingPlan": 1,
          "bcdEncoding": 1,
          "natureOfAddress": 4
        }
      },
      "mask": "K/K",
      "primaryAddress": 10,
      "secondaryAddress": 11,
      "newCallingPartyAddress": 0
    }
```

```
        ]
```

Sccp routes settings

Setting	Format	Description
localPointCode	Number	Decimal representation of the remote point code
remotePointCode	Number	Decimal representation of the remote subsystem number
networkIndicator	Number	1 for Internatinal, 2 for National
localGlobalTile	String	The local global title digits to be used for the route

Example: 1 SCCP route

```
"routes": [
     {
       "localPointCode": 1,
       "remotePointCode": 2,
       "networkIndicator": 2,
       "localGlobalTile": "972531209810"
     }
   ]
```

Tcap settings

Setting	Format	Description
ssn	Number	Tcap stack serving subsystem number
dialogIdleTimeout	Number	Tcap dialogue time to live in seconds
invokeTimeout	Number	Tcap invoke response timeout in seconds
maxDialogs	Number	Maximum number of concurrent dialogues in the tcap stack

Cap settings

Setting	Format	Description
natureOfAddress	Number	Default NAI for CAP IE number format
numberingPlan	Number	Default NPI for CAP IE number format
ssn	Number	SCCP Subsystem number to be used by the microservice instance

Map settings

Setting	Format	Description

Setting	Format	Description
natureOfAddress	Number	Default NAI for MAP IE number format
numberingplan	Number	Default NPI for MAP IE number format

Inap settings

Setting	Format	Description
numberingPlan	Number	Default NPI for CAP IE number format
natureOfAddress	Number	Default NAI for CAP IE number format
ssn	Number	SCCP Subsystem number to be used by the microservice instance

5.2.5 Diameter settings

Configuration of the diameter stack global parameters.

Setting	Format	Description
dictionaryFile	String	Path to the dictionary file
mode	String	Typically remains "server" for a load balacing configuration but the stack can also be configures as "client"
useSctpTransport	Boolean	Set to true to use SCTP otherwise, uses TCP
loadBalancingMode	String	A load balancer enables distribution of network traffic dynamically across resources to support an application
localPeer	localPeer	see local peer parameters below
params	params	see params parameters below
network	network	see network parameters below
ro	ro	see ro parameters below
swx	swx	see swx parameters below
swm	swm	see swm parameters below
sy	sy	see sy parameters below
s6a	s6a	see s6a parameters below

Example: Diameter general params

```
"diameter": {
   "dictionaryFile": "config/dictionary.xml",
     "mode": "server",
     "useSctpTransport": true,
     "loadBalancingMode": "NONE",
```

```
    ...
}
```

Diameter local peer configuration The local peer element contains parameters that affect the local Diameter peer.

Setting	Format	Description
uri	String	Specifies the URI for the local peer. The URI has the following format: "aaa://FQDN:port".
ipAddresses	List of String	Contains one or more child IPAddress element, which contain a single, valid IP address for the local peer, stored in the value attribute of the IPAddress
realm	String	Specifies the realm of the local peer, using the value attribute.
vendorID	Number	Specifies a numeric identifier that corresponds to the vendor ID allocated by IANA
productName	String	Specifies the name of the local peer product
firmwareRevision	Number	Specifies the version of the firmware
overloadMonitor	overloadMonitor	see overloadMonitor parameters below
application	List	see application parameter below

Example: local peer

```
"diameter": {
    ...
    "uri": "aaa://chf-iwf-4.modulo.com.gt:13888",
        "ipAddresses": [
          "10.253.96.110"
         ]
    }
```

#Overload monitor settings:

Setting	Format	Description
lowThreshold	Number	The low threshold for activation of the overload monitor
highThreshold	Number	The high threshold for activation of the overload monitor
vendorId	Number	Specifies a numeric identifier that corresponds to the vendor ID allocated by IANA
authAppId	Number	The Authentication Application ID for application definition. It supports a single property: "value"

Setting	Format	Description
acctAppId	Number	The Account Application ID for application definition. It supports a single property: "value"

#Application settings:

Setting	Format	Description
id	Number	Identifier of application
vendorId	Number	Specifies a numeric identifier that corresponds to the vendor ID allocated by IANA
authAppId	Number	The Authentication Application ID for application definition. It supports a single property: "value"
acctAppId	Number	The Account Application ID for application definition. It supports a single property: "value"
applicationId	Number	Unique identier of Diameter application

Diameter params configuration

Setting	Format	Description
acceptUndefinedPeer	Boolean	Specifies whether the stack will accept connections from undefined peers. The default value is false.
duplicateProtection	Boolean	Specifies whether duplicate message protection is enabled. The default value is false.
duplicateTimer	Number	Specifies the time each duplicate message is valid for (in extreme cases, it can live up to 2 * DuplicateTimer - 1 milliseconds). The default, minimum value is 240000 (4 minutes in milliseconds).
duplicateSize	Number	Specifies the number of requests stored for duplicate protection. The default value is 5000.
useUriAsFqdn	Bollean	Determines whether the URI should be used as FQDN. If it is set to true, the stack expects the destination/origin host to be in the format of "aaa://isdn.domain.com:3868" rather than the normal "isdn.domain.com". The default value is false.
queueSize	Number	Determines how many tasks the peer state machine can have before rejecting the next task. This queue contains FSM events and messaging.

Setting	Format	Description
messageTimeOut	Number	Determines the timeout for messages other than protocol FSM messages. The delay is in milliseconds.
stopTimeOut	Number	Determines how long the stack waits for all resources to stop. The delays are in milliseconds.
ceaTimeOut	Number	Determines how long it takes for CER/CEA exchanges to timeout if there is no response. The delays are in milliseconds.
iacTimeOut	Number	Determines how long the stack waits to retry the communication with a peer that has stopped answering DWR messages. The delay is in milliseconds.
dwaTimeOut	Number	Determines how long it takes for a DWR/DWA exchange to timeout if there is no response. The delay is in milliseconds.
dpaTimeOut	Number	Determines how long it takes for a DPR/DPA exchange to timeout if there is no response. The delay is in milliseconds.
recTimeOut	Number	Determines how long it takes for the reconnection procedure to timeout. The delay is in milliseconds.
sessionTimeOut	Number	Determines how long it takes for a session exchange to timeout if there is no response. The delay is in milliseconds
bindDelay	Number	Determines how long time to wait before binding. The delay is in milliseconds
threadPoolSize	Number	Size of thread pool
peerFSMThreadCount	Number	Determines the number of threads for handling events in the Peer FSM.
concurrentThreadgroupSize	Number	Defines the number of threads that can concurrently process Diameter messages, optimizing performance by balancing load and resource usage.
concurrentProcessingMessageTimerSize	Number	Specifies the number of timer threads allocated for managing timeouts and retries of concurrently processed Diameter messages.
concurrentDuplicationMessageTimerSize	Number	Number of timer threads dedicated to handling duplicate message detection and processing.

Setting	Format	Description
concurrentRedirectMessageTimerSize	Number	Determines the number of timer threads allocated for managing the redirection of Diameter messages.
concurrentPeerOverloadTimerSize	Number	Number of timer threads dedicated to managing peer overload situations.
concurrentConnectionTimerSize	Number	Specifies the number of timer threads allocated for managing connection-related timers.
concurrentStatisticTimerSize	Number	Defines the number of timer threads used for managing and updating statistics-related tasks.
statisticsLoggerPause	Number	Specifies the interval or duration for which the statistics logging is paused
statisticsLoggerDelay	Number	Specifies delay or interval before logging statistics, controlling how frequently performance and usage metrics are recorded.
statisticsLoggerEnabled	Boolean	Enable or disable the logging of performance and usage statistics.

Diameter network configuration

Setting	Format	Description
peers	list	see peers parameters below
realms	list	see realms parameters below

#Diameter peers and realms The network element contains elements that specify parameters for external peers and realms. Peers parent element containing the child element "peer", which specifies external peers and the way they connect. Realms parent element containing the child element "realm", which specifies all realms that connect into the Diameter network.

Peer settings: Peer specifies the name of external peers, whether they should be treated as a server or client, and what rating the peer has externally.

Setting	Format	Description
name	String	Specifies the name of the peer in the form of a URI. The structure is "aaa://[fqdn
attemptConnect	Boolean	Determines if the stack should try to connect to this peer
rating	Number	Specifies the rating of this peer in order to achieve peer priorities/sorting
ip	String	Ip address of the peer
portRange	String	Defines the range of local ports that a system can use for establishing network connections with remote peers

Setting	Format	Description
localIp	String	Specifies the local IP address used by a system to communicate with a remote peer
extraLocalIp	String	Additional local IP addresses that can be used by a system

Realm settings:

Setting	Format	Description
name	String	realm string
peers	String	Comma separated list of peers. Each peer is represented by an IP Address or FQDN
localAction	String	Determines the action the Local Peer will play on the specified realm: Act as a LOCAL peer
dynamic	Boolean	Specifies if this realm is dynamic. When set, peers that connect to this realm name will be added to the realm peer list if not present already
expTime	Number	The time before a peer belonging to this realm is removed if no connection is available
vendorId	Number	Specifies a numeric identifier that corresponds to the vendor ID allocated by IANA
authAppId	Number	The Authentication Application ID for application definition.
acctAppId	Number	The Account Application ID for application definition.

Example: Diameter network configuration

```
"diameter": {
    ...
    "network": {
        "peers": [
          {
            "id": 0,
            "name": "aaa://cen-rg-vlte-03.clarogt.americamovil.ca1:3868",
            "attemptConnect": true,
            "rating": 1,
            "ip": "10.253.96.109",
            "portRange": "3868-3868"
          }
        ],
        "realms": [
          {
            "id": 0,
            "name": "modulo.com.gt",
            "peers": "cen-rg-vlte-03.clarogt.americamovil.ca1",
            "localAction": "LOCAL",
```

```
            "dynamic": true,
            "expTime": 1,
            "vendorId": 10415,
            "authAppId": 4
          }
        ]
      }
    ...
```

Diameter ro configuration

Setting	Format	Description
disabled	Boolean	Indicates whether the Diameter RO (Recharge Online) interface is disabled
defaultValidityTime	Number	Specifies the default validity period for a recharge request, in seconds.
defaultTxTimer	Number	Sets the default transaction timer duration, in seconds
sendOnlyLastUsuInTermination	Boolean	
sendSummedUsuInUpdate	Boolean	
defaultDirectDebitFailureHandling	Enum	Defines the handling strategy for direct debit failures, (see directDebitFailureHandling table below)
defaultCreditControlFailureHandling	Enum	Specifies how credit control failures should be managed (see directDebitFailureHandling table below)

directDebitFailureHandling enum:

Field	Type	Description
TERMINATE	0	Stops further processing or attempts after a direct debit transaction fails
CONTINUE	1	Allows the process to proceed despite the direct debit failure

creditControlFailureHandling enum:

Field	Type	Description
TERMINATE_OR_BUFFER	0	Ends the transaction or temporarily buffers it for later processing if credit control fails
CONTINUE	1	Proceeds with the process even if credit control fails
RETRY_AND_TERMINATE	2	Retries the credit control process a set number of times, and terminates the process if it continues to fail

Example: Diameter ro configuration

```
"diameter": {
   ...
       "ro": {
        "disabled": false,
        "defaultValidityTime": 60,
        "defaultTxTimer": 10,
        "defaultDirectDebitFailureHandling": "CONTINUE",
        "defaultCreditControlFailureHandling": "CONTINUE",
        "sendOnlyLastUsuInTermination": false
    },
    ...
}
```

Diameter swx configuration

Setting	Format	Description
disabled	Boolean	Indicates whether the Diameter swx interface is disabled

Example: Diameter swx configuration

```
"diameter": {
   ...
    "swx": {
      "disabled": true
    },
    ...
}
```

Diameter swm configuration

Setting	Format	Description
disabled	Boolean	Indicates whether the Diameter swm interface is disabled

Example: Diameter swm configuration

```
"diameter": {
   ...
    "swm": {
      "disabled": true
    },
    ...
}
```

Diameter sy configuration

Setting	Format	Description
disabled	Boolean	Indicates whether the Diameter sy interface is disabled

Example: Diameter sy configuration

```
"diameter": {
   ...
    "sy": {
      "disabled": true
    },
    ...
}
```

Diameter s6 configuration

Setting	Format	Description
disabled	Boolean	Indicates whether the Diameter s6 interface is disabled

Example: Diameter s6 configuration

```
"diameter": {
   ...
    "s6": {
      "disabled": true
    },
    ...
}
```

5.3 Logger configuration file

The default logger configuration is set to:

- write application logs to app.log, rolling the file each hour and keep files back for 24 hours
- write audit logs to audit.log, rolling the file each day and keep files back for 7 days
- write cdr logs to cdr.log, rolling the file each day and keep files back for 7 days
- write alarm logs to alarm.log, rolling the file each day and keep files back for 7 days
- write error logs to alarm.log, rolling the file each day and keep files back for 7 days

The service use log4j as logger, for full documentation of the log4j module refer to https://logging.apache.org/log4j/2.x/manual/

This version introduce a json-based configuration file Default logger.json

```
{
   "configuration": {
      "name": "Default",
      "status": "warn",
      "monitorInterval": "15",
      "appenders": {
         "Console": {
            "name": "STDOUT",
            "PatternLayout": {
               "pattern": "%highlight{%d{yyyy-MM-dd
HH:mm:ss,SSS}|%p|%c{1.1.1.*}|%t|%M|%L|%X %m%n}"
            }
         },
         "Syslog": [
            {
               "name": "SYSLOG",
               "host": "localhost",
               "port": 514,
               "protocol": "UDP",
               "immediateFlush": true,
               "format": "RFC5424",
               "facility": "LOCAL0",
               "appName": "chf-iwf",
               "newLine": true,
               "includeMDC": false,
               "messageId": "LOG"
            },
            {
               "name": "SYSALARM",
               "host": "localhost",
               "port": 514,
               "protocol": "UDP",
               "immediateFlush": true,
               "format": "RFC5424",
               "facility": "LOCAL0",
               "appName": "chf-iwf",
               "newLine": true,
               "includeMDC": false,
               "messageId": "ALARM"
            }
         ],
         "RollingFile": [
            {
               "name": "FILE",
               "fileName": "logs/app.log",
               "filePattern": "logs/app-%d{yyyy-MM-dd-HH}.gz",
               "PatternLayout": {
                  "pattern": "%highlight{%d{yyyy-MM-dd
HH:mm:ss,SSS}|%p|%c{1.1.1.*}|%t|%M|%L|%X %m%n}"
               },
               "Policies": {
                  "TimeBasedTriggeringPolicy": {
                     "interval": "1",
```

```
                    "modulate": true
                  }
               },
               "DefaultRolloverStrategy": {
                  "max": "24"
               }
            },
            {
               "name": "CDR",
               "fileName": "logs/cdr.log",
               "filePattern": "logs/cdr-%d{yyyy-MM-dd}.gz",
               "PatternLayout": {
                  "pattern": "%m%n"
               },
               "Policies": {
                  "TimeBasedTriggeringPolicy": {
                     "interval": "1",
                     "modulate": true
                  }
               },
               "DefaultRolloverStrategy": {
                  "max": "24"
               }
            },
            {
               "name": "AUDIT",
               "fileName": "logs/audit.log",
               "filePattern": "logs/audit-%d{yyyy-MM-dd}.gz",
               "PatternLayout": {
                  "pattern": "%m%n"
               },
               "Policies": {
                  "TimeBasedTriggeringPolicy": {
                     "interval": "1",
                     "modulate": true
                  }
               },
               "DefaultRolloverStrategy": {
                  "max": "24"
               }
            },
            {
               "name": "SNMP",
               "fileName": "logs/alarm.log",
               "filePattern": "logs/alarm-%d{yyyy-MM-dd}.gz",
               "PatternLayout": {
                  "pattern": "%highlight{%d{yyyy-MM-dd
HH:mm:ss,SSS}|%p|%c{1.1.1.*}|%t|%M|%L|%X %m%n}"
               },
               "Policies": {
                  "TimeBasedTriggeringPolicy": {
                     "interval": "1",
                     "modulate": true
                  }
```

```
                },
                "DefaultRolloverStrategy": {
                   "max": "24"
                }
             },
             {
                "name": "ERROR",
                "fileName": "logs/error.log",
                "filePattern": "logs/error-%d{yyyy-MM-dd}.gz",
                "PatternLayout": {
                   "pattern": "%highlight{%d{yyyy-MM-dd
HH:mm:ss,SSS}|%p|%c{1.1.1.*}|%t|%M|%L|%X %m%n}"
                },
                "Policies": {
                   "TimeBasedTriggeringPolicy": {
                      "interval": "1",
                      "modulate": true
                   }
                },
                "DefaultRolloverStrategy": {
                   "max": "24"
                }
             },
             {
                "name": "DIAMETER",
                "fileName": "logs/dmt.log",
                "filePattern": "logs/dmt-%d{yyyy-MM-dd-HH}.gz",
                "PatternLayout": {
                   "pattern": "%d{yyyy-MM-dd
HH:mm:ss,SSS}|%c{1.1.1.*}|%t|%M|%L|%X %m%n"
                },
                "Policies": {
                   "TimeBasedTriggeringPolicy": {
                      "interval": "1",
                      "modulate": true
                   }
                },
                "DefaultRolloverStrategy": {
                   "max": "24"
                }
             }
          ]
       },
       "loggers": {
          "logger": [
             {
                "name": "co.slicce.microservices.common.snmp.manager",
                "level": "info",
                "additivity": false,
                "AppenderRef": [
                   {
                      "ref": "SNMP"
                   }
                ]
```

```
            },
            {
               "name": "co.slicce.microservices.common.audit.log",
               "level": "info",
               "additivity": false,
               "AppenderRef": [
                  {
                     "ref": "AUDIT"
                  }
               ]
            },
            {
               "name": "co.slicce.microservices.common.cdr.writer",
               "level": "info",
               "additivity": false,
               "AppenderRef": [
                  {
                     "ref": "CDR"
                  }
               ]
            },
            {
               "name": "jdiameter.statistic",
               "level": "info",
               "additivity": true,
               "AppenderRef": [
                  {
                     "ref": "DIAMETER"
                  }
               ]
            }
         ],
         "root": {

            "level": "trace",
            "appender-ref": [
               {
                  "level": "warn",
                  "ref": "STDOUT"
               },
               {
                  "level": "warn",
                  "ref": "FILE"
               },
               {
                  "level": "error",
                  "ref": "ERROR"
               }
            ]
         }
      }
   }
}
```

5.3.1 Changing logging level

By default, the logging level is set to WARN. Changing the logging can be done at runtime by editing the logger.json file and applying a new logging level.

Example: changing logging level from WARN to DEBUG before change

```
{
  ...
         "root": {
            "level": "trace",
            "appender-ref": [
               {
                  "level": "warn",
                  "ref": "STDOUT"
               },
               {
                  "level": "warn",
                  "ref": "FILE"
               },
               {
                  "level": "error",
                  "ref": "ERROR"
               }
            ]
         }
      }
   }
```

after change

```
{
  ...
         "root": {
            "level": "trace",
            "appender-ref": [
               {
                  "level": "debug",
                  "ref": "STDOUT"
               },
               {
                  "level": "debug",
                  "ref": "FILE"
               },
```

```
                {
                   "level": "error",
                   "ref": "ERROR"
                }
             ]
          }
       }
```

It's possible to change the logging level for console prints only (STDOUT) or for log file only (FILE).

NOTE DO NOT alter the other logger settings to make sure the CDR, AUDIT, ALARM and ERROR log files functionality is not broken.

---

6. Operation

6.1 Command line interface operations

6.1.1 Service control

Start the chf-iwf service

```
sudo systemctl start chf-iwf
```

Stop the chf-iwf service

```
sudo systemctl stop chf-iwf
```

Restart the chf-iwf service

```
sudo systemctl restart chf-iwf
```

Query the status of the chf-iwf service

```
sudo systemctl status chf-iwf
```

Enable automatic start at system boot

```
sudo systemctl enable chf-iwf
```

6.1.2 Working with files

Confilg files are backed up automatically at pre-defined intervals in the same config directory. After backup the config file is reloaded. A change in a config file will therefore happen after a lapse of time or after a service restart.

NOTE A malformed config file breaking the json format could prevent the service from starting.

6.2 Web-based interface operations

The web-based interface is available at the url configured in the 'useURL' parameter of the 'appsettings.json' configuration file.

The web-based interface allows the following operations

Operation	Description	Comments
Dashboard	Visualization of the system status, link status and high level traffic information	Read only
General Settings	Review service configuration	
Ss7 Settings	Review ss7 configuration	
Diameter Settings	Review Diameter configuration	
Maintenance	Review and control the service state	
API	Swagger documentation of the service APIs	

6.3 APIs

4 families of APIs available for remote control and provisiong

API Family	Description
Admin	APIs available for service administration, control and configuration

6.3.1. Admin APIs

6.3.1.1 Get Log Files

Route -

```
[ip-address]:[port]/api/v1.2.1/admin/files/logs
```

Request -

```
curl -X 'GET' \
  'https://[ip-address]:[port]/api/v1.2.1/admin/files/logs' \
  -H 'accept: application/json'
'
```

Response -

```
{
  "status": "success",
  "data": [
    {
      "fullname": "./logs/app-2024-06-26-15.gz",
      "name": "app-2024-06-26-15.gz",
      "created": "2024-06-26T17:08:45.29807169Z",
      "modified": "2024-06-26T17:08:45.29807169Z",
      "type": "log",
      "size": 659
    },
    ...

      ],
  "message": "file list retrieved."
}
```

6.3.1.2 Delete Log Files

Route -

```
[ip-address]:[port]/api/v1.2.1/admin/files/logs/[fileName]
```

Request -

```
curl -X 'GET' \
  'https://[ip-address]:[port]/api/v1.2.1/admin/files/logs/.%2Flogs%2Fapp-
2024-06-26-15.gz' \
  -H 'accept: application/json'
'
```

Response -

```
{

  "status": "success",
  "data": {
    "status": true
  },
  "message": "file deleted."
}
```

6.3.1.3 Get Audit Log Files

Route -

```
[ip-address]:[port]/api/v1.2.1/admin/files/logs/audit
```

Request -

```
curl -X 'GET' \
  'https://[ip-address]:[port]/api/v1.2.1/admin/files/logs/audit' \
  -H 'accept: application/json'
```

Response -

```
{
  "status": "success",
  "data": [
    "audit-2025-01-07.gz",
    "audit.log",
    "audit-2025-02-05.gz",
    "audit-2025-01-14.gz",
    "audit-2025-02-12.gz",
    "audit-2025-01-16.gz",
    "audit-2025-01-28.gz",
    "audit-2025-02-11.gz",
    "audit-2025-02-06.gz",
    "audit-2025-01-22.gz",
    "audit-2025-02-09.gz",
    "audit-2025-01-23.gz",
    "audit-2025-01-27.gz",
    "audit-2025-01-26.gz"
  ],
  "message": "Audit files retreived."
}
```

6.3.1.4 Get Audit Log File Content

Route -

```
[ip-address]:[port]/api/v1.2.1/admin/files/logs/audit/[fileName]?page=
[pageNumber]&limit=[numberOfLogsPerPage]&search=[searchString]
```

Request -

```
curl -X 'GET' \
  'https://[ip-address]:[port]/api/v1.2.1/admin/files/logs/audit/audit.log?
page=1&limit=1&search=200' \
  -H 'accept: application/json'
```

Response -


```
{
  "status": "success",
  "data": {
    "data": [
      {
        "timestamp": "2025-02-13T06:56:07.193558569Z",
        "username": null,
        "direction": 0,
        "request": {
          "timeStamp": "2025-02-13T06:56:07.194Z",
          "method": "GET",
          "scheme": "HTTP/1.1",
          "host": "10.0.0.43",
          "path": "/api/v1.2.1/admin/files/logs/audit",
          "queryParams": null,
          "body": ""
        },
        "response": {
          "timeStamp": "2025-02-13T06:56:07.194Z",
          "statusCode": 200,
          "body": "{\"status\":\"success\",\"data\":[\"audit-2025-01-
07.gz\",\"audit.log\",\"audit-2025-02-05.gz\",\"audit-2025-01-
14.gz\",\"audit-2025-02-12.gz\",\"audit-2025-02-12\",\"audit-2025-01-
16.gz\",\"audit-2025-01-28.gz\",\"audit-2025-02-11.gz\",\"audit-2025-02-
06.gz\",\"audit-2025-01-22.gz\",\"audit-2025-02-09.gz\",\"audit-2025-01-
23.gz\",\"audit-2025-01-27.gz\",\"audit-2025-01-
26.gz\"],\"message\":\"Audit files retreived.\"}"
        },
        "duration": 532
      }
    ],
    "totalCount": 607
```

```
  },
  "message": "File retrieved."
}
```

6.4 KPI Collection vi API

Request:

```
curl -X 'POST' \
  'http://[ip-address]:[port]/api/v1.2.1/admin/service/kpis' \
  -H 'Content-Type: application/json'
```

Response:

```
{
  "status": "success",
  "data": [
    {
      "name": "Active Calls",
      "value": 0,
      "threshold": 5000,
      "timestamp": "14-08-2024 09:52:31 Z"
    },
    {
      "name": "Ro Sessions",
      "value": 0,
      "threshold": 5000,
      "timestamp": "14-08-2024 09:52:31 Z"
    },
    {
      "name": "Memory",
      "value": 371,
      "threshold": 4194,
      "timestamp": "14-08-2024 09:52:31 Z"
    },
    {
      "name": "Cap Sessions",
      "value": 0,
      "threshold": 5000,
      "timestamp": "14-08-2024 09:52:31 Z"
    },
    {
      "name": "CPU",
      "value": 0.21,
      "threshold": 2,
      "timestamp": "14-08-2024 09:52:31 Z"
    },
    {
```

```
        "name": "Threads",
        "value": 28,
        "threshold": 32768,
        "timestamp": "14-08-2024 09:52:31 Z"
      }
    ],
    "message": "kpis retrieved."
  }
```


6.5 CDR format

The CDR generated at the end of each call flow in the file cdr.log is formated as following: Top level record:

Field	Format	Description
cap	Object	The CAP level call related information (see CAP table below)
dialogId	Number	Tcap Dialog Id
invokeId	Number	Invoke Id of Cap message
serviceKey	Number	Idp Service Key
detectionPoint	Number	Indicate orignating or terminating
callingPartyNPI	Number	Calling party Numbering Plan Indicator
callingPartyNOA	Number	Calling Party Nature Of Address
callingPartyDigits	String	Calling Party
calledPartyNPI	Number	Called Party Numbering Plan Indicator
calledPartyNOA	Number	Called Party Nature Of Address
calledPartyDigits	String	Called Party
callRefrenceNumber	Number	Idp Call ref
dmt	Object	The DMT level call related information (see DMT table below)
sessionId	String	Diameter Session Id
subbscriptions	String	Subsciber List
ref	String	Set to co-relate between diameter and cap
sessionType	Enum	Type of the session (see sessionType table below)
sessionDirection	Enum	Is it "MO" or "MT" session
audibleIndicator	Boolean	Indicates whether an audible signal is enabled or disabled
maxCallDuration	Number	
releaseIfduractionExceeded	Boolean	True/ false if release the call when duraction exceeded
grantedSU	List	How much quota allocated

Field	Format	Description
usedSU	List	How much quota actually used
timeStamp	String	The time of the call flow initiation
id	String	A unique id assigned to each specific call
services	String	List of Service
responseTime	Number	The duration elapsed in milliseconds between the initiation of the call flow and the first response to initialDP (continue, connect or release)
duration	Number	The duration elapsed in milliseconds between the initiation of the call flow and its termination (tcap end or ccr-t)
response	String	THe latest text representation of the last status of the call (see RESPONSE table below)
sendContinueOnError	Boolean	Set to true/false to enable/disable send continue on error

Response options:

Field	Description
ENDED	Normal call flow termination
ERROR	Internal error
UABORT	TCAP User abort
PABORT	TCAP Provider abort
ABANDONED	Abandonned EBCSM event
BUSY	Busy EBCSM event
NOANSWER	No answer EBCSM event
ROUTEFAILURE	Route select failure EBCSM event
TIMEOUT	Timeout on tcap transaction
BLOCKED	Call blocked and announcement triggered
BANNED	Call banned and released

sessionType options:

Field	Description
DIAMETER	DIAMETER

CAP level record:

Field	Format	Description
dialogId	Number	The internal dialog transaction id on the local stack
invokeId	Number	The initial invokeId of the session
serviceKey	Number	The service key reported in the initial DP
detectionPoint	Number	Indicate a specific event that has occurred during the call process.
service	String	Voice, SMS or Data
callingPartyNPI	Number	The number representation for the Numbering Plan Indicator of the original calling party number
callingPartyNOA	Number	The number representation for the Nature of Address indicator of the original calling party number
callingPartyDigits	String	The digits string of the original calling party number
calledPartyNPI	Number	The number representation for the Numbering Plan Indicator of the original called party number
calledPartyNOA	Number	The number representation for the Nature of Address indicator of the original called party number
calledPartyDigits	String	The digits string of the original called party numbe
callReferenceNumber	String	Call reference number assigned to the call

Example of CAP CDR:


```
"cap":
{"dialogId":3951703,"invokeId":0,"serviceKey":0,"detectionPoint":2,"calling
PartyNPI":1,"callingPartyNOA":4,"callingPartyDigits":"xxx58714912","calledP
artyNPI":1,"calledPartyNOA":4,"calledPartyDigits":"xxx46977663","callRefren
ceNumber":"45379683"}
```


DMT level record:

Field	Format	Description
sessionId	String	Call reference number
subbscriptions	List	Identify a subscribers within a network

Example of DMT CDR:


```
"dmt":{"sessionId":"GTATS01-7439058;1731220661;1123;27","subbscriptions":
["+50258714912"]}
```

Example of CDR:


```
{"cap":
{"dialogId":3951703,"invokeId":0,"serviceKey":0,"detectionPoint":2,"calling
PartyNPI":1,"callingPartyNOA":4,"callingPartyDigits":"xxx58714912","calledP
artyNPI":1,"calledPartyNOA":4,"calledPartyDigits":"xxx46977663","callRefren
ceNumber":"45379683"},"dmt":{"sessionId":"GTATS01-
7439058;1731220661;1123;27","subbscriptions":
["+50258714912"]},"ref":"GTATS01-
7439058;1731220661;1123;27","sessionType":"DIAMETER","sessionDirection":"MO
","audibleIndicator":false,"maxCallDuration":1800,"releaseIfduractionExceed
ed":false,"grantedSU":[180,180],"usedSU":[0,16],"timeStamp":"2024-11-
10T06:37:41.797752-06:00","id":"eec88aaf-9a8f-485e-9973-
61585f70ea56","services":
[],"responseTime":63,"duration":15645,"response":"ENDED","sendContinueOnErr
or":false}
```


7. Location Handling (IMS Flows)

7.a. VoLTE Calls (ECGI from PANI)

For VoLTE-based calls, location information is derived from the P-Access-Network-Info (PANI) AVP. The E-UTRAN Cell Global Identifier (ECGI) is extracted and directly mapped to the CAMEL Cell ID Location Information Element (IE).

7.b. VoWiFi Calls (IP-based Location)

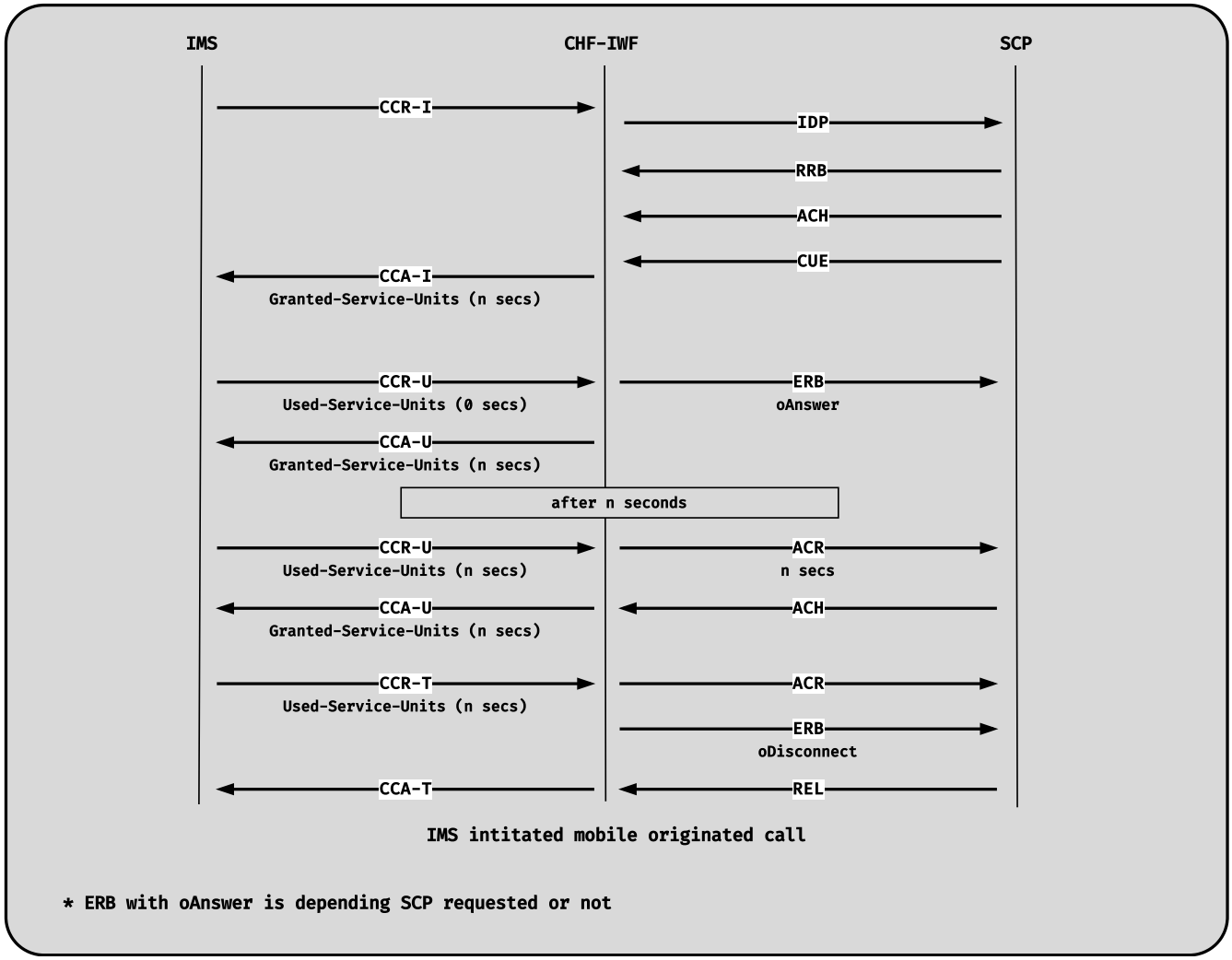
For VoWiFi calls, as ECGI is not available, the UE IP address is used as an alternative to represent location. The IP address is converted into a numeric format and populated into the CAMEL Cell ID Location IE in place of the ECGI.

7.c. IPv6 Handling

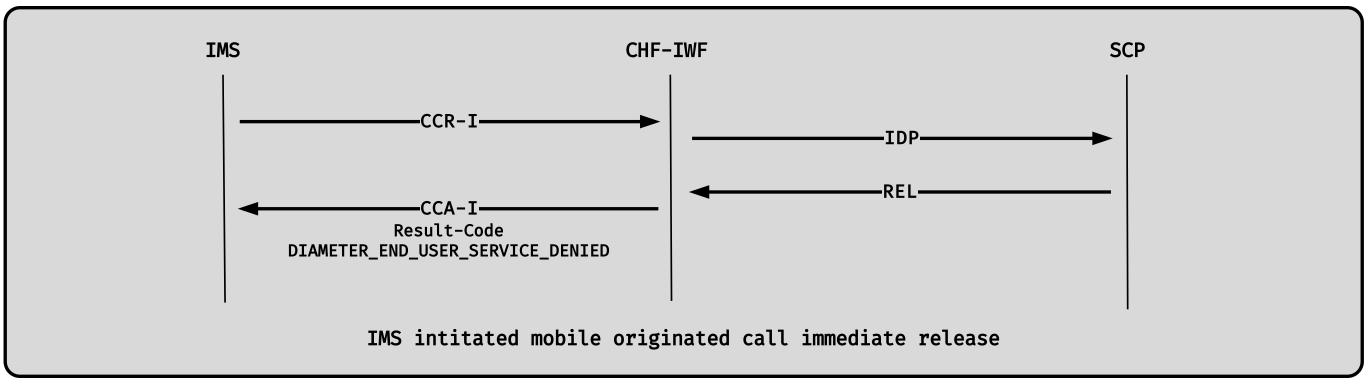
When the UE is assigned an IPv6 address, only the IPv6 prefix is used instead of the full address. This ensures compliance with the size and format limitations of the CAMEL Cell ID Location IE while still preserving meaningful location-related information.

8. IMS Initiated call flows

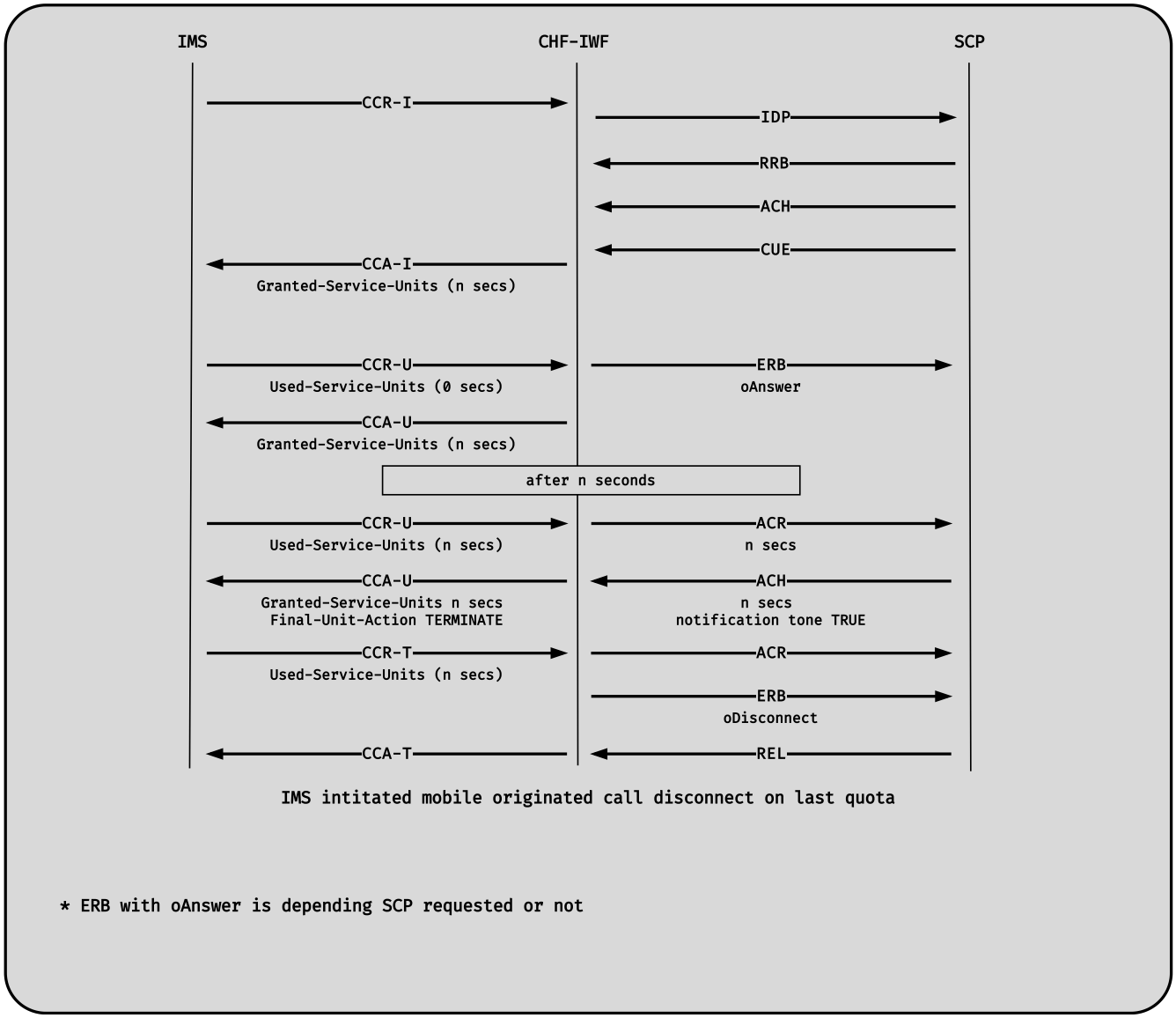
8.1 Mobile originated call



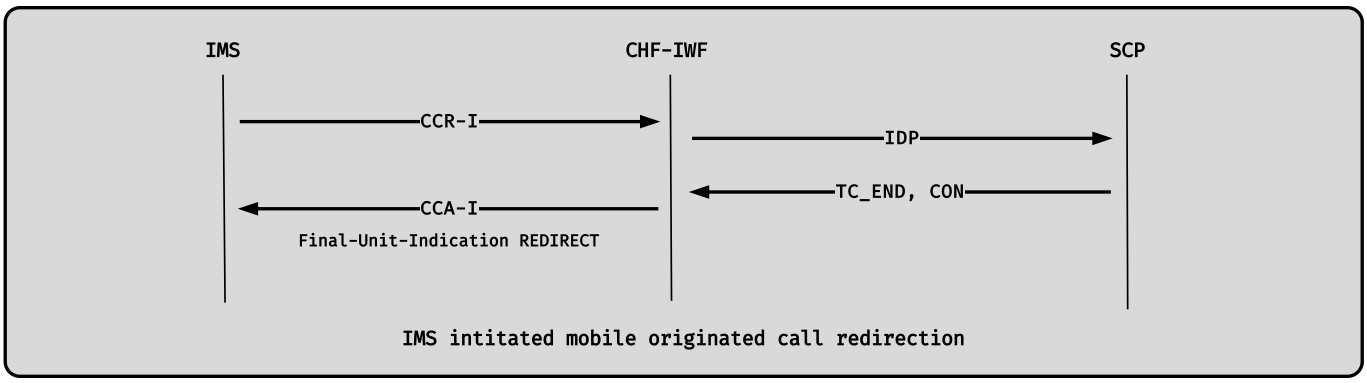
8.2 Mobile originated call immediate release



8.3 Mobile originated call disconnect on last quota

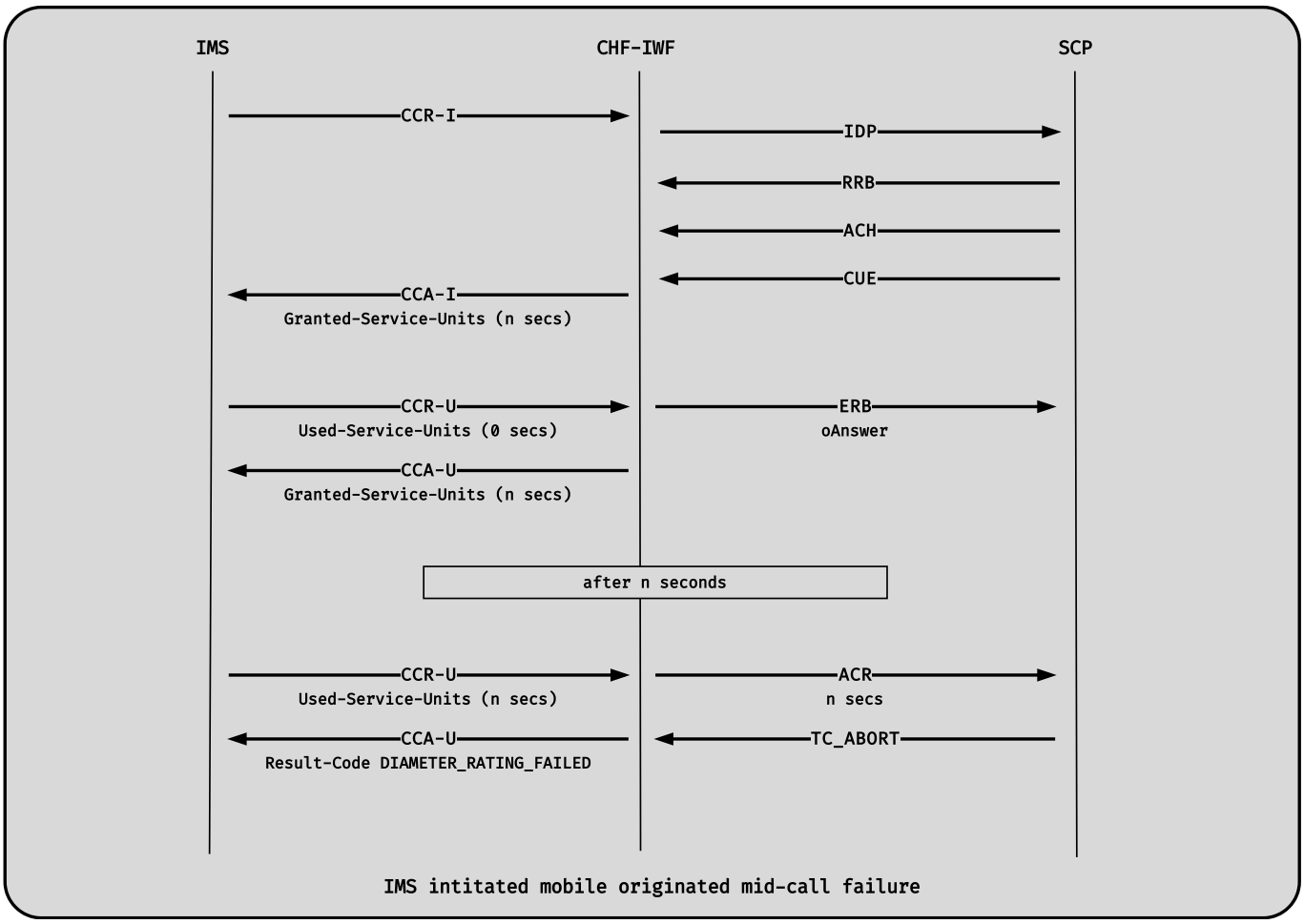


8.4 Mobile originated call redirection

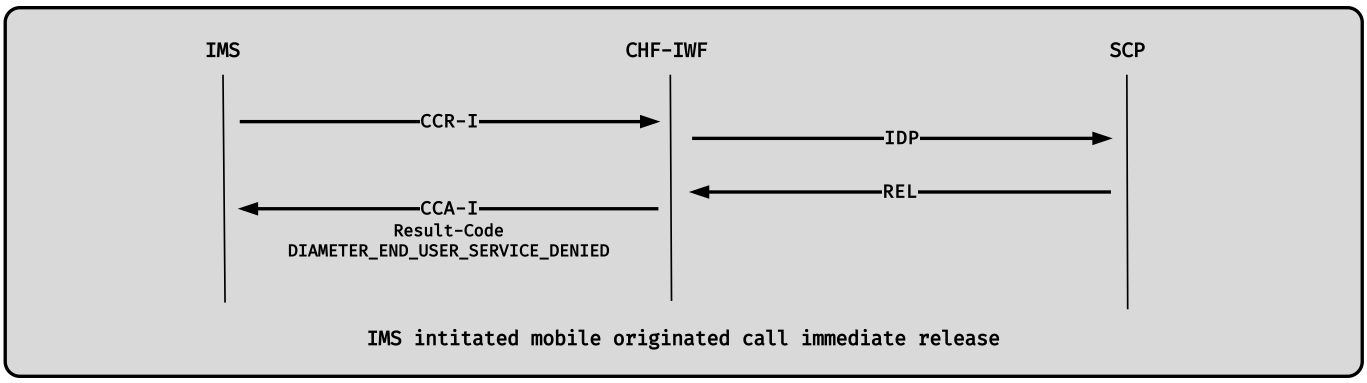


IMS intitated mobile originated call redirection

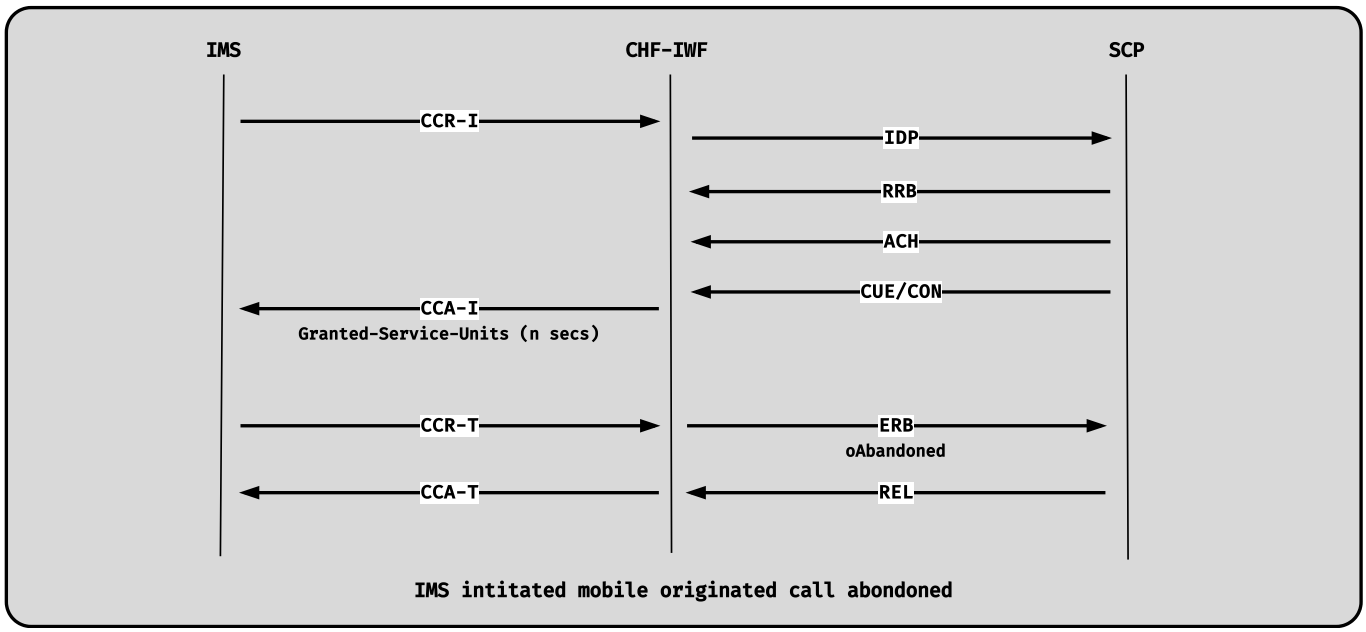
8.5 Mobile originated call - mid session failure



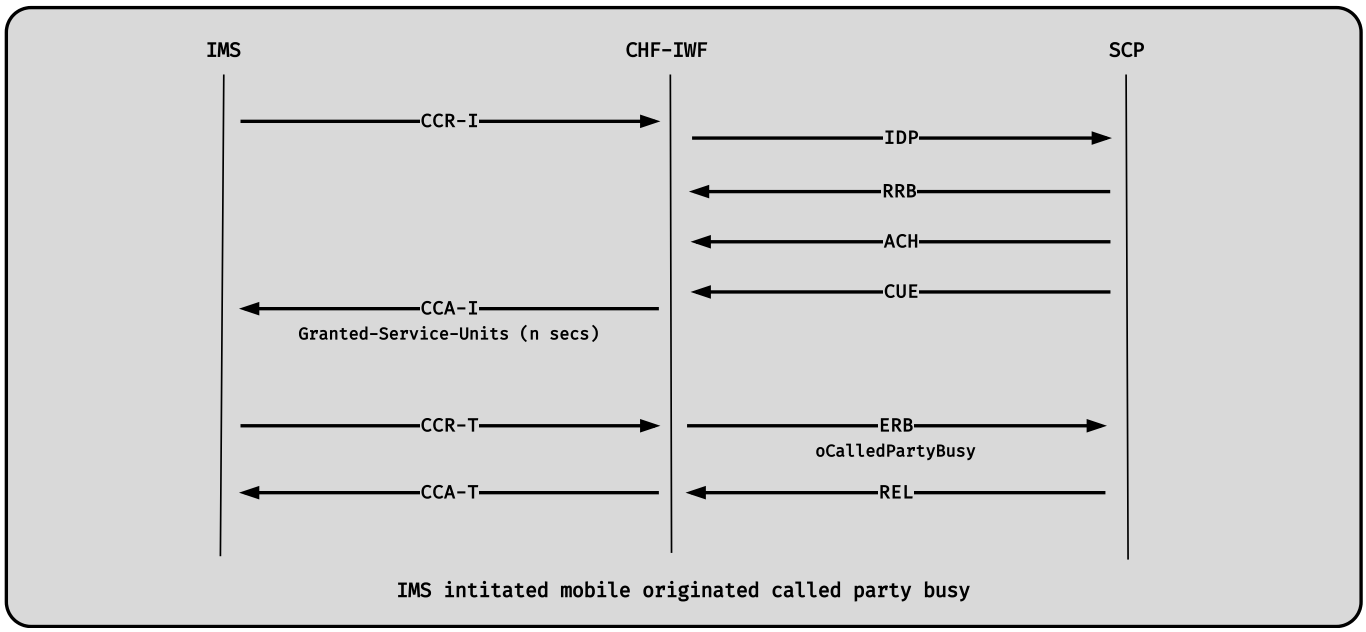
8.6 Mobile originated call - invalid called party number



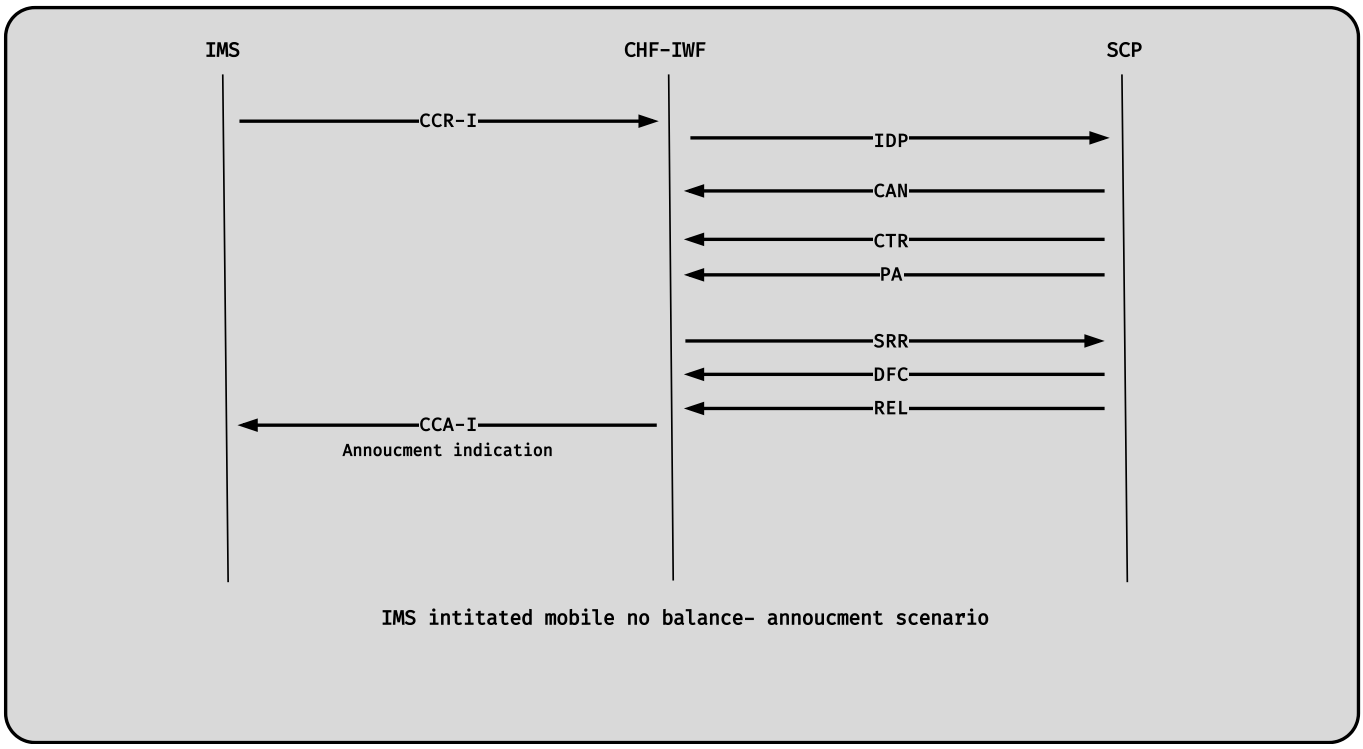
8.7 Mobile originated call - abandonned call



8.8 Mobile originated call - destination busy

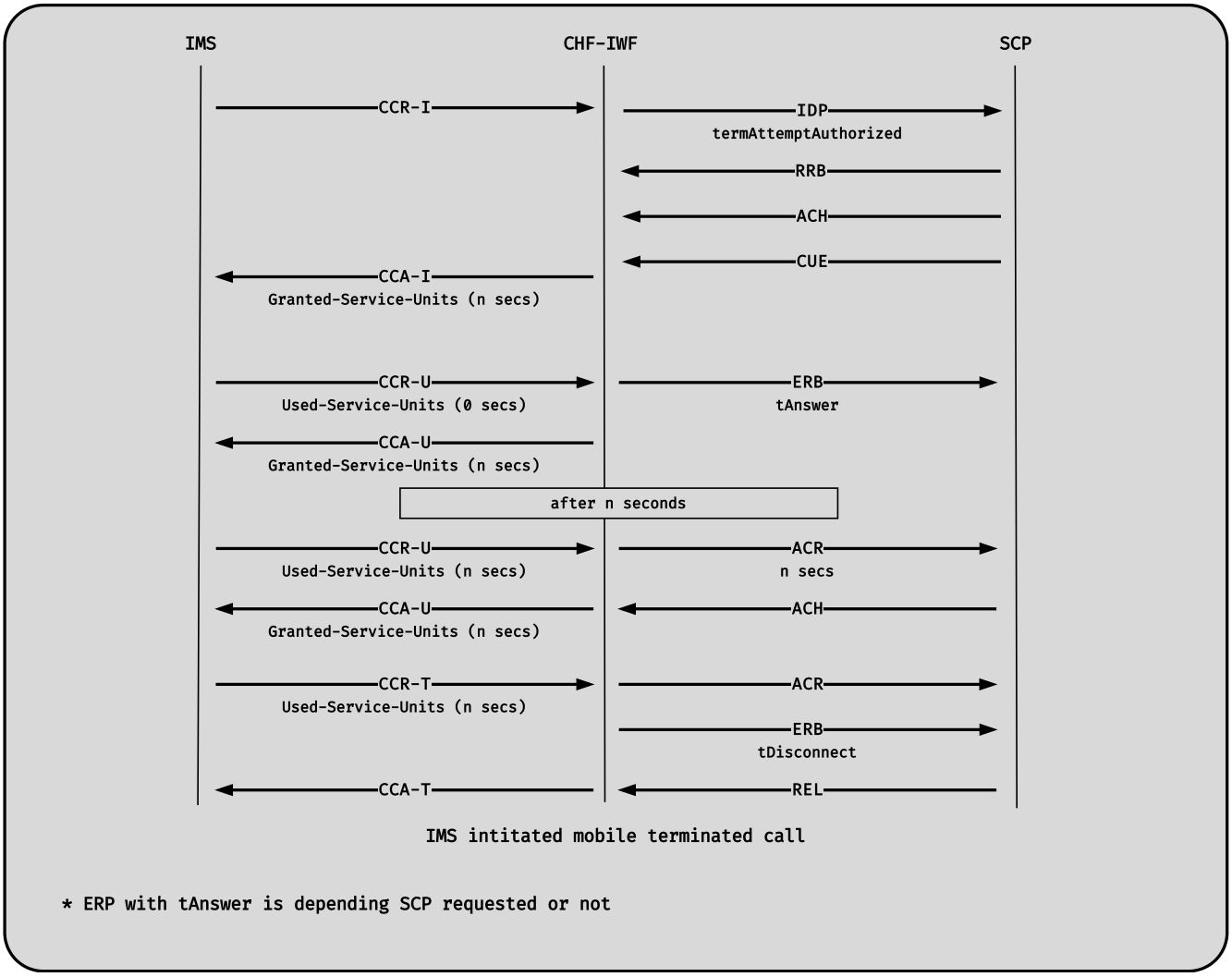


8.9 No balance - with annoucment



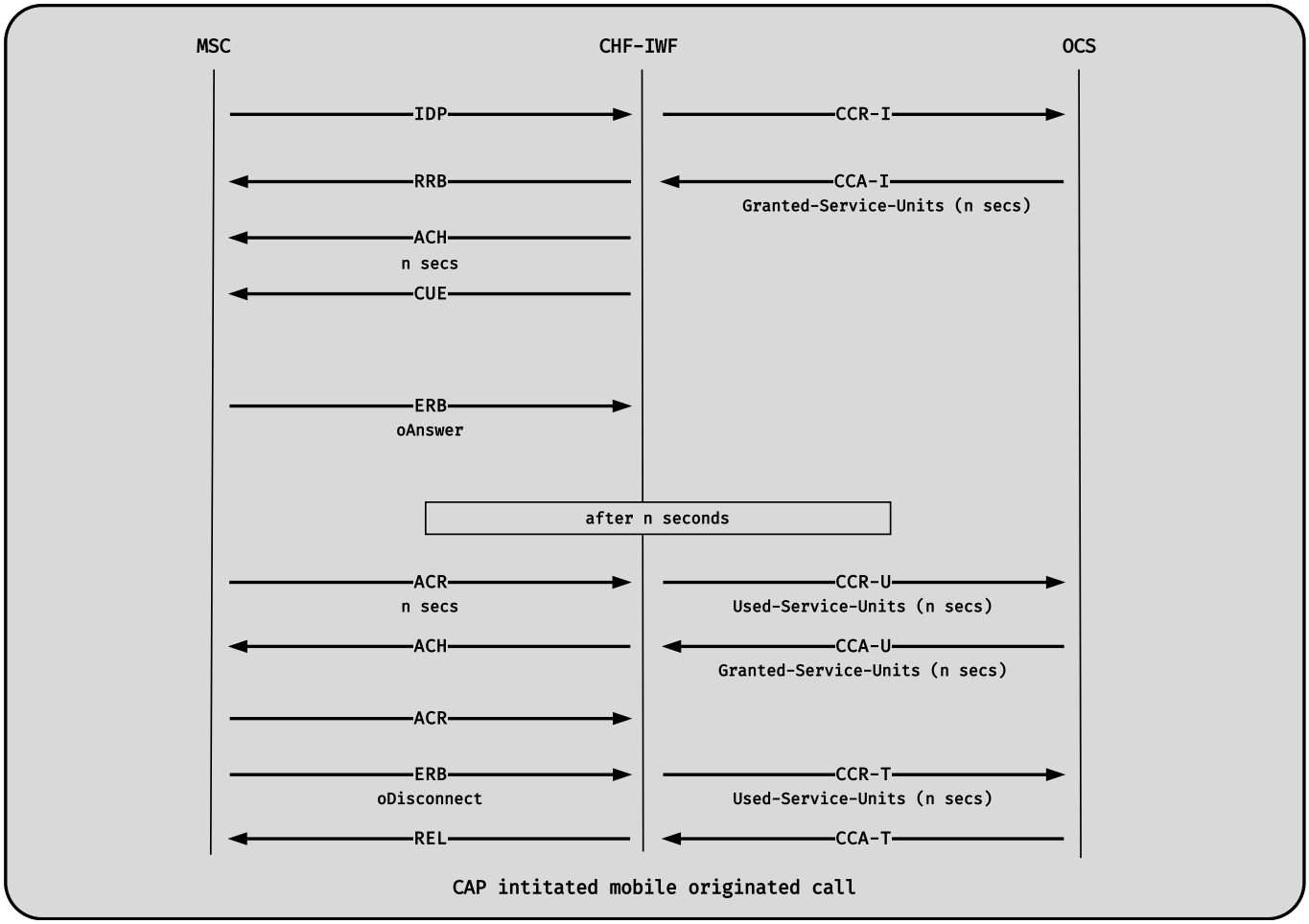
IMS intitated mobile no balance- annoucment scenario

8.10 Mobile terminated call

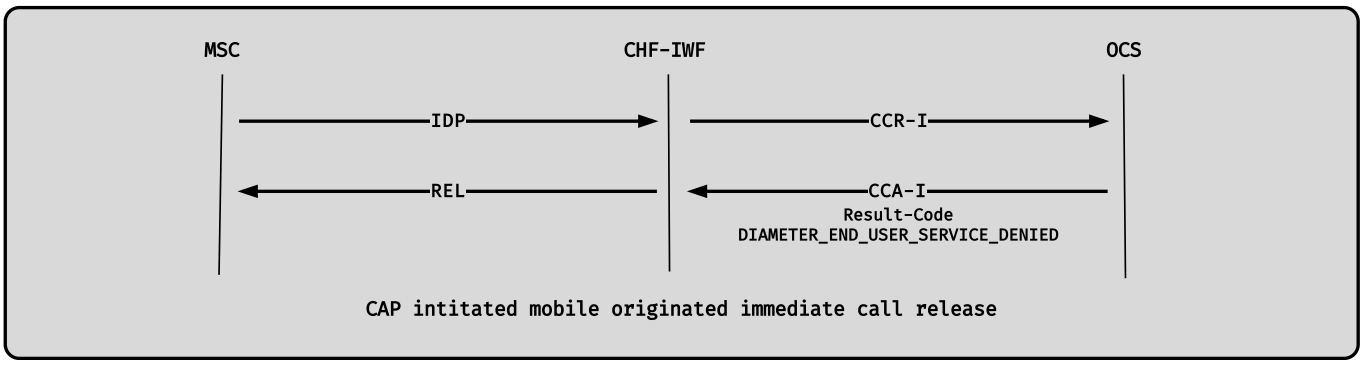


9. CAP Initiated call flows

9.1 Mobile originated call

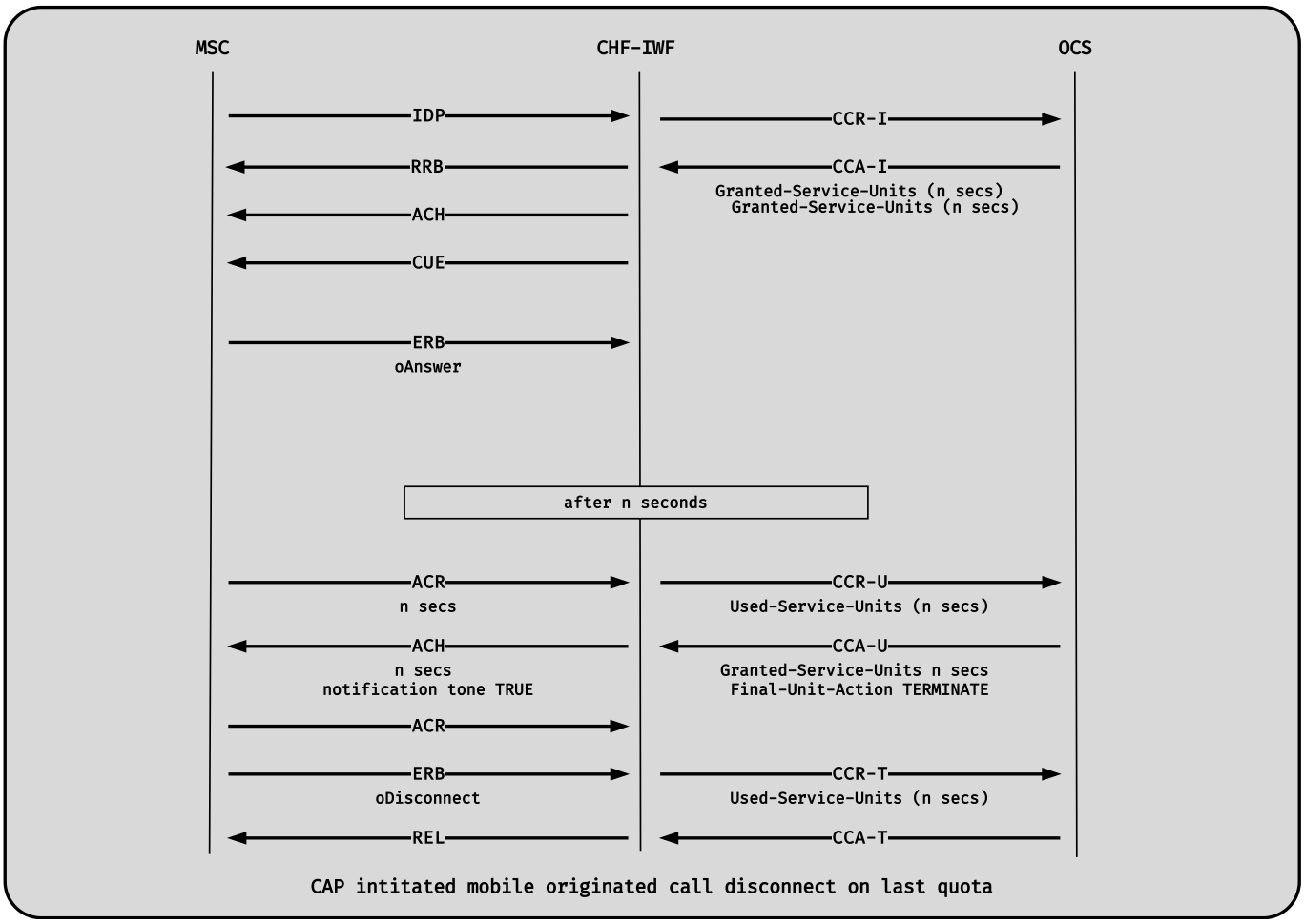


9.2 Mobile originated call immediate release



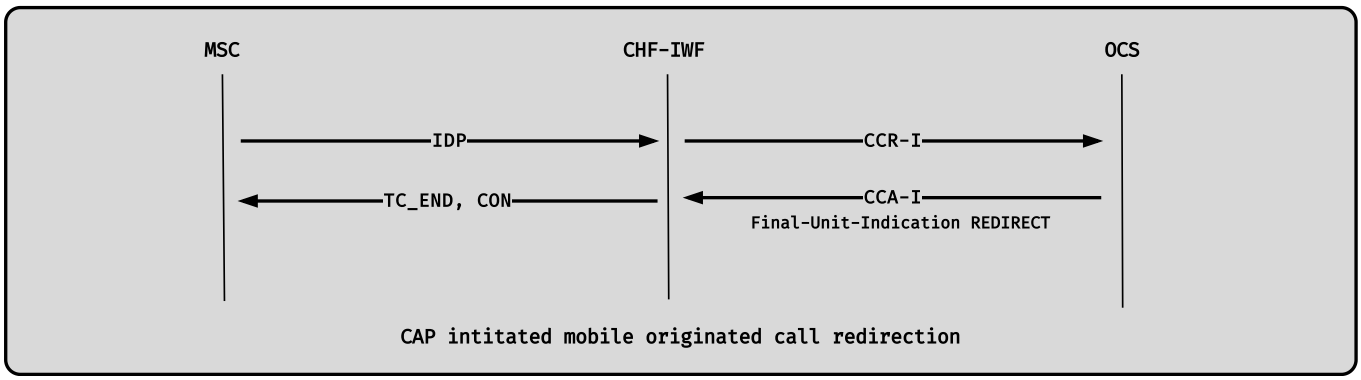
CAP intitated mobile originated immediate call release

9.3 Mobile originated call disconnect on last quota

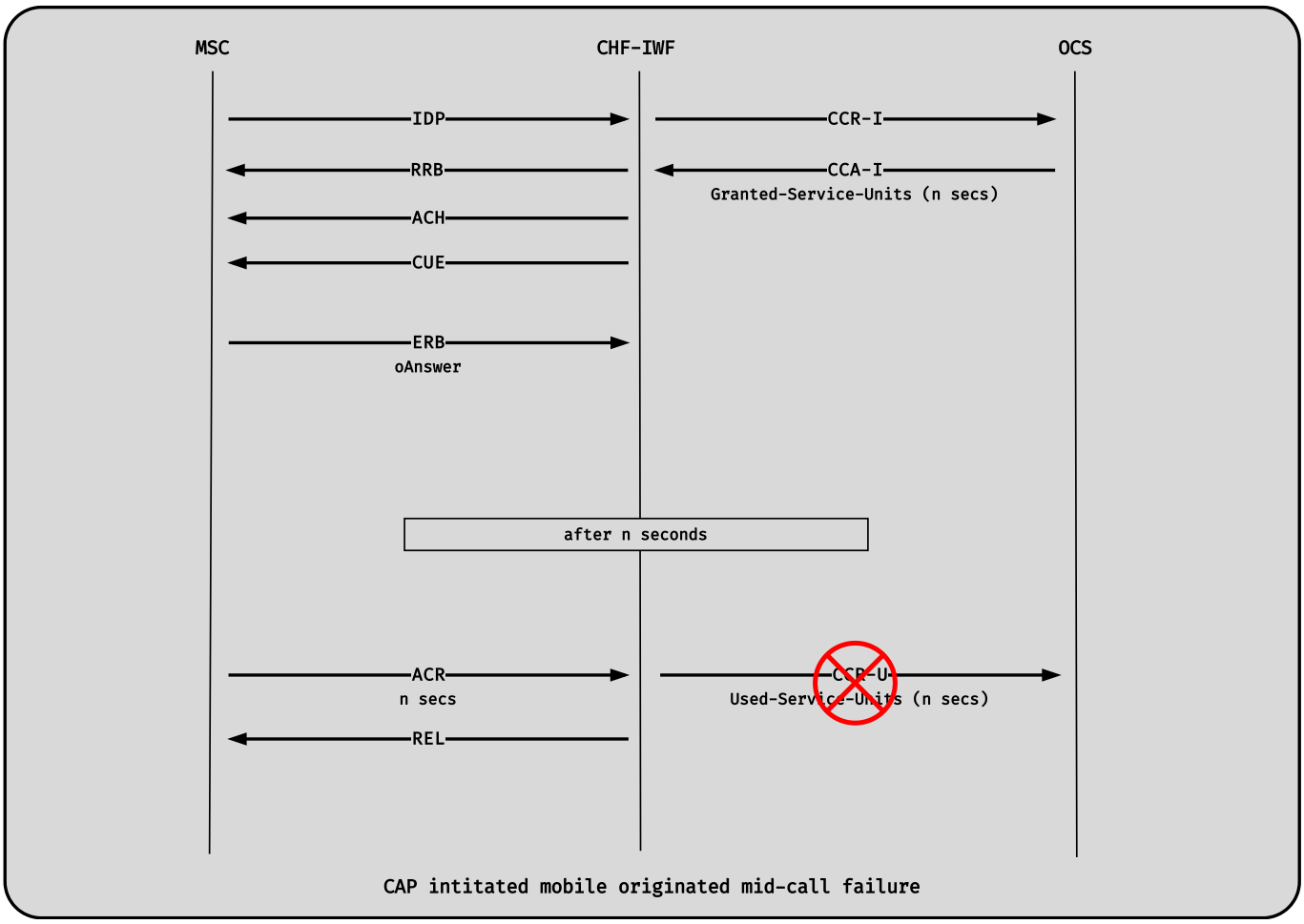


CAP intitated mobile originated call disconnect on last quota

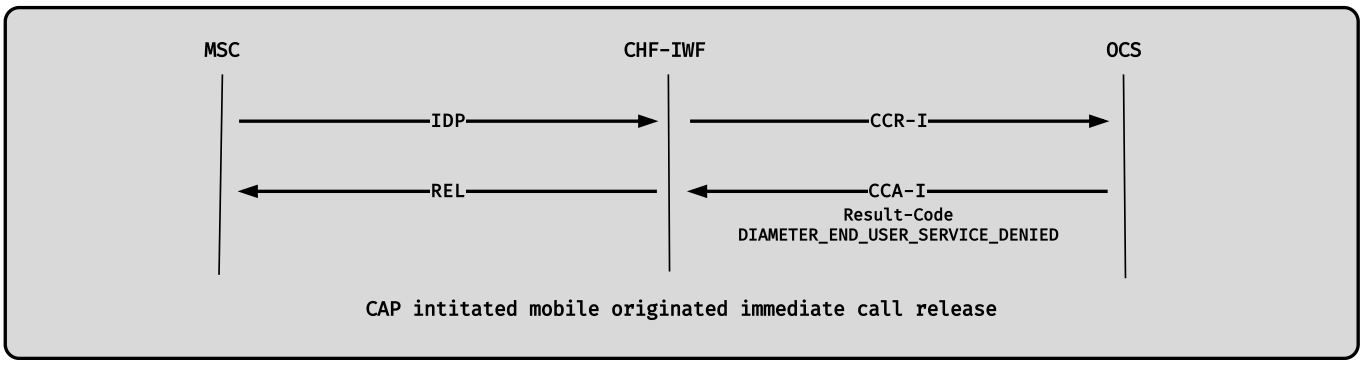
9.4 Mobile originated call redirection



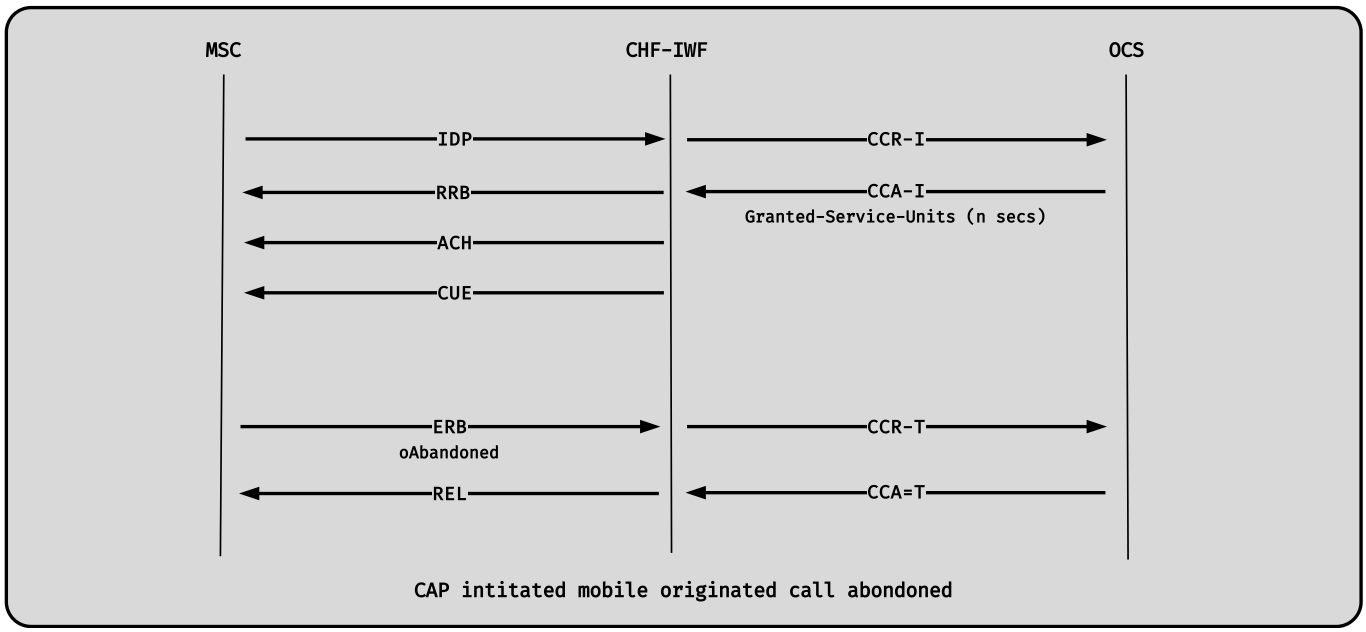
9.5 Mobile originated call - mid session failure



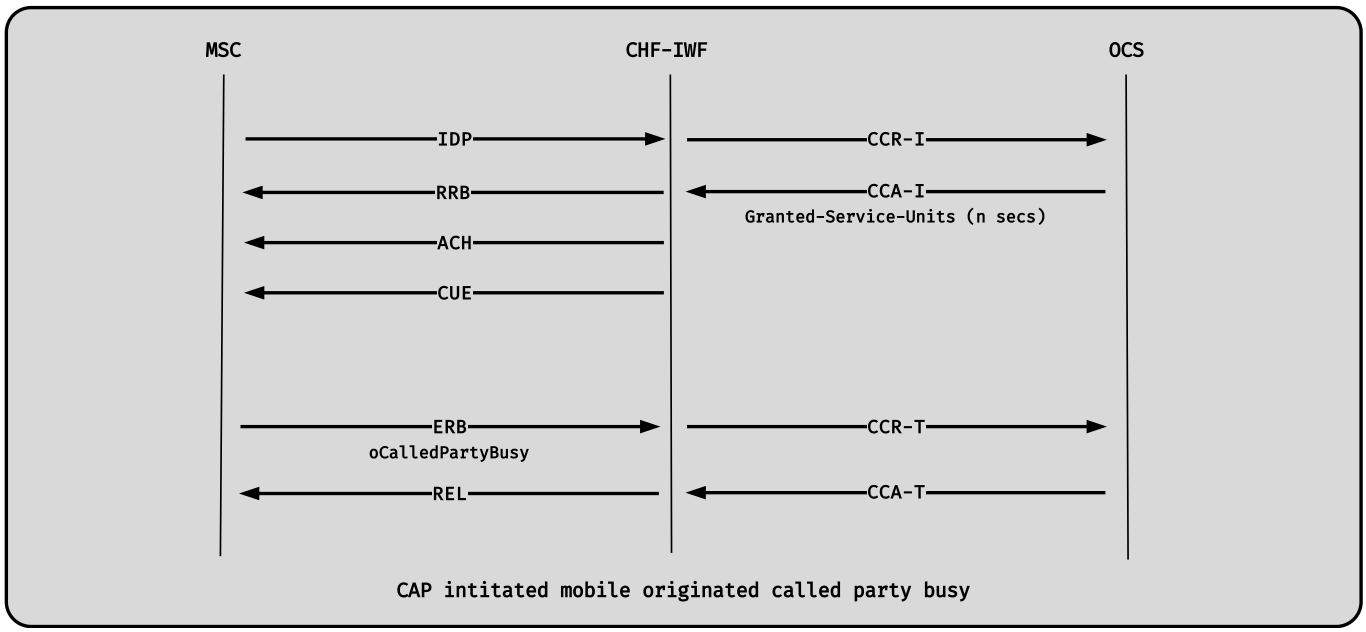
9.6 Mobile originated call - invalid called party number



9.7 Mobile originated call - abandonned call



9.8 Mobile originated call - destination busy



9.9 Mobile terminated call