Fonctionnalités Avancées de Contrôle des Appels

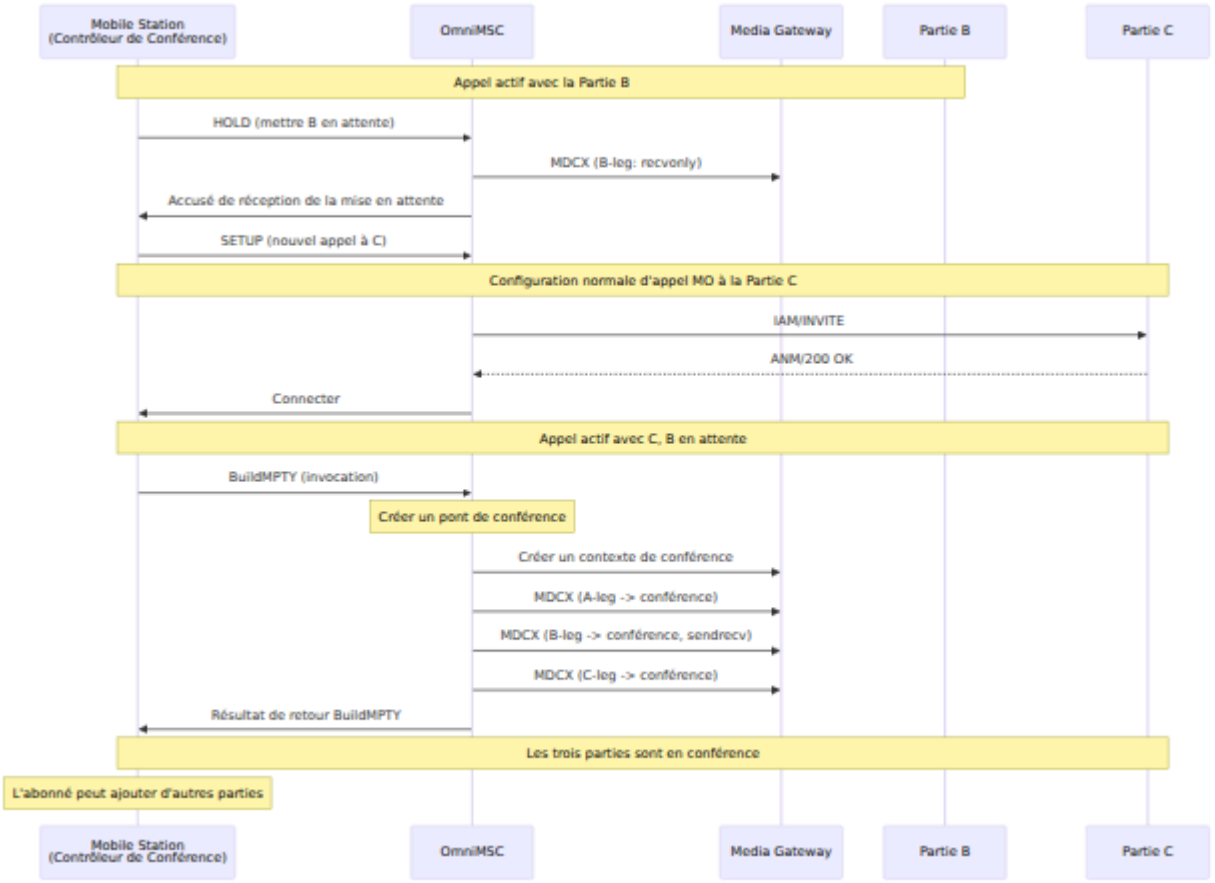
Ce document décrit les fonctionnalités avancées de contrôle des appels commutés par circuit mises en œuvre dans OmniMSC, y compris les appels multipartites, le transfert d'appel, la complétion d'appel, la déviation d'appel, le multicall, les services prioritaires et la facturation.

Pour les services supplémentaires de base (renvoi d'appel, interdiction, CLIP/CLIR, USSD), voir Services Supplémentaires. Pour les diagrammes de flux d'appel, voir Diagrammes de Flux d'Appel. Pour les paramètres de configuration, voir Référence de Configuration. Pour les opérations générales, voir Guide des Opérations.

MPTY (Appels Multipartites / Conférence)

MPTY permet à un abonné d'établir un appel de conférence avec plusieurs parties distantes selon la norme 3GPP TS 24.084. L'abonné agit en tant que contrôleur de conférence, reliant les appels en attente et actifs en une seule conversation multipartite.

Séquence MPTY



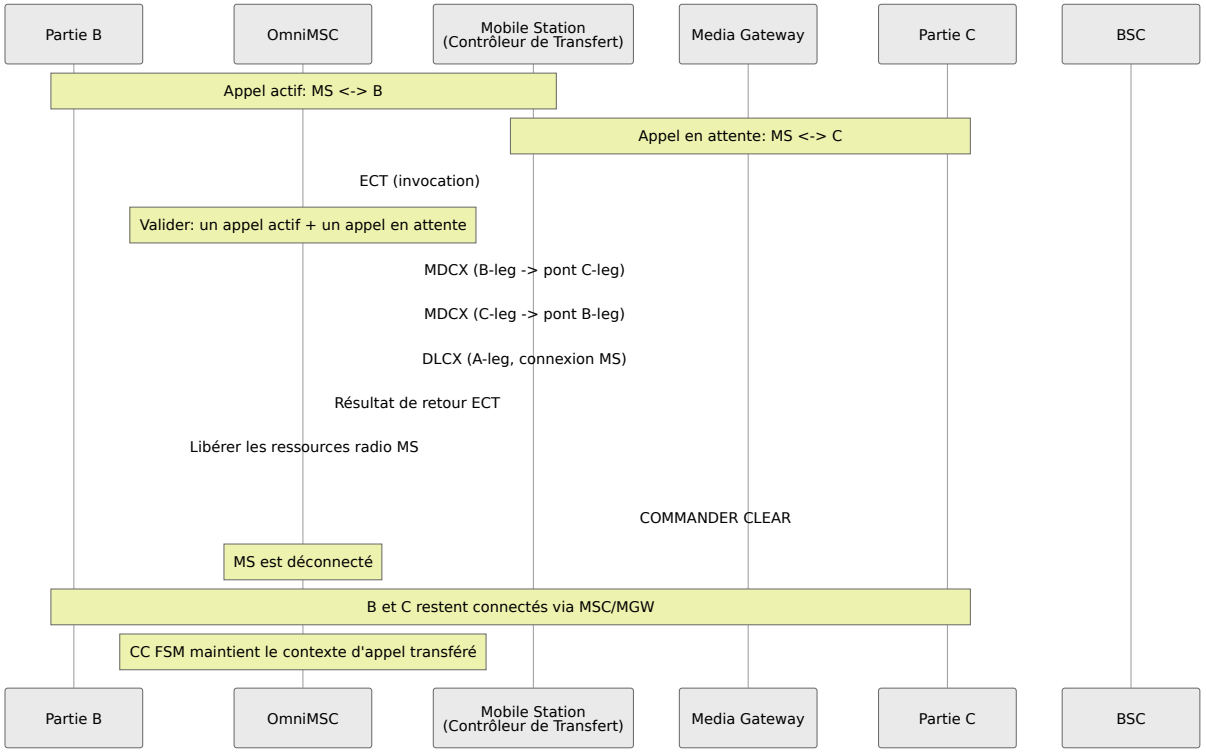
Configuration MPTY

MPTY n'a pas de configuration statique ; il n'impose aucune limite de parties dans le code, et tous les paramètres sont dérivés par appel des opérations de service supplémentaire MPTY.

ECT (Transfert d'Appel Explicite)

ECT permet à un abonné de connecter deux appels ensemble puis de se retirer de la connexion selon la norme 3GPP TS 24.091. L'abonné doit avoir un appel actif et un appel en attente. Après ECT, les deux parties distantes sont connectées directement via le MSC.

Séquence ECT



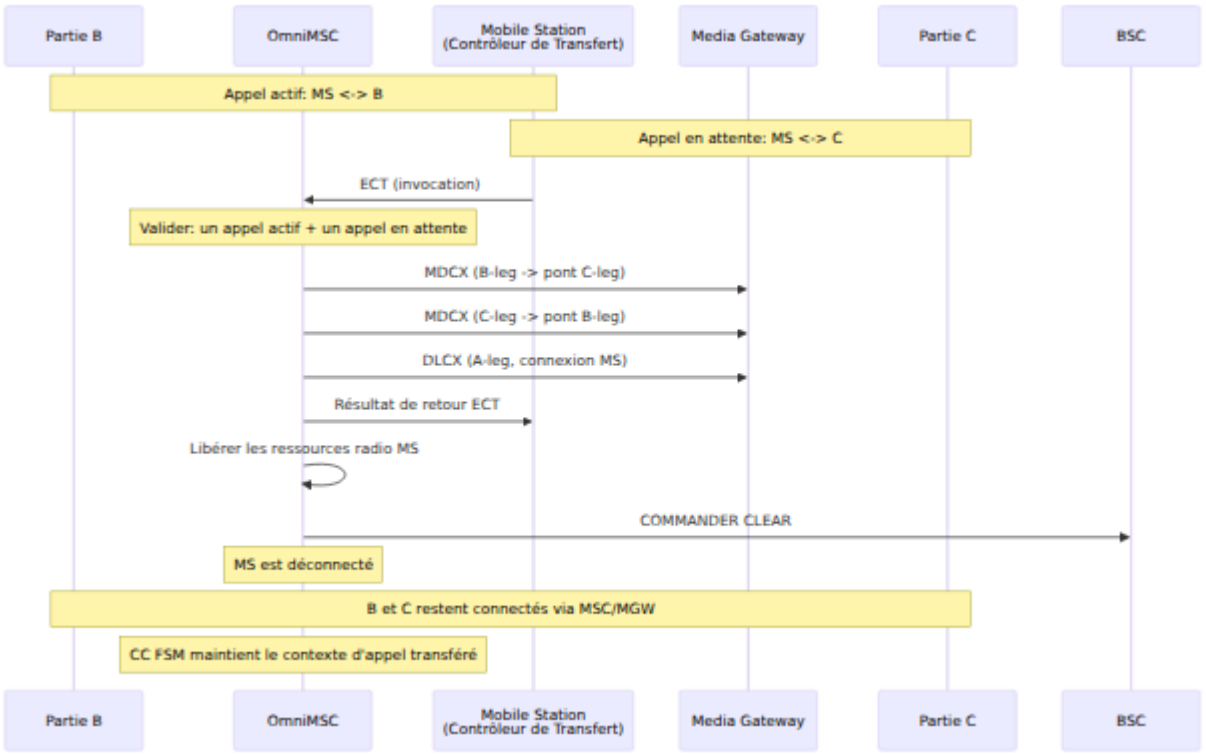
Configuration ECT

ECT n'a pas de configuration statique ; son comportement est déterminé par appel par l'invocation du service supplémentaire ECT.

CCBS (Complétion d'Appel vers Abonné Occupé)

CCBS permet à un appelant de demander un rappel automatique lorsque l'abonné appelé occupé devient libre, selon les normes 3GPP TS 24.093 et 3GPP TS 23.135. Le MSC surveille l'état de l'abonné appelé et initie un rappel lorsqu'il devient inactif.

Flux CCBS



Configuration CCBS

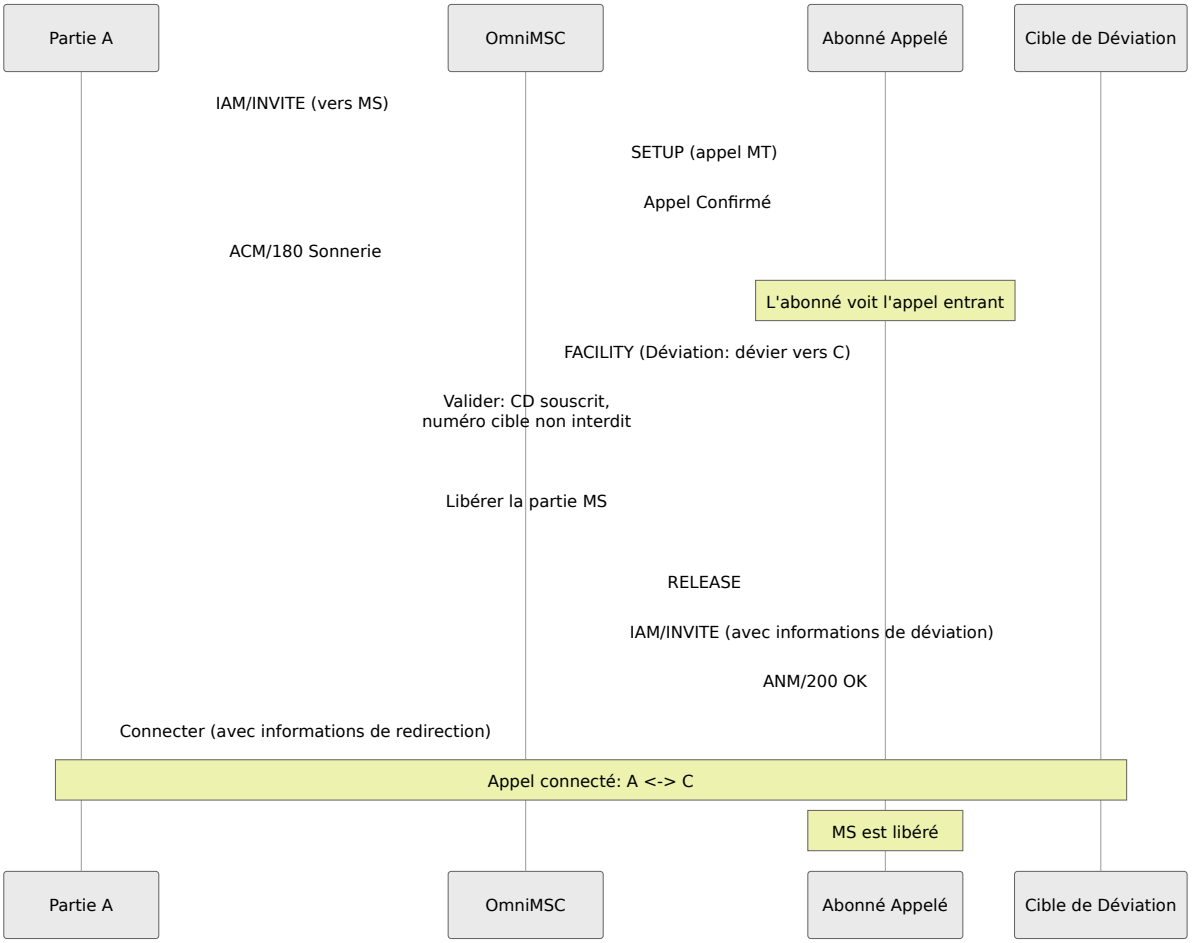
CCBS est configuré sous `config :omnimsc, :ccbs` :

Paramètre	Type	Par défaut	Description
`:max_queue_size`	`integer`	`5`	Nombre maximum de demandes CCBS en attente par abonné. Les demandes supplémentaires sont rejetées. Selon la norme 3GPP TS 23.135 Sec 4.2.
`:request_lifetime_ms`	`integer`	`180_000`	Durée de vie en millisecondes d'une demande CCBS mise en file d'attente. Si l'abonné appelé ne devient pas libre dans ce délai, la demande expire.
`:recall_timeout_ms`	`integer`	`30_000`	Temps en millisecondes à attendre pour que l'abonné d'origine réponde au rappel CCBS.

Déviation d'Appel

La Déviation d'Appel (CD) permet à un abonné appelé de rediriger un appel entrant vers un autre numéro avant de répondre, selon la norme 3GPP TS 24.072. Contrairement au renvoi d'appel, la CD est une action à la demande initiée par l'abonné pendant la phase d'alerte.

Séquence de Déviation d'Appel



Configuration de Déviation d'Appel

La Déviation d'Appel n'a pas de configuration statique ; elle est invoquée par appel via le service supplémentaire CD pendant la phase d'alerte.

Configuration Multicall

Le Multicall permet à un abonné de maintenir plusieurs appels CS simultanés selon la norme 3GPP TS 23.135. Cela est distinct de MPTY (conférence) : dans le multicall, chaque appel a un audio indépendant. L'abonné passe d'un appel à l'autre en utilisant le mécanisme HOLD/RETRIEVE.

Le multicall n'a pas de configuration au niveau de l'application. La limite par abonné est une valeur HLR/abonnement, `:max_calls`, fournie avec le profil de

l'abonné :

Paramètre	Type	Par défaut	Description
`:max_calls`	`integer`	`2`	Nombre maximum d'appels CS simultanés pour l'abonné, selon l'abonnement HLR. Un appel est actif, les autres sont en attente. La valeur est plafonnée à un maximum absolu de 7.

---

eMLPP (Précedence et Préemption Multi-Niveaux Améliorés)

eMLPP fournit un traitement prioritaire des appels selon la norme 3GPP TS 24.067. Les appels se voient attribuer un niveau de priorité, et les appels de priorité supérieure peuvent préempter les appels de priorité inférieure lorsque les ressources sont rares.

Niveaux de Priorité

Sept niveaux de priorité sont définis (valeur numérique, plus bas = priorité plus élevée) :

Valeur	Nom	Description
0	`flash_override`	Priorité la plus élevée (Flash Override). Réservé aux autorités nationales d'urgence.
1	`flash`	Flash. Réservé aux hauts fonctionnaires gouvernementaux/militaires.
2	`immediate`	Immédiat. Haute priorité gouvernementale/militaire.
3	`priority`	Priorité. Trafic de priorité générale.
4	`routine`	Routinière. Appels standards d'abonnés (par défaut).
5	`spare_3`	Niveau de réserve 3.
6	`spare_4`	Niveau de réserve 4.

Configuration eMLPP

eMLPP n'a pas de configuration statique ; le niveau de priorité (et toute préemption) est appliqué par appel à partir de l'abonnement eMLPP de l'abonné et de la priorité demandée de l'appel.

AoCC (Avis de Charge - Facturation)

AoCC fournit des informations de charge en temps réel à l'abonné pendant un appel selon la norme 3GPP TS 24.086. Le MSC envoie des informations sur le taux de charge et des indications de charge accumulée à la station mobile.

Configuration AoCC

AoCC n'a pas de configuration statique ; la devise et le montant de la charge sont fournis par appel en tant que paramètres à la session AoCC.

Références de Spécification 3GPP

Spécification	Titre	Fonctionnalité
TS 24.084	Service Supplémentaire Multi-Party (MPTY)	MPTY / Appels de conférence
TS 24.091	Service Supplémentaire de Transfert d'Appel Explicite (ECT)	ECT
TS 24.093	Complétion d'Appel vers Abonné Occupé (CCBS)	CCBS
TS 23.135	Multicall	Multicall, procédures réseau CCBS
TS 24.072	Service Supplémentaire de Déviation d'Appel	Déviation d'Appel
TS 24.067	Précedence et Préemption Multi-Niveaux Améliorés (eMLPP)	Niveaux de priorité eMLPP
TS 24.086	Services Supplémentaires d'Avis de Charge (AoC)	Facturation AoCC
TS 24.083	Appel en Attente et Mise en Attente	Hold/Retrieve pour multicall

API REST

Ce document décrit l'API REST d'OmniMSC, qui fournit un accès programmatique aux données des abonnés, aux appels actifs, à la configuration de routage, aux pairs SIP, aux passerelles multimédias, aux connexions RAN et à l'état du système. L'API écoute sur le port 8444 et sert une spécification OpenAPI 3 (OAS3) auto-générée.

Pour le panneau de contrôle basé sur le web, voir Panneau de Contrôle. Pour les concepts de routage référencés par les points de terminaison de routage, voir Configuration de Routage.

Documentation OpenAPI

OmniMSC génère automatiquement une spécification OpenAPI 3 à partir du routeur API. L'interface interactive Swagger UI est disponible à `http://<host>:8444/api/docs` et fournit une interface navigable et testable pour tous les points de terminaison. La spécification OAS3 brute est servie à `http://<host>:8444/api/schema`.

Points de Terminaison

Tous les points de terminaison sont servis sous le préfixe de chemin `/api`. Les corps de requête et de réponse utilisent l'encodage JSON.

Abonnés

Méthode	Chemin	Description
GET	/api/subscribers	Lister les abonnés VLR. Prend en charge un paramètre de requête `search` optionnel qui filtre par IMSI ou MSISDN (correspondance partielle).
GET	/api/subscribers/{id}	Récupérer les détails complets d'un seul abonné, y compris l'identité, la localisation, l'état d'authentification, le profil de service et les services supplémentaires.
DELETE	/api/subscribers/{id}	Purger un enregistrement d'abonné du VLR local (supprime uniquement l'enregistrement VLR ; aucun MAP PurgeMS n'est envoyé au HLR).
POST	/api/subscribers/{id}/actions	Exécuter une action sur un abonné, comme initier un détachement, forcer une ré-authentification ou déclencher une mise à jour de localisation.
POST	/api/subscribers/{id}/ss	Gérer les services supplémentaires pour un abonné, y compris l'activation, la désactivation et l'interrogation du barring d'appels, du renvoi d'appels et d'autres services.

Appels

Méthode	Chemin	Description
GET	/api/calls	Lister toutes les transactions d'appels CC FSM actifs, y compris la référence d'appel, la direction, les parties, l'état et la durée.
GET	/api/calls/{id}	Récupérer les détails complets d'un seul appel, y compris le timing, le codec, le BSC/RNC de service et l'historique d'état CC FSM.
DELETE	/api/calls/{id}	Libérer un appel actif. Initie la déconnexion côté réseau et la commande BSSMAP CLEAR.

SMS

Méthode	Chemin	Description
GET	/api/sms	Lister les transactions SMS actives avec ID de transaction, direction, abonné, état et adresse du Centre SMS.

Routes

Méthode	Chemin	Description
GET	/api/routes	Lister toutes les entrées dans la table de routage, y compris le préfixe, le type de destination, la priorité et les paramètres spécifiques à la destination.
POST	/api/routes	Ajouter une nouvelle route à la table de routage. La route prend effet immédiatement sans redémarrage.
DELETE	/api/routes/{prefix}	Supprimer une route de la table de routage par préfixe.
GET	/api/routes/lookup	Rechercher la route qui serait sélectionnée pour un numéro de partie appelée donné. Utile pour vérifier le comportement de routage sans passer d'appel.

Pairs SIP

Méthode	Chemin	Description
GET	/api/sip/peers	Lister tous les pairs SIP configurés avec adresse, transport, état, appels actifs et capacité.
GET	/api/sip/peers/{name}	Récupérer les détails complets d'un seul pair SIP, y compris la liste des codecs, l'état de maintien d'OPTIONS et les statistiques d'appel.
PUT	/api/sip/peers/{name}	Déclencher un ping OPTIONS keepalive immédiat vers le pair. Cela ne modifie pas la configuration du pair.

Passerelles Multimédias

Méthode	Chemin	Description
GET	/api/mgw	Lister les passerelles multimédias configurées avec nom, adresse, protocole (MGCP ou Megaco) et état de connectivité.

RAN et STP

Méthode	Chemin	Description
GET	/api/ran/connections	Lister les connexions RAN actives (sessions orientées connexion SCCP) avec ID de connexion, IMSI de l'abonné, BSC/RNC et état.
GET	/api/ran/bscs	Lister les BSC connus avec code de point, titre global, nombre de cellules et dernier horodatage BSSMAP RESET.
GET	/api/stp	Obtenir l'état des liens STP, y compris l'état ASP M3UA, les détails de l'association SCTP et les compteurs de trafic.

Paging

Méthode	Chemin	Description
POST	/api/paging	Initier une demande de paging pour un abonné par IMSI ou MSISDN. Envoie BSSMAP PAGING aux BSC appropriés.
GET	/api/paging	Lister les demandes de paging en attente avec identité de l'abonné, LAC cible, cause de paging et temps écoulé.

Avis de Charge

Méthode	Chemin	Description
POST	/api/aoc	Envoyer un message d'Avis de Charge à un abonné pendant un appel actif. Prend en charge AoCI (information) et AoCE (facturation) selon 3GPP TS 24.086.

Appel Silencieux et SMS

Méthode	Chemin	Description
POST	/api/silent	Initier un appel silencieux ou un SMS silencieux vers un abonné. Utilisé à des fins d'interception légale et de tests réseau.

Cellules de Transfert

Méthode	Chemin	Description
GET	/api/handover/cells	Lister les cellules configurées comme cibles de transfert, y compris l'identité de la cellule, LAC, BSC et priorité de transfert.
POST	/api/handover/cells	Ajouter une cellule à la liste des cibles de transfert avec identité de cellule, LAC et paramètres de priorité.

Système

Méthode	Chemin	Description
GET	/api/health	Point de terminaison de vérification de santé. Retourne un simple indicateur d'état adapté aux sondes de l'équilibreur de charge.
GET	/api/status	État du système incluant les statistiques de la VM BEAM, l'allocation de mémoire, l'état du superviseur, le nombre d'alarmes actives et un résumé de la configuration MSC.
GET	/metrics	Point de terminaison de collecte de métriques Prometheus. Retourne tous les compteurs et jauges de télémétrie OmniMSC au format d'exposition Prometheus. **Remarque :** `/metrics` est servi par le point de terminaison Phoenix du Panneau de Contrôle sur le port **4000**, pas par l'API REST sur le port 8444. Voir Métriques et Surveillance.

Format de Réponse

Tous les points de terminaison retournent des réponses JSON. Les requêtes réussies retournent les données demandées dans un objet ou un tableau de niveau supérieur. Les réponses d'erreur incluent un objet JSON avec un champ `error` contenant un message lisible par l'homme.

Les réponses de détails d'abonnés et d'appels incluent des objets imbriqués pour les données connexes (identité, localisation, authentification, timing) correspondant à la structure décrite dans les sections détails de l'abonné du Panneau de Contrôle et détails de l'appel.

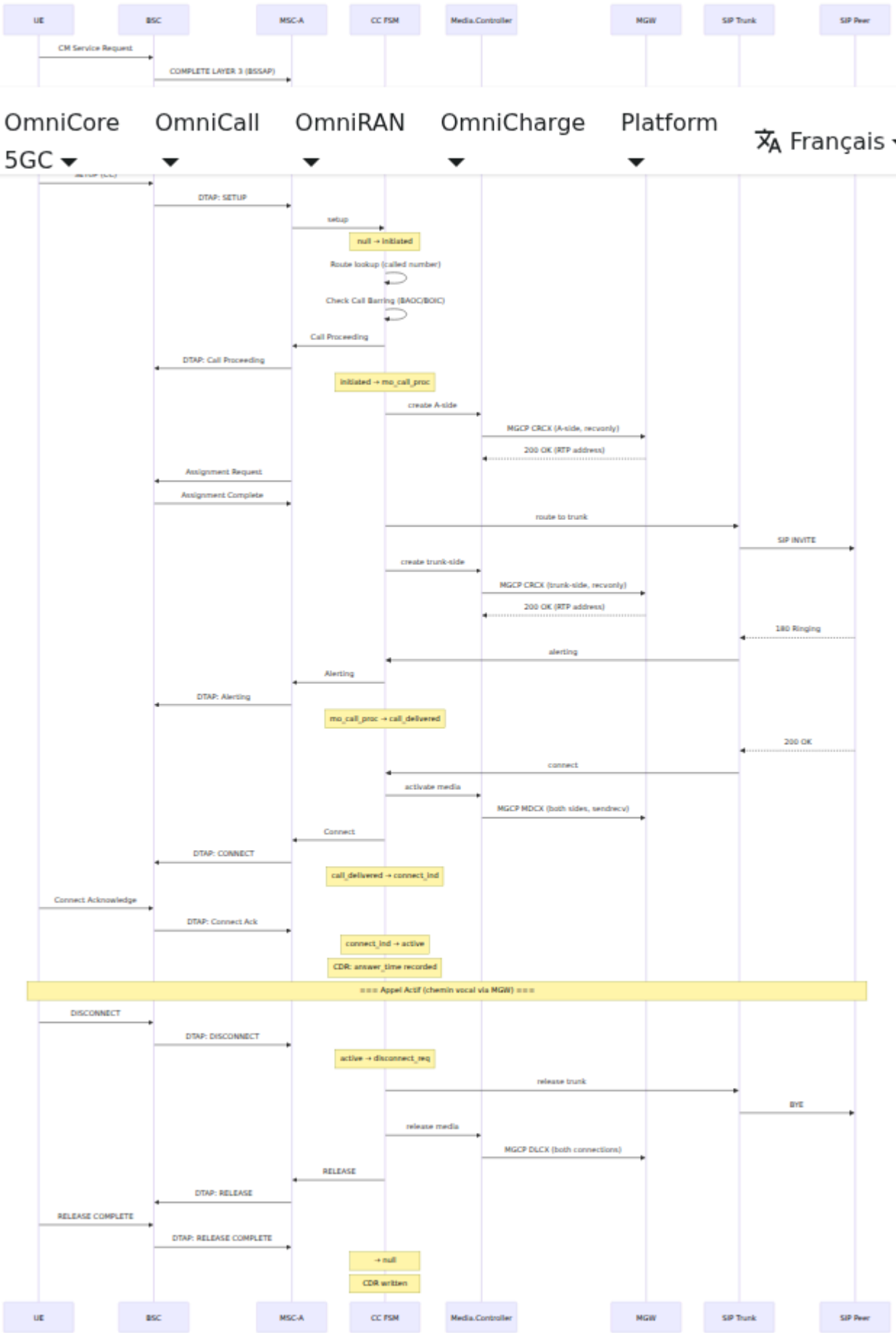
Diagrammes de Flux d'Appel

Ce document contient des diagrammes de séquence pour tous les principaux scénarios d'appel gérés par OmniMSC. Chaque diagramme montre le flux de signalisation entre les éléments du réseau.

Pour les définitions d'état de la FSM CC, voir Diagramme d'État de la FSM CC ci-dessous. Pour la configuration de routage, voir Configuration de Routage. Pour les détails de signalisation de la liaison SIP, voir Liaison SIP. Pour la signalisation de la liaison ISUP, voir Liaison ISUP. Pour le contrôle de la passerelle multimédia lors de l'établissement de l'appel, voir Contrôle Multimédia. Pour les flux de services supplémentaires (mise en attente, MPTY, ECT), voir Services Supplémentaires.

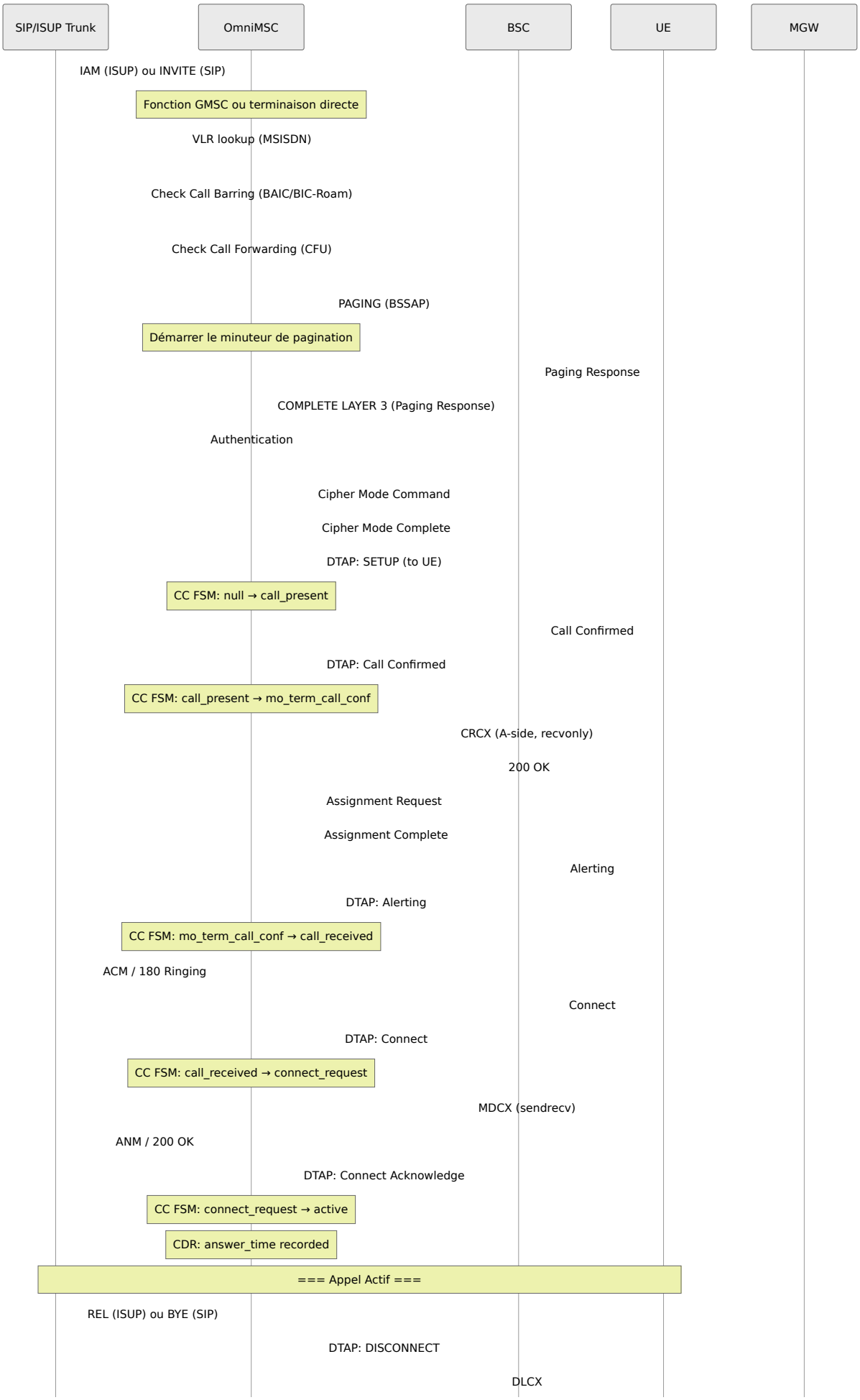
Appel Mobile Émis (MO)

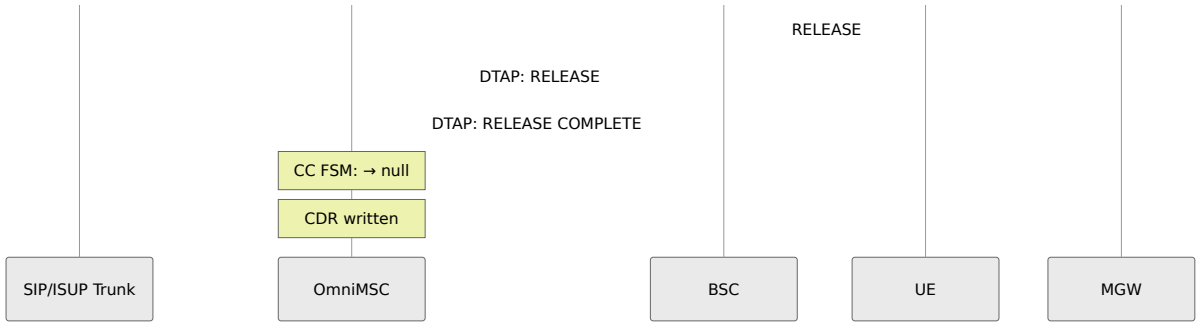
Un abonné initie un appel sortant. Le MSC gère l'établissement de l'appel, l'authentification (si nécessaire), le mode de chiffrement, l'attribution et l'allocation de la liaison.


UE
BSC
MSC-A
CC FSM
Media.Controller
MGW
SIP Trunk
SIP Peer
CM Service Request
COMPLETE LAYER 3 (BSSAP)
DTAP: SETUP
setup
null → initiated
Route lookup (called number)
Check Call Barring (BAOC/BOIC)
Call Proceeding
DTAP: Call Proceeding
initiated → mo_call_proc
create A-side
MGCP CRCX (A-side, recvonly)
200 OK (RTP address)
Assignment Request
Assignment Complete
route to trunk
SIP INVITE
create trunk-side
MGCP CRCX (trunk-side, recvonly)
200 OK (RTP address)
180 Ringing
alerting
Alerting
DTAP: Alerting
mo_call_proc → call_delivered
200 OK
connect
activate media
MGCP MDCX (both sides, sendrecv)
Connect
DTAP: CONNECT
call_delivered → connect_ind
Connect Acknowledge
DTAP: Connect Ack
connect_ind → active
CDR: answer_time recorded
=== Appel Actif (chemin vocal via MGW) ===
DISCONNECT
DTAP: DISCONNECT
active → disconnect_req
release trunk
BYE
release media
MGCP DLCX (both connections)
RELEASE
DTAP: RELEASE
RELEASE COMPLETE
DTAP: RELEASE COMPLETE
→ null
CDR written

Appel Mobile Reçu (MT)

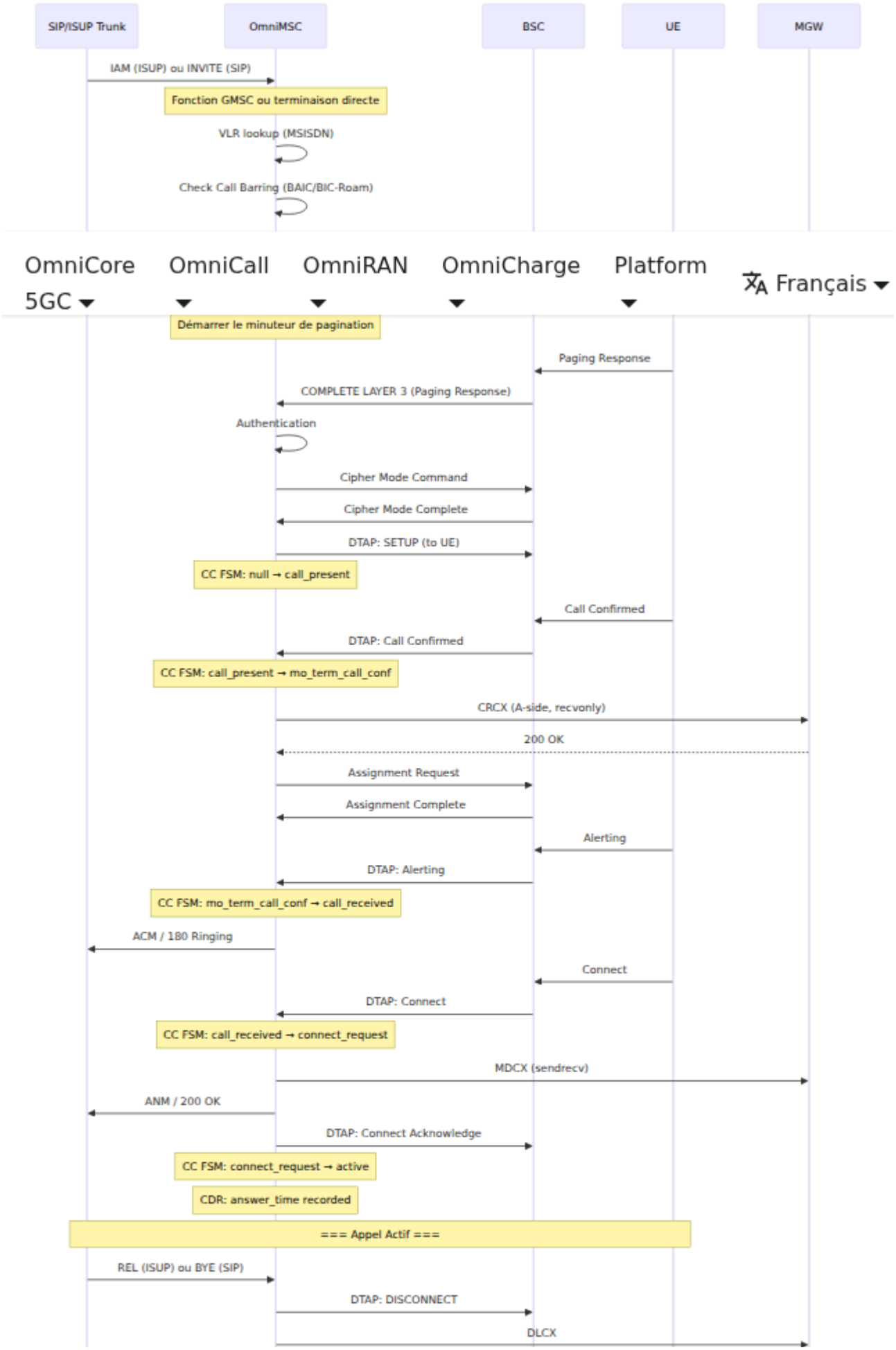
Un appel entrant arrive du PSTN ou d'un pair SIP. Le MSC page l'abonné, établit le chemin radio et connecte l'appel. La signalisation côté liaison peut être SIP ou ISUP selon la route.

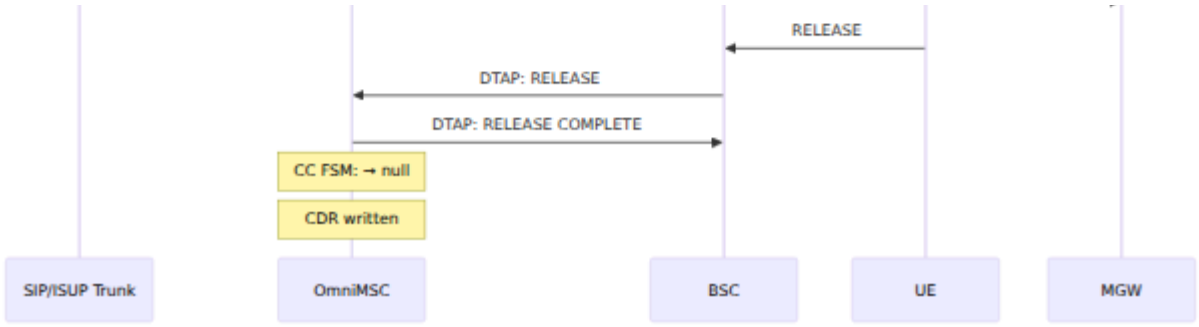

SIP/ISUP Trunk
OmniMSC
BSC
UE
MGW
IAM (ISUP) ou INVITE (SIP)
Fonction GMSC ou terminaison directe
VLR lookup (MSISDN)
Check Call Barring (BAIC/BIC-Roam)
Check Call Forwarding (CFU)
PAGING (BSSAP)
Démarrer le minuteur de pagination
Paging Response
COMPLETE LAYER 3 (Paging Response)
Authentication
Cipher Mode Command
Cipher Mode Complete
DTAP: SETUP (to UE)
CC FSM: null → call_present
Call Confirmed
DTAP: Call Confirmed
CC FSM: call_present → mo_term_call_conf
CRCX (A-side, recvonly)
200 OK
Assignment Request
Assignment Complete
Alerting
DTAP: Alerting
CC FSM: mo_term_call_conf → call_received
ACM / 180 Ringing
Connect
DTAP: Connect
CC FSM: call_received → connect_request
MDCX (sendrecv)
ANM / 200 OK
DTAP: Connect Acknowledge
CC FSM: connect_request → active
CDR: answer_time recorded
=== Appel Actif ===
REL (ISUP) ou BYE (SIP)
DTAP: DISCONNECT
DLCX



Mise en Attente et Récupération d'Appel

La mise en attente et la récupération d'appel permettent à un abonné de suspendre et de reprendre un appel actif selon la norme 3GPP TS 24.083. Pendant qu'un appel est en attente, la passerelle multimédia place la partie maintenue en mode de réception uniquement, réduisant le chemin audio au silence. L'abonné peut établir un second appel pendant que le premier est en attente.


SIP/ISUP Trunk
OmniMSC
BSC
UE
MGW
IAM (ISUP) ou INVITE (SIP)
Fonction GMSC ou terminaison directe
VLR lookup (MSISDN)
Check Call Barring (BAIC/BIC-Roam)
OmniCore 5GC
OmniCall
OmniRAN
OmniCharge
Platform
Français
Démarrer le minuteur de pagination
Paging Response
COMPLETE LAYER 3 (Paging Response)
Authentication
Cipher Mode Command
Cipher Mode Complete
DTAP: SETUP (to UE)
CC FSM: null → call_present
Call Confirmed
DTAP: Call Confirmed
CC FSM: call_present → mo_term_call_conf
CRCX (A-side, recvonly)
200 OK
Assignment Request
Assignment Complete
Alerting
DTAP: Alerting
CC FSM: mo_term_call_conf → call_received
ACM / 180 Ringing
Connect
DTAP: Connect
CC FSM: call_received → connect_request
MDCX (sendrecv)
ANM / 200 OK
DTAP: Connect Acknowledge
CC FSM: connect_request → active
CDR: answer_time recorded
=== Appel Actif ===
REL (ISUP) ou BYE (SIP)
DTAP: DISCONNECT
DLCX



Le message HOLD de l'UE ne contient aucun paramètre. Le MSC répond avec HOLD ACK en cas de succès ou HOLD REJECT si l'opération n'est pas autorisée (par exemple, si l'abonné n'a pas le service de mise en attente provisionné). RETRIEVE suit le même schéma avec RETRIEVE ACK ou RETRIEVE REJECT.

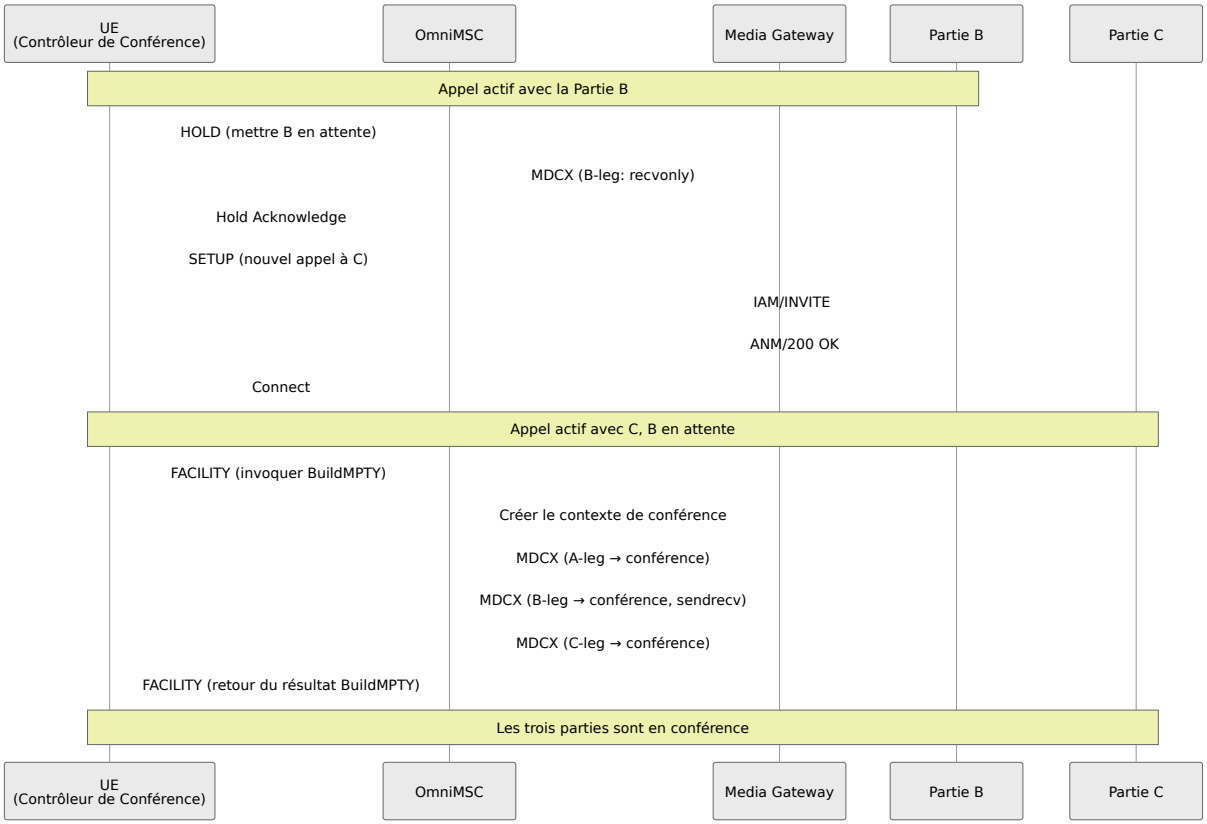
Conférence Multi-Party (MPTY)

MPTY permet à un abonné de relier plusieurs appels dans une conférence selon la norme 3GPP TS 24.084. L'abonné agit en tant que contrôleur de la conférence. Tout l'audio de la conférence est mélangé via un pont de conférence sur la passerelle multimédia.

Pour la configuration, voir Fonctionnalités Avancées d'Appel.

BuildMPTY

L'abonné établit deux appels (un actif, un en attente), puis invoque BuildMPTY via un message CC FACILITY pour les fusionner en une conférence.



HoldMPTY, RetrieveMPTY, SplitMPTY

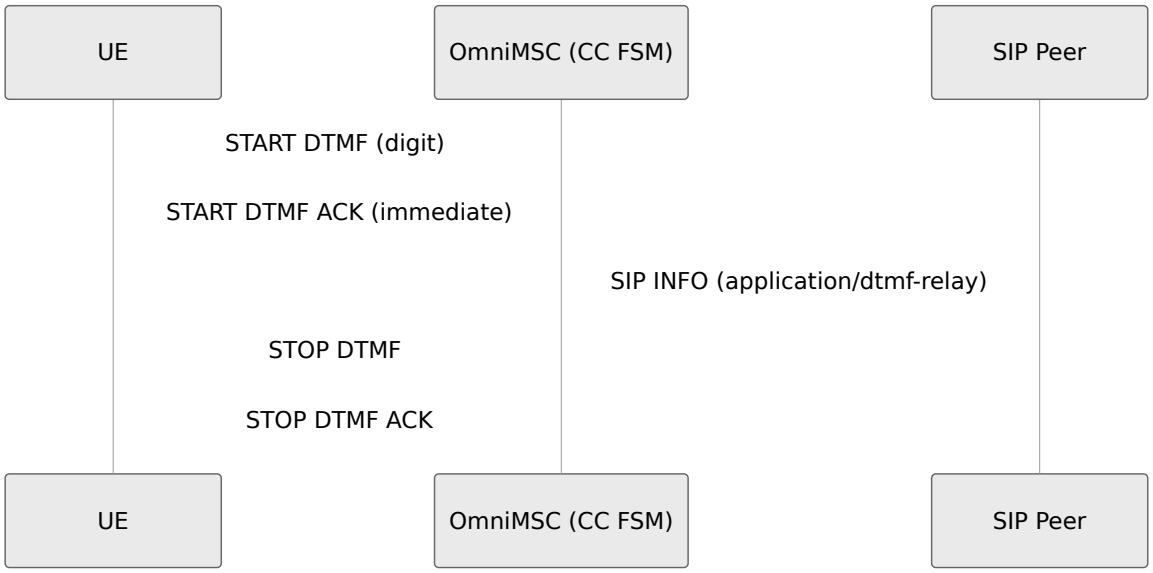
Une fois qu'une conférence est établie, le contrôleur dispose de trois opérations supplémentaires :

Opération	Effet
HoldMPTY	Place l'ensemble de la conférence en attente. Toutes les parties distantes entendent le silence. Le contrôleur peut établir un appel privé en dehors de la conférence.
RetrieveMPTY	Reprend une conférence mise en attente. Toutes les parties sont reconnectées au pont de conférence.
SplitMPTY	Extrait une partie de la conférence dans un appel séparé en attente. Les parties restantes continuent en conférence. Si seulement deux parties restent après la séparation, le contexte de conférence est libéré et l'appel revient à une connexion normale point à point.

Chaque opération est invoquée par l'UE via un message CC FACILITY et reconnue par le MSC avec un résultat de retour correspondant ou une erreur.

Relais DTMF

OmniMSC relaie les tons DTMF de l'interface radio vers le côté de la liaison. L'UE envoie un message START DTMF (3GPP TS 24.008) contenant le chiffre. La FSM CC reconnaît immédiatement l'UE et transmet le chiffre au pair SIP.



Le corps SIP INFO utilise le type de contenu `application/dtmf-relay` avec les champs Signal et Duration. Le MSC envoie immédiatement START DTMF ACK à l'UE sans attendre la réponse du pair SIP, évitant ainsi le clipping audio sur le chemin radio. Le relais DTMF est géré dans tout état d'appel où une connexion côté liaison existe.

Appels d'Urgence

Les appels d'urgence reçoivent un traitement prioritaire. Le MSC détecte les appels d'urgence par le type de message CC Emergency Setup (3GPP TS 24.008 §9.3.8, type de message 0x0E) et le type de demande de service CM (`:emergency`).

L'authentification est tentée normalement. Si elle réussit, le mode de chiffrement est établi et le MSISDN de l'abonné est utilisé comme partie appelante. Si l'authentification échoue, l'appel se poursuit quand même — le mode de chiffrement est ignoré et l'IMEI est utilisé comme partie appelante à la place. Les appels des UEs sans SIM sont acceptés.

Contrairement à la configuration CC normale, le message Emergency Setup ne contient pas de numéro BCD de la partie appelée — le terminal envoie uniquement une capacité de support optionnelle et une catégorie de service d'urgence. Le MSC utilise l'`adresse_psap` configurée comme numéro appelé pour la recherche dans la table de routage et l'URI de demande SIP INVITE sortante. Voir Référence de Configuration pour les paramètres d'urgence.

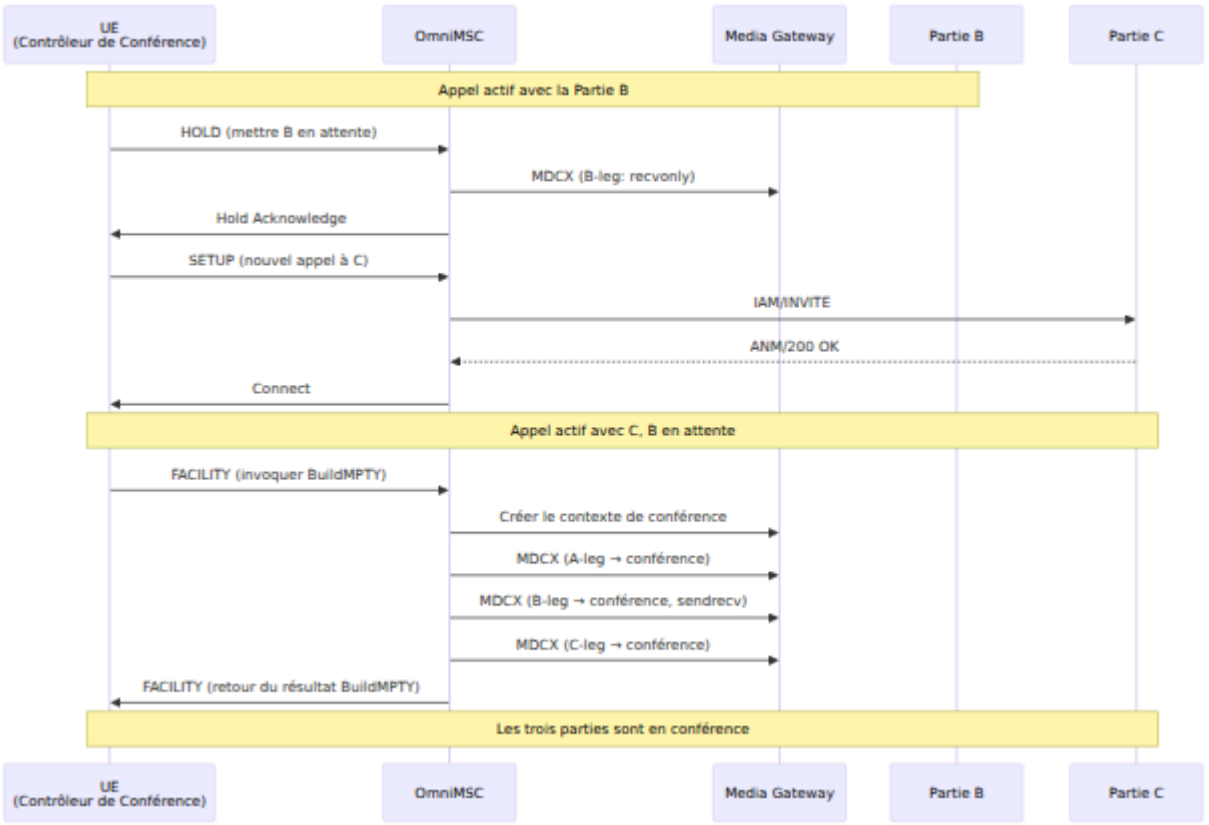


Diagramme d'État de la FSM CC

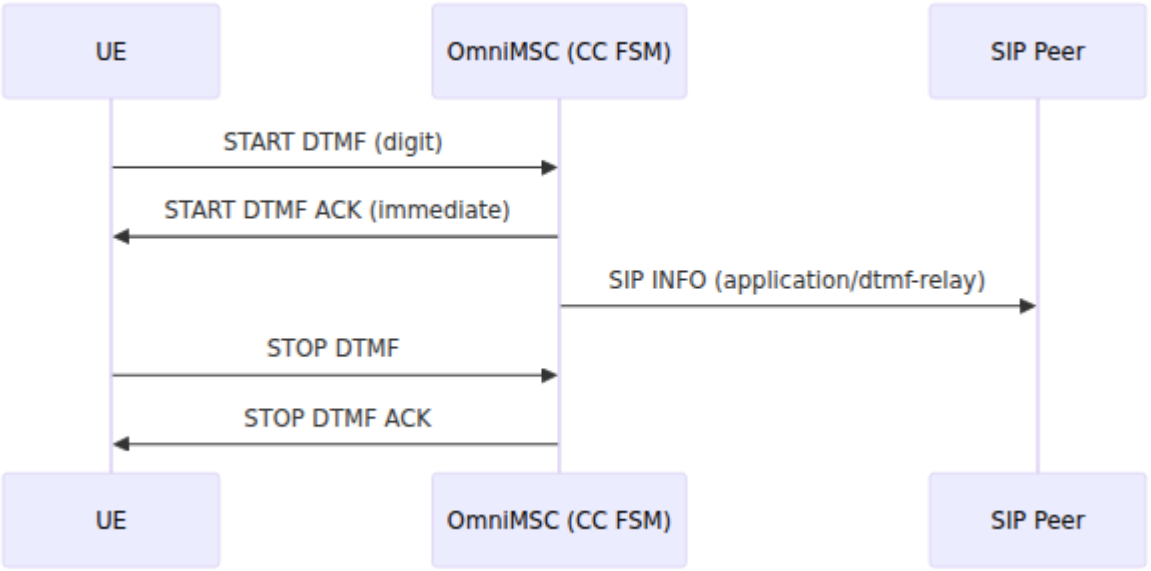
La FSM CC (Machine à États Finis de Contrôle d'Appel) gère le cycle de vie d'un seul appel commuté par circuit selon la norme 3GPP TS 24.008. Les chemins MO et MT partagent des états communs mais entrent par différentes transitions. L'état d'appel en direct, la durée, le codec et le BSC/RNC de service

sont visibles dans la page des Appels Actifs du panneau de contrôle — voir Guide du Panneau de Contrôle.

États d'Appel MO


null
MS SETUP received
initiated
Call Proceeding sent
mo_call_proc
Alerting (remote ringing)
call_delivered
Connect sent to MS
RELEASE COMPLETE
connect_ind
Connect Ack from MS
active
MS DISCONNECT
Network release
disconnect_req
disconnect_ind
RELEASE sent
RELEASE sent
release_req

États d'Appel MT



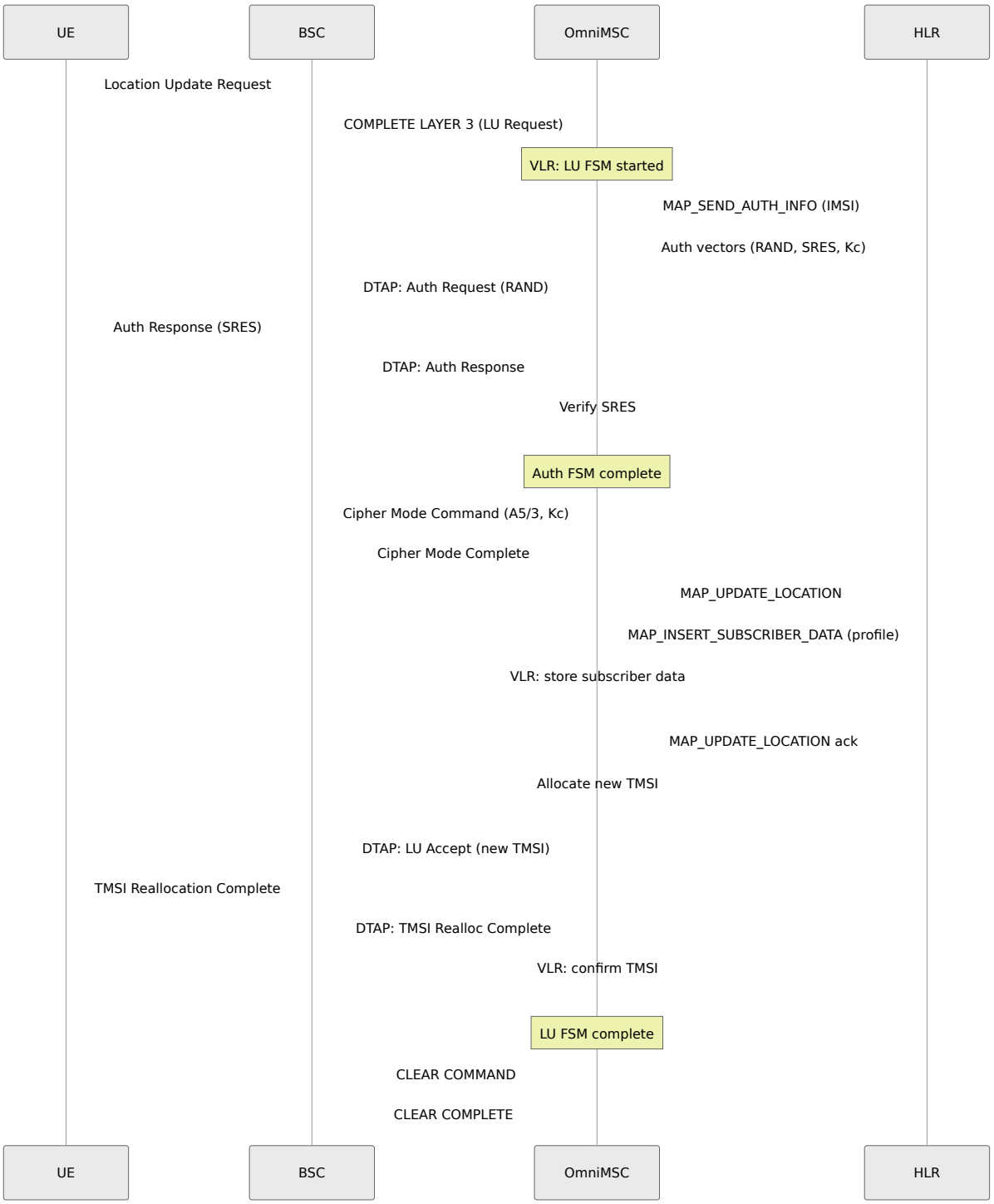
Libération de Connexion

Lorsque la connexion A-interface est perdue (échec de lien radio, effacement BSC ou échec de transport), MSC-A envoie un événement `connection_lost` à toutes les FSM CC associées à cet abonné. Chaque FSM CC recevant cet événement libère ses ressources côté liaison (SIP BYE ou ISUP REL) et les connexions de la passerelle multimédia (MGCP DLCX), puis passe à l'état nul et écrit le CDR.

Cela garantit qu'aucune ressource de liaison ou multimédia n'est perdue lorsque le chemin radio est perdu de manière inattendue. La FSM CC gère `connection_lost` dans tout état sauf nul.

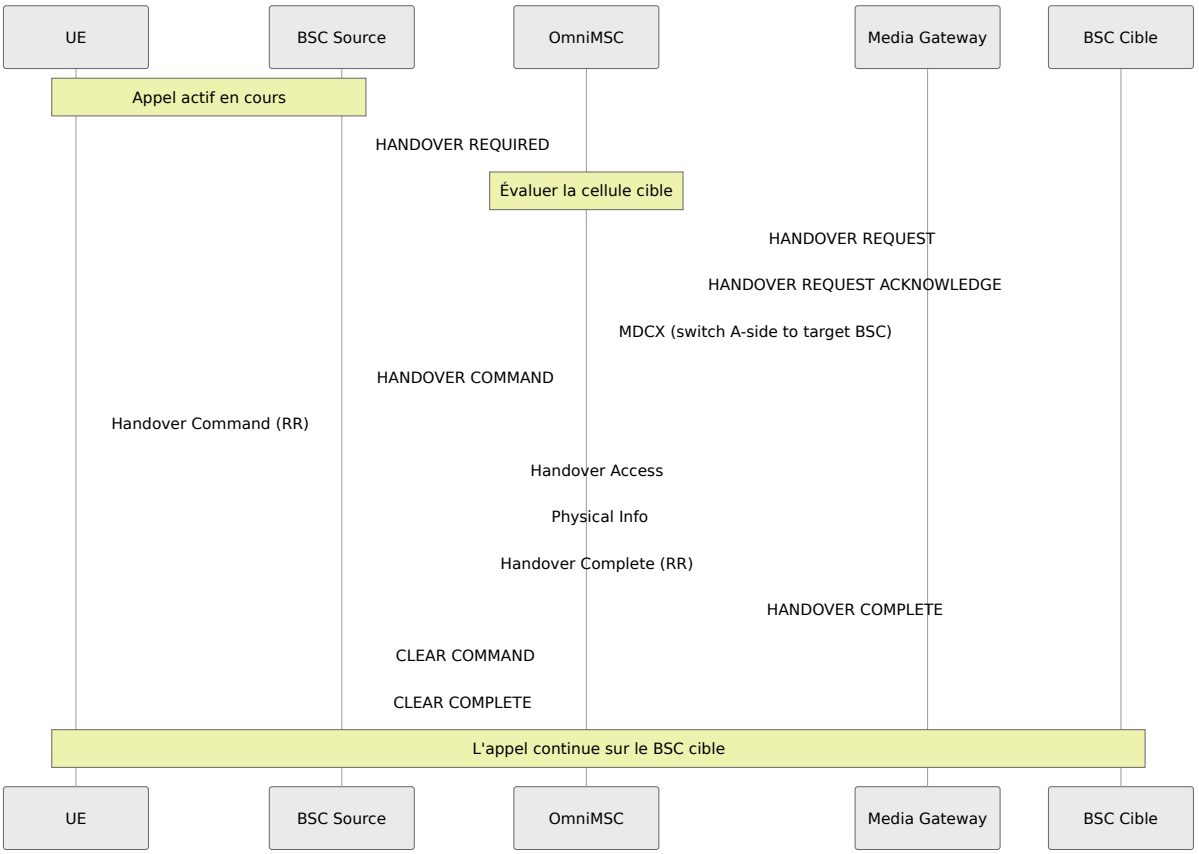
Mise à Jour de Localisation

L'abonné s'enregistre auprès du MSC. Le MSC authentifie l'abonné et met à jour le HLR.



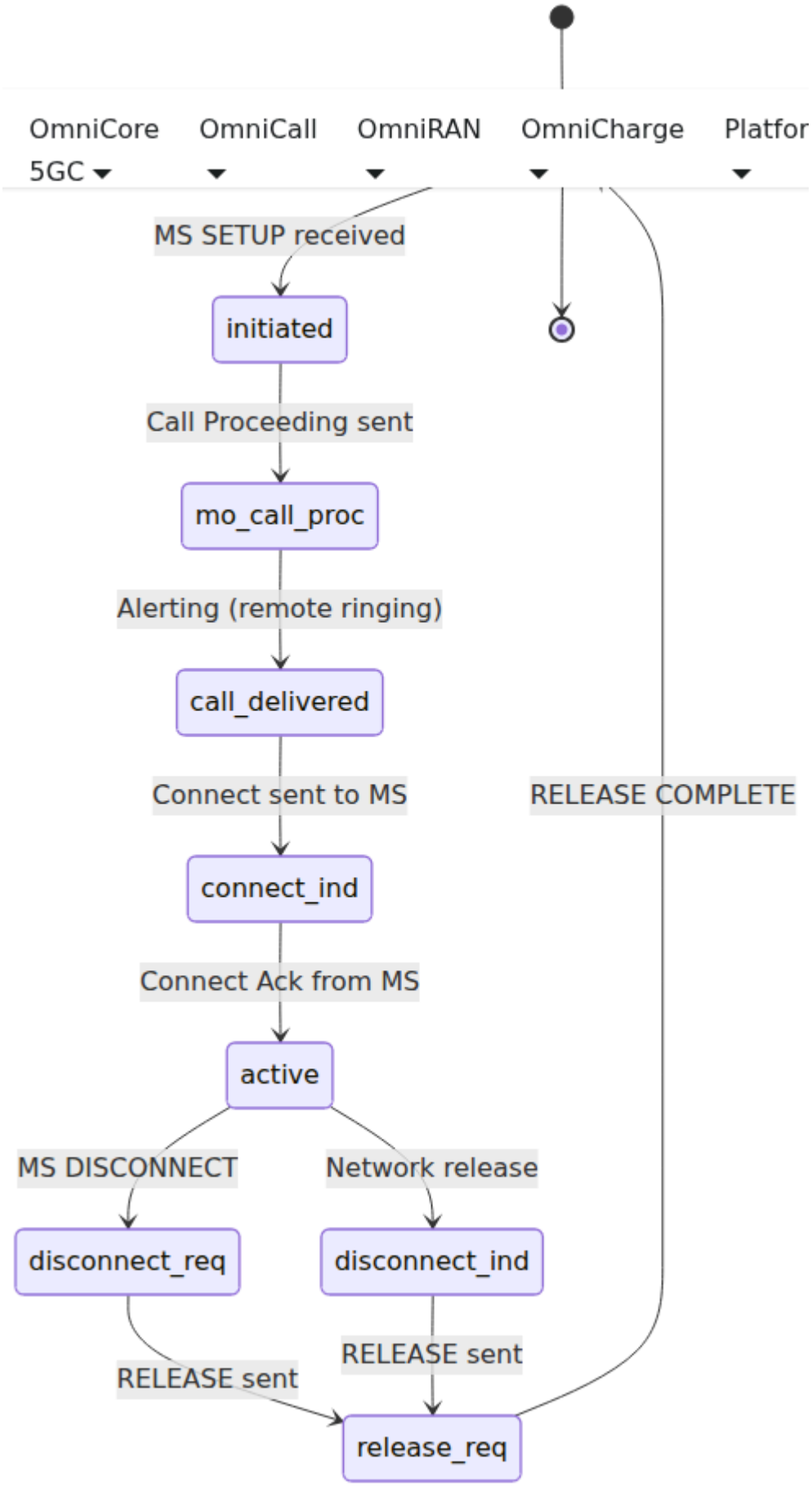
Transfert Intra-MSC

Transfert d'un appel actif entre deux BSC desservis par le même MSC.



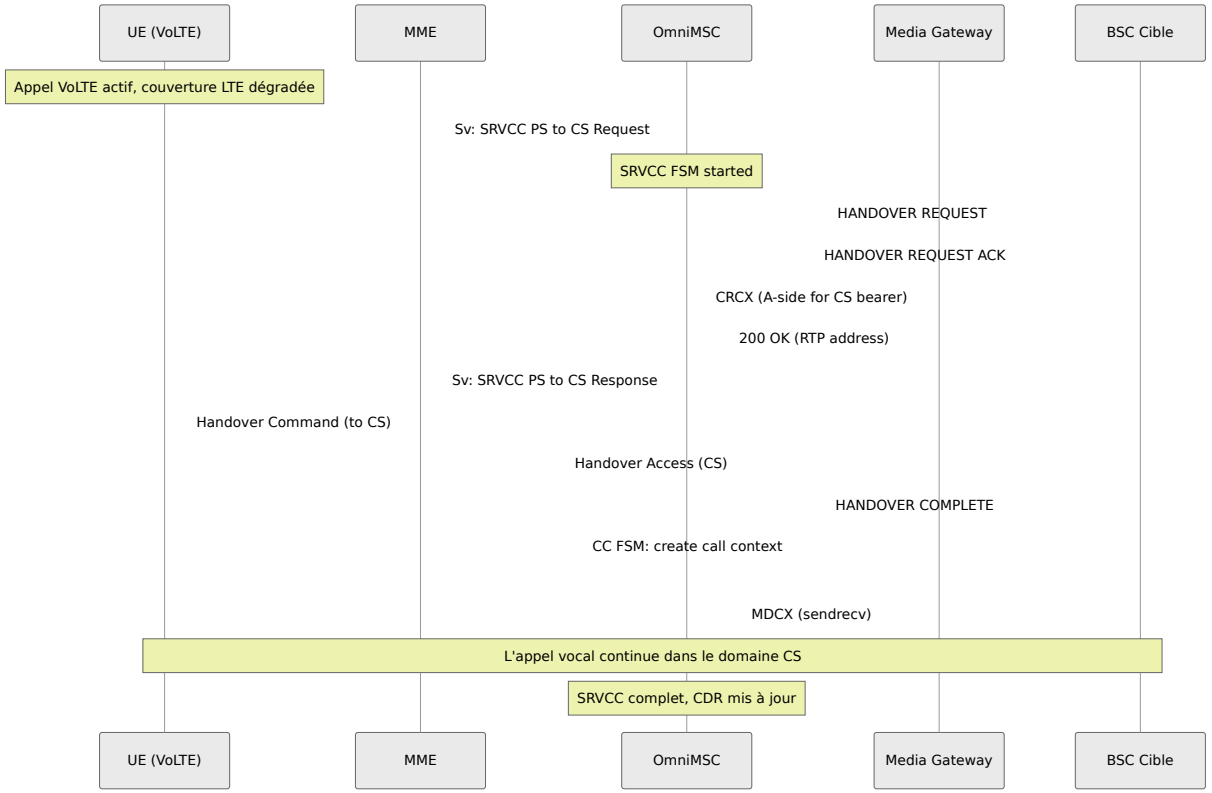
Transfert Inter-MSC

Transfert d'un appel actif d'OmniMSC (MSC-A) vers un MSC cible (MSC-B).


OmniCore
5GC
OmniCall
OmniRAN
OmniCharge
Platfor
MS SETUP received
initiated
Call Proceeding sent
mo_call_proc
Alerting (remote ringing)
call_delivered
Connect sent to MS
connect_ind
Connect Ack from MS
active
RELEASE COMPLETE
MS DISCONNECT
Network release
disconnect_req
disconnect_ind
RELEASE sent
RELEASE sent
release_req

SRVCC (Continuité d'Appel Voix sur Radio Unique)

Transfert d'un appel VoLTE du domaine IMS/LTE vers le domaine CS selon la norme 3GPP TS 23.216.



Appel Déclenché par CAMEL (Interaction SCP)

Appel avec interaction CAMEL Originating BCSM (O-BCSM) selon la norme 3GPP TS 23.078.

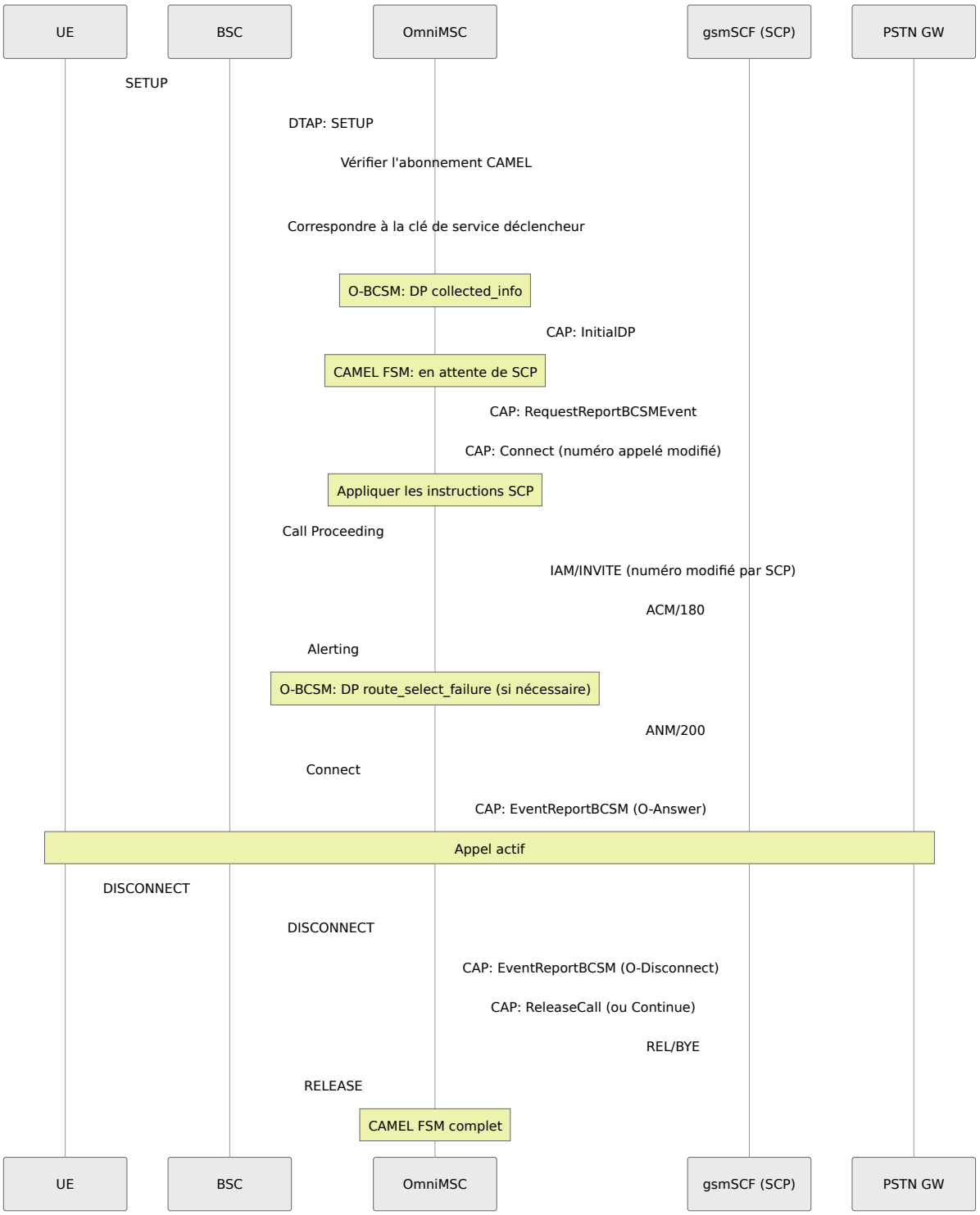


Diagramme de Séquence MPTY (BuildMPTY)

Configuration d'appel de conférence multi-parties. L'abonné établit deux appels, puis les relie en une conférence selon la norme 3GPP TS 24.084. Pour la

configuration, voir Fonctionnalités Avancées d'Appel.

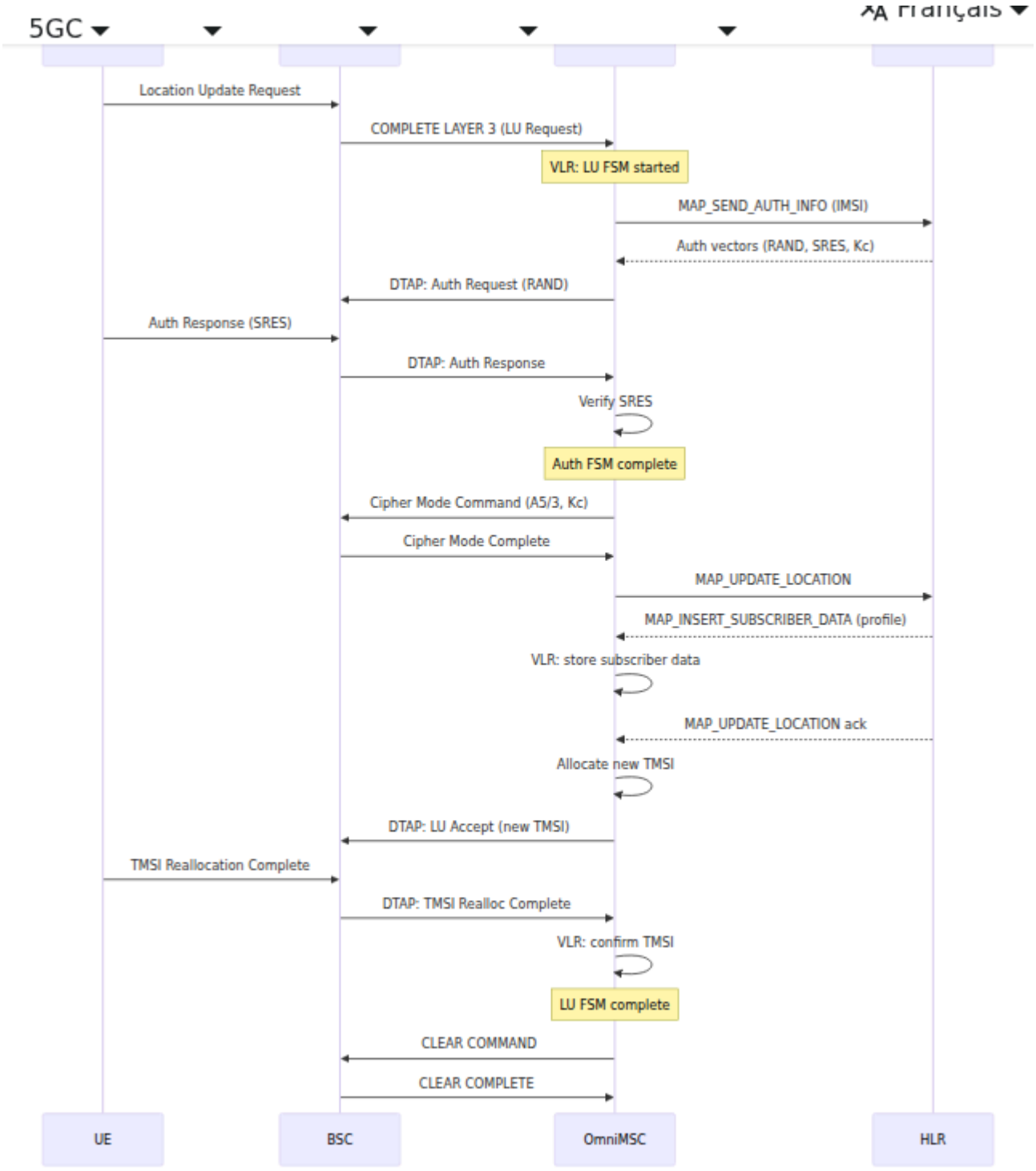


Diagramme de Séquence ECT (Transfert d'Appel Explicite)

Le Transfert d'Appel Explicite connecte deux parties distantes et libère l'abonné transférant selon la norme 3GPP TS 24.091. Pour la configuration, voir Fonctionnalités Avancées d'Appel.

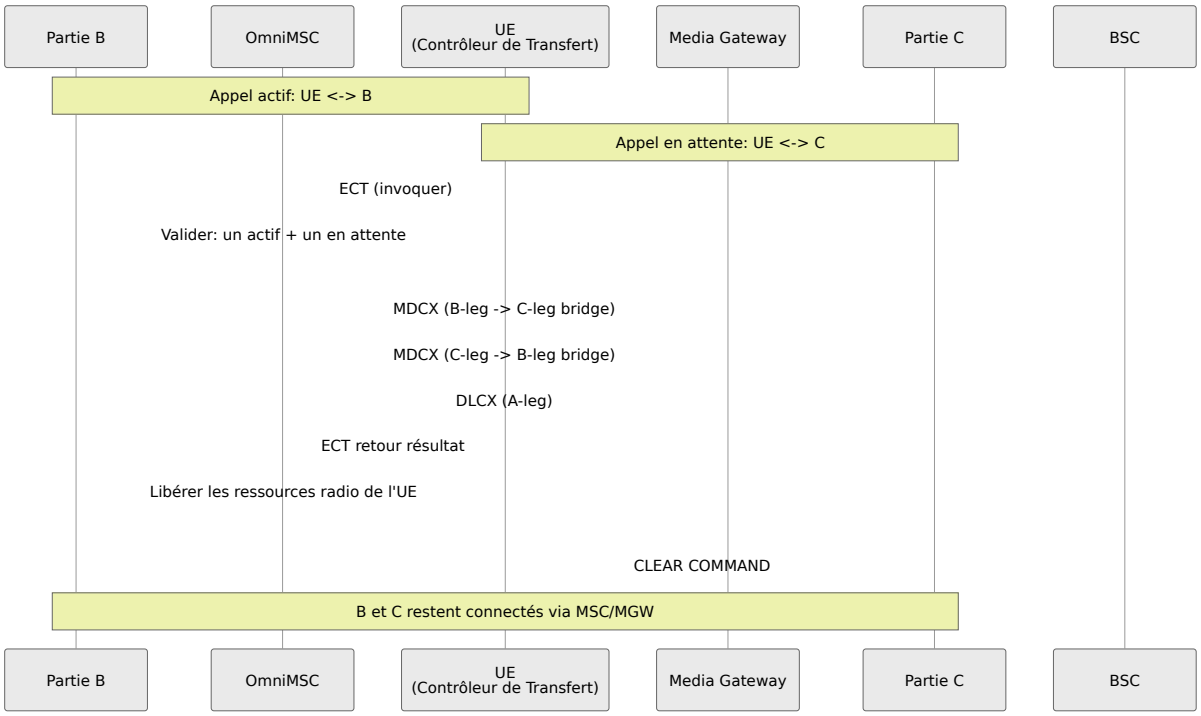


Diagramme de Séquence d'Appel MT CSFB

Appel mobile entrant à un abonné attaché LTE via Circuit-Switched Fallback selon la norme 3GPP TS 23.272. Le MSC page via l'interface SGs, l'UE revient à 2G/3G, et l'appel se poursuit sur l'A-interface. Pour les détails SGs, voir Interface SGs & CSFB.

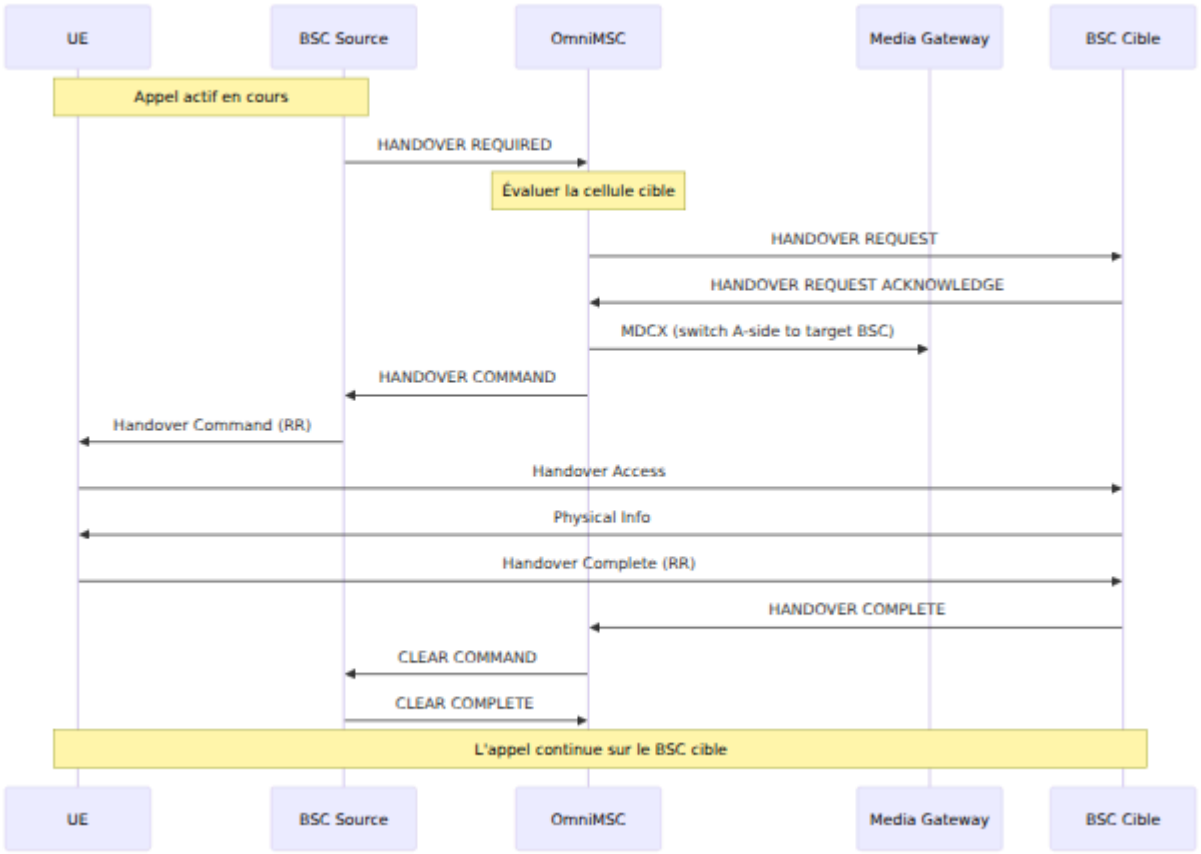
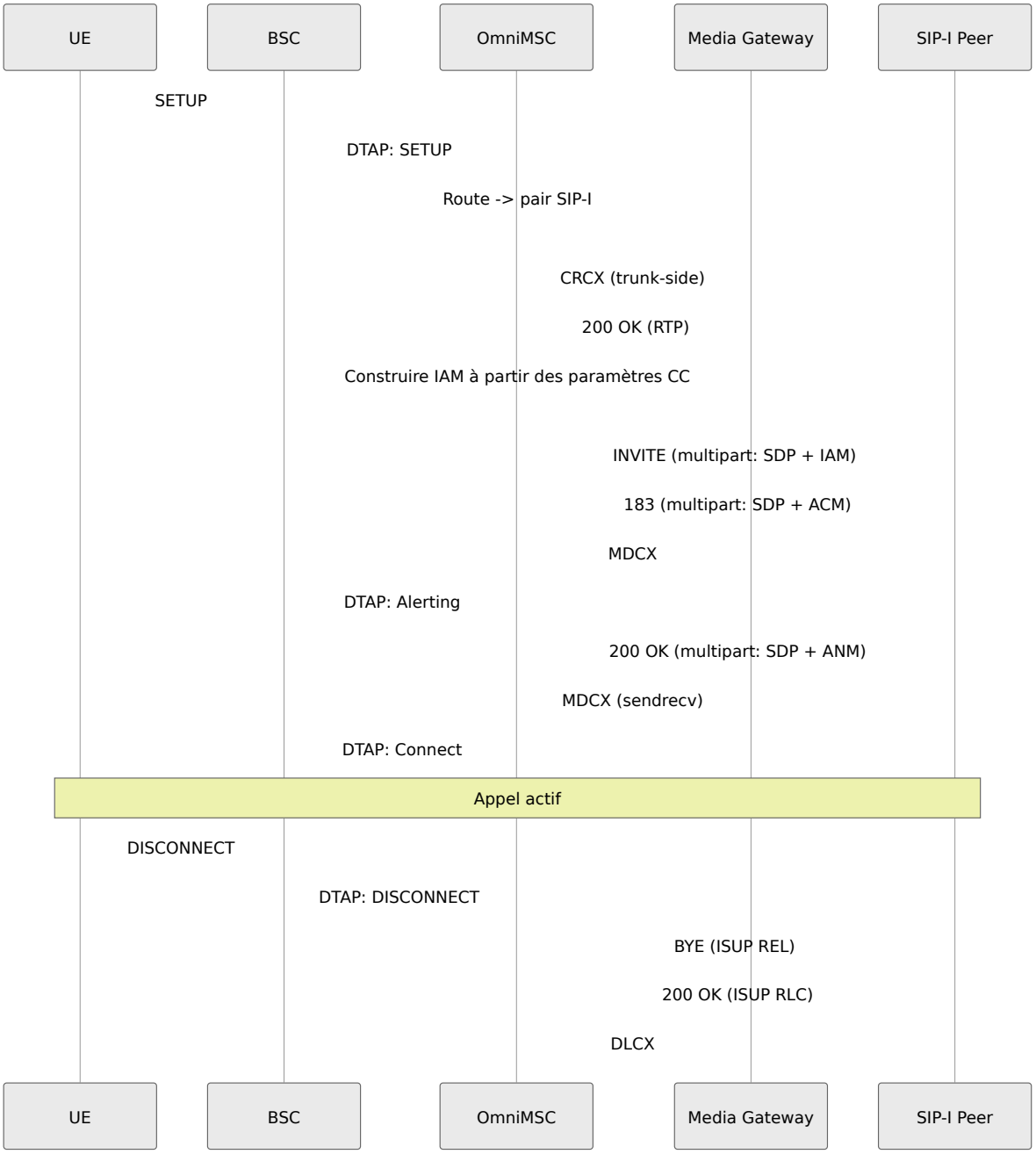


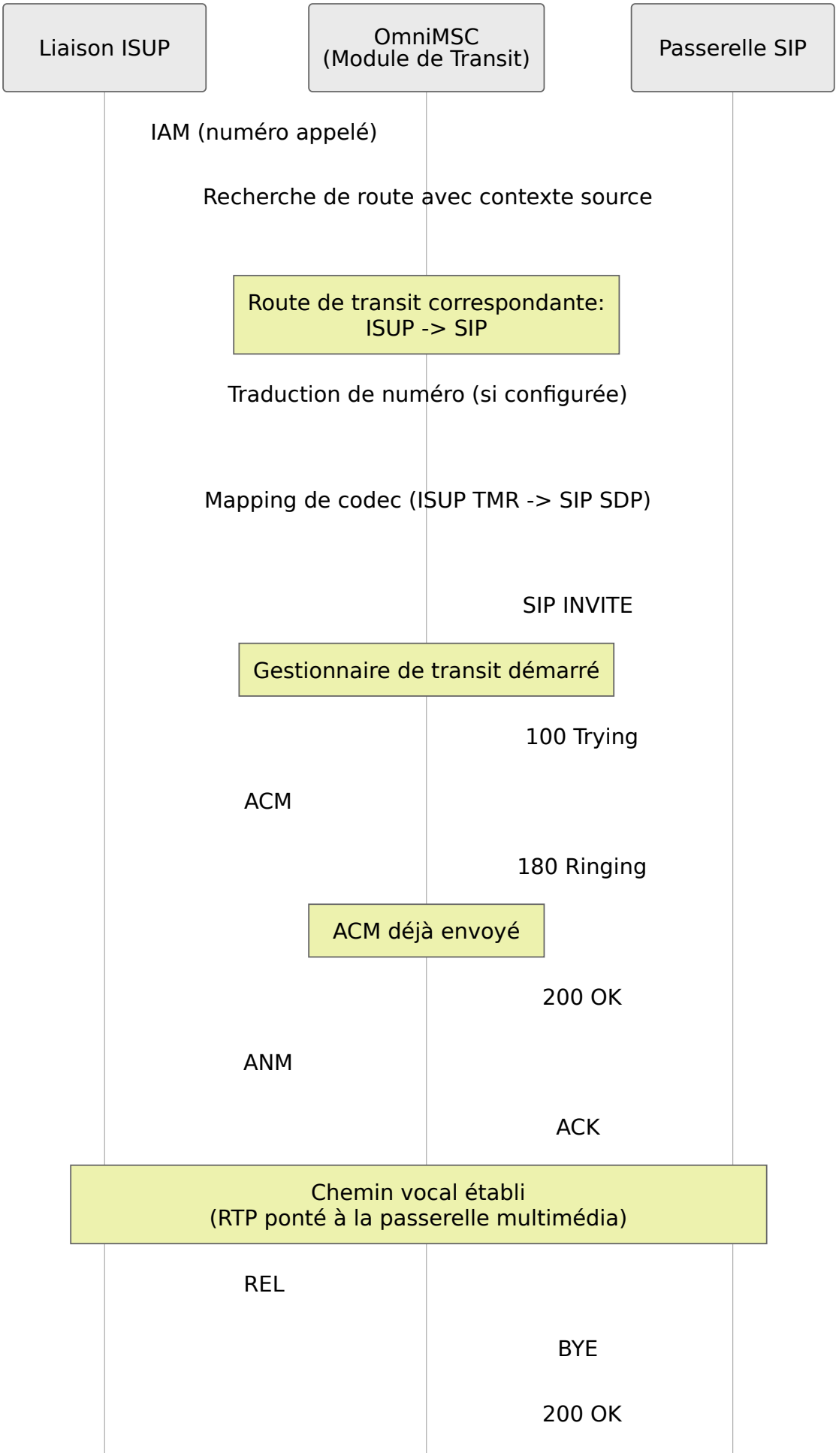
Diagramme de Séquence d'Appel SIP-I

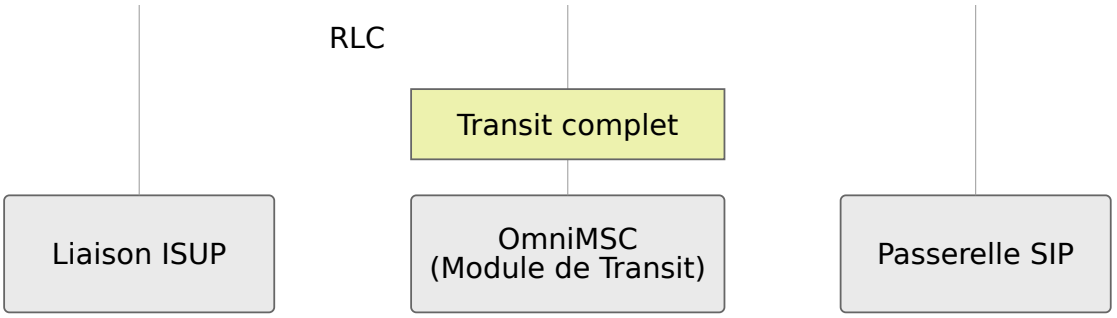
Appel sortant via une liaison SIP-I avec ISUP encapsulé selon l'ITU-T Q.1912.5. L'INVITE transporte un corps multipart contenant SDP et l'ISUP IAM. Pour les détails SIP-I, voir Liaison SIP-I.



Appel de Transit ISUP vers SIP

Appel de transit interopérant entre une liaison ISUP et un pair SIP, contournant la FSM CC.


Liaison ISUP
OmniMSC
(Module de Transit)
Passerelle SIP
IAM (numéro appelé)
Recherche de route avec contexte source
Route de transit correspondante:
ISUP -> SIP
Traduction de numéro (si configurée)
Mapping de codec (ISUP TMR -> SIP SDP)
SIP INVITE
Gestionnaire de transit démarré
100 Trying
ACM
180 Ringing
ACM déjà envoyé
200 OK
ANM
ACK
Chemin vocal établi
(RTP ponté à la passerelle multimédia)
REL
BYE
200 OK


RLC
Transit complet
Liaison ISUP
OmniMSC
(Module de Transit)
Passerelle SIP

CAMEL / CAP

Ce document décrit l'implémentation de CAMEL (Applications Personnalisées pour la Logique Améliorée Mobile) dans OmniMSC, y compris la configuration des clés de service, la gestion des dialogues CAP, les points de détection BCSM, les opérations CAP prises en charge et le transport TCAP.

Pour le diagramme de séquence d'appel déclenché par CAMEL complet (InitialDP, Connect, EventReportBCSM), voir Diagrammes de Flux d'Appel. Pour savoir comment les déclencheurs CAMEL s'intègrent dans le pipeline de routage (flux d'analyse de numéro), voir Configuration de Routage. Pour les champs CDR liés à CAMEL (FurnishChargingInformation, cause_for_term), voir Enregistrements de Détails d'Appel. Pour la configuration des clés de service CAMEL, voir Référence de Configuration.

Aperçu

CAMEL fournit un cadre pour les opérateurs mobiles afin de déployer des services de Réseau Intelligent (IN) sur le réseau central GSM/UMTS. OmniMSC agit en tant que gsmSSF (Fonction de Commutation de Service GSM), interagissant avec un gsmSCF externe (Fonction de Contrôle de Service GSM, également connue sous le nom de SCP) pour fournir des services de contrôle d'appel en temps réel tels que la facturation prépayée, la traduction de numéros, le filtrage d'appels et les réseaux privés virtuels.

Le gsmSCF contrôle le traitement des appels en envoyant des instructions à OmniMSC à des points de détection définis dans le Modèle d'État de Base d'Appel (BCSM). OmniMSC rapporte les événements d'appel au gsmSCF et exécute les instructions reçues (continuer, se connecter à un autre numéro, libérer l'appel, appliquer la facturation).

Configuration des Clés de Service

Chaque abonné peut avoir une ou plusieurs abonnements CAMEL provisionnés via MAP INSERT SUBSCRIBER DATA depuis le HLR. Un abonnement CAMEL comprend une clé de service, qui identifie le service IN à invoquer, et l'adresse du gsmSCF (Titre Global) à contacter.

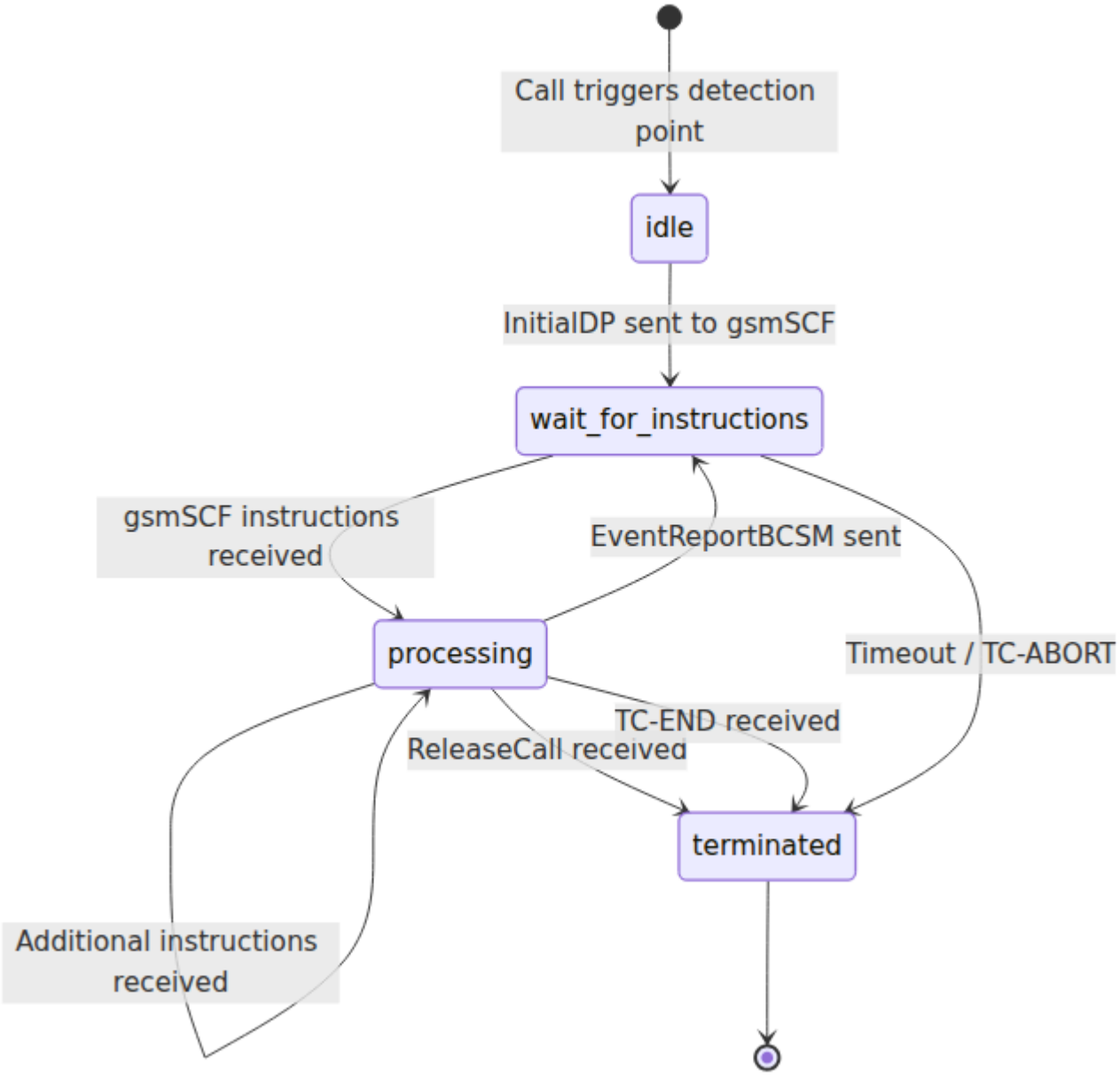
Lorsqu'un appel déclenche un point de détection CAMEL (tel que collected_info pour les appels MO ou terminating_attempt_authorized pour les appels MT), OmniMSC vérifie les données d'abonnement CAMEL de l'abonné. Si une clé de service correspondante est trouvée, OmniMSC ouvre un dialogue CAP avec le gsmSCF et envoie une opération InitialDP.

Paramètre d'Abonnement	Description
Clé de service	Entier identifiant le service IN (par exemple, 1 pour prépayé, 2 pour VPN)
Adresse gsmSCF	Titre Global du SCP à contacter
Gestion des appels par défaut	Action si le SCP est inaccessible : `:continue_call` ou `:release_call`
Liste TDP	Liste des points de détection de déclenchement armés pour cet abonnement
Phase CAMEL	Phase CAMEL prise en charge (Phase 1, 2, 3 ou 4)

Si le gsmSCF est inaccessible ou si le dialogue TCAP échoue, OmniMSC applique l'action de gestion des appels par défaut à partir des données d'abonnement CAMEL de l'abonné.

États du Dialogue CAP

Chaque interaction CAMEL fonctionne comme un dialogue CAP indépendant au sein d'une transaction TCAP. Le dialogue suit l'état de l'interaction SSF-SCF depuis InitialDP jusqu'à la terminaison.



État	Description
idle	Point de détection déclenché, préparation de l'InitialDP
wait_for_instructions	InitialDP envoyé, en attente de la réponse du gsmSCF
processing	Exécution des instructions du gsmSCF (Continue, Connect, ApplyCharging)
terminated	Dialogue terminé, transaction TCAP fermée

Opérations CAP

OmniMSC prend en charge les opérations CAP suivantes pour l'interaction de service CAMEL Phase 2 et Phase 3.

SSF à SCF (OmniMSC à gsmSCF)

Opération	Description
InitialDP	Signale un point de détection déclenché avec les paramètres d'appel (clé de service, numéro appelé/appelant, type d'événement, informations de localisation)
EventReportBCSM	Signale un événement d'appel à un point de détection armé (réponse, déconnexion, abandon, échec de sélection de route)
ApplyChargingReport	Signale le résultat d'une opération de facturation (durée d'appel, unités de charge consommées)
CallInformationReport	Signale les informations d'appel demandées par le gsmSCF (durée d'appel, cause de libération)

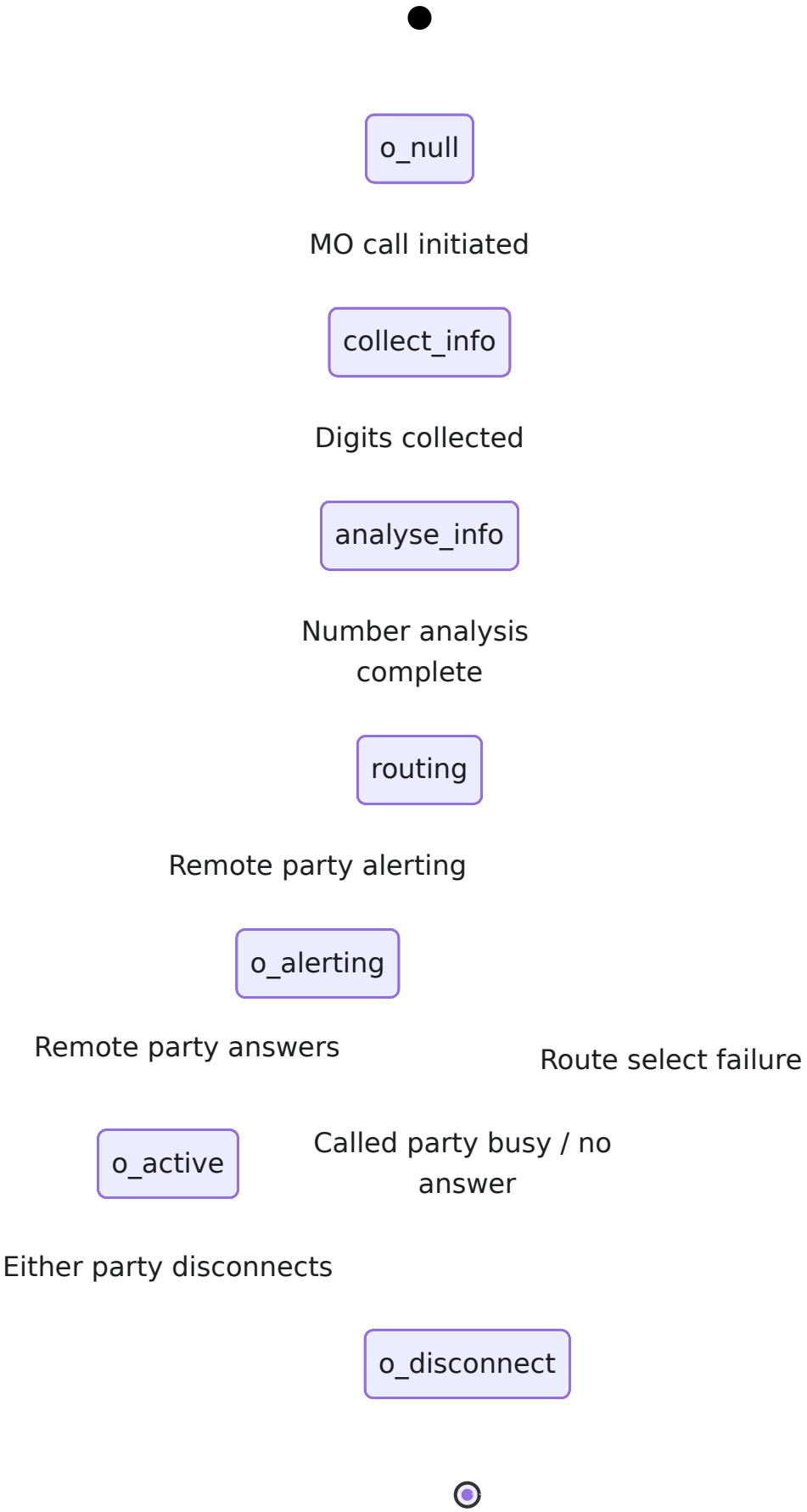
SCF à SSF (gsmSCF à OmniMSC)

Opération	Description
Continue	Reprendre le traitement de l'appel à l'état BCSM actuel
Connect	Acheminer l'appel vers un numéro de destination différent (traduction de numéro, routage VPN)
ReleaseCall	Libérer l'appel avec un code de cause spécifié
RequestReportBCSMEvent	Armer des points de détection pour un reporting d'événements futurs (réponse, déconnexion, abandon)
ApplyCharging	Appliquer les paramètres de facturation (durée d'appel maximale, avis de facturation)
FurnishChargingInformation	Fournir des données de facturation en format libre à inclure dans le CDR
ResetTimer	Réinitialiser le minuteur d'inactivité SSF pour éviter un timeout lors d'un long traitement SCP
SendChargingInformation	Envoyer des informations d'avis de facturation à la station mobile
CallInformationRequest	Demander des informations d'appel à signaler lors de la libération de l'appel

---

Points de Détection O-BCSM

Le Modèle d'État de Base d'Appel d'Origine définit les points de détection disponibles pour les appels MO selon la 3GPP TS 23.078.

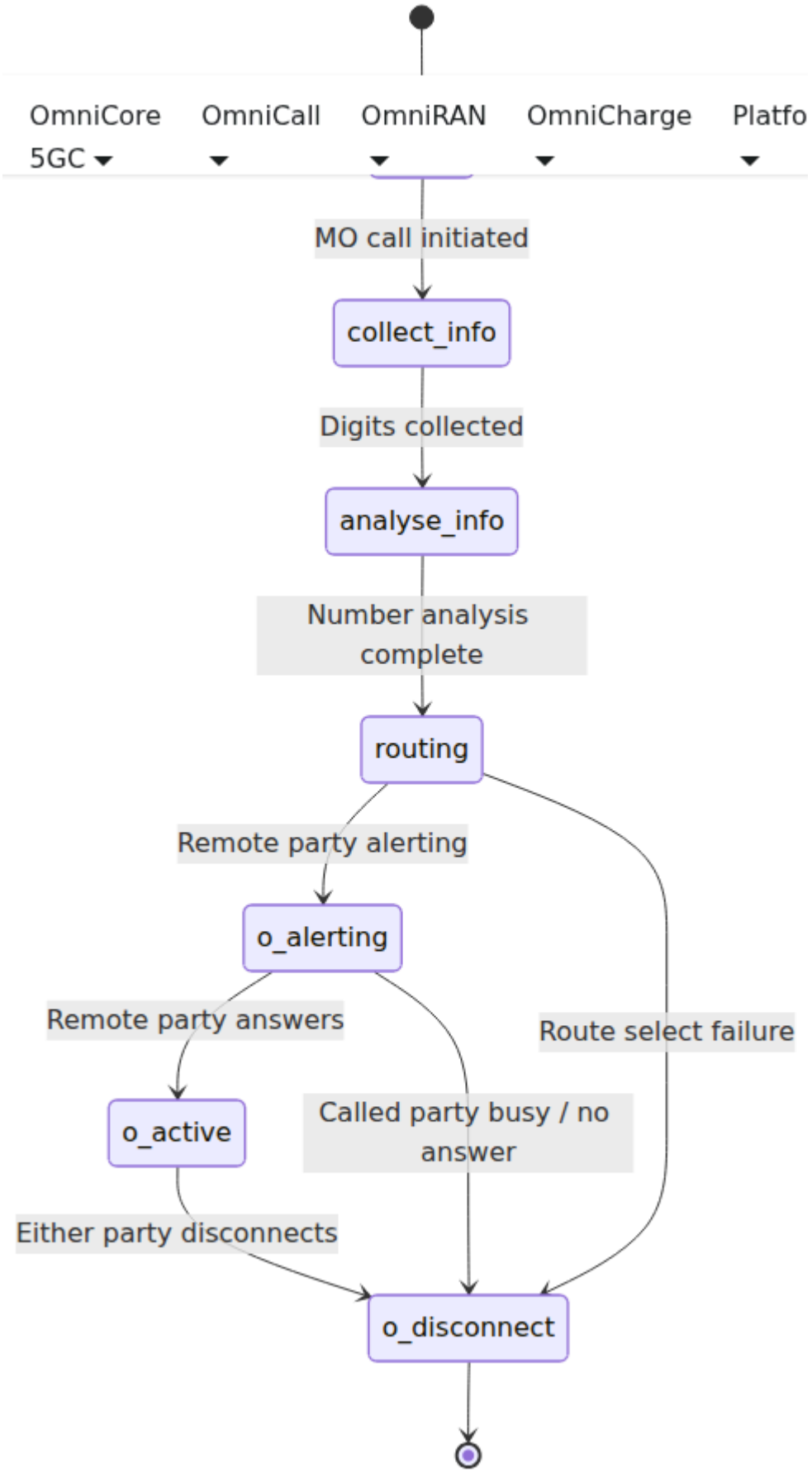

o_null
MO call initiated
collect_info
Digits collected
analyse_info
Number analysis complete
routing
Remote party alerting
o_alerting
Remote party answers
Route select failure
o_active
Called party busy / no answer
Either party disconnects
o_disconnect

Point de Détection	État BCSM	Déclencheur
collected_info (DP 2)	collect_info	Chiffres composés disponibles, avant l'analyse de numéro
analysed_info (DP 3)	analyse_info	Analyse de numéro complète, avant le routage
route_select_failure (DP 4)	routing	Échec du routage (pas de route, trunk occupé, pair hors service)
o_called_party_busy (DP 5)	o_alerting	Partie appelée occupée
o_no_answer (DP 6)	o_alerting	Partie appelée ne répond pas dans le délai
o_answer (DP 7)	o_active	Partie appelée répond
o_disconnect (DP 9)	o_disconnect	L'une ou l'autre des parties initie la déconnexion

---

Points de Détection T-BCSM

Le Modèle d'État de Base d'Appel de Terminaison définit les points de détection disponibles pour les appels MT.


OmniCore
5GC
OmniCall
OmniRAN
OmniCharge
Platfo
MO call initiated
collect_info
Digits collected
analyse_info
Number analysis complete
routing
Remote party alerting
o_alerting
Remote party answers
Route select failure
o_active
Called party busy / no answer
Either party disconnects
o_disconnect

Point de Détection	État BCSM	Déclen
terminating_attempt_authorized (DP 12)	terminating_attempt_authorized	Appel M reçu, av paginat
t_busy (DP 13)	t_alerting	Abonné appelé occupé
t_no_answer (DP 14)	t_alerting	Abonné appelé répond dans le
t_answer (DP 15)	t_active	Abonné appelé répond
t_disconnect (DP 17)	t_disconnect	L'une ou l'autre d parties la déconne

---

Transport TCAP/CAP

Les opérations CAP sont transmises via des dialogues TCAP (Transaction Capabilities Application Part), qui utilisent à leur tour la pile de transport SCCP/M3UA/SCTP. OmniMSC utilise un décodeur BER générique via le module TcapDecoder pour analyser les PDU TCAP et CAP entrants.

Paramètre de Transport	Valeur
SSN (à distance, gsmSCF)	146
SSN (local, MSC/VLR/SSF)	8
Type de dialogue TCAP	Structuré (TC-BEGIN, TC-CONTINUE, TC-END)
Encodage	ASN.1 BER (Règles de Codage de Base)
Contexte d'application	CAP v3 uniquement : 0.4.0.0.1.0.50.1, 0.4.0.0.1.0.50.2, 0.4.0.0.1.0.50.3

L'adresse du gsmSCF est un Titre Global, routé via la Traduction de Titre Global SCCP vers le nœud SCP. OmniMSC maintient une transaction TCAP pendant toute la durée de chaque dialogue CAP, utilisant TC-CONTINUE pour échanger des opérations au sein du dialogue et TC-END pour le fermer.

Références

Référence	Titre	Pertinence
3GPP TS 23.078	CAMEL Phase 3 -- Stage 2	Architecture CAMEL, modèle BCSM, points de détection
3GPP TS 29.078	CAMEL Application Part (CAP) -- Stage 3	Encodage du protocole CAP, définitions ASN.1
ITU-T Q.771-Q.775	Capacités de Transaction	Gestion des dialogues et transactions TCAP
ITU-T Q.711-Q.716	SCCP	Connexion de signalisation pour le transport TCAP
3GPP TS 22.078	CAMEL -- Description du Service	Exigences de service CAMEL

Enregistrements de Détails d'Appel

Ce document décrit le sous-système d'Enregistrement de Détails d'Appel (CDR) dans OmniMSC par Omnitouch. Les CDR sont générés conformément à la norme 3GPP TS 32.298 et fournissent la facturation et la traçabilité pour tous les services commutés par circuit gérés par le MSC.

Pour les paramètres de configuration liés aux CDR, voir Référence de Configuration. Pour la page des Statistiques CDR dans l'interface web, voir Guide du Panneau de Contrôle. Pour les métriques Prometheus et les événements d'alarme liés aux CDR, voir Métriques et Surveillance.

Aperçu

OmniMSC génère des CDR pour les appels vocaux, les transactions SMS, les mises à jour de localisation et les événements d'itinérance. Chaque CDR capture l'identité de l'abonné, les détails du service, les horodatages, la localisation et la cause de terminaison pour une seule transaction. Les CDR sont collectés en mémoire, mis en tampon et périodiquement vidés dans des fichiers au format ASN.1 BER suivant les structures d'enregistrement définies dans 3GPP TS 32.298.

Le sous-système CDR se compose de deux composants :

- **Collecteur CDR** -- reçoit des événements du FSM de Contrôle d'Appel, des procédures de mise à jour de localisation VLR et des gestionnaires SMS. Il corrèle les événements pour les appels actifs (établissement, alerte, réponse, libération) en enregistrements CDR complets et gère les numéros de séquence par type d'enregistrement.
- **Écrivain CDR** -- écrit les enregistrements CDR encodés dans des fichiers sur disque, gérant la rotation des fichiers en fonction de la taille, du nombre d'enregistrements et de l'intervalle de temps.

Types d'Enregistrements

OmniMSC prend en charge les types d'enregistrements CDR suivants, chacun identifié par un tag ASN.1 unique par TS 32.298.

Tag ASN.1	Type d'Enregistrement	Description
0	MOCallRecord	Appel vocal d'origine mobile. Généré lorsqu'un abonné initie un appel vocal.
1	MTCallRecord	Appel vocal terminé mobile. Généré lorsqu'un abonné reçoit un appel vocal.
3	TransitRecord	Appel de transit. Généré pour les appels qui transitent par le MSC sans s'initier ou se terminer à un abonné local.
5	MOSMSRecord	SMS d'origine mobile. Généré lorsqu'un abonné envoie un message court.
6	MTSMSRecord	SMS terminé mobile. Généré lorsqu'un abonné reçoit un message court.
10	SSActionRecord	Action de service complémentaire. Généré lorsqu'un abonné invoque une action de service complémentaire.
13	LocUpdateHLRRecord	Mise à jour de localisation (HLR). Généré pour les procédures de mise à jour de localisation au niveau HLR, suivant les changements MSC/VLR.
14	LocUpdateVLRRecord	Mise à jour de localisation (VLR). Généré pour les procédures de mise à jour de localisation au niveau VLR, suivant les changements de zone de localisation, les résultats d'authentification et l'allocation TMSI.
17	RoamingRecord	Événement d'itinérance. Généré pour les événements d'itinérance inter-MSC.

Champs CDR

Enregistrements d'Appels Vocaux

(MOCallRecord et MTCallRecord)

Champ	Description
served_imsi	IMSI de l'abonné qui a initié ou reçu l'appel
served_msisdn	MSISDN (numéro de téléphone) de l'abonné servi
served_imei	IMEI de l'équipement mobile utilisé
calling_number	Numéro de la partie appelante (A-number)
called_number	Numéro de la partie appelée (B-number), présent dans les enregistrements MO
connected_number	Numéro de la partie réellement connectée (peut différer du numéro appelé en raison du renvoi)
recording_entity	Adresse du MSC qui a généré le CDR
msc_address	Adresse E.164 du MSC
msc_incoming_tkgp	Nom du groupe de troncs entrants
msc_outgoing_tkgp	Nom du groupe de troncs sortants
location	Localisation de l'abonné au moment de l'appel, y compris le Code de Zone de Localisation (LAC) et l'Identité de Cellule (CI)
basic_service	Code de service de transport ou de téléservice identifiant le type de service
seizure_time	Horodatage UTC lorsque l'appel a été initié (message d'établissement reçu)

Champ	Description
answer_time	Horodatage UTC lorsque l'appel a été répondu (peut être nul pour les appels non répondus)
release_time	Horodatage UTC lorsque l'appel a été libéré
call_duration	Durée de l'appel en secondes, mesurée de la réponse à la libération. Zéro pour les appels non répondus.
radio_chan_used	Type de canal radio utilisé (taux plein ou taux réduit)
cause_for_term	Raison de la terminaison de l'appel (voir Cause de Terminaison ci-dessous)
diagnostics	Informations de diagnostic : code de cause GSM 04.08, code d'erreur MAP, ou cause spécifique au réseau
call_reference	Numéro de référence d'appel unique
sequence_number	Numéro de séquence par type d'enregistrement pour la détection de lacunes par les systèmes de facturation en aval
ms_classmark	Informations de classmark de la station mobile
system_type	Type de réseau d'accès : GERAN, UTRAN, ou inconnu
partial_record_type	Pour les CDR partiels : indique s'il s'agit d'un enregistrement partiel intermédiaire ou final

Enregistrements SMS (MOSMSRecord et MTSMSRecord)

Champ	Description
served_imsi	IMSI de l'abonné
served_msisdn	MSISDN de l'abonné
served_imei	IMEI de l'équipement mobile
service_centre	Adresse du Centre de Service SMS
recording_entity	Adresse du MSC d'enregistrement
location	Localisation de l'abonné (LAC/CI)
message_reference	Numéro de référence du message SMS (MO uniquement)
destination_number	Numéro de destination SMS (MO uniquement)
originating_number	Numéro de l'expéditeur SMS (MT uniquement)
origination_time	Horodatage de l'origine du SMS (MO) ou de la livraison (MT)
sms_result	Résultat de la livraison du SMS : succès, échec de livraison, ou transféré

Enregistrements de Mise à Jour de Localisation

Champ	Description
served_imsi	IMSI de l'abonné
served_msisdn	MSISDN de l'abonné (enregistrements VLR uniquement)
recording_entity	Adresse de l'entité d'enregistrement
update_time	Horodatage UTC de la mise à jour de localisation
update_type	Type de mise à jour : mise à jour de localisation normale, mise à jour de localisation périodique, attachement IMSI, ou détachement IMSI
old_location / new_location	Informations de localisation précédente et nouvelle (enregistrements VLR : LAC/CI)
old_msc / new_msc	Adresses MSC précédentes et nouvelles (enregistrements HLR)
old_vlr / new_vlr	Adresses VLR précédentes et nouvelles (enregistrements HLR)
vlr_result / hlr_result	Résultat de la procédure de mise à jour de localisation
authentication_result	Résultat de l'authentification : succès, échec (pas de vecteurs), échec (mismatch d'authentification), ou non effectué (enregistrements VLR uniquement)
tmsi_allocated	Nouvelle valeur TMSI si une a été allouée pendant la procédure (enregistrements VLR uniquement)

Cause de Terminaison

Le champ cause_for_term enregistre pourquoi un appel a été terminé. Les valeurs suivantes sont définies par la TS 32.298.

Cause	Valeur Entière	Description
normal_release	0	Libération normale de l'appel par l'une ou l'autre des parties
partial_record	1	CDR partiel généré pour un appel de longue durée (enregistrement intermédiaire)
partial_record_call_reestablishment	2	Enregistrement partiel en raison de la réétablissement de l'appel
unsuccessful_call_attempt	3	Échec de l'établissement de l'appel avant la réponse (occupé, pas de réponse, échec de routage)
abnormal_release	4	Libération anormale due à une défaillance de lien radio, une erreur de protocole, ou une erreur système
CAMEL_init_call_release	5	Appel libéré par le service CAMEL (libération initiée par SCP)
management_intervention	52	Appel libéré par intervention de l'opérateur

Collecteur CDR

Le Collecteur est un GenServer qui agit comme le point central de collecte des événements CDR. Il reçoit des notifications d'événements du FSM de Contrôle d'Appel, du VLR et des gestionnaires SMS, et les corrèle en enregistrements CDR complets.

Flux d'Événements

Pour les appels vocaux, le Collecteur reçoit une séquence d'événements pendant la durée de l'appel :

1. Établissement de l'appel -- enregistre l'identité de l'abonné, les numéros appelés/appelants, la direction (MO ou MT), l'heure de saisie et le type de service.
2. Alerte d'appel -- enregistré pour le diagnostic mais ne génère pas de champ CDR.
3. Réponse à l'appel -- enregistre l'horodatage de la réponse et démarre le minuteur CDR partiel pour les longs appels.
4. Libération de l'appel -- calcule la durée de l'appel, sélectionne la cause de terminaison, génère l'enregistrement CDR final et le met en tampon pour écriture.

Pour les SMS et les mises à jour de localisation, le Collecteur génère un enregistrement CDR immédiatement à partir d'une seule notification d'événement.

Tamponnage et Vidage

Les enregistrements CDR sont accumulés dans un tampon en mémoire. Le tampon est vidé vers l'Écrivain sous deux conditions :

- Un minuteur de vidage périodique se déclenche (intervalle par défaut : 5000 ms).
- Le tampon atteint sa taille maximale (par défaut : 1000 enregistrements), déclenchant un vidage immédiat.

Génération de CDR Partiels

Pour les appels de longue durée, le Collecteur génère des enregistrements CDR partiels intermédiaires à un intervalle configurable (par défaut : 3600 secondes / 1 heure). Chaque CDR partiel capture l'état de l'appel jusqu'à ce point. L'enregistrement CDR final lors de la libération de l'appel est marqué comme le dernier partiel si des intermédiaires ont été générés. Cela garantit que les systèmes de facturation en aval peuvent reconstruire la durée complète de l'appel même si le MSC échoue avant la fin de l'appel.

Numéros de Séquence

Le Collecteur maintient des compteurs de numéros de séquence indépendants pour chaque type d'enregistrement (appel MO, appel MT, SMS MO, SMS MT, itinérance, mise à jour de localisation HLR, mise à jour de localisation VLR). Les numéros de séquence s'incrémentent de manière monotone et se réinitialisent à 10000. Les systèmes de facturation en aval utilisent les numéros de séquence pour détecter les lacunes indiquant des enregistrements CDR perdus.

Nommage des Fichiers CDR

Les fichiers CDR suivent une convention de nommage qui inclut l'identité du MSC, l'horodatage et le numéro de séquence :

<NodeID><*Date*><Time>_<SeqNum>.dat

Où :

- NodeID est le nom du MSC (provenant de la configuration recording_entity).
- Date est au format AAAAMMJJ.
- Time est au format HHMMSS.
- SeqNum est un numéro de séquence à 4 chiffres avec des zéros en tête (se réinitialise à 10000).

Par exemple : MSC01_20260329_143022_0001.dat

Les fichiers sont écrits au format ASN.1 BER contenant une séquence d'enregistrements CDR comme défini dans la TS 32.298.

Rotation des Fichiers

Les fichiers CDR sont tournés (fermés et un nouveau fichier ouvert) lorsque l'une des conditions suivantes est remplie :

- Le fichier dépasse la taille maximale configurée (par défaut : 10 Mo).
- Le fichier contient le nombre maximal d'enregistrements configuré (par défaut : 100 000).
- L'intervalle de temps configuré s'est écoulé depuis l'ouverture du fichier (par défaut : 3600 secondes).
- Une rotation explicite est déclenchée via l'API.

Configuration

Le sous-système CDR est configuré via les paramètres de démarrage du Collecteur et de l'Écrivain.

Paramètres du Collecteur

Paramètre	Par Défaut	Description
recording_entity	(requis)	Adresse ou nom du MSC d'enregistrement, écrit dans chaque enregistrement CDR
msc_address	Identique à recording_entity	Adresse E.164 du MSC incluse dans les enregistrements d'appel
flush_interval	5000 ms	Intervalle entre les vidages périodiques du tampon vers l'Écrivain
buffer_size	1000	Nombre maximum d'enregistrements CDR conservés dans le tampon avant un vidage forcé
partial_cdr_interval	3600 secondes	Intervalle pour générer des CDR partiels intermédiaires lors d'appels de longue durée

Paramètres de l'Écrivain

Paramètre	Par Défaut	Description
output_dir	(requis)	Répertoire où les fichiers CDR sont écrits. Créé automatiquement s'il n'existe pas.
node_id	(requis)	Identifiant de l'élément de réseau utilisé dans les noms de fichiers CDR
extension	.dat	Extension de fichier pour les fichiers CDR
max_file_size	10 000 000 octets (10 Mo)	Taille maximale du fichier avant rotation
max_records	100 000	Nombre maximum d'enregistrements par fichier avant rotation
rotation_interval	3600 secondes	Temps maximum qu'un fichier reste ouvert avant rotation. Défini sur nil pour désactiver la rotation basée sur le temps.

Interface Web CDR

La page des Statistiques CDR dans le Panneau de Contrôle affiche des informations en temps réel sur le sous-système CDR.

Page des Statistiques CDR montrant l'état de l'écrivain, la profondeur du tampon, les appels suivis actifs, et les numéros de séquence par type.

Champ	Description
Enregistrements dans le Fichier	Nombre d'enregistrements CDR écrits dans le fichier de sortie actuel
En Attente dans le Tampon	Nombre d'enregistrements CDR mis en tampon en mémoire en attente du prochain vidage
Appels Actifs Suivis	Nombre d'appels avec un état CDR ouvert (entre l'établissement et la libération)
Fichier Actuel	Chemin du fichier de sortie CDR actuel, ou "Aucun fichier ouvert" si inactif
Numéros de Séquence	Compteurs de séquence par type d'enregistrement montrant le prochain numéro de séquence pour chaque type de CDR

La page se rafraîchit automatiquement toutes les 5 secondes via WebSocket.

Références de Spécification 3GPP

Spécification	Titre	Pertinence
TS 32.298	Règles d'Encodage des Enregistrements de Données de Facturation	Types d'enregistrements CDR, structure ASN.1, définitions de champs
TS 32.205	Description des Données de Facturation pour le Domaine CS	Principes de facturation du domaine CS et exigences de contenu des CDR
TS 32.015	Facturation et Tarification	Contexte général de l'architecture de facturation

Référence de Configuration

Ce document couvre tous les paramètres de configuration pour OmniMSC. La configuration est spécifiée dans les fichiers de configuration Elixir (`config.exs`, `dev.exs`, `runtime.exs`) et peut être remplacée à l'exécution via des variables d'environnement.

Pour un exemple de démarrage rapide, consultez le Guide des Opérations.

Identité MSC

`config :omnimsc, :msc`

Définit l'identité du réseau SS7 de l'MSC, utilisée pour l'adressage SCCP, les opérations MAP, l'identification de la zone de localisation et la génération de CDR. Les paramètres d'identité MSC actifs sont visibles dans la page Système du panneau de contrôle — pour plus d'informations, voir Guide du Panneau de Contrôle.

```
config :omnimsc, :msc,
  point_code: 500,
  global_title: "14155550100",
  name: "OMNIMSC01",
  msc_number: "14155550100",
  vlr_number: "14155550100",
  mcc: 999,
  mnc: 99,
  lac: 0x1092,
  allowed_a5: [:a5_1, :a5_3]
```

Paramètre	Type	Requis	Par défaut	Description
`point_code`	`integer` ou `[integer, integer, integer]`	Oui	`0`	Code de point SS7. Peut être spécifié comme un entier plat ou au format ITU 14 bits `[a, b, c]` (codé comme `a*2048 + b*8 + c`).
`global_title`	`string`	Oui	`"00000000000"`	Titre global SCCP (numéro E.164) pour le routage MAP vers HLR, SMSc et nœuds pairs.
`name`	`string`	Oui	`"OMNIMSC01"`	Nom logique de l'MSC. Utilisé dans le champ `recording_entit` du CDR, descriptions d'alarme et messages de journal.
`msc_number`	`string`	Oui	--	Adresse E.164 de l'MSC, envoyée au HLR dans la mise à jour de localisation MAP utilisée pour le routage des appels MT.

Paramètre	Type	Requis	Par défaut	Description
`vlr_number`	`string`	Oui	--	Adresse E.164 du VLR co-localisé, envoyée au HLR dans la mise à jour de localisation MAP. Typiquement la même que `msc_number`.
`mcc`	`integer`	Oui	--	Code de pays mobile (3 chiffres). Combiné avec `mnc` et `lac` pour former l'identité de la zone de localisation (LAI) diffusée dans les informations système.
`mnc`	`integer`	Oui	--	Code de réseau mobile (2 ou 3 chiffres).
`lac`	`integer`	Oui	--	Code de zone de localisation (16 bits). Identifie la zone de localisation desservie par ce MSC/VLR.
`allowed_a5`	`list(atom)`	Non	`[:a5_1, :a5_3]`	Algorithmes de chiffrement A5

Paramètre	Type	Requis	Par défaut	Description
				autorisés pour le chiffrement de l'interface radio. Valeurs valides : `:a5_0`, `:a5_1`, `:a5_2`, `:a5_3`. La négociation d'algorithmes préfère A5/3 > A5/1 > A5/0 (3GI TS 48.008).

HLR

`config :omnimsc, :hlr`

Configure l'adresse HLR distante pour les opérations MAP (Envoyer des informations d'authentification, Mettre à jour la localisation, Insérer des données d'abonné, Purger MS).

```
config :omnimsc, :hlr,
  address: "14155550200",
  point_code: [3, 14, 2]
```

Paramètre	Type	Requis	Par défaut	Description
`address`	`string`	Oui	--	Titre global HLR (numéro E.164) pour le routage MAP.
`point_code`	`integer` ou `[integer, integer, integer]`	Non	--	Code de point SS7 HLR pour le routage MTP3 direct lorsque la traduction de titre global n'est pas utilisée. Peut être un entier plat ou au format ITU 14 bits `[a, b, c]`.

VLR

`config :omnimsc, :vlr`

Contrôle le comportement du Registre de Localisation des Visiteurs, y compris la politique d'authentification, la gestion des TMSI et les modes laboratoire/invité.

```
config :omnimsc, :vlr,
  hlr_adapter: Omnimsc.VLR.HLR.Live,
  auth_required: true,
  tmsi_realloc: true,
  num_auth_vectors: 1
```

Paramètre	Type	Requis	Par défaut	
`hlr_adapter`	`module`	Non	`Omnimsc.VLR.HLR.Default`	Mod vale lorsc est `Omn` un a jour opér `Omn` envc opér `Omn` four intég labo `con` défi `Omn`
`auth_required`	`boolean`	Non	`true`	Indic GSM avar serv mise se p d'inf d'au
`tmsi_realloc`	`boolean`	Non	`true`	Indic un n chac loca Amé de l'

Paramètre	Type	Requis	Par défaut	
`num_auth_vectors`	`integer`	Non	`1`	Nom d'au dem envo d'au 3GP vale rédu MAP mén
`lab_mode`	`boolean`	Non	`false`	Lors tout d'au SRE test des ne c
`guest_mode`	`boolean`	Non	`false`	Lors abor de s MSIS aléa les r dém

M3UA / STP

`config :omnimsc, :m3ua_asp`

Configure la connexion M3UA ASP (Application Server Process) à un Point de Transfert de Signalisation. Toute la signalisation SS7 (interface A, MAP vers

HLR/SMSc, ISUP) est routée par ce lien.

```
config :omnimsc, :m3ua_asp,
  enabled: true,
  local_ip: {10, 5, 198, 200},
  local_port: 0,
  remote_ip: {10, 179, 4, 10},
  remote_port: 2905,
  routing_context: 10,
  receive_watchdog: false,
  receive_watchdog_idle: 15
```

Paramètre	Type	Requis	Par défaut	Description
`enabled`	`boolean`	Non	`false`	Indique s'il faut démarrer le client M3UA ASP. Lorsque `false`, aucune connexion STP n'est établie.
`local_ip`	`tuple`	Non	`{0, 0, 0, 0}`	Adresse IP de liaison SCTP locale sous forme de tuple Erlang.
`local_port`	`integer`	Non	`0`	Port de liaison SCTP local. Utilisez `0` pour laisser le système d'exploitation attribuer un port éphémère.
`remote_ip`	`tuple`	Oui	--	Adresse IP SCTP STP sous forme de tuple Erlang.
`remote_port`	`integer`	Non	`2905`	Port SCTP STP. Le port 2905 est le port M3UA attribué par l'IANA.

Paramètre	Type	Requis	Par défaut	Description
`routing_context`	`integer`	Non	--	Valeur de contexte de routage M3UA. Doit correspondre à la configuration AS du STP pour cet ASP.
`receive_watchdog`	`boolean`	Non	`true`	Indique s'il faut activer le watchdog de battement M3UA. Lorsque `true`, l'ASP surveille les accusés de réception BEAT manquants et déclenche la récupération du lien.
`receive_watchdog_idle`	`integer`	Non	`15`	Intervalle d'inactivité en secondes avant que le watchdog de réception considère le lien comme bloqué.

Le code de point local est pris de `:msc` `point_code` ; un `point_code` défini sous `:m3ua_asp` n'est pas lu. L'indicateur de réseau MTP3 n'est pas configurable ici.

Les écouteurs SCTP directs (pour les connexions BSC sans STP) sont configurés sous `config :omnimsc, :sctp` :

```
config :omnimsc, :sctp,
  listeners: [
    [name: :a_interface, ip: {0, 0, 0, 0}, port: 2905, ppid: 3]
  ]
```

Paramètre	Type	Requis	Par défaut	Description
`name`	`atom`	Oui	--	Nom logique de l'écouteur pour les recherches d'association SCTP et l'affichage dans le panneau de contrôle.
`ip`	`tuple`	Non	`{0, 0, 0, 0}`	Adresse IP de liaison. Utilisez `{0, 0, 0, 0}` pour toutes les interfaces.
`port`	`integer`	Non	`2905`	Port de liaison SCTP.
`ppid`	`integer`	Non	`3`	Identifiant de protocole de charge SCTP. La valeur `3` indique M3UA (RFC 4666).

Remplacement à l'exécution : Définissez les variables d'environnement `SCTP_LISTEN_IP` et `SCTP_LISTEN_PORT`.

SIP

`config :omnimsc, :sip`

Configure l'écouteur SIP et les passerelles SIP pour l'interconnexion VoIP.

```
config :omnimsc, :sip,
  signaling_address: "10.5.198.200",
  listen_ip: {0, 0, 0, 0},
  listen_port: 5060,
  transport: :udp,
  peers: [
    [name: "Default-GW", address: "10.1.1.50", port: 5060,
     transport: :udp, codecs: [:pcmu, :pcma],
     max_channels: 100, options_interval: 60],
    [name: "International-GW", address: "10.1.1.51", port: 5062,
     transport: :udp, codecs: [:pcmu, :pcma, :amr, :amr_wb]]
  ]
```

Paramètres de l'Écouteur SIP

Paramètre	Type	Requis	Par défaut	Description
`signaling_address`	`string`	Non	--	Adresse IP utilisée dans les en-têtes de contact SIP et les lignes SDP `c=`. Doit être accessible par les pairs SIP. Revient à l'adresse de l'écouteur SCTP si non définie.
`listen_ip`	`tuple`	Non	`{0, 0, 0, 0}`	Adresse de liaison de l'écouteur SIP.
`listen_port`	`integer`	Non	`5060`	Port de l'écouteur SIP.
`transport`	`atom`	Non	`:udp`	Protocole de transport par défaut. Un des `:udp`, `:tcp`, `:tls`.

Paramètres des Pairs SIP

Chaque pair dans la liste `peers` accepte les éléments suivants :

Paramètre	Type	Requis	Par défaut	Description
`name`	`string`	Oui	--	Nom logique du pai Référencé dans les entrées de la table routage avec le typ `:sip`.
`address`	`string`	Oui	--	Adresse IP ou nom d'hôte du pair.
`port`	`integer`	Non	`5060`	Port SIP du pair.
`transport`	`atom`	Non	`:udp`	Transport pour ce p `:udp`, `:tcp`, ou `:tl`
`codecs`	`list(atom)`	Non	`[:pcmu, :pcma]`	Codecs audio pris e charge. Valeurs val : `:pcmu`, `:pcma`, `:a` `:amr_wb`.
`max_channels`	`integer`	Non	`100`	Nombre maximum d'appels simultanés ce pair. Les nouvea appels sont rejetés avec `max_channels_reac` lorsque la limite est atteinte.
`options_interval`	`integer` ou `nil`	Non	`nil`	Intervalle en secon pour les sondes de maintien de vie SIP OPTIONS. L'état du pair passe à `:down` les réponses OPTIO

Paramètre	Type	Requis	Par défaut	Description
				cessent. Définissez `nil` pour désactive

Pour la configuration de routage qui fait référence à ces pairs, voir Configuration de Routage. Pour le comportement de maintien de vie SIP OPTIONS et les états de santé des pairs, voir SIP Trunking.

MGCP / Média

`config :omnimsc, :mgcp` et `config :omnimsc, :media`

MGCP (Media Gateway Control Protocol, RFC 3435) est utilisé pour contrôler les passerelles multimédias pour la configuration du chemin de transport. L'MSC agit en tant qu'Agent d'Appel MGCP, émettant des commandes CRCX, MDCX et DLCX aux passerelles. La clé `:media` sélectionne quel protocole de contrôle multimédia utiliser.

```
config :omnimsc, :mgcp,
  listen_port: 2727,
  gateways: [
    %{name: "MGW-01", address: "10.1.1.50", port: 2427, domain:
"mgw"}
  ]

config :omnimsc, :media,
  gateway: "MGW-01",
  mode: :mgcp
```

Paramètres MGCP

Paramètre	Type	Requis	Par défaut	Description
`listen_port`	`integer`	Non	`2727`	Port UDP local pour l'Agent d'Appel MGCP (RFC 3435 Sec 2.2). Définissez sur `0` pour désactiver le transport MGCP (par exemple, en test).
`gateways`	`list(map)`	Non	`[]`	Liste des passerelles multimédias gérées.

Paramètres de Passerelle

Paramètre	Type	Requis	Par défaut	Description
`name`	`string`	Oui	--	Identifiant logique de la passerelle utilisé pour les recherches et l'affichage dans le panneau de contrôle.
`address`	`string`	Oui	--	Adresse IP de la passerelle multimédia.
`port`	`integer`	Non	`2427`	Port MGCP sur la passerelle.
`domain`	`string`	Oui	--	Nom de domaine de la passerelle utilisé dans la nomination des points de terminaison (par exemple, `aaln/1@mgw`). Requis — il n'y a pas de valeur par défaut.
`endpoints`	`list`	Non	`[]`	Identifiants de points de terminaison pré-déclarés sur la passerelle.
`max_connections`	`integer`	Non	`1000`	Nombre maximum de connexions simultanées que l'MSC placera sur cette passerelle.

Mode Média

Paramètre	Type	Requis	Par défaut	Description
`gateway`	`string`	Non	`"MGW-01"`	Nom de la passerelle par défaut (doit correspondre à un `name` de passerelle dans la configuration MGCP ou Megaco).
`mode`	`atom`	Non	`:megaco`	Protocole de contrôle multimédia : `:mgcp` pour RFC 3435 ou `:megaco` pour ITU-T H.248. La valeur par défaut intégrée lorsqu'elle n'est pas définie est `:megaco`; le fichier `config.exs` expédié définit explicitement `:mgcp`.

Transport Megaco

`config :omnimsc, :megaco`

Utilisé lorsque le `:media` `mode` est `:megaco` (ITU-T H.248).

Paramètre	Type	Requis	Par défaut	Description
`listen_port`	`integer`	Non	`2944`	Port UDP local pour le Contrôleur de Passerelle Multimédia Megaco/H.248.

SMSc

`config :omnimsc, :smsc`

Configure l'adresse du Centre de Services de Messages Courts pour les opérations MAP MT-ForwardSM et MO-ForwardSM.

```
config :omnimsc, :smsc,
  address: "14155550300"
```

Paramètre	Type	Requis	Par défaut	Description
`address`	`string`	Oui	--	Titre global SMSc (numéro E.164) pour le routage MAP.

CDR

`config :omnimsc, :cdr`

Les enregistrements CDR sont générés par le Collecteur CDR selon 3GPP TS 32.250 et écrits dans des fichiers au format ASN.1 BER (3GPP TS 32.298) par le Rédacteur CDR. La nomenclature des fichiers suit le modèle `<NodeID>_<YYYYMMDD>_<HHMMSS>_<SeqNum>.dat`.

```
config :omnimsc, :cdr,
  output_dir: "/var/cdr/omnimsc",
  max_file_size: 10_000_000,
  max_records: 100_000,
  rotation_interval: 3600
```

Paramètre	Type	Requis	Par défaut	Desc
`output_dir`	`string`	Oui	`"/tmp/omnimsc/cdr"`	Répertoi les fichie sortie CD être acce écriture processu Créé automati s'il n'exis
`max_file_size`	`integer`	Non	`10,000,000`	Taille ma fichier CI octets (e Mo). Un fichier es lorsque c est dépa
`max_records`	`integer`	Non	`100,000`	Nombre d'enregis CDR par
`rotation_interval`	`integer`	Non	`3600`	Intervalle rotation basé sur en secon nouveau CDR est après ce période, indépend de la tail nombre d'enregis

Routes

`config :omnimsc, :routes`

Définit des règles de routage basées sur des préfixes qui mappent les préfixes de numéros composés aux destinations. La table de routage utilise le match de préfixe le plus long avec la priorité comme critère de départage.

```
config :omnimsc, :routes, [
  %{prefix: "000", type: :sip, peer: "Default-GW", priority: 100},
  %{prefix: "04", type: :local, priority: 50},
  %{prefix: "02", type: :local, priority: 50},
  %{prefix: "001", type: :sip, peer: "International-GW", priority:
10},
  %{prefix: "", type: :sip, peer: "Default-GW", priority: 1}
]
```

Paramètre	Type	Requis	Par défaut	Description
`prefix`	`string`	Oui	--	Préfixe de numéro à faire correspondre. La chaîne vide `""` agit comme une route par défaut catch-all.
`type`	`atom`	Oui	--	Type de destination : `:local`, `:sip`, `:isup`, `:transit`, `:gmsc`, `:sip_i`, ou `:sip_with_failover`.
`priority`	`integer`	Non	`10`	Priorité de la route. Des valeurs plus élevées ont la priorité lorsque plusieurs routes correspondent au même préfixe.
`peer`	`string`	Conditionnel	--	Nom du pair SIP (requis lorsque `type` est `:sip`, `:sip_i`, ou `:sip_with_failover`). Doit correspondre à un `name` de pair dans la configuration SIP.
`trunk_group`	`string`	Conditionnel	--	Nom du groupe de troncs ISUP (requis lorsque `type` est `:isup`).
`point_code`	`[integer, integer,`	Conditionnel	`[0, 0, 0]`	Code de point de destination pour le

Paramètre	Type	Requis	Par défaut	Description
	`integer]`			routage ISUP.
`cic_range`	`{integer, integer}`	Non	`{1, 31}`	Plage inclusive de codes d'identification de circuit pour les troncs ISUP.
`transport`	`atom`	Non	`:udp`	Remplacement du transport SIP pour cette route.

Les routes peuvent également être gérées à l'exécution via l'API REST (`POST /routes`, `DELETE /routes`) et l'interface Web. Pour des exemples de routage détaillés, voir Configuration de Routage.

Informations MM

`config :omnimsc, :mm_info`

Contrôle le message d'INFORMATION MM envoyé à la station mobile après Acceptation de la Mise à Jour de Localisation (3GPP TS 24.008 section 9.2.15a). Contient le nom du réseau, l'heure et le fuseau horaire.

```
config :omnimsc, :mm_info,
  network_name: "Omnitouch",
  short_name: "OT",
  timezone_offset: 0
```

Paramètre	Type	Requis	Par défaut	Description
`network_name`	`string`	Non	`"Omnitouch"`	Nom complet du réseau affiché sur le terminal. Codé dans l'alphabet par défaut GSM 7 bits (3GPP TS 24.008 10.5.3.5a).
`short_name`	`string` ou `nil`	Non	`nil`	Nom court du réseau. Omis du message d'INFORMATION MM lorsque `nil`.
`timezone_offset`	`integer`	Non	`0`	Décalage UTC en quarts d'heure. Par exemple, UTC+5:30 (Inde) est `22`, UTC-5 (US Eastern) est `-20`. Codé en BCD selon 3GPP TS 24.008 10.5.3.8.

Pool MSC

`config :omnimsc, :pool`

Configure l'opération MSC-in-Pool selon 3GPP TS 23.236. Le mode pool permet à plusieurs instances d'MSC de partager des BSC via A-Flex, fournissant une

distribution de charge et une résilience.

```
config :omnimsc, :pool,
  enabled: true,
  pool_id: "POOL-01",
  nri_bitlength: 10,
  nri_values: [1, 2],
  members: [
    %{name: "MSC-02", nri_values: [3, 4], address: "10.1.1.2",
port: 2905},
    %{name: "MSC-03", nri_values: [5, 6], address: "10.1.1.3",
port: 2905}
  ]
```

Paramètre	Type	Requis	Par défaut	Description
`enabled`	`boolean`	Non	`false`	Indique s'il faut activer l'opération de pool MSC. Lorsque `false`, l'MSC fonctionne en mode autonome.
`pool_id`	`string`	Conditionnel	`nil`	Identifiant de la zone de pool. Requis lorsque `enabled` est `true`.
`nri_bitlength`	`integer`	Non	`10`	Nombre de bits pour le champ d'identifiant de ressource réseau extrait du TMSI. Doit être identique pour tous les membres du pool.
`nri_values`	`list(integer)`	Conditionnel	`[]`	Valeurs NRI possédées par cette

Paramètre	Type	Requis	Par défaut	Description
				instance d'MSC. Ne doit pas chevaucher d'autres membres du pool. Requis lorsque `enabled` est `true`.
`null_nri`	`integer`	Non	`0`	Valeur NRI indiquant un TMSI non attribué. Déclenche le reroutage basé sur NRI vers le membre de pool correct.
`members`	`list(map)`	Non	`[]`	Autres instances d'MSC dans le pool. Chaque membre a `name`, `nri_values`, `address`, et `port`.

Pour des détails sur l'architecture du pool et la disposition des bits NRI, voir Pool MSC & NRI.

Surcharge

`config :omnimsc, Omnimsc.Overload`

Seuils de protection contre la surcharge. Lorsque l'un des seuils est dépassé, les nouvelles demandes de service (appels, pagination, mises à jour de localisation) sont rejetées avec la cause GSM 42 (congestion de l'équipement de commutation). La fonction `admit?/0` fournit des lectures sans verrou via `persistent_term` pour un surcoût minimal dans le chemin chaud.

```
config :omnimsc, Omnimsc.Overload,
  max_calls: 10_000,
  max_subscribers: 50_000,
  max_process_count: 500_000,
  max_paging_rate: 1_000,
  check_interval: 5_000
```

Paramètre	Type	Requis	Par défaut	Description
`max_calls`	`integer`	Non	`10,000`	Nombre maximum d'appels actifs simultanés avant d'entrer dans l'état de surcharge.
`max_subscribers`	`integer`	Non	`50,000`	Nombre maximum d'abonnés enregistrés VLR avant surcharge.
`max_process_count`	`integer`	Non	`500,000`	Nombre maximum de processus VM BEAM avant surcharge. Surveille la pression totale des processus VM.
`max_paging_rate`	`integer`	Non	`1,000`	Nombre maximum de demandes de pagination par seconde avant surcharge.
`check_interval`	`integer`	Non	`5,000`	Intervalle en millisecondes entre les vérifications de seuil de surcharge.

Les transitions d'état de surcharge émettent des événements de télémétrie `[:omnimsc, :overload, :state_change]` pour la surveillance externe. Voir Référence des Métriques.

SGs / CSFB

`config :omnimsc, :sgs`

Configure l'interface SGs-AP pour le Circuit-Switched Fallback (CSFB) et les SMS sur SGs avec des MME LTE selon 3GPP TS 29.118.

```
config :omnimsc, :sgs,
  listen_port: 29118,
  vlr_name: "vlr.omnimsc.local"
```

Paramètre	Type	Requis	Par défaut	Description
`listen_port`	`integer`	Non	`29118`	Port d'écoute SCTP pour les connexions SGs-AP des MME. Le port 29118 est le défaut attribué par 3GPP. Définissez sur `0` pour désactiver SGs.
`vlr_name`	`string`	Non	`"vlr.omnimsc.local"`	Nom VLR (FQDN) envoyé aux MME dans l'Acceptation de Mise à Jour de Localisation SGs-AP. Le MME utilise cela pour identifier et router vers cette instance VLR.

Pour des détails sur le protocole SGs, les états d'association et les flux d'appels CSFB, voir SGs / CSFB.

USSD

`config :omnimsc, :ussd`

Configure les passerelles USSD externes pour le routage des demandes de données de service supplémentaires non structurées. Chaque passerelle gère des codes de service USSD spécifiques (par exemple, `*100#` pour le solde). Une passerelle avec `codes: :all` agit comme le fallback par défaut pour les codes non appariés.

```
config :omnimsc, :ussd,
  gateways: [
    %{name: "Balance", address: "14155550300", ssn: 147, codes:
["*100"]},
    %{name: "Recharge", address: "14155550301", ssn: 147, codes:
["*123"]},
    %{name: "Default", address: "14155550302", ssn: 147, codes:
:all}
  ]
```

Paramètres de Passerelle USSD

Chaque passerelle dans la liste `gateways` accepte les éléments suivants :

Paramètre	Type	Requis	Par défaut	Description
`name`	`string`	Non	`"unnamed"`	Nom logique de la passerelle pour la journalisation et l'affichage dans le panneau de contrôle.
`address`	`string`	Oui	--	Titre global de la passerelle (numéro E.164) pour le routage USSD MAP.
`ssn`	`integer`	Non	`147`	Numéro de sous-système SCCP pour la passerelle. Le SSN 147 est le SSN USSD standard.
`codes`	`list(string)` ou `:all`	Non	`:all`	Codes de service USSD gérés par cette passerelle (par exemple, `["*100", "*101"]`). Définissez sur `:all` pour une passerelle par défaut catch-all.

Pour des détails sur le protocole USSD et le comportement de relais, voir USSD.

Urgence

`config :omnimsc, Omnimsc.Emergency`

Configure la détection des numéros d'urgence, la classification des catégories de service et le routage PSAP selon 3GPP TS 22.101.

Les messages de configuration d'urgence (3GPP TS 24.008 §9.3.8) ne portent pas d'IE Numéro BCD de Partie Appelée — contrairement à la configuration CC régulière, le terminal n'inclut pas les chiffres composés. OmniMSC utilise l'adresse `psap_address` configurée comme numéro appelé pour la recherche dans la table de routage et l'URI de requête SIP sortante. Cette valeur doit correspondre à un préfixe dans la table de routage afin que l'appel puisse être routé vers le pair SIP ou le tronc approprié.

```
config :omnimsc, Omnimsc.Emergency,
  numbers: ["112", "911", "999", "000", "110", "119"],
  psap_address: "000",
  allow_without_sim: true
```

Paramètre	Type	Requis	Par défaut	Description
`numbers`	`list(string)`	Non	`["112", "911", "999", "000", "110", "119"]`	Numéros d'urgence reconnus. Les appels à ces numéros contournent l'authentificatio le chiffrement e l'interdiction d'appels.
`psap_address`	`string`	Non	`"112"`	Numéro appelé utilisé pour le routage des appels d'urgence. Étan donné que les messages de configuration d'urgence ne portent aucun numéro appelé, cette valeur est utilisée comme partie appelée pour la recherche dans la table de routage et le tronc sortant (URI de requête SIP INVITE ou numéro de parti appelée ISUP

Paramètre	Type	Requis	Par défaut	Description
				IAM). Définissez ceci sur un numéro qui correspond à un préfixe de route d'urgence dans la table de routage.
`allow_without_sim`	`boolean`	Non	`true`	Indique s'il faut autoriser les appels d'urgenc depuis des stations mobiles sans SIM insérée (IMSI absent). Selon 3GPP TS 22.101, les réseaux devraient permettre cela.

Noeud & Exécution

Clés de niveau supérieur `config :omnimsc` qui contrôlent l'identité du nœud et l'arbre de supervision.

```
config :omnimsc,
  node_id: "OMNIMSC01",
  point_code: 500,
  max_restarts: 3,
  overload_monitor: true
```

Paramètre	Type	Requis	Par défaut	Description
`node_id`	`string`	Non	`"OMNIMSC01"`	Identifiant du nœud utilisé dans `recording_entity` CDR, noms de fichiers CDR et état du système.
`point_code`	`integer`	Non	`500`	Code de point SS7 local utilisé comme `local_msc_id` du collecteur CDR.
`max_restarts`	`integer`	Non	`3`	Nombre maximum de redémarrages du superviseur de niveau supérieur dans sa fenêtre de redémarrage avant que le nœud ne s'arrête.
`overload_monitor`	`boolean`	Non	`true`	Indique s'il faut démarrer le moniteur périodique de surcharge/nombre de processus. Définissez sur `false` en test.

Pagination

`config :omnimsc, :paging`

Contrôle le comportement de réessai de pagination pour les procédures terminées par mobile.

```
config :omnimsc, :paging,
  max_retries: 2,
  retry_interval_ms: 5_000
```

Paramètre	Type	Requis	Par défaut	Description
`max_retries`	`integer`	Non	`2`	Nombre de retransmissions de pagination avant d'abandonner une demande terminée par mobile.
`retry_interval_ms`	`integer`	Non	`5_000`	Intervalle en millisecondes entre les retransmissions de pagination.

EIR

`config :omnimsc, :eir`

Configure la vérification IMEI du Registre d'Identité de l'Équipement.

```
config :omnimsc, :eir,
  enabled: false,
  check_on: [:location_updating, :cm_service_request],
  backend: Omnimsc.EIR.Backend.Default
```

Paramètre	Type	Requis	Par défaut	De
`enabled`	`boolean`	Non	`false`	Ind vér IME effe Lor `fal` l'éc est con éta list bla
`check_on`	`list(atom)`	Non	`[:location_updating, :cm_service_request]`	Pro sur les une vér IME déc
`backend`	`module`	Non	`Omnimsc.EIR.Backend.Default`	Mo bac util rés sta

Transfert

`config :omnimsc, :handover`

Configure le pool de numéros de transfert utilisé pour le transfert inter-MSC.

```
config :omnimsc, :handover,
  ho_number_prefix: "8888",
  ho_number_count: 100
```

Paramètre	Type	Requis	Par défaut	Description
`ho_number_prefix`	`string`	Non	`"8888"`	Préfixe pour les num��ros de transfert attribués.
`ho_number_count`	`integer`	Non	`100`	Nombre de numéros de transfert dans le pool d'attribution.

SRVCC (Interface Sv)

`config :omnimsc, :srvcc`

Configure l'interface Sv (SRVCC GTPv2-C) pour la Continuité d'Appel Vocal sur Radio Unique.

```
config :omnimsc, :srvcc,
  sv_enabled: false,
  sv_port: 2123,
  local_ip: {0, 0, 0, 0}
```

Paramètre	Type	Requis	Par défaut	Description
`sv_enabled`	`boolean`	Non	`false`	Indique s'il faut démarrer le transport SRVCC Sv (GTPv2-C).
`sv_port`	`integer`	Non	`2123`	Port UDP pour l'interface Sv. Le port 2123 est le défaut GTP-C.
`local_ip`	`tuple`	Non	--	IP de liaison locale pour le transport Sv sous forme de tuple Erlang.

LCS

`config :omnimsc, :lcs`

Configure les Services de Localisation.

```
config :omnimsc, :lcs,
  default_location: {0.0, 0.0}
```

Paramètre	Type	Requis	Par défaut	Description
`default_location`	`{number, number}`	Non	`{0.0, 0.0}`	Fallback `{latitude, longitude}` en degrés décimaux retourné pour une correction basée sur une cellule lorsque aucun résultat SMLC précis n'est disponible.

Sécurité

`config :omnimsc, :security`

Configure l'interdiction en cas d'échec d'authentification.

```
config :omnimsc, :security,
  auth_failure_threshold: 3
```

Paramètre	Type	Requis	Par défaut	Description
`auth_failure_threshold`	`integer`	Non	`3`	Nombre d'échecs d'authentification consécutifs après lesquels un abonné est interdit.

Routage (Analyse de Numéro)

`config :omnimsc, :routing`

Configure l'analyse de numéro pour la gestion des préfixes nationaux/internationaux et la détection d'urgence. Ceci est distinct de la table de routage basée sur les préfixes (`:routes`).

```
config :omnimsc, :routing,
  international_prefix: "00",
  national_prefix: "0",
  emergency_numbers: ["112", "911", "110"],
  country_code: "",
  area_code: "",
  short_codes: []
```

Paramètre	Type	Requis	Par défaut	Descriptio
`international_prefix`	`string`	Non	`"00"`	Préfixe de composition indiquant un numéro international
`national_prefix`	`string`	Non	`"0"`	Préfixe de composition indiquant un numéro national (tronc).
`emergency_numbers`	`list(string)`	Non	`["112", "911", "110"]`	Numéros classés comme d'urgence pa l'analyse de numéro.
`country_code`	`string`	Non	`""`	Code de pay préfixé lors d la normalisatio des numéros nationaux en E.164.
`area_code`	`string`	Non	`""`	Code de zon utilisé lors d la normalisatio des numéros

Paramètre	Type	Requis	Par défaut	Descriptio
				locaux d'abonnés.
`short_codes`	`list`	Non	`[]`	Entrées de code court sous forme d tuples `{code destination`

SCCP

`config :omnimsc, :sccp`

```
config :omnimsc, :sccp,
  local_subsystems: [7, 8]
```

Paramètre	Type	Requis	Par défaut	Description
`local_subsystems`	`list(integer)`	Non	`[7, 8]`	Numéros de sous-système SCCP que ce nœud héberge localement (utilisé par la gestion SCCP pour le traitement SSA/SSP).

CAMEL

Clés de niveau supérieur `config :omnimsc` pour le déclenchement de service CAMEL (Applications Personnalisées pour Réseaux Mobiles Logique Améliorée).

```
config :omnimsc, :camel_service_keys, %{}
config :omnimsc, :camel_default_scp_address, "14155550400"
config :omnimsc, :camel_timers, %{}
```

Paramètre	Type	Requis	Par défaut	Description
`camel_service_keys`	`map`	Non	`%{}`	Carte des clés de service CAMEL pour le remplacement d'adresses SCF
`camel_default_scp_address`	`string`	Non	--	Titre global gsmSCF (SCP) par défaut utilisé lorsqu'une clé de service n'a pas d'adresse explicite.
`camel_timers`	`map`	Non	`%{}`	Remplacement de temporisateurs CAMEL.

VLR Reaper

`config :omnimsc, :vlr_reaper`

Configure le nettoyeur périodique qui purge les enregistrements d'abonnés VLR obsolètes.

```
config :omnimsc, :vlr_reaper,
  scan_interval_ms: 60_000,
  notify_hlr: true,
  hlr: Omnimsc.VLR.HLR.Default
```

Paramètre	Type	Requis	Par défaut	Des
`scan_interval_ms`	`integer`	Non	`60_000`	Inte milli entr anal nett pour abor expi
`notify_hlr`	`boolean`	Non	`true`	Indi faut MAP MS a lors abor purg
`hlr`	`module`	Non	`Omnimsc.VLR.HLR.Default`	Ada HLR par nett pour Purg

SIP-I

`config :omnimsc, :sip_i`

Configure les pairs SIP-I (SIP avec ISUP encapsulé, ITU-T Q.1912.5) pour l'interconnexion inter-MSC et PSTN.

```
config :omnimsc, :sip_i,
  peers: [
    %{name: "InterMSC-01", address: "10.1.1.60", port: 5060,
      transport: :tcp, isup_version: :itu_t92,
      trunk_group_id: "TG-InterMSC-01", point_code: [3, 14, 5],
      codecs: [:pcmu, :pcma], max_channels: 100}
  ]
```

Chaque pair dans la liste `peers` accepte les éléments suivants :

Paramètre	Type	Requis	Par défaut	Description
`name`	`string`	Oui	--	Nom logique du pair. Référencé dans les entrées de la table de routage avec le type `:sip_i`.
`address`	`string`	Oui	--	Adresse IP ou nom d'hôte du pair.
`port`	`integer`	Non	`5060`	Port SIP du pair.
`transport`	`atom`	Non	`:tcp`	Transport pour ce pair : `:udp`, `:tcp`, ou `:tls`.
`isup_version`	`atom`	Non	`:itu_t92`	Variante ISUP transportée dans le corps encapsulé : `:itu_t92` ou `:ansi`.
`trunk_group_id`	`string` ou `nil`	Non	--	Identifiant de groupe de troncs utilisé pour le routage (par exemple, `"TG-InterMSC-01"`).

Paramètre	Type	Requis	Par défaut	Description
`point_code`	`[integer, integer, integer]` ou `integer` ou `nil`	Non	--	Code de point SS7 distant pour le contexte de routage ISUP.
`codecs`	`list(atom)`	Non	`[:pcmu, :pcma]`	Codecs audio pris en charge.
`max_channels`	`integer`	Non	`100`	Nombre maximum d'appels simultanés à ce pair.

Interface Web

`config :omnimsc, OmnimscWeb.Endpoint`

Le panneau de contrôle web est servi par un point de terminaison Phoenix avec LiveView. Il fournit des tableaux de bord en temps réel pour les abonnés, les appels, les connexions, le routage et les alarmes.

```
config :omnimsc, OmnimscWeb.Endpoint,
  http: [ip: {0, 0, 0, 0}, port: 4000],
  url: [host: "localhost"],
  secret_key_base: "generate-with-mix-phx-gen-secret",
  server: true,
  pubsub_server: Omnimsc.PubSub,
  live_view: [signing_salt: "oMnImScLv"]
```

Paramètre	Type	Requis	Par défaut	Des
`http.ip`	`tuple`	Non	`{0, 0, 0, 0}`	Adresse HTTP. U `{127, (` pour res localhos
`http.port`	`integer`	Non	`4000`	Port d'é pour le de cont
`url.host`	`string`	Non	`"localhost"`	Nom d'h la géné d'URL. D sur le n public e product
`secret_key_base`	`string`	Oui	--	Clé de s de sess Phoenix avec `mi` `phx.ger` Requis product partir d variable d'enviro `SECRET_`
`server`	`boolean`	Non	`true`	Indique démarr serveur Définiss `false` p désacti

Paramètre	Type	Requis	Par défaut	Des
				pannea contrôle
`check_origin`	`boolean`	Non	`true` (prod)	Indique vérifier têtes d' WebSoc Définiss `false` e dévelop
`pubsub_server`	`atom`	Non	`Omnimsc.PubSub`	Nom du PubSub diffusio LiveVie
`live_view.signing_salt`	`string`	Non	`"oMnImScLv"`	Sel de s de sess LiveVie

Remplacement à l'exécution : Définissez les variables d'environnement `SECRET_KEY_BASE`, `PHX_HOST`, et `PORT`. En production, HTTPS avec le port 443 est configuré automatiquement.

API REST

`config :api_ex`

L'API REST est servie par api_ex sur un port séparé, fournissant un accès programmatique aux abonnés, appels, routes, pairs SIP, connexions et état du système.

```
config :api_ex,
  api: %{
    port: 8444,
    listen_ip: "0.0.0.0",
    product_name: "Omnitouch MSC",
    title: "API - Omnitouch MSC",
    hostname: "localhost",
    enable_tls: false
  }
```

Paramètre	Type	Requis	Par défaut	Description
`port`	`integer`	Non	`8444`	Port d'écoute HTTP pour l'API REST.
`listen_ip`	`string`	Non	`"0.0.0.0"`	Adresse IP de liaison pour l'écouteur API.
`product_name`	`string`	Non	`"Omnitouch MSC"`	Nom du produit affiché dans l'interface Swagger.
`title`	`string`	Non	`"API - Omnitouch MSC"`	Titre de la page pour l'interface Swagger.
`hostname`	`string`	Non	`"localhost"`	Nom d'hôte pour la génération d'URL API.
`enable_tls`	`boolean`	Non	`false`	Indique s'il faut activer TLS pour le point de terminaison API.

Points de terminaison API Disponibles

Chemin	Méthodes	Description
`GET /subscribers`	GET, DELETE	Lister ou supprimer des abonnés VLR.
`POST /subscribers/:id/actions`	POST	Déclencher des actions d'abonné (pagination, détachement).
`GET /calls`	GET, DELETE	Lister ou libérer des appels actifs.
`GET /sms`	GET	Lister les transactions SMS.
`GET /routes`	GET, POST, DELETE	Gérer la table de routage.
`GET /routes/lookup`	GET	Rechercher une route par numéro composé.
`GET /sip/peers`	GET, PATCH	Lister ou mettre à jour la configuration des pairs SIP.
`GET /mgw`	GET	Lister l'état de la passerelle multimédia.
`GET /ran/connections`	GET	Lister les connexions RAN (interface A) actives.
`GET /ran/bscs`	GET	Lister les BSC connectés.
`GET /stp`	GET	Afficher l'état de connexion STP.

Chemin	Méthodes	Description
`GET /health`	GET	Vérification de la santé du système.
`GET /status`	GET	Résumé de l'état du système.
`POST /paging`	POST	Déclencher une demande de pagination.
`POST /silent`	POST	Initier un appel silencieux ou un SMS silencieux.

Exemple Complet de Configuration

de Production

```
# config/runtime.exs
import Config

config :omnimsc, :msc,
    point_code: 500,
    global_title: "14155550100",
    name: "OMNIMSC01",
    msc_number: "14155550100",
    vlr_number: "14155550100",
    mcc: 999,
    mnc: 99,
    lac: 0x1092,
    allowed_a5: [:a5_1, :a5_3]

config :omnimsc, :hlr,
  address: "14155550200",
  point_code: [3, 14, 2]

config :omnimsc, :vlr,
  hlr_adapter: Omnimsc.VLR.HLR.Live,
  auth_required: true,
  tmsi_realloc: true,
  num_auth_vectors: 1

config :omnimsc, :m3ua_asp,
  enabled: true,
  local_ip: {10, 5, 198, 200},
  local_port: 0,
  remote_ip: {10, 179, 4, 10},
  remote_port: 2905,
  routing_context: 10,
  receive_watchdog: true,
  receive_watchdog_idle: 15

config :omnimsc, :sip,
  signaling_address: "10.5.198.200",
  listen_ip: {0, 0, 0, 0},
  listen_port: 5060,
  transport: :udp,
  peers: [
```

```
    [name: "Default-GW", address: "10.1.1.50", port: 5060,
     transport: :udp, codecs: [:pcmu, :pcma],
     max_channels: 100, options_interval: 60],
    [name: "International-GW", address: "10.1.1.51", port: 5062,
     transport: :udp, codecs: [:pcmu, :pcma, :amr, :amr_wb],
     max_channels: 500]
  ]

config :omnimsc, :mgcp,
  listen_port: 2727,
  gateways: [
    %{name: "MGW-01", address: "10.1.1.50", port: 2427, domain:
"mgw"}
  ]

config :omnimsc, :media,
  gateway: "MGW-01",
  mode: :mgcp

config :omnimsc, :smsc,
  address: "14155550300"

config :omnimsc, :cdr,
  output_dir: "/var/cdr/omnimsc",
  max_file_size: 10_000_000,
  max_records: 100_000,
  rotation_interval: 3600

config :omnimsc, :routes, [
  %{prefix: "000", type: :sip, peer: "Default-GW", priority: 100},
  %{prefix: "04", type: :local, priority: 50},
  %{prefix: "02", type: :local, priority: 50},
  %{prefix: "001", type: :sip, peer: "International-GW", priority:
10},
  %{prefix: "", type: :sip, peer: "Default-GW", priority: 1}
]

config :omnimsc, :mm_info,
  network_name: "Omnitouch",
  short_name: "OT",
  timezone_offset: 0

config :omnimsc, Omnimsc.Overload,
  max_calls: 10_000,
```

```
  max_subscribers: 50_000,
  max_process_count: 500_000,
  max_paging_rate: 1_000,
  check_interval: 5_000

config :omnimsc, Omnimsc.Emergency,
  numbers: ["112", "911", "999", "000", "110", "119"],
  psap_address: "000",
  allow_without_sim: true

config :omnimsc, :sgs,
  listen_port: 29118,
  vlr_name: "vlr.omnimsc.local"

config :omnimsc, :ussd,
gateways: []

config :omnimsc, :pool,
enabled: false
```

Panneau de Contrôle

Ce document décrit le panneau de contrôle basé sur le web d'OmniMSC, une interface de surveillance et de gestion en temps réel construite avec Phoenix LiveView. Le panneau de contrôle est accessible à `http://<host>:4000` et fournit une visibilité en direct sur les abonnés, les appels, les connexions, le routage, les CDR et la santé du système.

Toutes les pages se rafraîchissent automatiquement via WebSocket. La plupart des pages se rafraîchissent toutes les 5 secondes ; la page des Appels Actifs se rafraîchit toutes les 2 secondes. Aucun rechargement manuel de la page n'est requis. Le commutateur de rafraîchissement automatique sur chaque page permet de mettre en pause les mises à jour lors de l'inspection d'un enregistrement particulier.

Pour la configuration des points de terminaison (adresse de liaison, port), voir Référence de Configuration. Pour l'API REST, voir Référence API.

Tableau de Bord

Le tableau de bord est la page d'accueil principale, fournissant un résumé instantané de l'ensemble du MSC.

Cartes de Résumé

La rangée supérieure affiche six compteurs en temps réel :

Carte	Description
Abonnés	Nombre d'abonnés actuellement enregistrés dans le VLR
Appels Actifs	Nombre de transactions d'appels CC FSM actifs
SMS Actifs	Nombre de transactions SMS en cours
Connexions RAN	Nombre de BSC et RNC avec des associations SCTP ÉTABLIES
État du Lien STP	État ASP M3UA vers le STP (ACTIF, INACTIF, HORS SERVICE)
Temps de Fonctionnement du Système	Temps écoulé depuis le démarrage de l'application

Tableau des Liens SS7

Affiche l'état de tous les liens de signalisation SS7 configurés, y compris l'état ASP M3UA et le mode de trafic.

Tableau des BSC Connus

Liste chaque BSC par nom, code de point, nombre de cellules et état d'association SCTP.

Tableau des Pairs SIP

Colonne	Description
Nom	Nom logique du pair
Adresse	Adresse IP du pair et port SIP
Appels	Nombre actuel d'appels actifs sur ce pair
État	Badge d'état de santé (Actif, Inactif, Inconnu)

Tableau des Passerelles Médias

Liste les passerelles médias configurées avec nom, adresse, protocole (MGCP ou Megaco) et état de connectivité.

Fil d'Événements Récents

Un fil défilant des événements de télémétrie les plus récents, chacun étiqueté avec un badge de type d'événement (APPEL, LU, PAIRES, INFO) et un horodatage UTC. Les événements sont poussés en temps réel au fur et à mesure qu'ils se produisent.

Abonnés

La page Abonnés fournit une liste consultable de tous les enregistrements d'abonnés VLR. Entrez un IMSI ou un MSISDN (correspondance partielle supportée) dans la boîte de recherche pour filtrer la liste en temps réel.

Colonnes de la Liste des Abonnés

Colonne	Description
IMSI	Identité Internationale de l'Abonné Mobile
MSISDN	Numéro ISDN de la Station Mobile
TMSI	Identité Mobile Abonné Temporaire allouée par le VLR
LAC	Code de Zone de Localisation de la cellule actuelle de l'abonné
État	État d'enregistrement VLR
Auth	État d'authentification
LU	État de complétion de la Mise à Jour de Localisation

Détails des Abonnés Dépliables

Cliquer sur une ligne d'abonné développe une vue détaillée organisée en sections suivantes.

Identité

Champ	Description
IMSI	Identité Internationale de l'Abonné Mobile
MSISDN	Numéro ISDN de la Station Mobile
TMSI	Identité Mobile Abonné Temporaire
IMEI	Identité Internationale de l'Équipement Mobile (si disponible)
Numéro HLR	Adresse du HLR d'origine de l'abonné

Localisation et État

Champ	Description
LAC	Code de Zone de Localisation
CI	Identité de Cellule
BSC Servant	Nom de la BSC servant actuellement cet abonné
Type RAN	Type d'accès radio (GERAN-A, UTRAN-Iu, ou SGs)
Compte d'Utilisation	Nombre de jetons de compte d'utilisation actifs détenus par le MSC-A de cet abonné
Expire	Horodatage d'expiration de l'enregistrement VLR
État	État actuel de l'abonné dans le VLR
Roaming	Si l'abonné est marqué comme en itinérance
SGs	État d'association SGs (si enregistré via MME pour CSFB)

Authentification

Champ	Description
Algorithme	Algorithme d'authentification en cours d'utilisation (COMP128v1, COMP128v3, Milenage)
Tuples	Nombre de triplets d'authentification restants
Quintuplet UMTS	Si les quintuplets d'authentification UMTS sont disponibles

Profil de Service

Affiche les services commutés par circuit reçus du HLR via MAP Insert Subscriber Data, y compris les abonnements de service de support et de téléservice.

Services Supplémentaires

Liste tous les services supplémentaires provisionnés avec des badges d'état :

Service	Description
BAOC	Interdiction de Tous les Appels Sortants
BOIC	Interdiction des Appels Internationaux Sortants
BOIC-exHC	Interdiction des Appels Internationaux Sortants sauf vers le Pays d'Origine
BAIC	Interdiction de Tous les Appels Entrants
BIC-Roam	Interdiction des Appels Entrants lors de l'Itinérance
CFU	Transfert d'Appel Inconditionnel
CFB	Transfert d'Appel en Cas d'Occupation
CFNRy	Transfert d'Appel en Cas de Non-Réponse
CFNRc	Transfert d'Appel en Cas de Non Joignable
CW	Attente d'Appel
HOLD	Mise en Attente d'Appel
MPTY	Multi-Parti
CLIP	Présentation de l'Identification de la Ligne Appelante
CLIR	Restriction de l'Identification de la Ligne Appelante

Chaque service affiche un badge d'état actif/inactif et, le cas échéant, le numéro de transfert et les paramètres de condition.

Connexion MSC-A

Affiche l'état actuel de la FSM MSC-A pour toute connexion active associée à cet abonné, y compris le nom de l'état, le nombre de jetons de compte

d'utilisation actifs et le temps écoulé dans l'état.

Connexions

La page Connexions fournit une visibilité sur tous les liens de signalisation, les connexions RAN et les pairs SIP.

Lien STP (M3UA ASP)

Champ	Description
IP Locale	Adresse de liaison SCTP locale
Distant	Adresse et port STP distant
ID d'Association	Identifiant d'association SCTP
État	Badge d'état ASP M3UA (ACTIF, INACTIF, HORS SERVICE)

Tout le transport de signalisation utilise SCTP (Stream Control Transmission Protocol) pour une livraison fiable et multi-homée selon la RFC 4960.

BSC Connus

Colonne	Description
Code de Point	Code de point SS7 BSC
Titre Global	Adresse de titre global BSC (si configurée)
Dernière Réinitialisation	Horodatage de l'échange RESET BSSMAP le plus récent avec ce BSC

Pairs SIP

Colonne	Description
Nom	Nom logique du pair
Adresse	Adresse IP du pair et port SIP
Transport	Protocole en cours d'utilisation (UDP, TCP, ou TLS)
Appels Actifs	Nombre actuel d'appels actifs vers ce pair
Capacité	Nombre maximum de canaux concurrents configurés pour ce pair
Dernières OPTIONS	Horodatage de la dernière réponse OPTIONS keepalive réussie
État	Badge d'état de santé (Actif, Inactif, Inconnu)

Appels Actifs

La page Appels Actifs affiche un tableau en direct de toutes les transactions d'appels CC FSM actuellement en cours.

Colonnes du Tableau des Appels

Colonne	Description
Réf d'Appel	Numéro de référence d'appel unique
Direction	Badge MO (Mobile Originate) ou MT (Mobile Terminate)
IMSI	IMSI de l'abonné
Appelant	Numéro de la partie appelante (A-number)
Appelé	Numéro de la partie appelée (B-number)
État	État CC FSM avec badge codé par couleur
Durée	Temps écoulé depuis la saisie de l'appel
Codec	Codec de parole négocié
BSC/RNC	Nom de la BSC ou RNC servant

Détails d'Appel Dépliables

Cliquer sur une ligne d'appel développe une vue détaillée avec deux panneaux.

Détails de l'Appel

Champ	Description
Réf d'Appel	Référence d'appel unique
Direction	MO ou MT
État CC FSM	État actuel de la machine à états finis de contrôle d'appel
IMSI	IMSI de l'abonné
MSISDN	Numéro de téléphone de l'abonné
IMEI	Identité de l'équipement mobile
Partie Appelante	A-number tel que présenté sur l'interface de signalisation
Partie Appelée	B-number tel que présenté sur l'interface de signalisation

Timing et Ressources

Champ	Description
Durée	Durée d'appel écoulée
Temps de Saisie	Horodatage UTC du début de la configuration de l'appel
Temps de Réponse	Horodatage UTC de la réponse à l'appel (vide si pas encore répondu)
Service de Base	Service de support ou téléservice associé à l'appel
Minuteur CC Actif	Minuteur de protocole CC actuellement en cours (le cas échéant)
BSC/RNC	Nom de la BSC ou RNC servant gérant le côté radio

Routes et Trunks

La page Routes et Trunks fournit trois vues par onglets pour gérer la configuration de routage des appels en temps réel.

Onglet Tableau des Routes

Affiche toutes les règles de routage basées sur les préfixes avec filtrage de recherche par préfixe ou type de destination.

Colonne	Description
Préfixe	Préfixe numérique (une chaîne vide indique la route par défaut catch-all)
Type de Destination	Badge indiquant le type de route : EMRG, SIP, SIP+FO, LOCAL, ISUP, TRANSIT, GMSC
Détails	Informations spécifiques à la destination telles que le nom du pair ou le groupe de trunks
Priorité	Valeur de priorité numérique (des valeurs plus élevées ont la priorité)
Actions	Boutons Modifier et Supprimer pour chaque route

Le bouton **Ajouter une Route** ouvre un formulaire modal supportant tous les types de destination. Les modifications de route prennent effet immédiatement sans nécessiter un redémarrage.

Pour des concepts de routage détaillés et la configuration, voir Configuration de Routage.

Onglet des Trunks ISUP

Affiche les groupes de trunks ISUP configurés avec disponibilité des circuits et comptes d'appels.

Onglet des Pairs SIP

Affiche l'état des pairs SIP avec adresse, transport, support de codec, capacité de canal et comptes d'appels actifs.

SMS

La page SMS liste tous les FSM de transactions SMS actifs, montrant l'ID de transaction, l'IMSI de l'abonné, la direction (MO ou MT), l'état de la transaction et l'adresse du Centre SMS. Les transactions complètes sont automatiquement supprimées de la liste.

CDRs

La page Statistiques CDR fournit une visibilité sur le sous-système des Enregistrements de Données de Chargement.

Compteurs de Résumé

Compteur	Description
Enregistrements dans le Fichier	Nombre d'enregistrements CDR écrits dans le fichier de sortie actuel
En Attente dans le Tampon	Nombre d'enregistrements CDR mis en mémoire en attente du prochain cycle d'écriture
Appels Actifs Suivis	Nombre d'appels avec des enregistrements CDR ouverts (pas encore finalisés)

État de l'Écrivain

Champ	Description
Chemin de Fichier Actuel	Chemin du système de fichiers du fichier de sortie CDR actif
Enregistrements Écrits	Total des enregistrements écrits dans le fichier actuel
Tampon en Attente	Enregistrements en file d'attente dans le tampon d'écriture

Numéros de Séquence

Les compteurs de séquence par type d'enregistrement suivent le numéro de séquence croissant monotoniquement pour chaque catégorie de CDR :

Type d'Enregistrement	Description
LU HLR	Mise à Jour de Localisation vers HLR
LU VLR	Mise à Jour de Localisation dans VLR
Appel MO	Appel vocal Mobile Originate
Appel MT	Appel vocal Mobile Terminate
SMS MO	Message court Mobile Originate
SMS MT	Message court Mobile Terminate
Itinérance	Enregistrements d'événements d'itinérance

Pool

La page Pool est accessible lorsque le mode pool MSC est activé. Elle affiche l'état de tous les membres du pool MSC, y compris le nom du membre, le code de point, la plage NRI, l'état de santé (Actif, Inactif ou Vidange), et l'horodatage de la dernière sonde de santé réussie. Un graphique de distribution des abonnés montre l'allocation NRI à travers les membres du pool.

Pour la configuration du pool et le routage basé sur NRI, voir Pool MSC et NRI.

Système

La page Système fournit des informations détaillées sur le BEAM VM, l'allocation de mémoire, l'identité du MSC, les liens de transport et la santé de l'arbre de supervision.

BEAM VM

Champ	Description
Version OTP	Version majeure d'Erlang/OTP
Processus	Nombre actuel de processus et limite configurée
Ports	Nombre de ports ouverts
Atomes	Taille de la table des atomes
Planificateurs	Nombre de planificateurs en ligne
Temps de Fonctionnement	Temps de fonctionnement du BEAM VM depuis le démarrage

Mémoire

Champ	Description
Total	Mémoire totale allouée par le BEAM VM
Processus	Mémoire consommée par les processus Erlang/Elixir
ETS	Mémoire consommée par les tables ETS
Binaire	Mémoire consommée par les données référencées par des binaires
Atome	Mémoire consommée par la table des atomes
Système	Mémoire consommée par le système d'exécution (non-processus)

Configuration MSC

Affiche les paramètres d'identité MSC actifs :

Champ	Description
Nom	Nom logique du MSC
Code de Point	Code de point SS7 local
Titre Global	Adresse de titre global MSC
A5 Autorisé	Algorithmes de chiffrement A5 autorisés pour GERAN

Transport SCTP

Champ	Description
Lien	Nom du lien de transport
IP Locale	Adresse de liaison SCTP locale
Distant	Adresse et port STP distant
État	Badge d'état d'association SCTP

Santé de l'Arbre de Supervision

Liste tous les enfants du superviseur OmniMSC de niveau supérieur (le compte est calculé dynamiquement), chacun affiché avec :

Champ	Description
PID	Identifiant de processus Erlang
Type	Type de processus (travailleur ou superviseur)
État	Badge de santé (En cours, Redémarrage, ou Arrêté)

Cette vue est utile pour vérifier que tous les sous-systèmes sont opérationnels après le démarrage ou suite à un événement de récupération de faute.

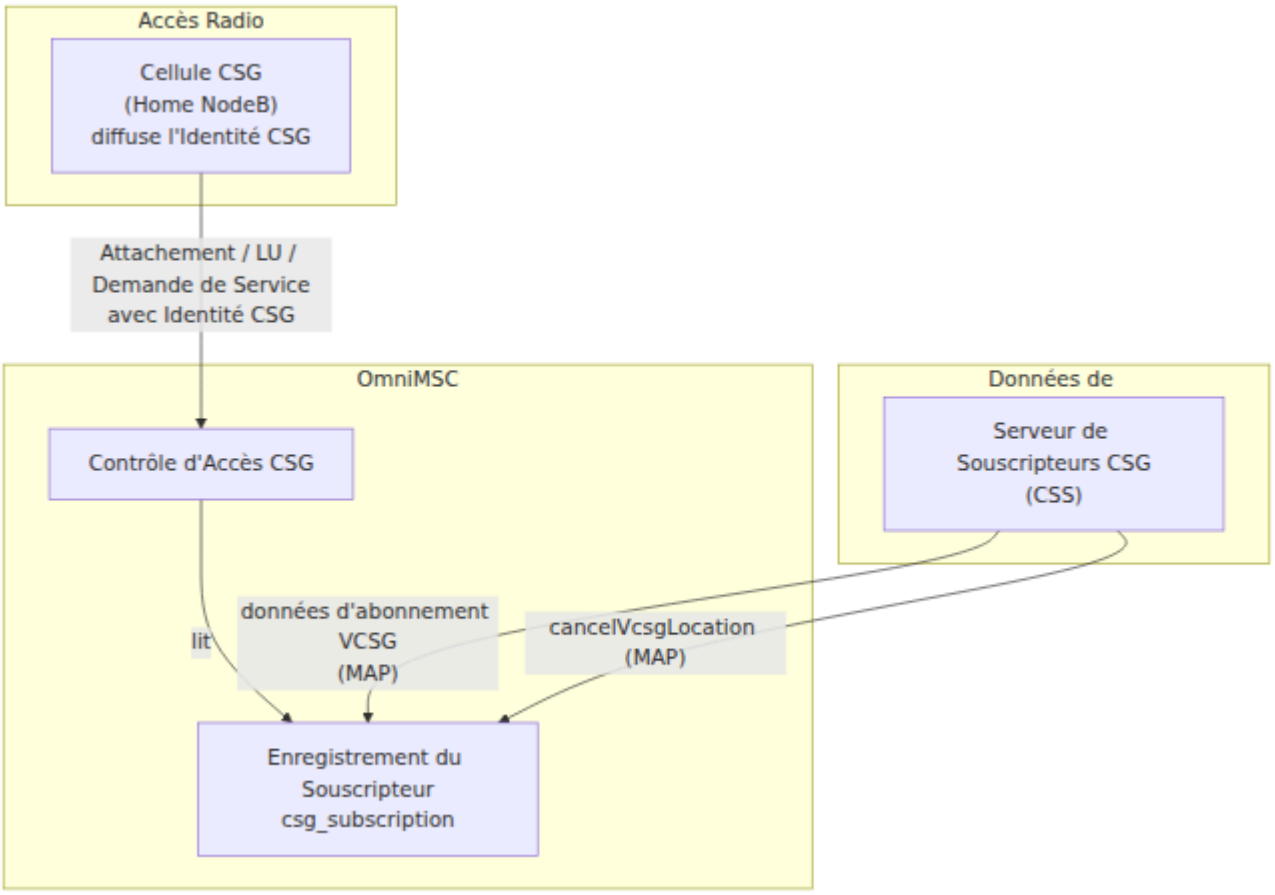
Groupes de Souscripteurs Fermés (CSG / VCSG)

Ce document décrit comment OmniMSC gère les Groupes de Souscripteurs Fermés (CSG) : les données d'abonnement CSG détenues par souscripteur, la décision de contrôle d'accès prise lorsqu'un souscripteur tente d'utiliser une cellule CSG, et l'interaction MAP avec le Serveur de Souscripteurs CSG (CSS) qui maintient ces données d'abonnement à jour. Pour le modèle de données de souscripteur général et comment les données d'abonnement sont téléchargées depuis le HLR, voir Opérations MAP. Pour le Barring Déterminé par l'Opérateur, un mécanisme de contrôle d'accès connexe, voir Services Supplémentaires.

Aperçu

Un **Groupe de Souscripteurs Fermés** identifie un ensemble de souscripteurs autorisés à accéder à une ou plusieurs cellules CSG (par exemple, un Home NodeB / femtocell servant un domicile, un bureau ou un campus spécifique). Chaque CSG est identifié par une **Identité CSG** (une valeur de 27 bits, codée selon la 3GPP TS 23.003). Une cellule CSG diffuse son Identité CSG dans les informations système ; un souscripteur campant sur cette cellule reçoit un service normal uniquement lorsque le souscripteur est membre de ce CSG et que l'adhésion n'a pas expiré (TS 22.011 Section 8).

L'ensemble des CSG auxquels un souscripteur peut accéder est les **données d'abonnement VCSG** (également appelées liste des CSG autorisés). Ces données sont détenues par le **Serveur de Souscripteurs CSG (CSS)** et fournies au nœud de service (VLR / SGSN). OmniMSC les stocke dans l'enregistrement du souscripteur et évalue l'accès au moment de l'utilisation, de la même manière que le Barring Déterminé par l'Opérateur est appliqué par le nœud de service plutôt que par le HLR.



Données d'Abonnement CSG

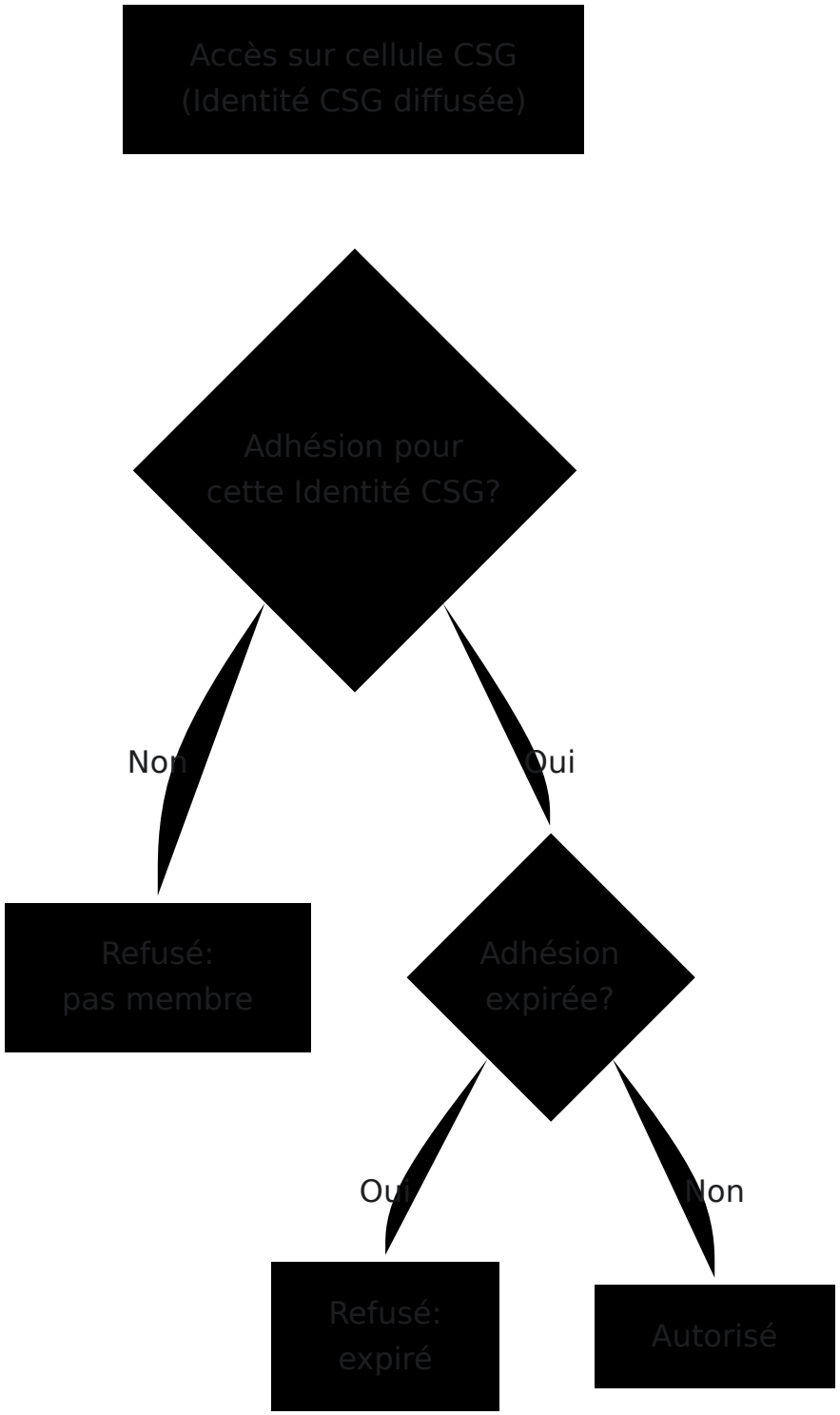
Chaque enregistrement de souscripteur contient une liste d'adhésion CSG. Chaque entrée décrit un Groupe de Souscripteurs Fermés auquel le souscripteur appartient et, éventuellement, quand cette adhésion expire.

Champ	Type	Description
`csg_id`	Entier	Identité CSG diffusée par la cellule CSG. Une valeur de 27 bits codée selon TS 23.003.
`expiry`	DateTime / null	Expiration de l'adhésion. Une adhésion avec une expiration `null` n'expire jamais. Une fois que l'heure actuelle atteint ou dépasse l'instant d'expiration, l'adhésion est considérée comme expirée et l'accès est refusé.

La liste d'adhésion est peuplée à partir des données d'abonnement VCSG fournies par le CSS et est effacée par MAP cancelVcsgLocation (voir Interaction MAP). La suppression uniquement des données d'abonnement CSG garde le souscripteur enregistré ; d'autres données d'abonnement (services de base, services supplémentaires, CAMEL, Barring Déterminé par l'Opérateur) restent intactes.

Contrôle d'Accès

Lorsque un souscripteur tente d'accéder à une cellule qui diffuse une Identité CSG, OmniMSC évalue la liste d'adhésion du souscripteur par rapport à l'Identité CSG diffusée. Une cellule qui ne diffuse pas d'Identité CSG est une cellule normale (non-CSG) et est toujours accessible ; la vérification ci-dessous s'applique uniquement aux cellules CSG.



La décision a trois résultats :

Résultat	Condition	Signification
Autorisé	Le souscripteur a une adhésion pour l'Identité CSG diffusée et elle n'a pas expiré.	Le souscripteur reçoit un service normal sur la cellule CSG.
Refusé (pas membre)	Le souscripteur n'a pas d'adhésion pour l'Identité CSG diffusée (y compris le cas où le souscripteur n'a pas de données d'abonnement CSG du tout).	L'accès à la cellule CSG est rejeté.
Refusé (expiré)	Le souscripteur a une adhésion pour l'Identité CSG diffusée, mais son expiration est passée.	L'accès à la cellule CSG est rejeté. L'adhésion périmée reste jusqu'à ce que le CSS la mette à jour ou l'annule.

La limite d'expiration est inclusive : lorsque l'heure actuelle est égale à l'instant d'expiration, l'adhésion est considérée comme expirée.

Interaction MAP avec le CSS

Le Serveur de Souscripteurs CSG maintient la copie maîtresse des données d'abonnement VCSG d'un souscripteur et garde le nœud de service à jour en utilisant des opérations MAP (3GPP TS 29.002). OmniMSC gère ce qui suit.

Opération	Opcode	Direction	Effet
updateVcsgLocation	53	Nœud de service vers CSS	Enregistre le nœud de service pour le service VCSG et récupère les données d'abonnement CSG du souscripteur.
cancelVcsgLocation	36	CSS vers nœud de service	Annule l'enregistrement VCSG de ce nœud de service pour le souscripteur. OmniMSC supprime toutes les données d'abonnement CSG tout en maintenant le souscripteur enregistré.

cancelVcsgLocation est envoyé par le CSS lorsque l'enregistrement VCSG du souscripteur doit être supprimé de ce nœud (par exemple, l'adhésion CSG du souscripteur a été révoquée, ou le souscripteur a déménagé vers un autre nœud). L'argument contient l'identité du souscripteur (IMSI). À la réception, OmniMSC efface la liste d'adhésion CSG du souscripteur et accuse réception de l'opération.

Parse error on line 9: ...ur reste enregistré;
l'accès ultérie ----------
---^ Expecting 'SPACE', 'NEWLINE', 'create', 'box', 'end', 'autonumber',
'activate', 'deactivate', 'title', 'legacy_title', 'acc_title', 'acc_descr',
'acc_descr_multiline_value', 'loop', 'rect', 'opt', 'alt', 'par', 'par_over', 'critical',
'break', 'option', 'and', 'else', 'participant', 'participant_actor', 'destroy', 'note',
'links', 'link', 'properties', 'details', 'ACTOR', got 'INVALID'

Réessayer

Les données d'abonnement CSG peuvent également être retirées dans le cadre de MAP DeleteSubscriberData (la catégorie de données CSG), qui supprime la liste d'adhésion CSG tout en laissant le souscripteur enregistré et d'autres données intactes. Voir Opérations MAP pour la procédure générale DeleteSubscriberData.

Références de Spécification 3GPP

Spécification	Titre	Pertinence
TS 23.060	Service Général de Paquet Radio (GPRS); Description du service	Contrôle d'accès CSG et gestion de la localisation VCSG dans le domaine des paquets
TS 22.011	Accessibilité du service	Concept CSG, liste des CSG autorisés, adhésion CSG et expiration
TS 23.003	Numérotation, adressage et identification	Codage de l'Identité CSG (27 bits)
TS 29.002	Spécification de la Partie d'Application Mobile (MAP)	updateVcsgLocation, cancelVcsgLocation, données d'abonnement CSG, interaction CSS

Trunking ISUP

Ce document décrit l'interface de trunk ISUP (ISDN User Part) mise en œuvre par OmniMSC, y compris la gestion des groupes de trunks, l'allocation des circuits, l'encodage des messages, le support des minuteries, la vérification de continuité et l'intégration avec la table de routage et SIP-I.

Pour le mappage des codes de cause ISUP-SIP, voir Trunking SIP. Pour SIP-I (SIP avec ISUP encapsulé), voir Trunking SIP-I. Pour la configuration de routage et le type de route `:isup`, voir Configuration de Routage. Pour les diagrammes de flux d'appels montrant le signalement ISUP dans le contexte (IAM/ACM/ANM, transit ISUP vers SIP), voir Diagrammes de Flux d'Appels.

Groupes de Trunks ISUP

OmniMSC organise les circuits ISUP en groupes de trunks. Chaque groupe de trunks représente un ensemble de circuits vocaux vers un échange SS7 distant, identifié par un code de point de destination et une plage de Codes d'Identification de Circuits (CIC).

Allocation de CIC

Lorsqu'un appel est acheminé vers un groupe de trunks ISUP, le gestionnaire de circuits alloue le premier circuit inactif trouvé dans la plage configurée. Le CIC alloué est inclus dans l'IAM sortant et réservé jusqu'à ce que l'appel soit libéré.

Paramètre	Type	Description
`name`	`string`	Identifiant unique du groupe de trunks, référencé dans les entrées de la table de routage
`dpc`	`integer`	Code de point de destination (entier codé, par exemple `a*2048 + b*8 + c` pour ITU 3-8-3)
`cic_range`	`{start, end}`	Plage inclusive de CIC disponibles pour ce groupe de trunks

Gestion de l'État des Circuits

Chaque circuit au sein d'un groupe de trunks suit un état indépendant. Le gestionnaire de circuits gère les opérations de blocage, de déblocage et de réinitialisation de groupe.

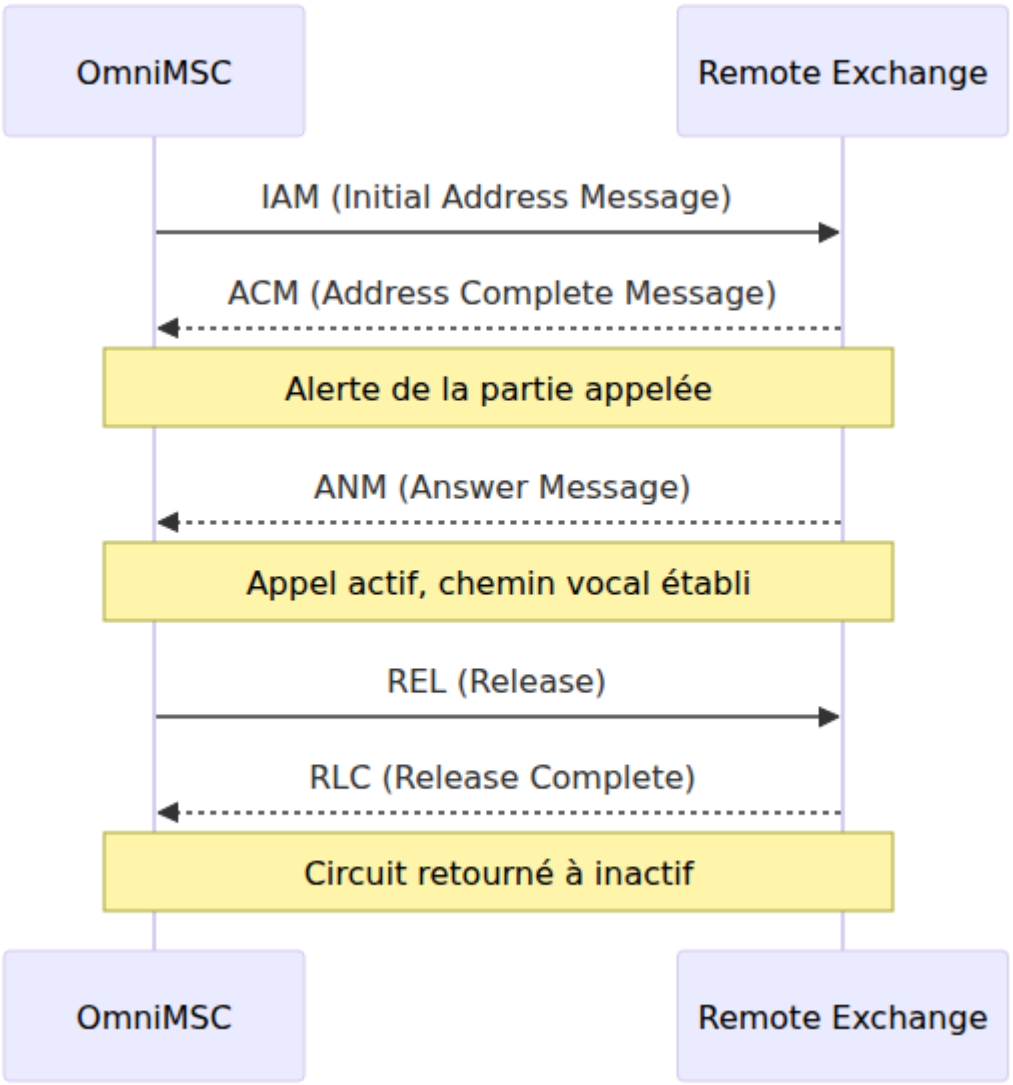
État du Circuit	Description
`:idle`	Disponible pour saisie
`:outgoing_busy`	Alloué pour un appel sortant (IAM envoyé)
`:incoming_busy`	Réservé pour un appel entrant (IAM reçu)
`:blocked`	Bloqué via BLO, indisponible pour saisie
`:unblocked_pending`	Déblocage (UBL) envoyé, en attente d'accusé de réception
`:reset_pending`	Réinitialisation du circuit en cours (RSC/GRS), en attente d'accusé de réception

Le blocage de circuit (BLO) et le déblocage (UBL) sont effectués par circuit uniquement. La réinitialisation de groupe (GRS/GRA) réinitialise tous les circuits

dans une plage à inactif et efface tout état de blocage ; un seul circuit peut également être réinitialisé avec RSC.

Flux de Messages ISUP

La séquence de signalement ISUP standard pour un appel réussi suit le modèle IAM-ACM-ANM-REL-RLC.

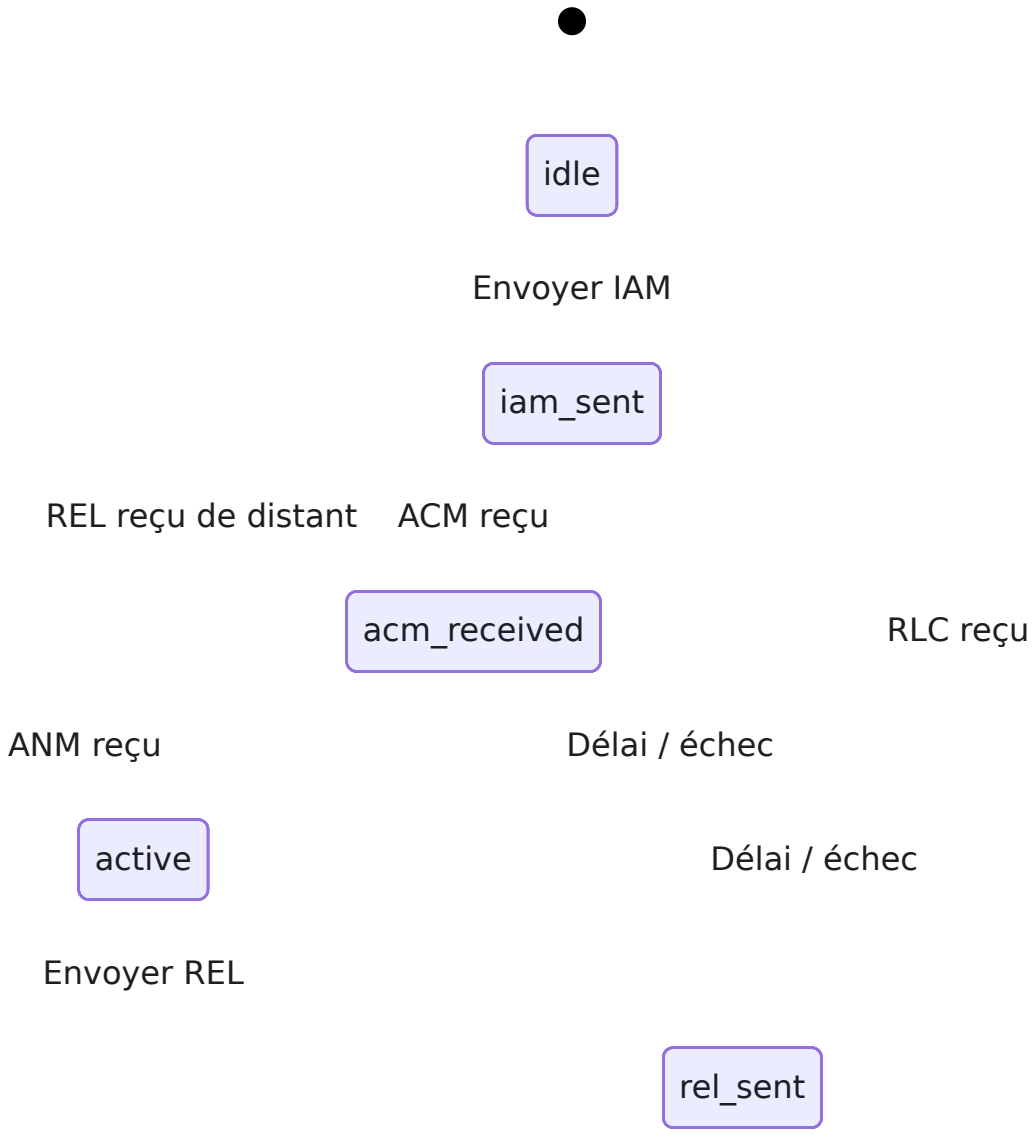


Pour les appels entrants, les directions sont inversées : IAM arrive de l'échange distant, et OmniMSC envoie ACM et ANM au fur et à mesure que l'appel progresse à travers l'alerte et la réponse.

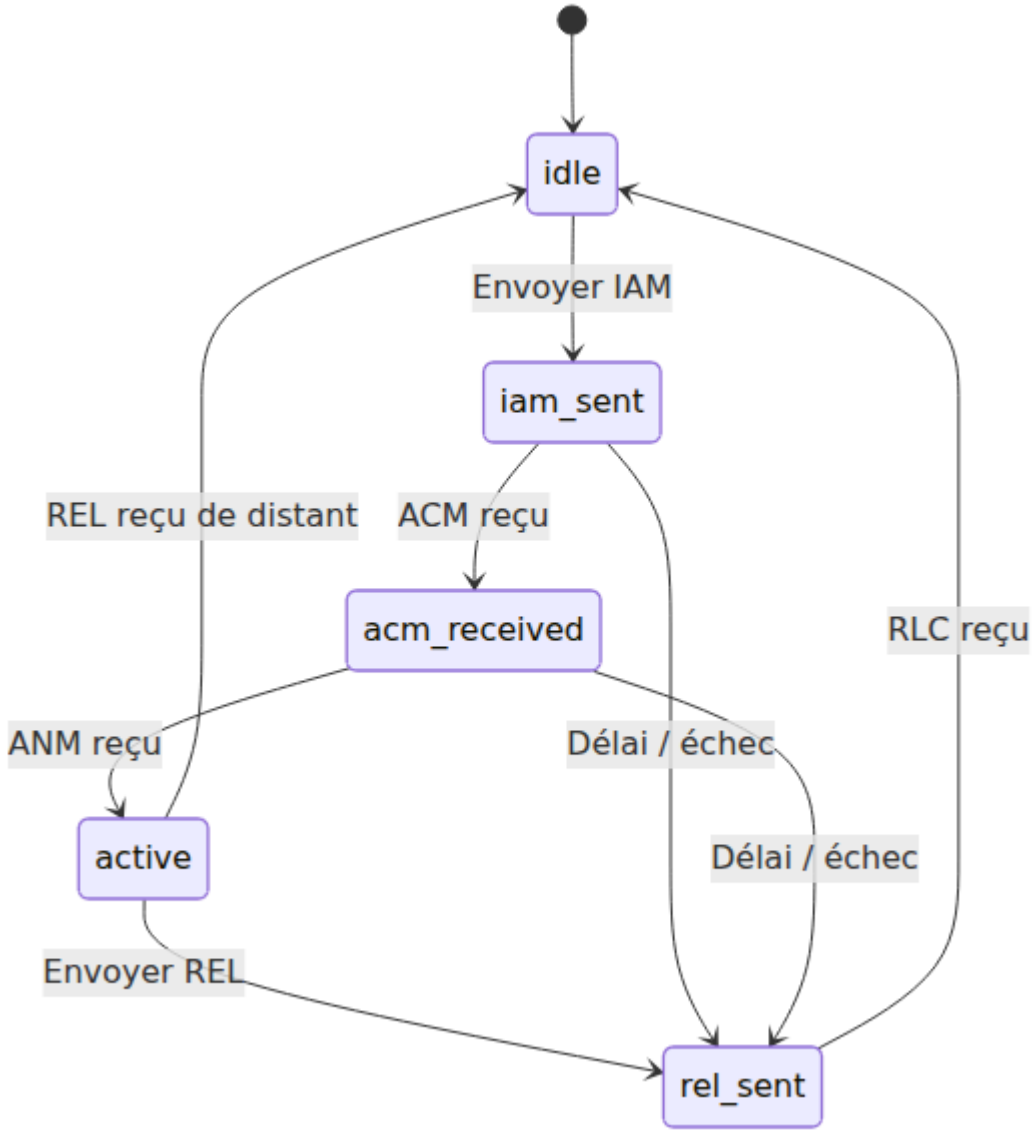
États du Gestionnaire ISUP

Le gestionnaire ISUP maintient un état par appel qui suit la progression du signalement pour chaque circuit.

États des Appels Sortants



États des Appels Entrants



Minuteries ISUP

OmniMSC met en œuvre les minuteries ISUP standard définies dans l'ITU-T Q.764. Ces minuteries protègent contre les échecs de signalement et garantissent que les circuits ne restent pas dans des états indéterminés.

Minuterie	Durée	Démarrée Après	Expire Quand	Action à l'Expiration
T1	20s	REL envoyé	RLC non reçu	Retransmettre REL
T5	300s	Première expiration de T1	RLC toujours non reçu	Envoyer alerte de maintenance, réinitialiser le circuit
T7	25s	IAM envoyé	ACM non reçu	Libérer l'appel, envoyer REL
T9	180s	ACM reçu	ANM non reçu	Libérer l'appel, envoyer REL

Lorsque T7 expire sans recevoir un ACM, OmniMSC envoie un REL avec la cause 16 (libération d'appel normale) et notifie le Contrôle d'Appel avec la cause 31 (normal, non spécifié). Lorsque T9 expire sans un ANM, OmniMSC envoie un REL avec la cause 19 (pas de réponse de l'utilisateur).

Encodage des Messages ISUP

OmniMSC met en œuvre un codec pour l'encodage et le décodage des cinq types de messages ISUP principaux utilisés dans l'établissement et la libération des appels. Tous les messages suivent le format ITU-T Q.763 avec des sections de paramètres fixes obligatoires, variables obligatoires et optionnelles.

Message	Code Type	Direction	Paramètres Clés
IAM	`0x01`	Origine	Nature de la Connexion, Indicateurs d'Appel Transféré, Catégorie de Partie Appelante, Exigence de Support de Transmission, Numéro de la Partie Appelée, Numéro de la Partie Appelante
ACM	`0x06`	Terminaison	Indicateurs d'Appel Rétro, Indicateurs d'Appel Rétro Optionnels, Indicateurs de Cause
ANM	`0x09`	Terminaison	Indicateurs d'Appel Rétro
REL	`0x0C`	Soit	Indicateurs de Cause
RLC	`0x10`	Soit	(aucun -- accusé de réception uniquement)

Messages supplémentaires pris en charge pour la maintenance des circuits :

Message	Code Type	But
BLO	`0x13`	Bloquer un circuit (maintenance locale)
UBL	`0x14`	Débloquer un circuit
RSC	`0x12`	Réinitialiser un seul circuit
GRS	`0x17`	Réinitialisation de groupe d'une plage de circuits
GRA	`0x29`	Accusé de réception de réinitialisation de groupe
COT	`0x05`	Résultat de vérification de continuité
CPG	`0x2C`	Progrès d'Appel (événement/progression en cours)

Vérification de Continuité

OmniMSC prend en charge la procédure de vérification de continuité ISUP pour vérifier le chemin de transport avant de connecter un appel. Lorsque les Indicateurs d'Appel Transféré dans un IAM sortant demandent une vérification de continuité, la séquence suivante se produit :

1. OmniMSC saisit le circuit et envoie IAM avec l'indicateur de vérification de continuité activé.
2. Un retour à l'expéditeur est appliqué à l'extrémité éloignée du circuit.
3. OmniMSC envoie un ton de test et vérifie le retour.
4. En cas de succès, OmniMSC envoie COT (vérification de continuité réussie) et l'appel se poursuit.
5. En cas d'échec, OmniMSC envoie COT (vérification échouée) et peut réessayer sur un circuit alternatif.

Pour les appels entrants, lorsque OmniMSC reçoit un IAM avec l'indicateur de vérification de continuité, il applique un retour à l'expéditeur sur le circuit spécifié et attend le message COT avant de procéder à l'établissement de l'appel.

Intégration de la Table de Routage

Les routes de type `:isup` dans la table de routage dirigent les appels vers un groupe de trunks ISUP. L'entrée de la route spécifie le nom du groupe de trunks, le code de point de destination et la plage de CIC.

Paramètre de Route	Description
`type`	`:isup`
`trunk_group`	Nom du groupe de trunks correspondant à un groupe de trunks configuré
`dpc`	Code de point de destination (entier codé)
`cic_range`	Plage de CIC sous la forme `{start, end}`

Lorsque le routage sélectionne une destination ISUP, le routeur de trunks demande un circuit libre au gestionnaire de circuits. Si aucun circuit n'est disponible dans le groupe de trunks principal, le système tente des groupes de trunks de débordement vers le même code de point de destination.

Pour des exemples de configuration de route, voir Configuration de Routage.

Support SIP-I

SIP-I (SIP avec ISUP encapsulé) fournit un transport basé sur IP pour les messages ISUP. Les routes de type `:sip_i` transportent le message ISUP

complet (IAM, ACM, ANM, REL) en tant que corps MIME `application/ISUP` dans le signalement SIP conformément à l'ITU-T Q.1912.5 et au RFC 3204.

Les pairs SIP-I sont configurés séparément des pairs SIP purs. L'encodeur/décodeur ISUP utilisé pour les trunks ISUP natifs est partagé avec SIP-I pour l'encodage et le décodage des corps ISUP encapsulés.

Pour la configuration SIP-I, les flux d'appels et le mappage des en-têtes, voir Trunking SIP-I.

SIP avec Échec de Basculement

Les routes de type `:sip_with_failover` tentent d'abord l'appel via un pair SIP. Si la route SIP échoue (pair injoignable, réponse 5xx, ou délai d'attente), le routeur de trunks réessaie automatiquement via le groupe de trunks ISUP configuré.

Déclencheur de Basculement	Description
État du pair `:down`	Pair SIP injoignable (OPTIONS keepalive échoué)
Réponse SIP 5xx	Erreur serveur du pair SIP
Délai d'attente SIP	Pas de réponse dans le délai de transaction SIP
`max_channels` dépassé	Pair SIP n'a pas de capacité disponible

Lors du basculement, le routeur de trunks alloue un CIC du groupe de trunks ISUP et envoie un IAM. Le FSM CC reste dans le même état tout au long du basculement -- la nouvelle tentative est transparente pour le signalement côté radio.

Pour la configuration de route de basculement, voir Configuration de Routage.

Références

Référence	Titre	Pertinence
ITU-T Q.761	Description Fonctionnelle de l'ISUP	Vue d'ensemble et architecture de l'ISUP
ITU-T Q.762	Fonction Générale des Messages et Signaux de l'ISUP	Définitions des messages
ITU-T Q.763	Formats et Codes de l'ISUP	Encodage des messages et formats de paramètres
ITU-T Q.764	Procédures de Signalisation de l'ISUP	Procédures d'établissement/libération d'appels, définitions des minuteries
ITU-T Q.850	Utilisation de la Cause et de la Localisation dans l'ISDN	Définitions des codes de cause utilisés dans REL
RFC 3204	Type de Média MIME pour les Objets ISUP et QSIG	Encapsulation ISUP dans SIP-I
ITU-T Q.1912.5	Interopérabilité entre SIP et BICC ou ISUP	Définition du protocole SIP-I

Opérations MAP

Ce document décrit les opérations MAP (Mobile Application Part) mises en œuvre par OmniMSC, y compris la gestion des dialogues, les procédures de localisation des abonnés, l'authentification, le transfert de SMS, l'USSD et la gestion des erreurs. Pour la configuration, voir Référence de Configuration. Pour la vue de la couche SMS de MO-ForwardSM et MT-ForwardSM, y compris les détails du protocole CP/RP, voir SMS. Pour la gestion des vecteurs d'authentification et l'Auth FSM, voir Sécurité. Pour savoir comment InsertSubscriberData remplit le profil de l'abonné visible dans le panneau de contrôle, voir Guide du Panneau de Contrôle.

Client MAP

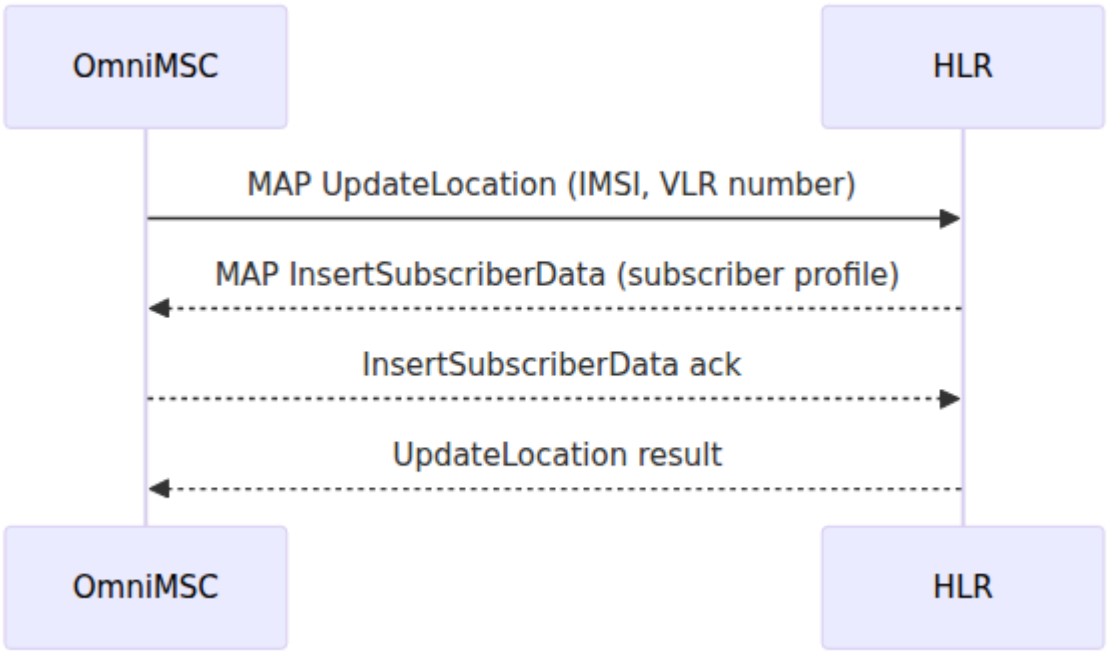
OmniMSC opère un client MAP qui gère les dialogues avec des pairs MAP distants (HLR, SMSc, passerelle USSD). Le client MAP gère le cycle de vie du dialogue, la corrélation des transactions TCAP et la supervision du délai d'attente du dialogue.

Lorsqu'un sous-système (VLR, gestionnaire de SMS, gestionnaire SS) a besoin d'invoquer une opération MAP, il demande un nouveau dialogue au client MAP. Le client alloue un ID de transaction local (otid), ouvre un TCAP BEGIN vers le pair et surveille le dialogue pendant une période fixe de 30 secondes. Si le pair ne répond pas dans le délai imparti, le client abandonne le dialogue et notifie le sous-système demandeur de l'échec.

Pour les dialogues MAP entrants initiés par des pairs distants (comme InsertSubscriberData du HLR ou MT-ForwardSM du SMSc), le client MAP accepte le TCAP BEGIN, le corrèle avec l'ID de transaction distant (dtid), génère un processus de gestion et supervise le dialogue jusqu'à son achèvement.

UpdateLocation

Le MSC envoie MAP UpdateLocation au HLR lorsqu'un abonné effectue une mise à jour de localisation. Le message contient l'IMSI de l'abonné et le numéro VLR (l'adresse E.164 de ce MSC/VLR). Le HLR utilise le numéro VLR pour acheminer les futures transactions MT (appels, SMS, USSD) vers le MSC correct.



À la réception du résultat de UpdateLocation, le VLR marque la mise à jour de localisation comme complète et le FSM LU procède à l'allocation de TMSI. Si le HLR retourne une erreur (abonné inconnu, itinérance non autorisée), le MSC rejette la mise à jour de localisation vers la station mobile avec la cause appropriée.

InsertSubscriberData

Le HLR envoie MAP InsertSubscriberData au MSC pendant la procédure UpdateLocation, et également de manière proactive lorsque le profil de l'abonné change (par exemple, activation de service supplémentaire via l'interface de provisionnement HLR). Le message contient le profil de l'abonné, y compris :

- MSISDN (le numéro de répertoire de l'abonné)

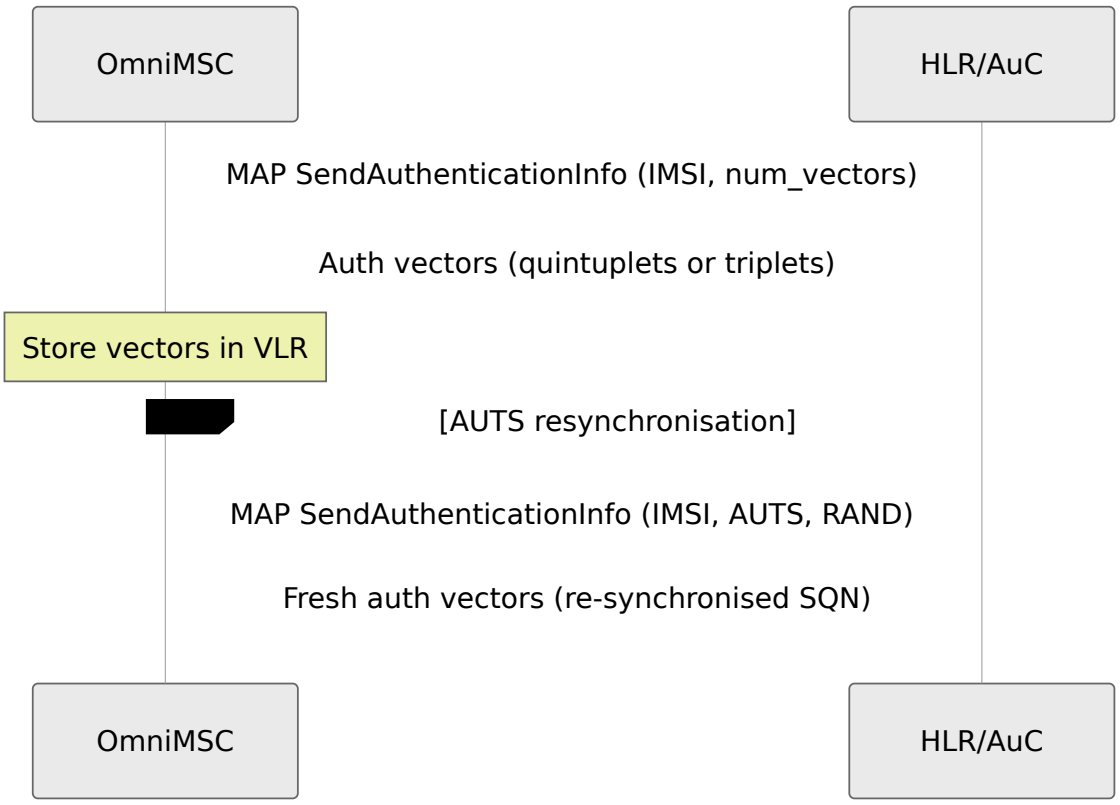
- Services et téléséries CS
- Catégories de barrages déterminés par l'opérateur (ODB)
- Données de service supplémentaire (numéros de renvoi d'appel, statut de barrage, mode CLIR, statut CW)
- Informations d'abonnement CAMEL (clés de service, adresses gsmSCF)

Le VLR stocke ces données dans l'enregistrement de l'abonné. Les configurations d'appels ultérieurs, la livraison de SMS et les opérations SS font référence à ce profil mis en cache localement pour éviter les allers-retours vers le HLR.

SendAuthenticationInfo

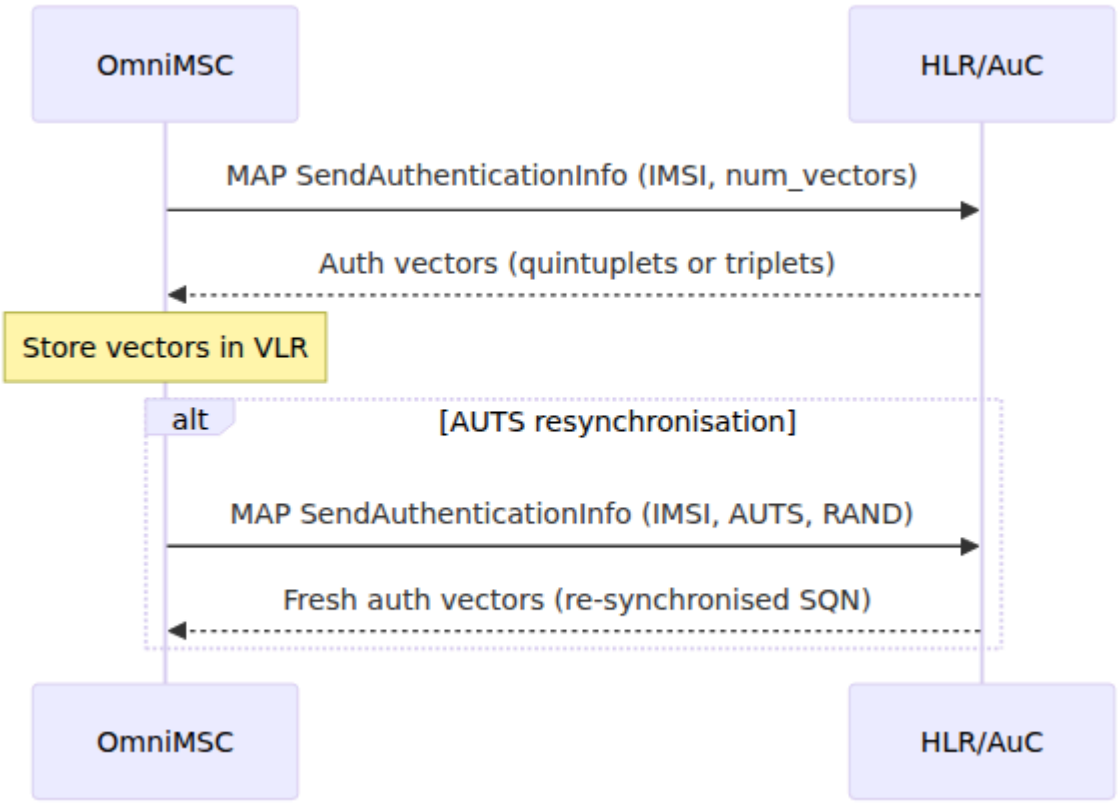
Le MSC envoie MAP SendAuthenticationInfo au HLR pour récupérer les vecteurs d'authentification pour un abonné. La demande contient l'IMSI, le nombre de vecteurs demandés et éventuellement des données de re-synchronisation (AUTS) si l'UE a signalé un échec de numéro de séquence.

Le HLR retourne des vecteurs d'authentification de l'AuC : quintuplets (RAND, XRES, CK, IK, AUTN) pour les abonnés capables de UMTS ou triplets (RAND, SRES, Kc) pour les abonnés uniquement GSM. Le MSC stocke les vecteurs dans le VLR et les utilise pour les tentatives d'authentification ultérieures sans contacter à nouveau le HLR jusqu'à épuisement de l'approvisionnement en vecteurs.



PurgeMS

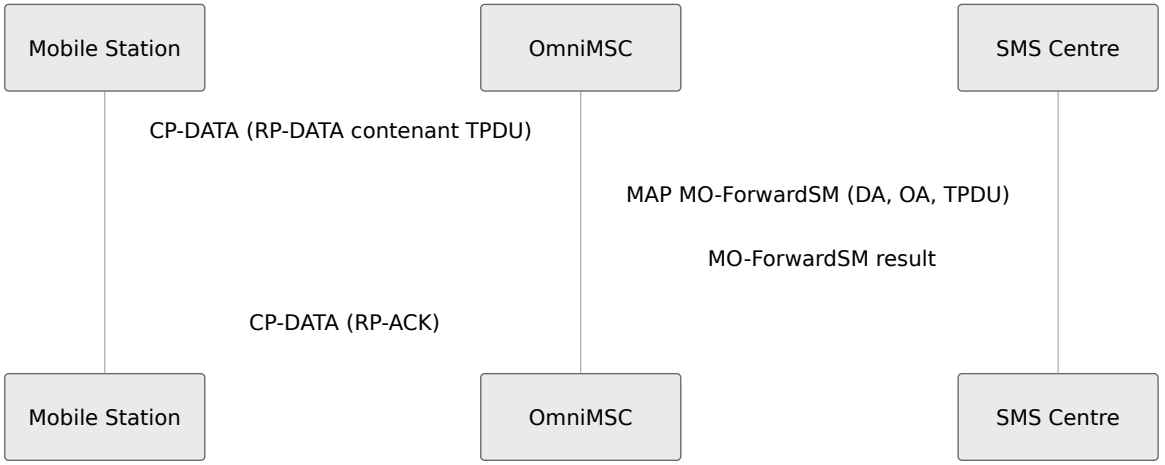
Le MSC envoie MAP PurgeMS au HLR lorsqu'un abonné effectue un détachement IMSI. Le message contient l'IMSI et le numéro VLR. À la réception de PurgeMS, le HLR efface l'adresse VLR de l'enregistrement de l'abonné. Cela garantit un routage correct du T-ADS (Terminating Access Domain Selection) : sans une adresse VLR valide, le HLR sait que l'abonné n'est pas joignable via le domaine CS et peut acheminer les services MT en conséquence (par exemple, déclencher le drapeau MNRF pour les SMS, retourner abonné absent pour les appels MT).



MO-ForwardSM

Le MSC envoie MAP MO-ForwardSM au Centre SMS pour les messages courts d'origine mobile. Le message contient le SM-RP-DA (destination, généralement l'adresse SMSc), SM-RP-OA (expéditeur, le MSISDN de l'abonné) et le SM-RP-UI (le TPDU contenant la charge utile SMS).

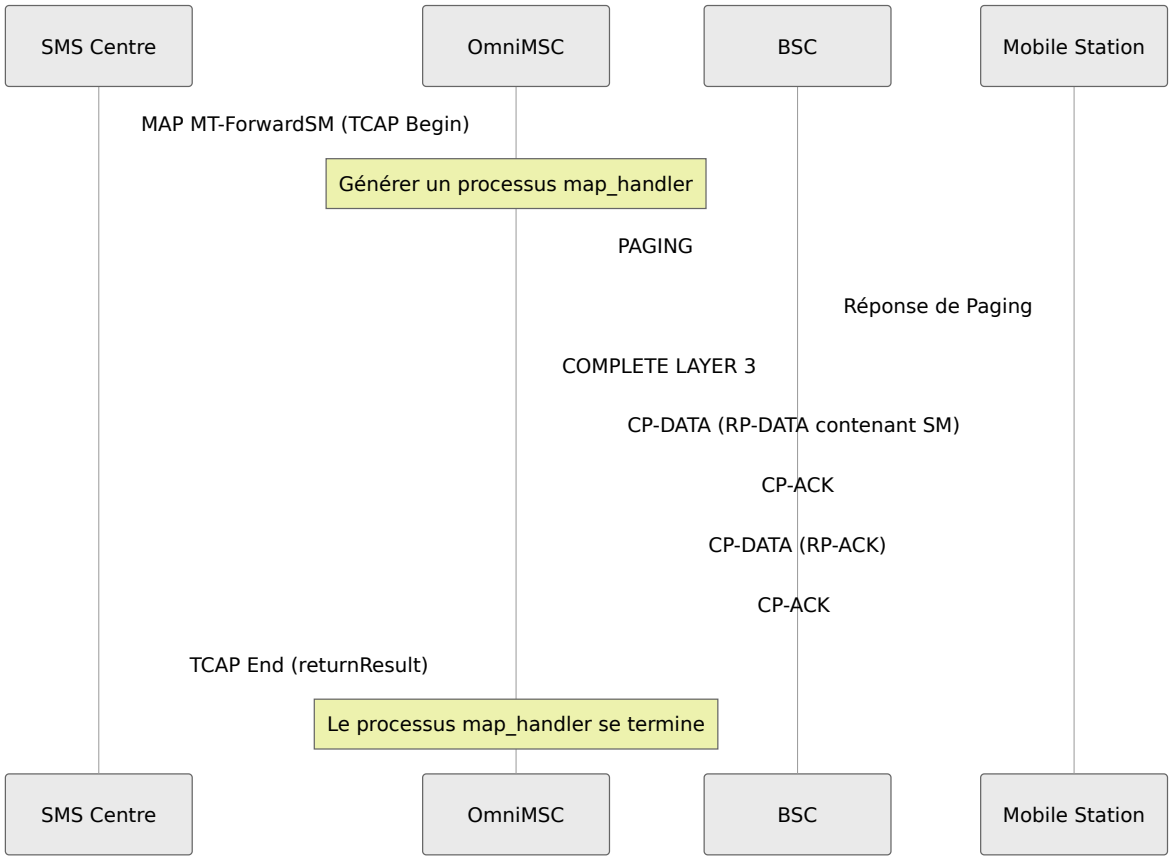
Le SMSc accuse réception avec un résultat de retour en cas d'acceptation réussie, ou une erreur de retour si le message ne peut pas être traité (par exemple, congestion du SMSc, destination invalide).



MT-ForwardSM

Le Centre SMS envoie MAP MT-ForwardSM au MSC pour la livraison de messages courts terminés mobiles. À la réception de cette opération, OmniMSC génère un processus map_handler dédié qui gère la tentative de livraison et maintient le dialogue MAP ouvert jusqu'à ce que le résultat soit connu.

Le gestionnaire recherche l'abonné dans le VLR, page si nécessaire, et livre le SM via DTAP. Une fois que la station mobile accuse réception de la livraison (RP-ACK) ou signale un échec (RP-ERROR), le gestionnaire envoie un TCAP End contenant soit un returnResult (livraison réussie) soit un returnError (échec de la livraison avec cause) au SMSc.



Si la livraison échoue (abonné absent, mémoire dépassée, erreur de protocole), le gestionnaire retourne l'erreur MAP appropriée :

Erreur	Cause
Abonné Absent	Abonné non joignable (non enregistré ou pas de réponse de paging)
Échec de Livraison SM	MS a retourné RP-ERROR (mémoire pleine, erreur non spécifiée)
Échec Système	Erreur de traitement interne

ProcessUnstructuredSS-Request

OmniMSC relaie les demandes USSD au HLR via MAP ProcessUnstructuredSS-Request lorsque la chaîne USSD cible un service nécessitant un traitement HLR (par exemple, gestion de services supplémentaires, requêtes de solde). Le MSC

transmet la chaîne USSD et le DCS (schéma de codage des données) au HLR, qui traite la demande et retourne une chaîne de réponse à afficher sur la station mobile.

Pour les codes USSD définis par l'opérateur qui sont gérés par une passerelle USSD externe plutôt que par le HLR, le MSC achemine le dialogue MAP vers l'adresse de passerelle configurée à la place.

Gestion des Transactions TCAP

Les dialogues MAP sont transportés dans des transactions TCAP. OmniMSC maintient une table de transactions qui corrèle les identifiants de transaction locaux et distants tout au long du cycle de vie du dialogue.

Message TCAP	Phase de Dialogue MAP	Description
TC-BEGIN	Ouverture	L'initiateur envoie le premier invoke ; contient l'ID de transaction d'origine (otid)
TC-CONTINUE	Actif	Les deux parties échangent des composants ; la réponse contient l'ID de transaction de destination (dtid) correspondant à l'otid du pair
TC-END	Fermeture	Message final ; contient des composants de résultat ou d'erreur ; dialogue terminé
TC-ABORT	Abandon	Terminaison anormale ; erreur de protocole ou délai d'attente

Le client MAP suit chaque dialogue actif par sa paire otid/dtid. Lorsqu'un TCAP CONTINUE ou END arrive, le client associe le dtid à un otid local pour localiser le processus de gestion correspondant. Cette corrélation est essentielle pour le

multiplexage de nombreux dialogues MAP concurrents sur une seule connexion SCCP.

Délai d'Attente du Dialogue

Chaque dialogue MAP a un délai d'attente fixe de 30 secondes. Si le pair distant ne répond pas dans le délai imparti, le client MAP envoie un TC-ABORT (initié localement) et notifie le sous-système demandeur. Cela empêche les fuites de ressources provenant de pairs non réactifs.

Gestion des Erreurs MAP

OmniMSC gère les erreurs MAP à la fois au niveau des composants (retour d'erreur dans un dialogue) et au niveau du dialogue (abandon, erreur de fournisseur).

Erreurs MAP Courantes

Erreur	Opération Typique	Gestion MSC
Abonné Absent	MT-ForwardSM, SendRoutingInfo	Signaler l'échec de livraison au SMSc ; définir MNRF dans le VLR
Échec de Livraison SM	MT-ForwardSM	Transmettre la cause de l'échec TP au SMSc
Abonné Inconnu	UpdateLocation	Rejeter la mise à jour de localisation
Itinérance Non Autorisée	UpdateLocation	Rejeter la mise à jour de localisation avec la cause appropriée
Échec Système	Tout	Réessayer ou signaler l'échec au sous-système demandeur
Données Manquantes	SendAuthenticationInfo	L'authentification ne peut pas se poursuivre ; rejeter le service
Valeur de Données Inattendue	InsertSubscriberData	Journaliser et rejeter le paramètre fautif

Échecs au Niveau du Dialogue

Lorsqu'un TCAP ABORT est reçu ou qu'un dialogue expire, le client MAP détermine quel sous-système a initié le dialogue et délivre une notification d'échec. Le sous-système applique ensuite sa propre logique de récupération (par exemple, le FSM LU rejette la mise à jour de localisation, le gestionnaire de SMS retourne un échec de livraison au SMSc).

Routage par Code de Point

Lorsque OmniMSC reçoit un dialogue MAP entrant (par exemple, MT-ForwardSM du SMSc, InsertSubscriberData du HLR), la couche M3UA enregistre le code de point d'origine à partir des informations de routage du message entrant. Lorsque le MSC envoie la réponse (TCAP Continue ou End), il utilise ce code de point enregistré comme code de point de destination (DPC) pour le message M3UA sortant.

Ce mécanisme garantit que les réponses sont routées vers le bon nœud d'origine, même lorsque plusieurs HLR ou SMSc avec différents codes de point sont accessibles via le même STP. Les routing_info de l'association M3UA entrante sont stockés par dialogue et utilisés pour tous les messages suivants dans ce dialogue.

Opérations Supplémentaires Supportées

Au-delà des opérations décrites en détail ci-dessus, l'encodeur MAP met en œuvre les opérations suivantes, identifiées par leur opcode local MAP :

Opération	Opcode	But
CancelLocation	3	HLR demande au VLR précédent d'annuler la localisation d'un abonné
SendRoutingInfo	22	GMSC demande des informations de routage (MSRN) pour un appel MT
SendRoutingInfoForSM	45	GMSC demande des informations de routage pour la livraison de SMS MT
ReportSM-DeliveryStatus	47	Signaler le résultat de la livraison de SMS MT au HLR (gestion MWD/MNRF)
SendIdentification	55	Récupérer IMSI et vecteurs d'authentification du VLR précédent (relais de pool)
RestoreData	57	Restaurer les données de l'abonné à partir du HLR
UnstructuredSS-Request	60	Demande USSD initiée par le réseau vers l'abonné
AlertServiceCentre	64	Notifier le SMSc qu'un abonné est à nouveau joignable
ReadyForSM	66	Informer le HLR que l'abonné est prêt à recevoir des SMS

Références de Spécification 3GPP

Spécification	Titre	Pertinence
TS 29.002	Spécification Mobile Application Part (MAP)	Toutes les opérations MAP, codes d'erreur, procédures de dialogue
ITU-T Q.771-Q.775	Transaction Capabilities Application Part (TCAP)	Gestion des transactions TCAP, gestion des composants
ITU-T Q.711-Q.716	Signalling Connection Control Part (SCCP)	Adressage et routage SCCP pour les dialogues MAP
RFC 4666	MTP3 User Adaptation Layer (M3UA)	Transport M3UA, routage par code de point

Contrôle des Médias

Ce document décrit le contrôle des passerelles multimédias dans OmniMSC, couvrant les protocoles de passerelle MGCP et Megaco/H.248, la machine d'état du contrôleur multimédia, la négociation de codec, le pontage de conférence et la génération SDP.

Pour des diagrammes de flux d'appels montrant la configuration des médias dans le contexte, voir Diagrammes de Flux d'Appels. Pour la configuration des codecs de trunk SIP, voir Trunk SIP. Pour les paramètres de configuration de la passerelle multimédia, voir Référence de Configuration. Pour le pontage de conférence MPTY du point de vue des services supplémentaires, voir Services Supplémentaires.

Contrôle de la Passerelle MGCP

OmniMSC contrôle les passerelles multimédias en utilisant le protocole de contrôle de passerelle multimédia (MGCP) selon la RFC 3435. L'agent d'appel MGCP émet trois commandes principales pour gérer les connexions RTP sur la passerelle.

Commandes

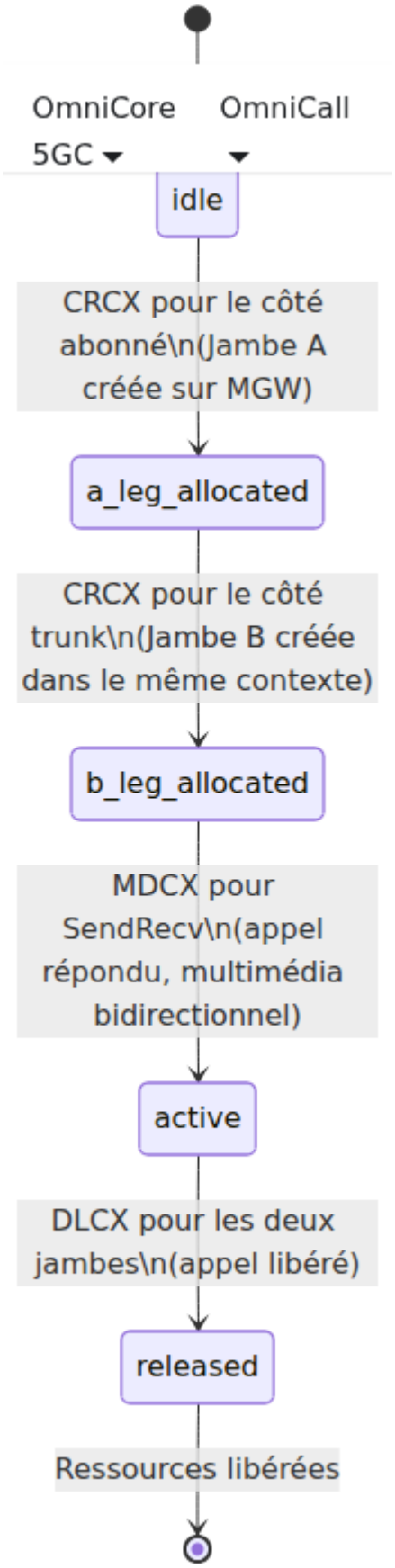
Commande	Objectif	Description
CRCX	Créer une Connexion	Alloue un nouveau point de terminaison RTP sur la passerelle multimédia et renvoie l'adresse IP locale, le port et le SDP pour ce point de terminaison.
MDCX	Modifier la Connexion	Met à jour les paramètres d'une connexion existante, par exemple en changeant le mode multimédia de réception seule à envoi et réception lorsque l'appel est répondu.
DLCX	Supprimer la Connexion	Détruit une connexion RTP et libère les ressources de point de terminaison associées sur la passerelle.

Nommage des Points de Terminaison

Les chemins des points de terminaison de la passerelle multimédia sont fournis par l'appelant plutôt que générés selon un modèle fixe. Lorsqu'un chemin de point de terminaison manque d'un `@`, il est qualifié avec le domaine configuré de la passerelle, produisant un point de terminaison entièrement qualifié tel que `ds/ds1-1/1@mgw01.local`. Chaque jambe d'appel occupe un point de terminaison dans un contexte de connexion sur la passerelle.

États du Contrôleur Multimédia

Le contrôleur multimédia gère le cycle de vie des ressources multimédias pour chaque appel. Il progresse à travers les états suivants à mesure que l'appel est établi et libéré.


OmniCore 5GC
OmniCall
idle
CRCX pour le côté abonné\n(Jambe A créée sur MGW)
a_leg_allocated
CRCX pour le côté trunk\n(Jambe B créée dans le même contexte)
b_leg_allocated
MDCX pour SendRecv\n(appel répondu, multimédia bidirectionnel)
active
DLCX pour les deux jambes\n(appel libéré)
released
Ressources libérées

Jambe A (Côté Abonné)

La jambe A représente le chemin multimédia entre la passerelle multimédia et le support d'accès radio de l'abonné via le BSC ou le RNC.

Lorsqu'un appel est initié, le contrôleur multimédia envoie une commande CRCX à la passerelle multimédia pour allouer le point de terminaison de la jambe A. Le mode de connexion initial est défini sur **RecvOnly**, ce qui signifie que la passerelle accepte les médias entrants du côté abonné mais ne transmet pas. Cela empêche le clipping et l'écho pendant la phase d'alerte.

Lorsque l'appel est répondu, le contrôleur multimédia envoie une commande MDCX pour changer le mode de la jambe A en **SendRecv**, permettant un flux multimédia bidirectionnel.

Jambe B (Côté Trunk)

La jambe B représente le chemin multimédia entre la passerelle multimédia et le trunk distant (pair SIP ou circuit ISUP).

La jambe B est allouée via une seconde commande CRCX dans le même contexte de connexion MGW que la jambe A. En plaçant les deux jambes dans le même contexte, la passerelle multimédia relie en interne les deux flux RTP, permettant la continuité du chemin vocal sans faire passer les médias par le MSC.

Négociation de Codec

OmniMSC négocie les codecs vocaux en fonction des capacités rapportées par le BSC dans la réponse de la demande d'attribution BSSMAP (liste des versions de la voix) et des préférences de codec du trunk sortant.

Codecs Supportés

Les types de charge utile sont assignés statiquement (non négociés dynamiquement) : GSM-FR utilise le type statique standard 3, PCMU/PCMA utilisent les types statiques standard 0/8, et les codecs vocaux 3GPP sont fixés aux types 96-101.

Codec	Charge Utile RTP	Description
PCMU	0	G.711 mu-law
GSM-FR	3	GSM Full Rate (13.0 kbit/s)
PCMA	8	G.711 A-law
GSM-EFR	96	GSM Enhanced Full Rate (6.60 kbit/s)
AMR-FR	97	Adaptive Multi-Rate Full Rate, mode octet-aligné (octet-align=1)
AMR-HR	98	Adaptive Multi-Rate Half Rate
GSM-HR	99	GSM Half Rate (5.60 kbit/s)
AMR-WB	100	Adaptive Multi-Rate Wideband (16 kHz)
OHR-AMR-WB	101	GSM Optimised Half Rate AMR Wideband (16 kHz)

La liste d'offre de codec est construite à partir de l'intersection des capacités de version de voix rapportées par le BSC et des préférences de codec configurées dans le MSC. Le SDP résultant est inclus dans l'invitation SIP sortante au pair de trunk, permettant au côté distant de sélectionner le codec préféré parmi l'ensemble proposé.

Pont de Conférence (Multi-Party)

OmniMSC prend en charge les appels de conférence multi-parties (MPTY) selon la 3GPP TS 24.083 en tirant parti de la capacité de pontage de conférence de la passerelle multimédia.

Lorsqu'un abonné invoque le service supplémentaire MPTY, le contrôleur multimédia alloue un contexte de conférence sur la passerelle multimédia. Les jambes d'appel individuelles sont ensuite ajoutées ou retirées de la conférence à mesure que les participants rejoignent ou quittent.

Opérations de Conférence

Opération	Description
Créer une Conférence	Alloue un nouveau contexte de conférence sur la passerelle multimédia avec un point de terminaison de mixage dédié.
Ajouter à la Conférence	Déplace une jambe d'appel existante dans le contexte de conférence via MDCX, connectant le participant au mixeur de conférence.
Retirer de la Conférence	Déplace une jambe d'appel hors du contexte de conférence vers une connexion point à point.

Le mixeur de conférence sur la passerelle multimédia gère le mélange des médias pour tous les participants. Le MSC contrôle l'appartenance à la conférence uniquement par signalisation et ne traite pas les médias directement.

Génération SDP

OmniMSC génère le SDP (Session Description Protocol) pour les messages SIP sortants en utilisant les conventions suivantes :

Champ SDP	Valeur
Origine (o=)	`OmniMSC` en tant que nom d'utilisateur de l'initiateur de session
Connexion (c=)	Adresse IP renvoyée par la passerelle multimédia dans la réponse CRCX
Médias (m=)	Port RTP renvoyé par la passerelle multimédia, avec les types de charge utile de codec de l'offre négociée
Attributs (a=)	Paramètres spécifiques au codec tels que `fmtp` pour le mode octet-align AMR

L'adresse de connexion et le port dans le SDP reflètent toujours le point de terminaison alloué de la passerelle multimédia, garantissant que les RTP circulent directement entre la passerelle multimédia et le pair distant sans traverser le chemin de signalisation du MSC.

Support Megaco/H.248

En alternative au MGCP, OmniMSC prend en charge le contrôle de la passerelle multimédia via le protocole Megaco/H.248 selon la Recommandation ITU-T H.248. Le choix entre MGCP et Megaco est un paramètre global unique — l'option `media mode` (par défaut `:megaco`) — et s'applique à toutes les passerelles multimédias, pas par passerelle.

Megaco utilise un modèle de commande basé sur les transactions avec des commandes Ajouter, Modifier, Soustraire et Déplacer qui se mappent conceptuellement aux opérations CRCX, MDCX et DLCX de MGCP. Le contrôleur Megaco gère les transactions H.248, l'allocation de contexte et le cycle de vie de terminaison sur la passerelle.

Les transports MGCP et Megaco utilisent par défaut UDP. Le contrôleur multimédia abstrait les différences de protocole afin que le FSM CC et d'autres

composants de gestion des appels interagissent avec une interface de contrôle multimédia unifiée, quelle que soit la passerelle sous-jacente.

Configuration de la Passerelle

Chaque passerelle multimédia est définie avec les paramètres d'identité suivants :

Paramètre	Description
Nom	Nom logique de la passerelle utilisé pour l'identification dans les journaux et le panneau de contrôle
Adresse	Adresse IP de la passerelle multimédia
Port	Port d'écoute MGCP ou Megaco sur la passerelle
Domaine	Nom de domaine de la passerelle utilisé dans l'adressage des points de terminaison MGCP (la portion `@mgw` des noms de points de terminaison)

Pour l'ensemble complet des paramètres de configuration multimédia, voir Référence de Configuration.

Références

- **RFC 3435** -- Protocole de Contrôle de Passerelle Multimédia (MGCP) Version 1.0
- **ITU-T H.248** -- Protocole de Contrôle de Passerelle (Megaco)
- **3GPP TS 24.083** -- Services supplémentaires d'attente d'appel et de mise en attente (MPTY)
- **RFC 4566** -- Protocole de Description de Session (SDP)

Métriques et Surveillance

Ce document décrit la télémétrie, les métriques, les alarmes et les points de terminaison de santé fournis par OmniMSC. Pour la configuration des seuils de surcharge, voir Référence de Configuration. Pour résoudre les conditions d'alerte, voir Guide de Dépannage. Pour la vue du tableau de bord en temps réel des appels actifs et du nombre d'abonnés, voir Guide du Panneau de Contrôle.

Vue d'ensemble de la Télémétrie

OmniMSC émet des événements de télémétrie Erlang/Elixir pour toutes les activités opérationnelles significatives. Ces événements sont exportés en tant que métriques Prometheus, disponibles à l'endpoint `/metrics` sur le port HTTP de Phoenix. Tous les noms de métriques sont espacés sous `omnimsc_` pour éviter les collisions avec d'autres applications. La page Système dans le panneau de contrôle fournit une vue en temps réel des statistiques de la VM BEAM, y compris le nombre de processus, la mémoire et la charge du planificateur — voir Guide du Panneau de Contrôle.

Les définitions de métriques ci-dessous reflètent les métriques exposées par OmniMSC. Tout scraper compatible avec Prometheus (Prometheus, Grafana Agent, Datadog, Victoria Metrics) peut collecter ces métriques à l'intervalle de scraping standard.

Référence des Métriques

Métrique	Type	Étiquettes	
`omnimsc_active_calls_count`	Gauge	--	Ap act
`omnimsc_vlr_subscribers_count`	Gauge	--	Ab en
`omnimsc_sccp_connections_count`	Gauge	--	Co act
`omnimsc_sms_sent_count`	Counter	--	Tot en
`omnimsc_location_update_complete_count`	Counter	`type`	Mis loc (im pé
`omnimsc_auth_failure_count`	Counter	`reason`	Éc d'a
`omnimsc_auth_skipped_count`	Counter	--	Au de val
`omnimsc_handover_attempt_count`	Counter	`type`	Ter (in int sub
`omnimsc_paging_attempt_count`	Counter	`result`	Ter (di d'a

Métrique	Type	Étiquettes	
`omnimsc_peer_status`	Gauge	`peer`	Éta (1=
`omnimsc_ss_operation_count`	Counter	`operation`, `ss_service`	Op sup
`omnimsc_ss_error_count`	Counter	`reason`	Err
`omnimsc_ussd_request_count`	Counter	`routing`	Re (lo
`omnimsc_map_dialogue_duration`	Histogram	`operation`	Ter dia
`omnimsc_call_release_count`	Counter	`type`	Lib (m

Valeurs des Étiquettes

omnimsc_location_update_complete_count -- l'étiquette `type` distingue les types de mise à jour de localisation selon 3GPP TS 24.008 :

Valeur	Description
`imsi_attach`	Attachement IMSI (abonné allumé)
`normal`	Mise à jour de localisation normale (abonné déplacé vers une nouvelle zone de localisation)
`periodic`	Mise à jour de localisation périodique (expiration du minuteur T3212)
`guest`	Abonné invité accepté (IMSI inconnu, provisionnement local d'invités)

omnimsc_auth_failure_count -- l'étiquette `reason` identifie la cause de l'échec. La FSM d'authentification émet actuellement une seule valeur :

Valeur	Description
`auth_failed`	Échec de l'authentification (mismatch SRES/RES ou échec signalé par le MS)

omnimsc_paging_attempt_count -- l'étiquette `result` suit les résultats de pagination :

Valeur	Description
`dispatched`	Pagination envoyée aux BSC(s)
`success`	Abonné a répondu à la pagination
`timeout`	Maximum de tentatives épuisées sans réponse

omnimsc_peer_status -- l'étiquette `peer` identifie le pair distant par son nom configuré (par exemple, Default-GW, International-GW, MSC-02).

omnimsc_ss_operation_count -- l'étiquette `operation` identifie l'opération SS (enregistrer, effacer, activer, désactiver, interroger) et l'étiquette `ss_service` identifie le service cible (cfu, cfb, cfnry, cfnrc, cw, clip, clir, baoc, baoic).

omnimsc_ussd_request_count -- l'étiquette `routing` distingue entre les requêtes SS traitées localement et celles relayées au HLR :

Valeur	Description
`local_ss`	Requête traitée localement par le MSC
`hlr_relay`	Requête relayée au HLR via MAP

omnimsc_call_release_count -- l'étiquette `type` distingue la direction de l'appel :

Valeur	Description
`mo`	Appel d'origine mobile libéré
`mt`	Appel terminé mobile libéré
`unknown`	Direction non déterminée au moment de la libération

Exemples de Requêtes PromQL

Les requêtes suivantes sont des points de départ utiles pour les tableaux de bord et les règles d'alerte.

Surveillance des appels actifs -- charge d'appels actuelle sur le MSC :

omnimsc_active_calls_count

Taux d'appels -- appels libérés par seconde, moyennés sur cinq minutes :

rate(omnimsc_call_release_count[5m])

Ratio d'échecs d'authentification -- échecs d'authentification par seconde par raison :

rate(omnimsc_auth_failure_count[5m])

Disponibilité des pairs -- identifier les pairs qui sont actuellement hors service :

omnimsc_peer_status

Débit SMS -- messages SMS par seconde :

rate(omnimsc_sms_sent_count[5m])

Taux de mise à jour de localisation par type -- répartition de l'activité LU :

sum by (type) (rate(omnimsc_location_update_complete_count[5m]))

Taux d'opération SS par service -- activité de service supplémentaire :

sum by (ss_service) (rate(omnimsc_ss_operation_count[5m]))

Répartition du routage USSD -- requêtes USSD locales vs relayées au HLR :

sum by (routing) (rate(omnimsc_ussd_request_count[5m]))

Système d'Alarme

OmniMSC déclenche et efface des alarmes pour des conditions nécessitant l'attention de l'opérateur. Chaque alarme a un niveau de gravité et un identifiant unique.

Types d'Alarme

Alarme	Gravité	Description
`sctp_link_down`	Critique	Association SCTP perdue vers STP
`hlr_unreachable`	Critique	HLR ne répond pas aux opérations MAP
`cdr_write_failure`	Majeur	Erreur d'écriture de fichier CDR
`overload`	Majeur	Seuil de surcharge du système dépassé

Événements de Télémétrie d'Alarme

Le sous-système d'alarme émet des événements de télémétrie qui peuvent être consommés par des systèmes de surveillance externes ou attachés aux métriques Prometheus :

Événement	Description
`[:omnimsc, :alarm, :raised]`	Émis lorsqu'une condition d'alarme est détectée. Les métadonnées incluent alarm_id, gravité, source et texte descriptif.
`[:omnimsc, :alarm, :cleared]`	Émis lorsqu'une condition d'alarme est résolue. Les métadonnées incluent alarm_id, gravité et source.

Les alarmes restent actives jusqu'à ce que la condition sous-jacente soit résolue, moment auquel l'événement d'effacement est émis. Plusieurs déclenchements du même alarm_id sans effacement intervenant sont dédupliqués.

Point de Terminaison de Santé

OmniMSC expose un point de vérification de santé à utiliser par les équilibreurs de charge et les systèmes d'orchestration.

GET /api/health renvoie l'état de santé global du système. La réponse indique si le MSC est opérationnel et accepte le trafic. Une réponse saine confirme que les sous-systèmes principaux (VLR, CC, client MAP, pile SIP) fonctionnent. Une réponse non saine indique qu'un ou plusieurs sous-systèmes critiques ont échoué.

Ce point de terminaison est adapté pour les sondes de vivacité et de préparation Kubernetes, ou pour les vérifications de santé des équilibreurs de charge dans des déploiements traditionnels.

Point de Terminaison d'État

GET /api/status renvoie des informations détaillées sur le système, y compris le nombre d'appels actifs, le nombre d'abonnés enregistrés, les états des liens de pairs, le résumé des alarmes, le nombre de processus BEAM et le temps de

fonctionnement. Ce point de terminaison fournit un instantané complet pour les tableaux de bord opérationnels et les fins de diagnostic.

La réponse d'état inclut toutes les informations nécessaires pour évaluer la capacité du système et identifier les composants dégradés sans nécessiter d'accès à Prometheus.

Protection contre la Surcharge

OmniMSC comprend un mécanisme de protection contre la surcharge configurable qui empêche le système de dépasser les limites de fonctionnement sûres. Le module de surcharge surveille en continu quatre métriques et les compare à des seuils configurables.

Seuils de Surcharge

Métrique	Seuil par Défaut	Description
Appels actifs	10,000	Maximum d'appels CS simultanés
Abonnés enregistrés	50,000	Maximum d'abonnés dans le VLR
Nombre de processus BEAM	500,000	Maximum de processus Erlang
Taux de pagination	1,000/sec	Maximum de requêtes de pagination par seconde

Lorsque l'un des seuils est dépassé, le module de surcharge rejette de nouvelles demandes de service avec la cause GSM 42 (congestion de l'équipement de commutation). Les appels déjà en cours ne sont pas affectés. L'état de surcharge est reflété dans l'événement de télémétrie `[:omnimsc, :overload, :state_change]` et l'alarme `overload`.

La protection contre la surcharge s'applique aux mises à jour de localisation, aux demandes d'établissement d'appels et aux transactions SMS. Les appels d'urgence contournent la protection contre la surcharge, quelle que soit la charge du système, conformément à 3GPP TS 22.101.

Pour la configuration des seuils, voir Référence de Configuration.

Piscine MSC et NRI

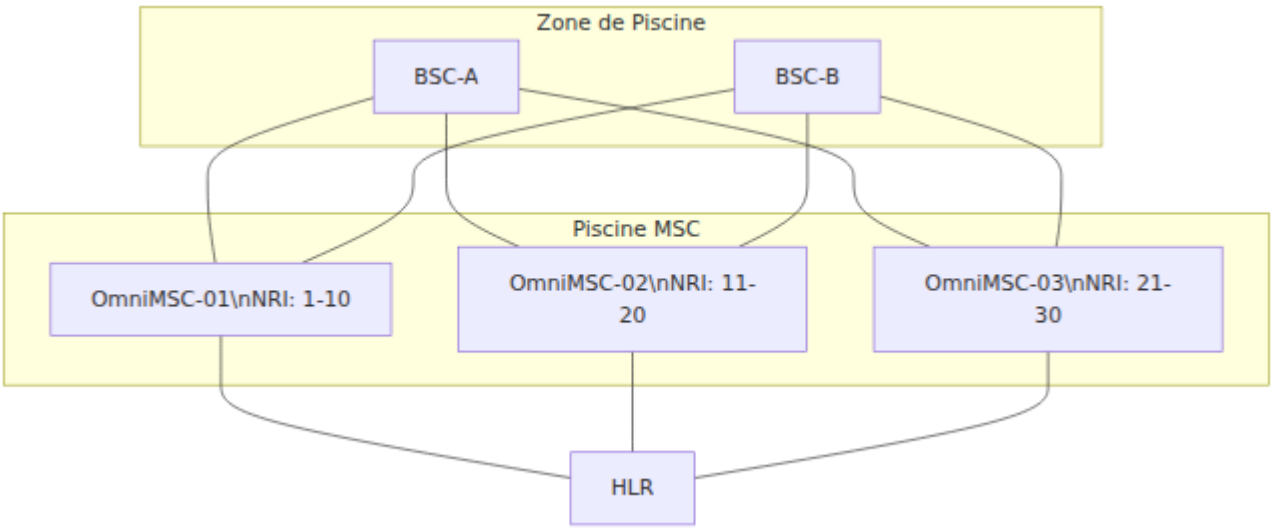
Ce document décrit l'architecture MSC-in-Pool mise en œuvre par OmniMSC par Omnitouch selon la norme 3GPP TS 23.236. Le pooling permet à plusieurs serveurs MSC de partager une zone de piscine commune, offrant une répartition de la charge entre les MSC et une résilience contre les pannes individuelles des MSC.

Pour un comportement de routage conscient de la piscine, voir Routage. Pour la page Pool dans l'interface web, voir Guide du Panneau de Contrôle. Pour les paramètres de configuration, voir Référence de Configuration. Pour les détails d'allocation TMSI, y compris le design sans rollback et l'intégration NRI, voir Sécurité.

Concept MSC-in-Pool

Dans une architecture traditionnelle, chaque BSC se connecte à un seul MSC. Si ce MSC échoue, tous les abonnés servis par ses BSC perdent le service. Le pooling MSC répond à cette limitation en permettant aux BSC de se connecter simultanément à plusieurs MSC via l'interface A-Flex. Tout MSC dans la piscine peut servir tout abonné arrivant de n'importe quel BSC dans la zone de la piscine.

Le mécanisme clé permettant le fonctionnement de la piscine est l'Identifiant de Ressource Réseau (NRI), un champ de bits intégré dans le TMSI qui identifie quel MSC a alloué ce TMSI. Lorsqu'un abonné présente un TMSI à un BSC, le BSC extrait le NRI et achemine le signalement vers le MSC correct. Si ce MSC n'est pas disponible, le BSC sélectionne un MSC alternatif dans la piscine, et le MSC récepteur gère l'abonné localement.



Chaque BSC maintient des associations SCTP avec chaque MSC dans la piscine. Pour les abonnés revenants, le BSC utilise le NRI dans le TMSI pour sélectionner le MSC qui a initialement enregistré l'abonné. Pour les nouveaux abonnés (sans TMSI ou NRI nul), le BSC utilise une sélection en round-robin ou basée sur la charge.

Identifiant de Ressource Réseau (NRI)

Le NRI est codé dans le TMSI de 32 bits alloué par le MSC. Les 8 bits les plus significatifs (bits 31-24) sont réservés ; le champ NRI commence au bit 23 et s'étend vers le bas sur `nri_bitlength` bits. Les bits de faible ordre restants (bit `23 - nri_bitlength` jusqu'au bit 0) sont la portion aléatoire du TMSI. La longueur du champ NRI est configurable et doit être identique entre tous les membres de la piscine.

Disposition des Bits TMSI

Pour un NRI de 10 bits, le champ réservé est les bits 31-24 (8 bits), le NRI occupe les bits 23-14 (10 bits), et la portion aléatoire est les bits 13-0 (14 bits) :



La longueur de bit NRI par défaut est de 10, supportant jusqu'à 1024 valeurs NRI distinctes. Les déploiements plus petits peuvent utiliser moins de bits. La portion aléatoire est toujours large de `24 - nri_bitlength` bits.

Longueur de Bit NRI	Valeurs NRI Maximales	Bits TMSI Restants (Aléatoires)
5	32	19
8	256	16
10	1024	14

Le "NRI nul" (valeur par défaut 0, configurable via `null_nri`) indique que le TMSI n'a pas été attribué par un membre de la piscine. Un abonné présentant un NRI nul est traité comme un nouvel abonné et accepté localement avec une nouvelle allocation de TMSI.

Allocation TMSI

Lorsque le mode piscine est actif, OmniMSC intègre l'une de ses valeurs NRI attribuées dans chaque TMSI qu'il alloue. Le processus d'allocation génère un TMSI de base aléatoire de 32 bits, puis écrase le champ de bits NRI avec la valeur NRI désignée du MSC. Cela garantit que tout BSC dans la zone de la piscine peut déterminer quel MSC possède un abonné donné en inspectant le TMSI. Pour le comportement général d'allocation et de confirmation TMSI (y compris le choix de design sans rollback), voir Sécurité.

Le MSC utilise sa première valeur NRI configurée comme valeur par défaut pour les nouvelles allocations. Toutes les valeurs NRI attribuées au MSC sont reconnues comme "locales" lors de l'évaluation des TMSI entrants.

Configuration

L'appartenance à la piscine est configurée sous la clé de piscine dans la configuration du MSC (voir Référence de Configuration). Les paramètres essentiels sont :

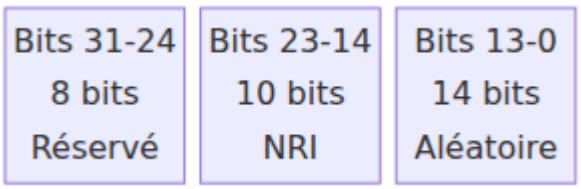
Paramètre	Par défaut	Description
enabled	false	Interrupteur principal pour le pooling. Doit être défini sur `true` pour que la configuration de la piscine prenne effet ; lorsque `false` (ou absent), le MSC fonctionne en mode autonome (non poolé).
pool_id	nil	Identifiant de la piscine. Tous les MSC dans la même piscine doivent partager le même pool_id.
nri_bitlength	10	Nombre de bits utilisés pour le champ NRI dans le TMSI. Doit être identique entre tous les membres de la piscine. Plage valide : 1 à 10.
nri_values	(liste vide)	Liste des valeurs NRI possédées par cette instance de MSC. Les TMSI alloués par ce MSC contiendront l'une de ces valeurs. Les plages NRI ne doivent pas se chevaucher entre les membres de la piscine.
members	(liste vide)	Liste des autres instances de MSC dans la piscine. Chaque entrée de membre comprend un nom logique, une adresse, un port et des valeurs NRI attribuées. Utilisé pour le relais d'abonnés basé sur le NRI et la surveillance de la santé.

Chaque entrée de membre dans la liste des membres nécessite :

Paramètre	Description
name	Nom logique du membre distant de la piscine
address	Adresse IP ou nom d'hôte du MSC distant, utilisé comme cible de la sonde de vivacité de santé
port	Port de signalisation sur le MSC distant (par défaut 2905), sondé via une tentative de connexion TCP ou SCTP pour déterminer la santé du membre
nri_values	Valeurs NRI attribuées au membre distant, utilisées pour identifier quel MSC possède un TMSI donné

Gestion des NRI Étrangers

Lorsqu'un abonné présente un TMSI contenant un NRI appartenant à un autre membre de la piscine, le MSC récepteur doit décider comment gérer l'abonné. Cette situation se produit lorsque la fonction de sélection basée sur le NRI du BSC (NNSF) achemine vers le mauvais MSC, ou lorsque le MSC propriétaire n'est pas disponible.



Le Gestionnaire de Piscine accepte toujours l'abonné localement et réalloue le TMSI avec une valeur NRI locale. La décision sur la façon de résoudre l'identité de l'abonné dépend de l'état de santé du MSC propriétaire :

État du MSC Propriétaire	Comportement
Accessible	Envoyer MAP SendIdentification au MSC propriétaire pour récupérer l'IMSI et les vecteurs d'authentification, puis continuer la mise à jour de localisation avec l'identité reçue
Inaccessible	Demander directement l'IMSI à l'UE via une Demande d'Identité, puis récupérer les vecteurs d'authentification depuis le HLR
Inconnu	Même comportement que inaccessible ; demander l'IMSI à l'UE

Dans tous les cas, l'abonné est réenregistré au MSC récepteur avec un nouveau TMSI contenant une valeur NRI locale.

Suivi de la Santé des Membres de la Piscine

Chaque MSC dans la piscine surveille la santé des autres membres de la piscine. L'état de santé est suivi par membre et affecte directement le comportement de gestion des NRI étrangers.

État du Membre	Description	Effet sur la Gestion des NRI Étrangers
Up	Le membre répond aux sondes de santé	Les abonnés NRI étrangers sont identifiés via MAP SendIdentification au MSC propriétaire
Down	Le membre n'a pas répondu dans la période de timeout	Les abonnés NRI étrangers sont identifiés en demandant l'IMSI à l'UE
Unknown	État initial avant que les sondes de santé ne soient complétées	Traité de la même manière que Down
Draining	Le membre a annoncé un drainage pour maintenance	Aucun nouvel abonné n'est relayé ; les sessions existantes sont maintenues jusqu'à leur achèvement

Lorsqu'un membre de la piscine redémarre, il diffuse un MAP Reset à tous les membres de la piscine. Les MSC récepteurs marquent tous les enregistrements d'abonnés appartenant à l'MSC réinitialisé pour réenregistrement lors du prochain contact. Les changements d'état de santé sont diffusés au Panneau de Contrôle via PubSub pour une visibilité en temps réel.

Procédure de Mise à Niveau Continue

L'architecture de la piscine permet des mises à niveau sans temps d'arrêt en drainant et en mettant à niveau un MSC à la fois.

1. Mettre l'MSC cible en état de drainage via le Panneau de Contrôle ou l'API. Les BSC cessent d'envoyer de nouveaux abonnés à cet MSC ; les sessions

existantes continuent.
2. Attendre que les appels actifs se terminent naturellement. Surveiller le nombre d'appels actifs sur le tableau de bord.
3. Émettre une Commande de Nettoyage à toutes les connexions BSC restantes.
4. Arrêter le processus MSC. Les abonnés restants se réenregistreront sur d'autres membres de la piscine lors du prochain contact.
5. Appliquer la mise à jour logicielle ou le changement de configuration.
6. Démarrer le MSC mis à niveau. Il établit des associations SCTP avec les BSC et s'annonce via MAP Reset.
7. Le MSC commence à accepter de nouveaux abonnés. Les BSC l'incluent dans leur algorithme de sélection.
8. Vérifier la santé sur la page de la Piscine : l'état du membre est Up, l'allocation NRI est correcte, les abonnés s'enregistrent.

Répéter pour chaque MSC dans la piscine.

Page LiveView de la Piscine

La page Piscine dans le Panneau de Contrôle affiche :

- Identité de la piscine : ID de la piscine, valeurs NRI locales, longueur de bit NRI.
- Tableau d'état des membres : nom, adresse et port, plage NRI, état de santé (Up, Down ou Draining), horodatage de la dernière sonde, et nombre d'abonnés par membre.
- Graphique de distribution NRI : distribution visuelle des abonnés à travers les plages NRI.
- Événements NRI étrangers : rencontres NRI étrangères récentes montrant le TMSI présenté, MSC propriétaire, et résultat (relayé via MAP SendIdentification, résolu via demande IMSI, ou échoué).
- Statistiques de la piscine : total des abonnés de la piscine, ratio NRI local par rapport aux NRI étrangers, taux de réussite du relais.

Références de Spécification 3GPP

Spécification	Titre	Pertinence
TS 23.236	Connexion intra-domaine des nœuds RAN à plusieurs nœuds CN	Architecture de piscine MSC, format NRI, sélection BSC
TS 23.012	Procédures de Gestion de Localisation	Interaction VLR avec l'opération de piscine
TS 29.002	Spécification MAP	MAP SendIdentification, MAP Reset pour la coordination de piscine
TS 48.008	Interface BSC-MSC (A-Flex)	Extensions A-Flex pour le signalement BSSAP conscient de la piscine

Routage

Ce document décrit comment OmniMSC par Omnitouch analyse les numéros appelés, sélectionne les itinéraires et livre les appels à leurs destinations. Il couvre le pipeline d'analyse des numéros, la table de routage, les types de destinations pris en charge, la fonction GMSC et les interfaces de gestion des itinéraires.

Pour des diagrammes de flux d'appel montrant comment le routage s'intègre à la configuration des appels, voir Diagrammes de flux d'appel. Pour les paramètres de configuration de la table de routage, voir Référence de configuration. Pour la surveillance de la santé des pairs SIP, voir Trunking SIP. Pour les détails du groupe de troncs ISUP, voir Trunking ISUP. Pour la gestion des itinéraires via le panneau de contrôle, voir Guide du panneau de contrôle.

Analyse des numéros

Lorsqu'un appel est initié, OmniMSC classe le numéro appelé pour déterminer son type et le normaliser au format E.164. La classification suit un ordre de priorité et utilise la configuration de routage pour le déploiement (code pays, préfixe national, préfixe international, numéros d'urgence et codes courts).

Ordre de classification

Le moteur d'analyse des numéros évalue le numéro appelé par rapport aux catégories suivantes dans l'ordre. La première correspondance l'emporte.

Priorité	Type de numéro	Règle de détection	Normalisation
1	Urgence	Correspondance exacte avec la liste de numéros d'urgence configurée (par défaut `["112", "911", "110"]`; configurable par l'opérateur)	Inchangé; l'indice de routage est défini sur :urgence
2	Code court	Correspondance exacte avec la table de codes courts configurée, où chaque code correspond à un type de service (assistance de l'opérateur, demande d'annuaire, etc.)	Inchangé; l'indice de routage est défini sur l'atome du type de service
3	International	Le numéro commence par "+" ou par le préfixe international configuré (par défaut "00")	Détaché du préfixe international et précédé de "+" pour produire E.164
4	National	Le numéro commence par le préfixe national configuré (par défaut "0")	Le préfixe national est détaché, puis le code pays est précédé de "+" pour produire E.164
5	Local	Tout numéro restant qui ne correspond pas aux précédents	Le code pays et le code régional sont précédés de "+" pour produire E.164

Après classification, le numéro E.164 normalisé est passé à la table de routage pour correspondance de préfixe le plus long.

Table de routage

La table de routage est une structure de données soutenue par ETS qui associe les préfixes de numéros aux destinations. C'est le point de décision central pour tout le routage des appels sortants dans OmniMSC.

Correspondance de préfixe le plus long

Lorsqu'un numéro est présenté pour le routage, la table de routage itère de la longueur complète du numéro jusqu'à un seul chiffre, vérifiant une correspondance de préfixe à chaque étape. La première correspondance (la plus longue) trouvée est utilisée. Si aucune correspondance spécifique de préfixe n'est trouvée, la table revient à l'itinéraire par défaut (le préfixe est la chaîne vide). Si aucun itinéraire par défaut n'existe, l'appel échoue avec une erreur de no-route-to-destination.

Ordre de priorité

Chaque entrée de routage porte une valeur de priorité numérique. Des valeurs plus élevées ont la priorit��. La priorité est utilisée lorsque la table de routage est affichée et lors de la gestion des entrées qui se chevauchent. Les itinéraires d'urgence doivent être configurés avec la priorité la plus élevée (par exemple, 100) pour s'assurer qu'ils ne sont jamais éclipsés par des entrées moins spécifiques.

Exemple de table de routage

Le tableau suivant illustre comment la table de routage résout différents numéros appelés.

Préfixe	Type	Destination	Priorité	But
000	:sip	Pair SIP "Default-GW"	100	Numéro d'urgence — l'itinéraire doit correspondre à `psap_address`
04	:local	Abonné VLR	50	Numéros de mobile australien
0412	:sip	Pair SIP "Mobile-GW"	50	Préfixe mobile spécifique routé vers une passerelle SIP
001	:sip	Pair SIP "International-GW"	10	Préfixe de composition internationale
07	:isup	Groupe de troncs "Mobile-Interconnect"	10	Interconnexion mobile via SS7
08	:sip_with_failover	Principal : Pair SIP "Primary-SIP-GW", Secours : Tronc ISUP "Backup-ISUP"	10	SIP avec secours ISUP automatique
09	:sip_i	Pair SIP-I "MSC-02-SIP-I"	10	SIP avec ISUP encapsulé vers un MSC pair

Préfixe	Type	Destination	Priorité	But
(vide)	:sip	Pair SIP "Default-GW"	1	Itinéraire par défaut catch-all

Avec cette table en place :

Numéro composé	Préfixe correspondant	Destination	Raison
000	000	SIP : Default-GW	Correspondance exacte sur le préfixe d'urgence
0412345678	0412	SIP : Mobile-GW	Correspondance la plus longue (4 chiffres bat l'entrée de 2 chiffres "04")
0498765432	04	Abonné VLR local	Correspond à "04" mais pas à "0412"
0011234567	001	SIP : International-GW	Correspondance la plus longue (3 chiffres)
0312345678	(vide)	SIP : Default-GW	Aucune correspondance de préfixe; tombe sur le par défaut

---

Types d'itinéraires

OmniMSC prend en charge les types de destinations suivants dans la table de routage.

Appels d'urgence

Les appels d'urgence ne sont pas un type d'itinéraire séparé. Le MSC détecte les appels d'urgence à partir du type de message CC Emergency Setup (3GPP TS 24.008 §9.3.8, type de message 0x0E) et du type de demande de service CM (`:emergency`). L'authentification est tentée mais l'appel se poursuit indépendamment du résultat. Le chiffrement est établi si l'authentification réussit ; sinon, l'appel se poursuit sans.

Les messages Emergency Setup ne portent pas de numéro BCD de partie appelée — le combiné envoie uniquement un IE de capacité de support optionnel et un IE de catégorie de service d'urgence. Le MSC utilise le `psap_address` de la configuration d'urgence comme numéro appelé pour la recherche dans la table de routage. Ce numéro est ensuite routé à travers la table de routage normale comme tout autre appel. L'entrée de routage à laquelle il correspond peut être de tout type (`:sip`, `:isup`, `:sip_i`, etc.).

Exemple : Pour router les appels d'urgence vers un pair SIP nommé "Default-GW" :

```
# Table de routage — psap_address "000" correspondra à cette
entrée
%{prefix: "000", type: :sip, peer: "Default-GW", priority: 100}

# Configuration d'urgence — psap_address est utilisé comme numéro
appelé
config :omnimsc, Omnimsc.Emergency,
  psap_address: "000"
```

Si l'authentification échoue, l'IMEI de l'appelant est utilisé comme numéro de partie appelante au lieu du MSISDN. Les numéros d'urgence sont également détectés lors de l'analyse des numéros et peuvent déclencher un traitement d'urgence même avant que la table de routage ne soit consultée.

:local

Routage de l'appel vers un abonné enregistré dans le VLR local. Le MSC recherche le MSISDN appelé dans le VLR, page l'abonné via le BSC ou RNC approprié, et établit l'appel via l'interface A ou l'interface Iu-CS.

:sip

Routage de l'appel vers un pair SIP configuré en envoyant une invitation SIP. L'entrée de routage spécifie le pair par son nom ; l'adresse IP, le port, le transport et la configuration du codec du pair sont résolus à partir de la table des pairs SIP. Le Trunk Router vérifie que le pair est joignable (le statut n'est pas "down") et que le pair a des canaux disponibles avant de router.

:isup

Routage de l'appel via un groupe de troncs ISUP SS7. L'entrée de routage spécifie le nom du groupe de troncs, le code de point de destination et la plage de CIC (Circuit Identification Code). Le Trunk Router alloue un circuit inactif du groupe de troncs, construit un message d'adresse initiale (IAM) et l'envoie via le transport M3UA/SCTP vers l'échange distant.

:sip_i

Routage de l'appel vers un pair SIP-I, où le message ISUP complet est encapsulé dans le corps SIP. SIP-I préserve tous les éléments d'information ISUP lors de l'interconnexion, évitant la perte d'information qui peut se produire avec la conversion standard SIP-ISUP. Pour les détails du protocole, voir Trunking SIP-I.

:sip_with_failover

Tente l'appel via un pair SIP principal en premier. Si le pair SIP est injoignable, renvoie une erreur 5xx ou expire, le Trunk Router réessaie automatiquement l'appel via un groupe de troncs ISUP de secours configuré. Ce type de destination nécessite à la fois un nom de pair SIP (principal) et un groupe de troncs ISUP avec code de point (secours).

:gmsc

Invoque la fonction Gateway MSC. Le MSC envoie une demande MAP SendRoutingInfo au HLR pour obtenir le MSRN (Mobile Station Roaming Number) pour l'abonné appelé, puis route l'appel vers le MSC de service en utilisant le MSRN retourné. Voir la section Fonction GMSC ci-dessous pour plus de détails.

:transit

Routage de l'appel en tant qu'appel de transit entre les types de troncs sans instancier un FSM de contrôle d'appel complet. Les itinéraires de transit sont utilisés pour l'opération passerelle ISUP vers SIP, l'interconnexion SIP vers ISUP, le commutateur tandem ISUP vers ISUP, et le transit proxy SIP vers SIP. Les itinéraires de transit incluent le contexte source (le type et le nom du tronc entrant) pour faire correspondre les appels entrants de troncs spécifiques.

Gestion de la table de routage

Interface Web

La page Routes et Trunks dans le panneau de contrôle OmniMSC fournit une interface à onglets pour gérer les itinéraires, les groupes de troncs ISUP et les pairs SIP. À partir de l'onglet Table de routage, les opérateurs peuvent ajouter, modifier et supprimer des itinéraires via des formulaires modaux. Les modifications d'itinéraires prennent effet immédiatement sans nécessiter de redémarrage. Les itinéraires chargés à partir de la configuration au démarrage peuvent être remplacés à l'exécution. Pour des détails sur l'interface web, voir Guide du panneau de contrôle.

API REST

Les itinéraires peuvent également être gérés de manière programmatique via l'API REST.

Méthode	Point de terminaison	Description
GET	/api/routes	Liste tous les itinéraires dans la table
POST	/api/routes	Ajoute un itinéraire. Le corps de la requête inclut le préfixe, le type, le pair (pour les types SIP) et la priorité.
DELETE	/api/routes/{id}	Supprime un itinéraire par son préfixe (le paramètre de chemin `id` est le préfixe de l'itinéraire)

Test de recherche d'itinéraire

Le point de terminaison de recherche d'itinéraire permet aux opérateurs et aux systèmes d'intégration de tester les décisions de routage sans passer un appel.

Méthode	Point de terminaison	Description
GET	/api/routes/lookup/:number	Renvoie la destination qui serait sélectionnée pour le numéro appelé donné, ou une indication de no-route si aucune correspondance n'existe

---

Fonction GMSC

Lorsque OmniMSC reçoit un appel pour un abonné mobile qui n'est pas enregistré dans le VLR local, il peut agir en tant que Gateway MSC (GMSC) conformément à la 3GPP TS 23.018. La fonction GMSC comble le fossé entre le réseau appelant et le MSC visité où l'abonné est actuellement enregistré.

Flux de routage des appels MT

1. Un appel entrant arrive d'un tronc PSTN ou d'une passerelle SIP avec le MSISDN de l'abonné comme numéro appelé.
2. La recherche dans la table de routage renvoie le type de destination :gmsc pour ce préfixe.
3. OmniMSC envoie une demande MAP SendRoutingInfo (SRI) au HLR de l'abonné, fournissant le MSISDN appelé.
4. Le HLR identifie le VLR de service et lui demande d'allouer un Mobile Station Roaming Number (MSRN).
5. Le HLR renvoie le MSRN à OmniMSC dans la réponse SRI.
6. OmniMSC route l'appel vers le MSC de service en utilisant le MSRN, soit via un IAM ISUP, soit via une invitation SIP en fonction du type d'interconnexion.
7. Le MSC de service page l'abonné et complète la configuration de l'appel MT.

Pool MSRN

OmniMSC maintient un pool de MSRNs pour allocation lors du routage des appels MT. Lorsqu'un abonné est pagé au MSC local, un MSRN est alloué à partir du pool, associé à l'IMSI de l'abonné, et renvoyé au GMSC qui interroge. Le MSRN est libéré de nouveau dans le pool une fois que l'appel entrant arrive ou que l'allocation expire.

Routage conscient du pool

Lorsque le mode de pool MSC est actif (voir Pool MSC et NRI), le module de routage prend en compte le NRI intégré dans le TMSI de l'abonné lors du routage des appels MT. Si le TMSI d'un abonné contient un NRI étranger (appartenant à un autre membre du pool), le MSC peut relayer l'abonné au MSC propriétaire via MAP SendIdentification, réenregistrer l'abonné localement si le MSC propriétaire est injoignable, ou router les appels MT vers le MSC propriétaire si l'abonné ne s'est pas encore réenregistré localement.

Le routage basé sur le NRI est automatique lorsque le mode pool est activé et ne nécessite pas d'entrées explicites dans la table de routage.

Flux d'analyse des numéros

Le flux complet de décision de routage, du numéro appelé à la destination, se déroule à travers les étapes suivantes :

1. Vérification de l'interdiction d'appel -- si l'abonné est interdit de ce type d'appel, l'appel est rejeté avec un code de cause GSM.
2. Vérification du déclencheur CAMEL -- si une clé de service CAMEL correspond, un InitialDP est envoyé au SCP. Le SCP peut modifier le numéro appelé, se connecter à une destination différente ou libérer l'appel.
3. Analyse du numéro -- le numéro appelé est classé et normalisé comme décrit ci-dessus.
4. Recherche dans la table de routage -- correspondance de préfixe le plus long contre la table de routage.
5. Dispatch de la destination -- l'appel est remis au gestionnaire approprié en fonction du type de destination correspondant.
6. Secours (le cas échéant) -- pour les itinéraires :sip_with_failover, une tentative SIP échouée déclenche un réessai automatique via le tronc de secours ISUP.

Groupes de troncs ISUP

Chaque groupe de troncs ISUP représente un ensemble de circuits vocaux vers un échange SS7 distant. Les groupes de troncs sont identifiés par un nom et configurés avec un code de point de destination et une plage de CIC. Lorsque le routage sélectionne un groupe de troncs ISUP, le Trunk Router alloue le premier circuit inactif trouvé dans le groupe de troncs et envoie un IAM.

Les groupes de troncs prennent en charge des niveaux de priorité : principal (premier choix), débordement (utilisé lorsque les circuits principaux sont

épuisés) et dernier recours. Seuls les groupes de troncs actifs sont sélectionnés pour le routage ; les groupes de troncs inactifs ou congestionnés sont ignorés.

Chaque groupe de troncs suit les compteurs de saisie, de réponse, de saturation, de congestion et de libération pour la surveillance opérationnelle.

Sélection des pairs SIP

Les pairs SIP représentent des passerelles VoIP distantes, des nœuds IMS ou des fournisseurs de trunking SIP. Chaque pair est configuré avec une adresse, un port, un transport (UDP, TCP ou TLS), des codecs pris en charge et un maximum de canaux concurrents.

La santé des pairs est surveillée via des keepalives SIP OPTIONS périodiques. Si un pair cesse de répondre, son statut passe à "down" et le pair est exclu du routage. Lorsqu'un itinéraire spécifie un pair SIP par son nom, le Trunk Router vérifie que le pair est joignable et dispose de la capacité disponible avant de router l'appel.

Références de spécification 3GPP

Spécification	Titre	Pertinence
TS 23.018	Gestion de base des appels	Fonction GMSC, routage des appels MT, analyse des numéros
TS 29.002	Spécification MAP	MAP SendRoutingInfo, allocation de MSRN
TS 23.078	CAMEL Phase 4	Gestion des déclencheurs CAMEL dans le flux de routage

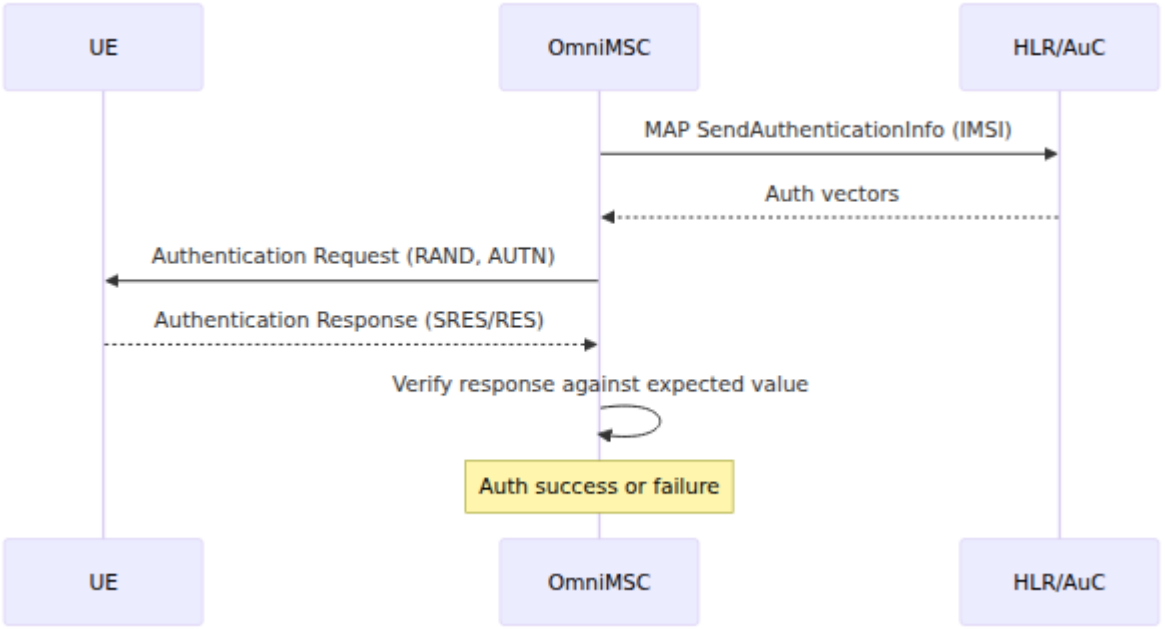
Sécurité

Ce document décrit les mécanismes d'authentification, de chiffrement et de gestion d'identité mis en œuvre par OmniMSC, y compris l'authentification GSM et UMTS, le chiffrement de l'interface radio, l'allocation de TMSI et les procédures de demande d'identité. Pour la configuration des algorithmes de chiffrement et des paramètres de sécurité, voir Référence de Configuration. Pour les opérations MAP qui prennent en charge l'authentification, voir Opérations MAP. Pour l'allocation de TMSI dans les déploiements de pool MSC avec encodage NRI, voir Pool MSC et NRI.

Vue d'ensemble de l'authentification

OmniMSC prend en charge à la fois l'authentification GSM (2G) et UMTS (3G) comme défini dans 3GPP TS 33.102 et TS 24.008 Section 4.3. L'authentification est effectuée lors des mises à jour de localisation et, en option, lors de l'établissement d'appels et des transactions SMS.

Le MSC ne stocke pas les identifiants d'abonné à long terme (Ki). Les vecteurs d'authentification sont obtenus auprès du HLR/AuC via MAP SendAuthenticationInfo (voir Opérations MAP). Le MSC envoie l'IMSI au HLR, qui renvoie un ensemble de vecteurs d'authentification. Le MSC défie ensuite l'UE et vérifie sa réponse. L'état d'authentification actuel de l'abonné et le nombre de tuples restants sont visibles dans le panneau de contrôle — voir Guide du Panneau de Contrôle.



UMTS AKA (Authentification et Accord de Clé)

L'Authentification et Accord de Clé UMTS fournit une authentification mutuelle -- le réseau authentifie l'abonné et l'abonné authentifie le réseau. C'est la méthode d'authentification préférée pour les terminaux équipés de USIM.

Le HLR renvoie des quintuplets, chacun contenant cinq valeurs :

Champ	Taille	Description
RAND	128 bits	Défi aléatoire généré par AuC
XRES	32-128 bits	Réponse attendue, utilisée par le MSC pour vérifier l'UE
CK	128 bits	Clé de chiffrement pour le chiffrement de l'interface radio
IK	128 bits	Clé d'intégrité pour la protection d'intégrité de l'interface radio
AUTN	128 bits	Jeton d'authentification, utilisé par l'UE pour vérifier le réseau

Le MSC envoie RAND et AUTN à l'UE. L'USIM vérifie AUTN pour authentifier le réseau, puis calcule RES, CK et IK. Le MSC compare le RES retourné avec XRES pour authentifier l'abonné.

Resynchronisation SQN

AUTN contient un numéro de séquence (SQN) que l'USIM vérifie pour prévenir les attaques par rejeu. Si l'USIM détermine que SQN est hors de portée (par exemple, après une longue période d'inactivité ou une restauration de base de données), il renvoie un Échec d'Authentification avec la cause "échec SQN" et inclut un AUTS (jeton de resynchronisation) de 112 bits. Le MSC transmet AUTS au HLR dans une nouvelle demande MAP SendAuthenticationInfo, permettant à l'AuC de resynchroniser son compteur SQN et de renvoyer des vecteurs frais.

GSM AKA

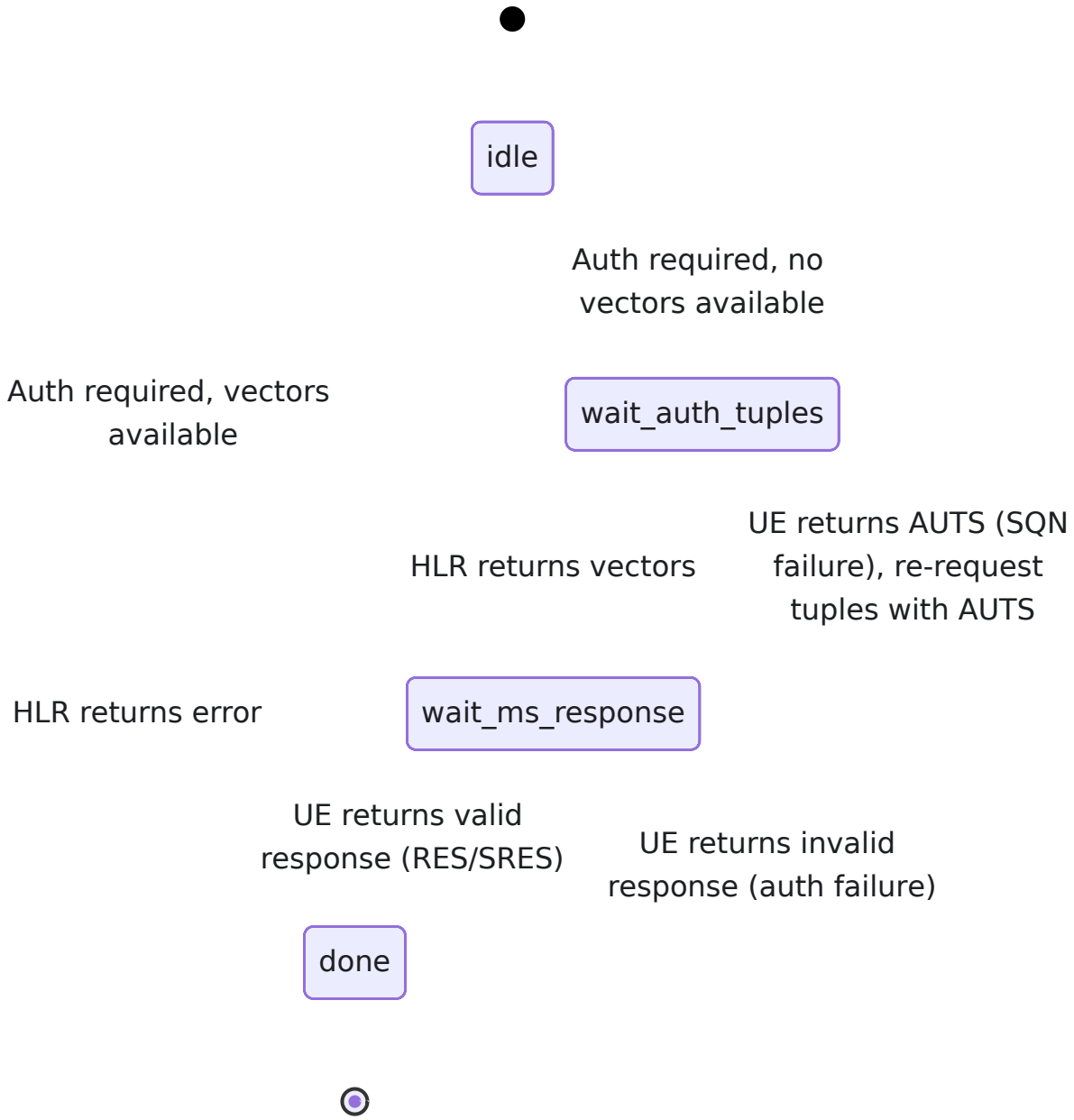
L'authentification GSM utilise des triplets pour les abonnés uniquement 2G (SIM sans application USIM). Chaque triplet contient :

Champ	Taille	Description
RAND	128 bits	Défi aléatoire
SRES	32 bits	Réponse signée, calculée par la SIM utilisant A3(Ki, RAND)
Kc	64 bits	Clé de chiffrement, calculée par la SIM utilisant A8(Ki, RAND)

L'authentification GSM est unidirectionnelle : le réseau authentifie l'abonné, mais l'abonné n'authentifie pas le réseau. Le MSC envoie RAND, la SIM calcule SRES et Kc, et le MSC vérifie SRES par rapport à la valeur attendue du triplet.

États de la FSM d'authentification

La procédure d'authentification est gérée par une machine à états finis au sein du VLR. La FSM suit l'avancement de chaque tentative d'authentification.



Dans l'état `wait_auth_tuples`, le MSC a envoyé MAP SendAuthenticationInfo et attend des vecteurs du HLR. Dans `wait_ms_response`, le MSC a envoyé une Demande d'Authentification à l'UE et attend la réponse. Lorsque l'UE signale un décalage de numéro de séquence (AUTS), la FSM réintègre `wait_auth_tuples` — elle redemande des vecteurs frais au HLR en envoyant MAP SendAuthenticationInfo portant le jeton de resynchronisation AUTS. Il n'y a pas d'état de resynchronisation séparé ; la resynchronisation est gérée comme un retour à `wait_auth_tuples`.

Chiffrement

Après une authentification réussie, le MSC initie le chiffrement de l'interface radio pour protéger la signalisation et le trafic utilisateur sur le chemin radio.

GERAN (2G/3G via BSC)

Pour l'interface A, le MSC envoie une commande de mode de chiffrement BSSMAP au BSC, portant la clé de chiffrement (Kc) et l'algorithme A5 sélectionné. Le BSC active le chiffrement sur le canal radio et renvoie le mode de chiffrement complet.

Algorithme	Sécurité	Description
A5/1	Modéré	Chiffre GSM original, largement déployé
A5/3	Fort	Chiffre basé sur KASUMI, recommandé pour tous les déploiements

UTRAN (3G via RNC)

Pour l'interface Iu-CS, le MSC envoie une commande de mode de sécurité RANAP au RNC, portant CK, IK, et les algorithmes UEA (chiffrement) et UIA (intégrité) sélectionnés. Le RNC active le chiffrement et la protection d'intégrité et renvoie le mode de sécurité complet.

Configuration A5 Autorisée

L'opérateur configure l'ensemble des algorithmes A5 autorisés. Le MSC sélectionne l'algorithme le plus fort pris en charge à la fois par la configuration du réseau et par les capacités rapportées de la station mobile.

Les algorithmes autorisés sont spécifiés sous forme de liste : `allowed_a5: [:a5_1, :a5_3]`. Le MSC croise cette liste avec les capacités de classe de la MS et sélectionne la correspondance de la plus haute force. Si aucun algorithme commun n'existe et que A5/0 n'est pas autorisé, le MSC rejette la connexion.

Allocation de TMSI

Le MSC alloue une Identité Mobile Abonnée Temporaire (TMSI) à chaque abonné après une mise à jour de localisation réussie. Le TMSI remplace l'IMSI pour les pages et l'identification ultérieures, réduisant l'exposition de l'identité permanente sur l'interface radio.

Allocation et Confirmation

Après avoir terminé l'authentification, le chiffrement et l'échange de mise à jour de localisation HLR, le MSC génère un nouveau TMSI et l'envoie à la station mobile dans le message d'Acceptation de Mise à Jour de Localisation. La MS stocke le TMSI et répond avec TMSI Reallocation Complete.

Si le TMSI Reallocation Complete n'est pas reçu dans le délai de réallocation, le MSC confirme le nouveau TMSI plutôt que de revenir en arrière. Ce choix de conception empêche un scénario où la MS a réussi à stocker le nouveau TMSI mais la confirmation a été perdue sur l'interface radio -- revenir en arrière laisserait le MSC et la MS avec des TMSI non concordants, rompant les pages ultérieures.

TMSI dans le Pool MSC

Lorsqu'il fonctionne dans un pool MSC (3GPP TS 23.236), le TMSI porte des bits NRI (Identifiant de Ressource Réseau) qui permettent au BSC de router les abonnés revenants vers le MSC correct dans le pool. Le NRI est intégré dans une plage de bits configurable au sein du TMSI. Lorsqu'un BSC reçoit une demande de service ou une réponse de page contenant un TMSI, il extrait le NRI et route la signalisation vers le MSC qui possède cette plage de NRI.

Pour la configuration du pool MSC et l'attribution de NRI, voir Pool MSC & NRI.

Demande d'Identité

Lorsque le MSC ne peut pas résoudre l'identité d'un abonné -- par exemple, lorsqu'un TMSI est présenté qui n'est pas trouvé dans le VLR local (après un redémarrage du MSC, un routage de pool, ou un débordement de VLR) -- le MSC envoie une Demande d'Identité à la station mobile demandant l'IMSI.

La MS r��pond avec une Réponse d'Identité contenant son IMSI. Le MSC procède ensuite à l'authentification en utilisant l'IMSI. Cette procédure est définie dans 3GPP TS 24.008 Section 4.3.3.

La Demande d'Identité est également utilisée pour obtenir l'IMEI (Identité Internationale d'Équipement Mobile) lorsque la vérification de l'équipement est requise.

Références de Spécification 3GPP

Spécification	Titre	Pertinence
TS 33.102	Sécurité 3G ; Architecture de Sécurité	UMTS AKA, quintuplets, resynchronisation SQN, hiérarchie de clés
TS 24.008	Couche 3 de l'Interface Radio Mobile	Demande/Réponse d'Authentification (Sec 4.3), Demande d'Identité (Sec 4.3.3), Réallocation de TMSI (Sec 4.3.1)
TS 43.020	Fonctions Réseau Liées à la Sécurité	Algorithmes de chiffrement GSM A3/A8, A5
TS 48.008	Interface MSC-BSS (BSSMAP)	Commande/Complète de Mode de Chiffrement
TS 25.413	Interface Iu UTRAN (RANAP)	Commande/Complète de Mode de Sécurité
TS 23.236	Connexion Intra-Domaine des Nœuds RAN à Plusieurs Nœuds CN	Allocation de NRI, structure de TMSI pour le pool MSC
TS 29.002	Spécification MAP	MAP SendAuthenticationInfo

Interface SGs et CSFB

Ce document décrit l'interface SGs et l'implémentation du Circuit-Switched Fallback (CSFB) dans OmniMSC par Omnitouch selon la norme 3GPP TS 29.118. L'interface SGs connecte le MSC/VLR au MME, permettant une attache combinée EPS/IMSI, la pagination CS via le réseau LTE, et la livraison de SMS sans CS fallback.

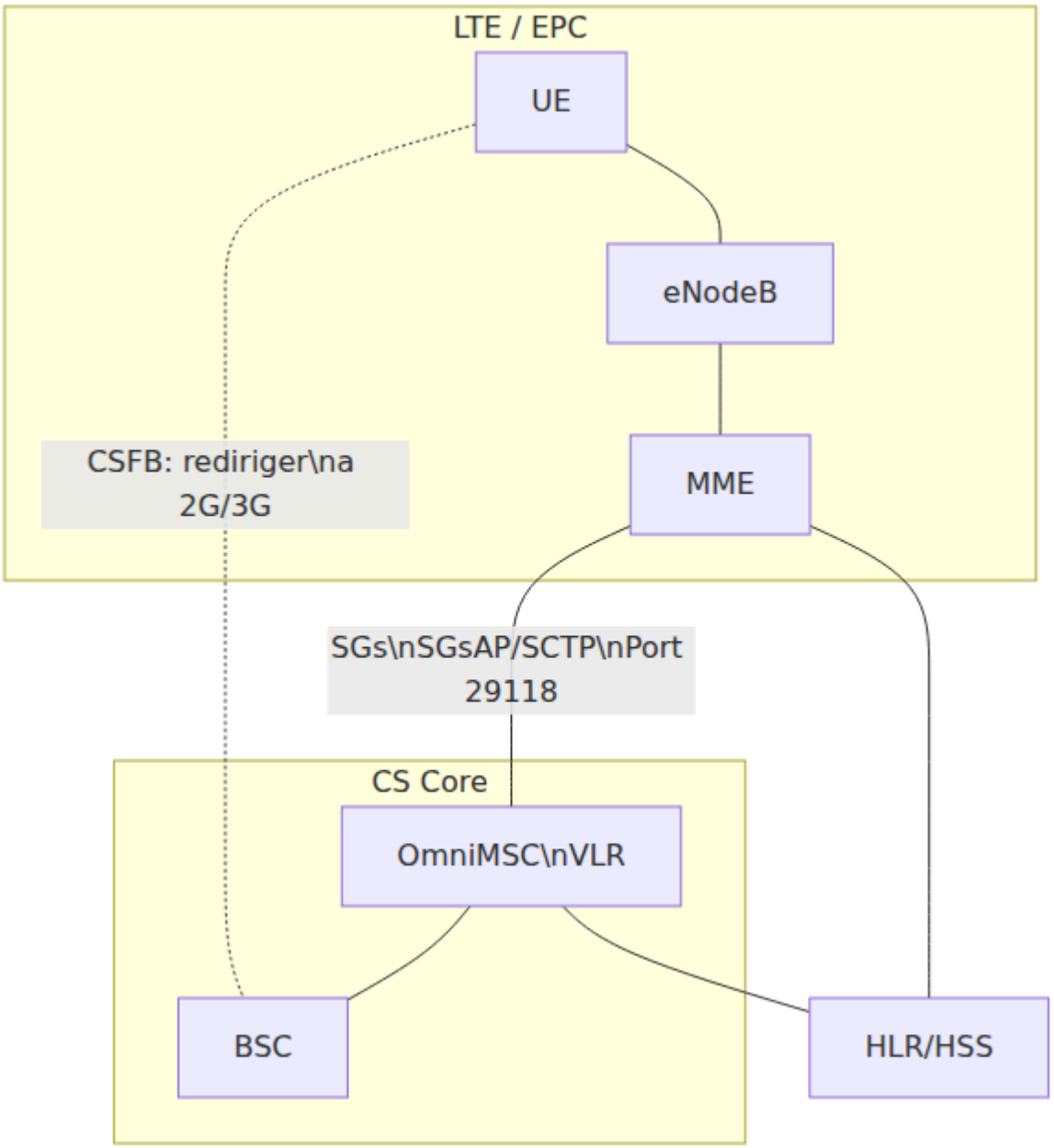
Pour le diagramme de séquence d'appel CSFB MT, voir Diagrammes de flux d'appel. Pour les paramètres de configuration, voir Référence de configuration. Pour l'authentification lors de l'attache combinée, voir Authentification & Sécurité. Pour les SMS sur SGs, voir SMS. Pour les considérations de Pool MSC avec CSFB, voir Pool MSC.

Vue d'ensemble

Dans les réseaux LTE, le MME gère la gestion de la mobilité pour les services à commutation de paquets. Cependant, le LTE ne prend pas en charge nativement la voix à commutation de circuit avant le déploiement de VoLTE. Le CSFB permet aux abonnés attachés en LTE de recevoir et de passer des appels vocaux CS et des SMS en revenant au domaine CS 2G/3G.

L'interface SGs est le lien de signalisation entre le MSC/VLR et le MME, transportant les messages SGsAP sur SCTP (port par défaut 29118). Grâce à SGs, le MSC peut :

- Effectuer une attache combinée EPS/IMSI, enregistrant un abonné à la fois dans le domaine EPC et dans le domaine CS simultanément.
- Pager les abonnés attachés en LTE pour des appels CS entrants, déclenchant un retour vers GERAN ou UTRAN.
- Livrer des SMS aux abonnés attachés en LTE sans CSFB, tunnelisant le PDU NAS à travers l'interface SGs.



Types de messages SGsAP

L'interface SGs transporte les types de messages SGsAP suivants selon la norme 3GPP TS 29.118.

Mise à jour de localisation

Message	Direction	But
SGsAP-LOCATION-UPDATE-REQUEST	MME vers MSC	Attache combinée EPS/IMSI ou mise à jour de zone de localisation périodique
SGsAP-LOCATION-UPDATE-ACCEPT	MSC vers MME	Mise à jour de localisation acceptée, inclut un nouveau TMSI
SGsAP-LOCATION-UPDATE-REJECT	MSC vers MME	Mise à jour de localisation rejetée avec un code de cause

Pagination et Service

Message	Direction	But
SGsAP-PAGING-REQUEST	MSC vers MME	Pager l'abonné pour un appel MT ou un SMS MT
SGsAP-SERVICE-REQUEST	MME vers MSC	Abonné répondant à la pagination CS (CSFB en cours)
SGsAP-SERVICE-ABORT-REQUEST	MSC vers MME	Abandonner une demande de service CS fallback

Tunnelisation SMS

Message	Direction	But
SGsAP-DOWNLINK-UNITDATA	MSC vers MME	Livraison de SMS MT : PDU NAS transporté vers l'UE via SGs
SGsAP-UPLINK-UNITDATA	MME vers MSC	Soumission de SMS MO : PDU NAS transporté depuis l'UE via SGs

Détachement

Message	Direction	But
SGsAP-EPS-DETACH-INDICATION	MME vers MSC	Abonné détaché de l'EPS
SGsAP-EPS-DETACH-ACK	MSC vers MME	Accuser réception du détachement EPS
SGsAP-IMSI-DETACH-INDICATION	MME vers MSC	Détachement IMSI de l'abonné
SGsAP-IMSI-DETACH-ACK	MSC vers MME	Accuser réception du d��tachement IMSI

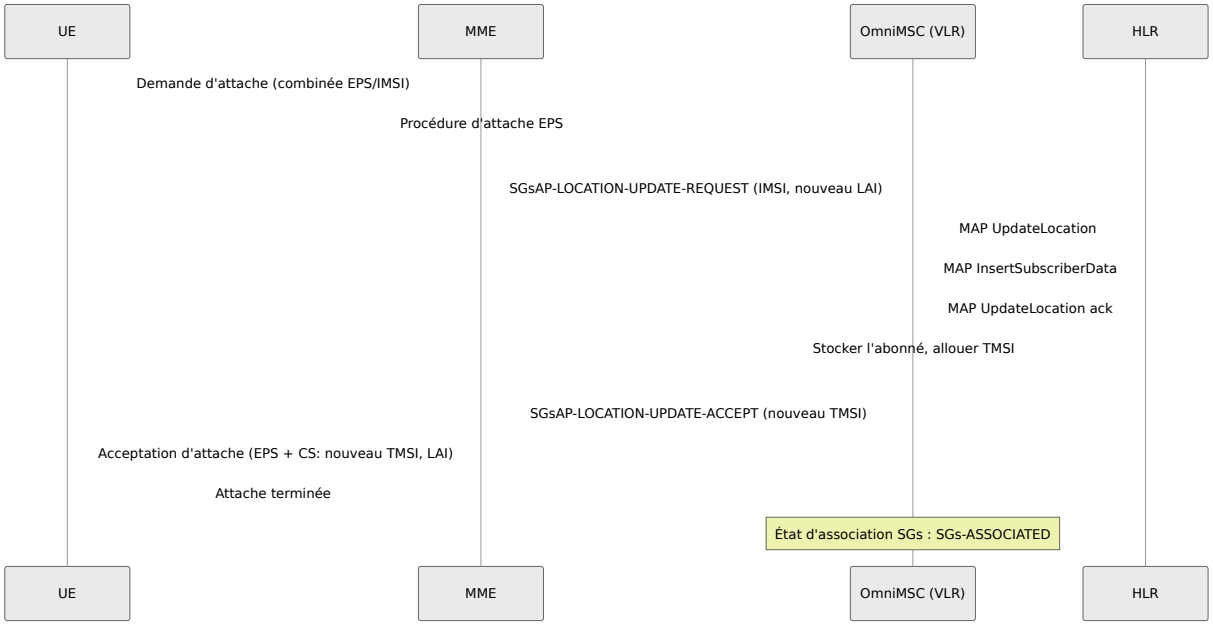
Réinitialisation et Statut

Message	Direction	But
SGsAP-RESET-INDICATION	Dans les deux sens	Le pair a redémarré ; le récepteur doit réenregistrer les abonnés concernés
SGsAP-RESET-ACK	Dans les deux sens	Accuser réception de l'indication de réinitialisation
SGsAP-STATUS	Dans les deux sens	Indication d'erreur avec cause et message erroné
SGsAP-MM-INFORMATION-REQUEST	MSC vers MME	Informations sur le nom du réseau et le fuseau horaire
SGsAP-ALERT-REQUEST	MSC vers MME	Demande d'alerte après échec de la pagination
SGsAP-ALERT-ACK	MME vers MSC	Accuser réception de l'alerte
SGsAP-UE-ACTIVITY-INDICATION	MME vers MSC	L'UE est devenue active
SGsAP-RELEASE-REQUEST	MSC vers MME	Libérer la connexion SGs pour cet abonné

Attache combinée EPS/IMSI

Lorsqu'un UE effectue une attache combinée EPS/IMSI en LTE, le MME envoie une SGsAP-LOCATION-UPDATE-REQUEST au MSC. Le MSC effectue une mise à jour de localisation VLR, qui peut inclure une interrogation HLR, et répond par

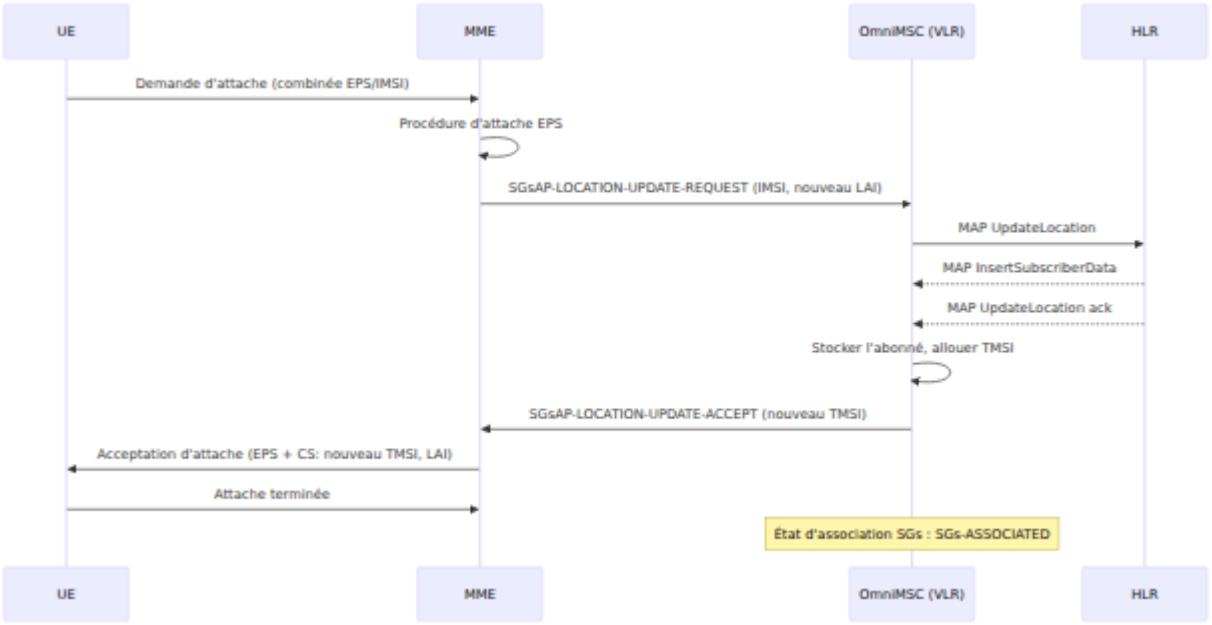
une acceptation ou un rejet. Lors de l'acceptation, l'abonné est enregistré à la fois dans l'EPC (via le MME) et dans le domaine CS (via le MSC/VLR) simultanément.



Après une attache combinée réussie, l'état d'association SGs de l'abonné passe à SGs-ASSOCIATED. Le MSC peut maintenant pager l'abonné via SGs et livrer des SMS sans CSFB.

Pagination d'appel MT via CSFB

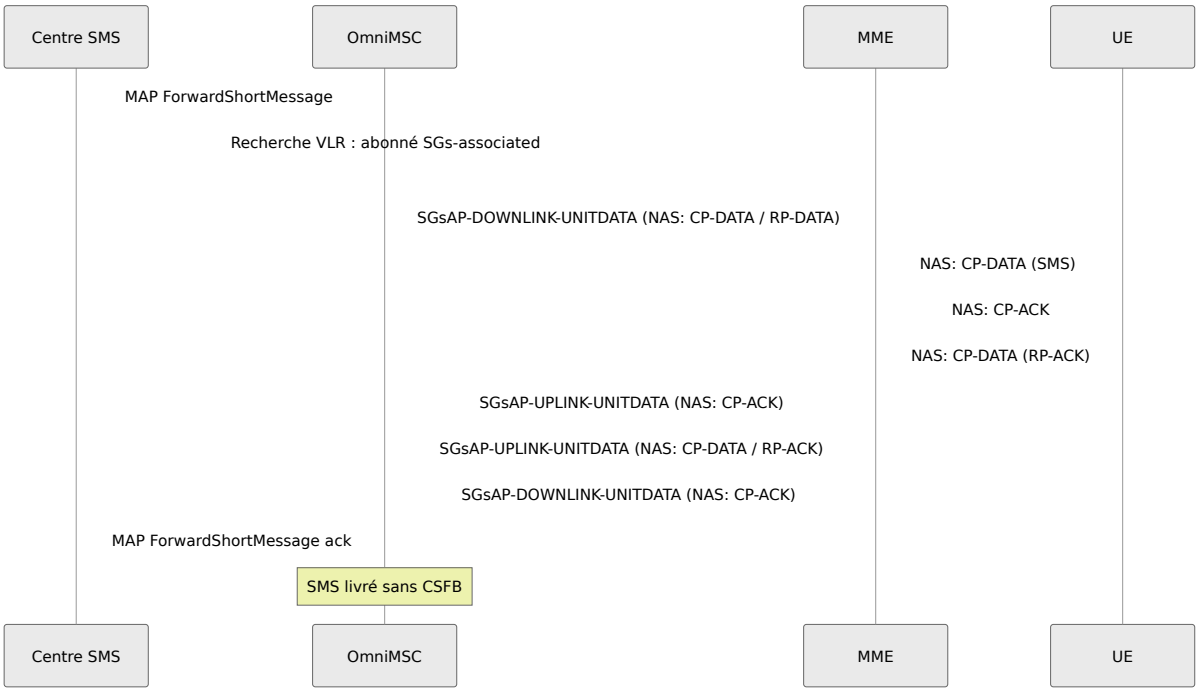
Lorsqu'un appel MT arrive pour un abonné qui est attaché via LTE (SGs-associated), le MSC page l'abonné par l'intermédiaire du MME plutôt que par les BSC. Le MME demande à l'UE de revenir à 2G ou 3G, où l'appel se poursuit via l'interface A ou l'interface Iu-CS.



Une fois que l'UE est revenu au domaine CS et a envoyé une réponse à la pagination via le BSC, l'appel se poursuit comme un appel MT normal. La machine d'état MSC-A gère le type de RAN E-UTRAN/SGs en omettant l'étape Clear Complete qui serait normalement attendue d'un BSC, puisque l'association SGs n'utilise pas la gestion de connexion BSSMAP.

SMS MT via SGs

Les SMS peuvent être livrés aux abonnés attachés en LTE sans nécessiter de CSFB. Le MSC tunnelise le PDU NAS SMS à travers l'interface SGs vers le MME, qui le livre à l'UE via l'interface radio LTE. Cela évite la latence et le coût des ressources radio d'un retour CS pour un court message.

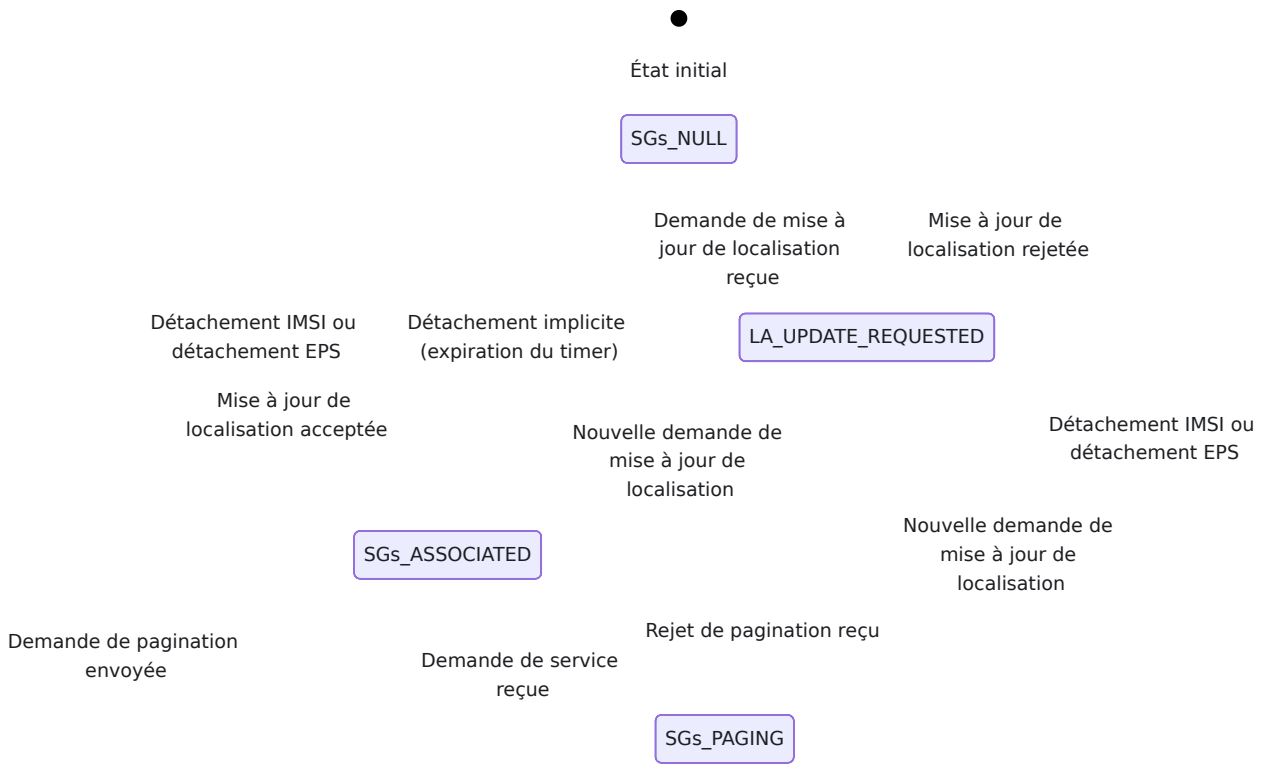


Les SMS MO suivent le chemin inverse : l'UE envoie le PDU NAS SMS via le MME en tant que SGsAP-UPLINK-UNITDATA, et le MSC le transmet au Centre SMS.

États d'association SGs

L'association SGs de chaque abonné est suivie comme une machine d'état selon la section 4 de la norme 3GPP TS 29.118.

État	Description
SGs-NULL	Aucune association SGs n'existe. La pagination CS via SGs n'est pas possible. C'est l'état initial.
LA-UPDATE-REQUESTED	Une mise à jour de localisation est en cours. Le MSC a reçu une demande du MME mais n'a pas encore terminé la mise à jour HLR.
SGs-ASSOCIATED	L'abonné a une association SGs valide. Le MSC peut pager via SGs et livrer des SMS sans CSFB.
SGs-PAGING	Une demande de pagination CS a été envoyée au MME et le MSC attend la réponse de l'abonné. Entré depuis SGs-ASSOCIATED sur une demande de pagination ; retourne à SGs-ASSOCIATED sur une demande de service ou un rejet de pagination.



Suivi MME

Le gestionnaire SGs maintient un registre des MMEs connus. Chaque MME est identifié par son FQDN (l'élément d'information MME Name dans les messages SGsAP). Pour chaque MME, le gestionnaire suit :

- La référence de connexion SCTP utilisée pour l'envoi de messages sortants.
- L'ensemble des IMSIs (abonnés) actuellement associés à ce MME.

Ce registre des abonnés par MME permet une gestion ciblée des réinitialisations : lorsqu'un MME échoue, seuls les abonnés associés à ce MME spécifique sont affectés.

Gestion des réinitialisations MME

Les procédures de réinitialisation garantissent la cohérence de l'état lorsque le MSC ou un MME redémarre.

Scénario	Initiateur	Action du récepteur
Redémarrage MSC	MSC envoie SGsAP-RESET-INDICATION à tous les MMEs connus	Chaque MME renvoie SGsAP-LOCATION-UPDATE-REQUEST pour ses abonnés associés, permettant au MSC de reconstruire l'état du VLR
Redémarrage MME	MME envoie SGsAP-RESET-INDICATION au MSC	Le MSC marque tous les abonnés associés à ce MME comme SGs-détachés (état SGs-NULL) et efface la liste des abonnés pour ce MME
Échec de lien SGs	Détecté par l'une ou l'autre des parties	Les deux parties traitent l'échec comme une réinitialisation implicite

Lorsque le MSC reçoit une indication de réinitialisation d'un MME, il itère sur tous les abonnés enregistrés contre ce MME, transitionne chacun vers l'état SGs-NULL, et efface l'ensemble des abonnés du MME. Lors du prochain contact de tout abonné affecté (mise à jour de localisation ou réponse à la pagination), le MSC effectue une réenregistrement complet.

Codec SGsAP

L'encodage et le décodage des messages SGsAP sont fournis par la bibliothèque partagée `sgs_ex` (`SgsEx.Codec`), que l'OmniMSC intègre comme une dépendance externe plutôt que comme un module intégré. Le codec gère les messages SGsAP selon les formats définis dans la norme 3GPP TS 29.118, traitant l'octet de type de message SGsAP binaire et les éléments d'information (IEs), supportant tous les IEs obligatoires et optionnels pour chaque type de message. Les messages encodés sont transmis sur SCTP ; les messages décodés sont dispatchés au gestionnaire SGs pour traitement.

Configuration

L'interface SGs est configurée sous la clé sgs dans la configuration du MSC.

Paramètre	Par défaut	Description
listen_port	29118	Port d'écoute SCTP pour les connexions SGsAP des MMEs. Le port 29118 est le port défini par la 3GPP pour SGs selon la TS 29.118. Définir `listen_port: 0` désactive le transport SGs (aucun socket n'est ouvert), ce qui est utile pour les déploiements de test.
vlr_name	(requis)	Nom du VLR au format FQDN, utilisé dans les messages SGsAP. Le MME utilise cela pour identifier le VLR. Doit correspondre au nom du VLR configuré du côté MME.

Type RAN : E-UTRAN via SGs

La machine d'état MSC-A prend en charge E-UTRAN via SGs comme un type RAN distinct (:eutran_sgs). Lorsqu'un abonné est SGs-associated, la FSM MSC-A ajuste son comportement pour l'interface SGs :

- Aucune gestion de connexion BSSMAP n'est utilisée ; il n'y a pas d'échange Clear Command / Clear Complete.
- La pagination est effectuée via SGsAP-PAGING-REQUEST au MME plutôt que via BSSMAP Paging aux BSC.
- La livraison de SMS utilise SGsAP Downlink/Uplink Unitdata plutôt que DTAP sur l'interface A.
- Une fois que l'abonné revient à GERAN ou UTRAN (après CSFB), la connexion passe au type RAN correspondant pour le reste de l'appel.

Références de spécification 3GPP

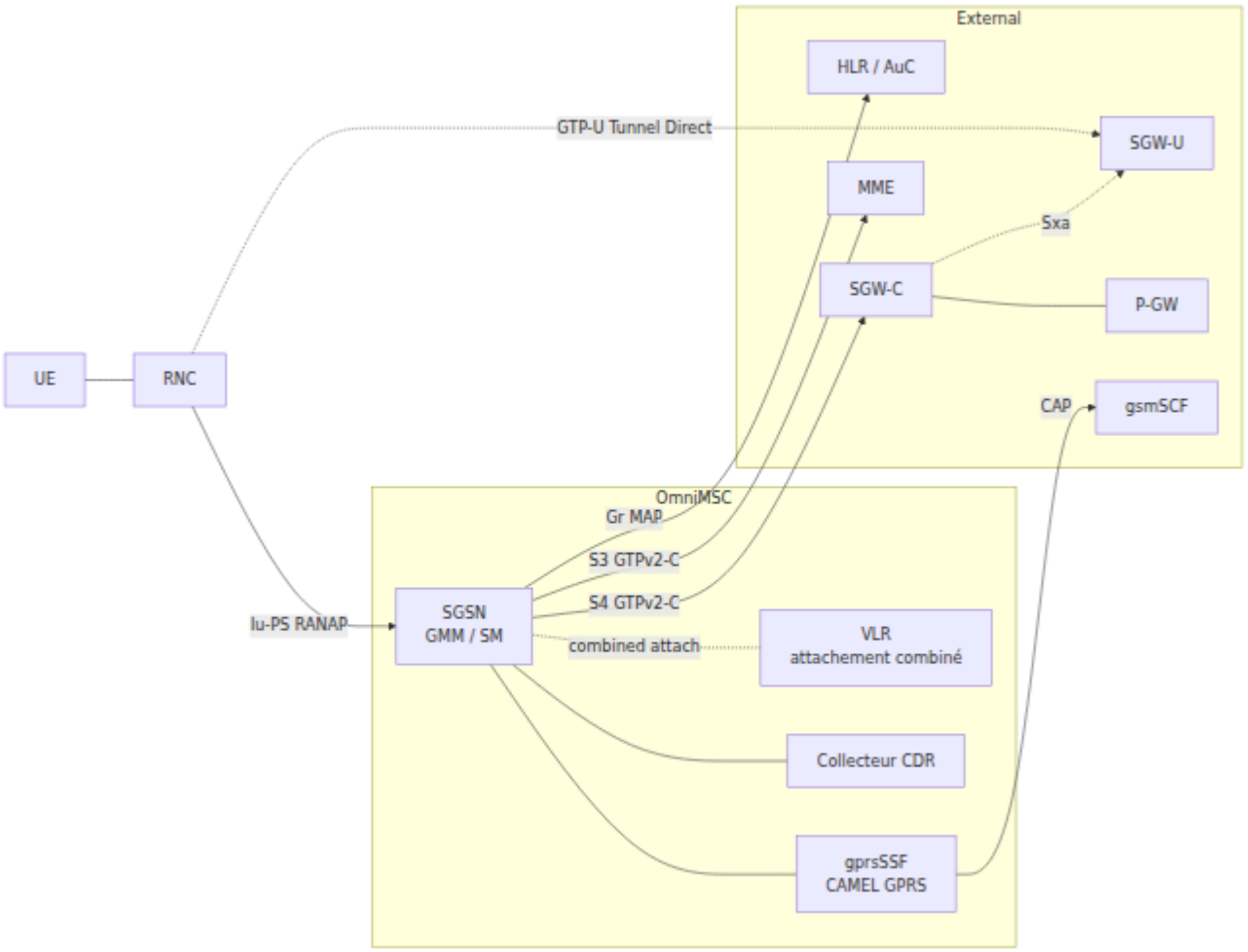
Spécification	Titre	Pertinence
TS 29.118	Spécification de l'interface MME-VLR SGs	Protocole SGsAP, formats de message, procédures
TS 23.272	Circuit Switched Fallback dans EPS	Architecture CSFB, flux d'appels, SMS sur SGs
TS 23.012	Procédures de gestion de localisation	Procédures de mise à jour de localisation VLR utilisées dans SGs
TS 24.008	Couche 3 de l'interface radio mobile	Messages NAS tunnelisés via SGs Unitdata

SGSN (Domaine de Paquet)

OmniMSC comprend un **S4-SGSN** intégré qui sert le domaine à commutation de paquets (PS) pour les abonnés 3G (UTRAN) via **Iu-PS**, ancrant leurs sessions de données sur le même S-GW/P-GW que LTE. Un seul nœud sert à la fois le domaine CS (voix, SMS) et le domaine PS (données par paquet) pour un abonné ; l'attachement combiné est géré en interne entre le SGSN et le VLR.

Le SGSN est désactivé par défaut et activé selon la configuration ci-dessous. La plupart des dépendances externes sont opt-in, de sorte qu'un laboratoire peut faire fonctionner le cœur de paquet avec un pair statique et des identifiants injectés avant qu'un HLR/DNS complet n'existe.

Architecture



Tunnel Direct est utilisé : le plan utilisateur GTP-U fonctionne directement entre le RNC et le S-GW-U. Le SGSN gère les points de terminaison du tunnel lors de la configuration du porteur mais ne transporte jamais les paquets du plan utilisateur. Lorsque l'UE devient inactif (PMM-IDLE), le SGSN ré-ancre le point de terminaison descendant sur lui-même afin que le S-GW tamponne et déclenche une Notification de Données Descendantes au lieu d'envoyer à un RNC libéré (TS 23.060 §15.6).

Interfaces

Interface	Pair	Protocole	Objectif	Référence
Iu-PS	RNC	RANAP sur SCCP/M3UA	Transport NAS, attribution de RAB, relocalisation	TS 25.413
Gr	HLR / AuC	MAP sur TCAP/SCCP	Mise à jour de localisation, vecteurs d'authentification, abonnement	TS 29.002
S4	S-GW (SGW-C)	GTPv2-C	Créer / Modifier / Supprimer Session, pagination	TS 29.274
S3	MME	GTPv2-C	Mobilité inter-RAT de 3G-PS à LTE	TS 29.274 §7.3
Gn/Gp (CAP)	gsmSCF	CAP sur TCAP/SCCP	Chargement / contrôle en ligne CAMEL GPRS	TS 29.078
GTP-U	RNC à S-GW-U	GTP-U (Tunnel Direct)	Plan utilisateur (pas à travers le SGSN)	TS 29.281

Iu-PS, Gr, S3 et CAP réutilisent les piles SS7 et GTPv2-C que le côté CS exécute déjà. S3 et Sv partagent le serveur GTPv2-C ; l'interface SRVCC Sv reste sur son propre socket.

Configuration

Le SGSN lit `config :omnimsc, :sgsn` et, pour les interfaces GTPv2-C, le bloc partagé `config :gtpc, :service`.

```
config :omnimsc, :sgsn,
  enabled: true,
  # Zone de routage que ce SGSN sert (annoncée aux UEs)
  rai: %{mcc: "001", mnc: "01", lac: 1, rac: 1},
  # Largeur NRI pour l'allocation P-TMSI dans un pool (0 = pas de
pool)
  nri_bits: 6,
  # F-TEIDs de contrôle S4/S3 de ce SGSN annoncés au S-GW / MME
  s4_f_teid: %{teid: "0a0a0a0a", ipv4: "10.0.0.10"},
  s3_f_teid: %{teid: "0b0b0b0b", ipv4: "10.0.0.10"},
  # Compteur de redémarrage de récupération GTP-C (TS 23.007 §18)
  recovery: 1,
  # Pairs de cœur de paquet statiques (utilisés sauf si la
sélection DNS est activée)
  sgw: %{ip: "10.179.1.25", port: 2123},
  pgw_c: "10.179.1.21",
  # APN-AMBR par défaut envoyé dans Créer Session lorsque
l'abonnement n'en fournit aucun
  default_apn_ambr: %{ul: 0, dl: 0},
  # Sélection P-GW/S-GW basée sur APN via DNS S-NAPTR (opt-in ;
désactivé par défaut)
  pgw_dns: false,
  sgw_dns: false,
  # Minuteur de garde de libération Iu (ms) après une commande de
libération Iu
  iu_release_guard_ms: 5000,
  # Remplacements de minuteurs de retransmission GMM / SM (ms)
  gmm_timers: %{t3350: 6000, t3360: 6000, t3370: 6000, t3312:
3_240_000},
  sm_timers: %{t3395: 8000},
  # Fallback d'abonnement lorsque Gr Insert Subscriber Data n'est
pas câblé
  subscribed_apns: ["internet"],
  default_apn: "internet",
  wildcard_apn: false

config :gtpc,
  service: %{
    name: :s3,
    listen_ip: "10.0.0.10",
    listen_port: 2123,
    control_module: Omnimsc.Gtpc.Router,
    t3: 5000,
```

```
    n3: 3
  }
```

Paramètres de base

Paramètre	Type	Obligatoire	Par défaut	Des
`enabled`	Booléen	Non	`false`	Interru princip l'arbre proces les inte
`rai`	Carte	Oui	-	Identit de rout (`mcc`/`m` annonc et utili réseau
`nri_bits`	Entier	Non	0	Largeu NRI da aligné MSC. `0` le pool
`s4_f_teid`	Carte	Oui	-	F-TEID S4 du S hex, `ip` S-GW a pour la signali porteu
`s3_f_teid`	Carte	Non	-	F-TEID S3 du S annonc pour la inter-R

Paramètre	Type	Obligatoire	Par défaut	Des
`recovery`	Entier	Non	0	Compt redéma récupé (TS 23. Incrém redéma SGSN.
`sgw`	Carte	Non	`%{ip: "10.179.1.25", port: 2123}`	Pair GT statiqu lorsque est dés
`pgw_c`	Chaîne	Non	`"10.179.1.21"`	Adress GW sta utilisée `pgw_dr` désact
`default_apn_ambr`	Carte	Non	`%{ul: 0, dl: 0}`	APN-AM placé c Sessior l'abonr fournit évite le laborat rejette valeur
`pgw_dns`	Booléen	Non	`false`	Résouc par API via DN (TS 29. Retoml

Paramètre	Type	Obligatoire	Par défaut	Des
				en cas résolut
`sgw_dns`	Booléen	Non	`false`	Résouc par API via DN Retoml en cas résolut
`iu_release_guard_ms`	Entier	Non	5000	Temps pour R Releas avant c connex (TS 25.

Paramètres de minuteurs

Paramètre	Type	Par défaut (ms)	Description
`gmm_timers.t3350`	Entier	6000	Retransmission de l'Acceptation d'Attachement / Acceptation RAU / Réallocation P-TMSI en attente de Complétion (TS 24.008 §11.2.2).
`gmm_timers.t3360`	Entier	6000	Retransmission de la Demande d'Authentification & de Chiffrement en attente de Réponse.
`gmm_timers.t3370`	Entier	6000	Retransmission de la Demande d'Identité en attente de Réponse d'Identité.
`gmm_timers.t3312`	Entier	3240000	Minuteur mobile-atteignable / RAU périodique ; à l'expiration (plus grâce) les contextes MM et PDP sont implicitement détachés (TS 24.008 §4.7.2.2).
`sm_timers.t3395`	Entier	8000	Retransmission d'une Demande de Désactivation de Contexte PDP demandée par le réseau en attente d'Acceptation (TS 24.008 §6.1.3.4.2).

Tous les minuteurs de retransmission plafonnent à 5 tentatives avant que la procédure ne soit abandonnée.

Paramètres d'abonnement et APN

Utilisés pour valider l'APN demandé lorsque Gr Insert Subscriber Data n'a pas peuplé un abonnement actif (voir Gr MAP). Lorsqu'un abonnement réel est présent, il a la priorité sur ces valeurs statiques.

Paramètre	Type	Par défaut	Description
`subscribed_apns`	Liste	`[]`	Noms d'APN autorisés. Un APN demandé en dehors de cette liste est rejeté avec la cause SM 33 (TS 24.008 §10.5.6.6). Vide désactive l'application (accepte tout).
`default_apn`	Chaîne	-	APN utilisé lorsque l'UE n'en demande aucun. Retombe sur le seul APN abonné si non défini.
`wildcard_apn`	Booléen	`false`	Lorsque `true`, tout APN demandé est autorisé (abonnement wildcard).

Seams d'injection de laboratoire

Ces clés injectent une fonction (ou `{module, fonction}`) afin que le cœur de paquet puisse fonctionner avant que l'état SS7/HLR ne soit complet. Elles sont optionnelles ; lorsqu'elles ne sont pas définies, le SGSN saute le tour externe correspondant et la procédure se termine toujours.

Paramètre	Type	Description
`quintet_source`	Fonction/`{m,f}`	Fournit un quintet UMTS AKA `(imsi, resync)` pour le défi d'authentification au lieu d'un Gr SendAuthenticationInfo en direct.
`gr_source`	Fonction/`{m,f}`	Fournit le résultat HLR UpdateGprsLocation / Insert Subscriber Data lors de l'attachement. Lorsqu'il n'est pas défini, l'attachement se poursuit sans enregistrement Gr.
`purge_ms_sink`	Fonction/`{m,f}`	Reçoit une notification de Purge MS lorsque le SGSN supprime un abonné.

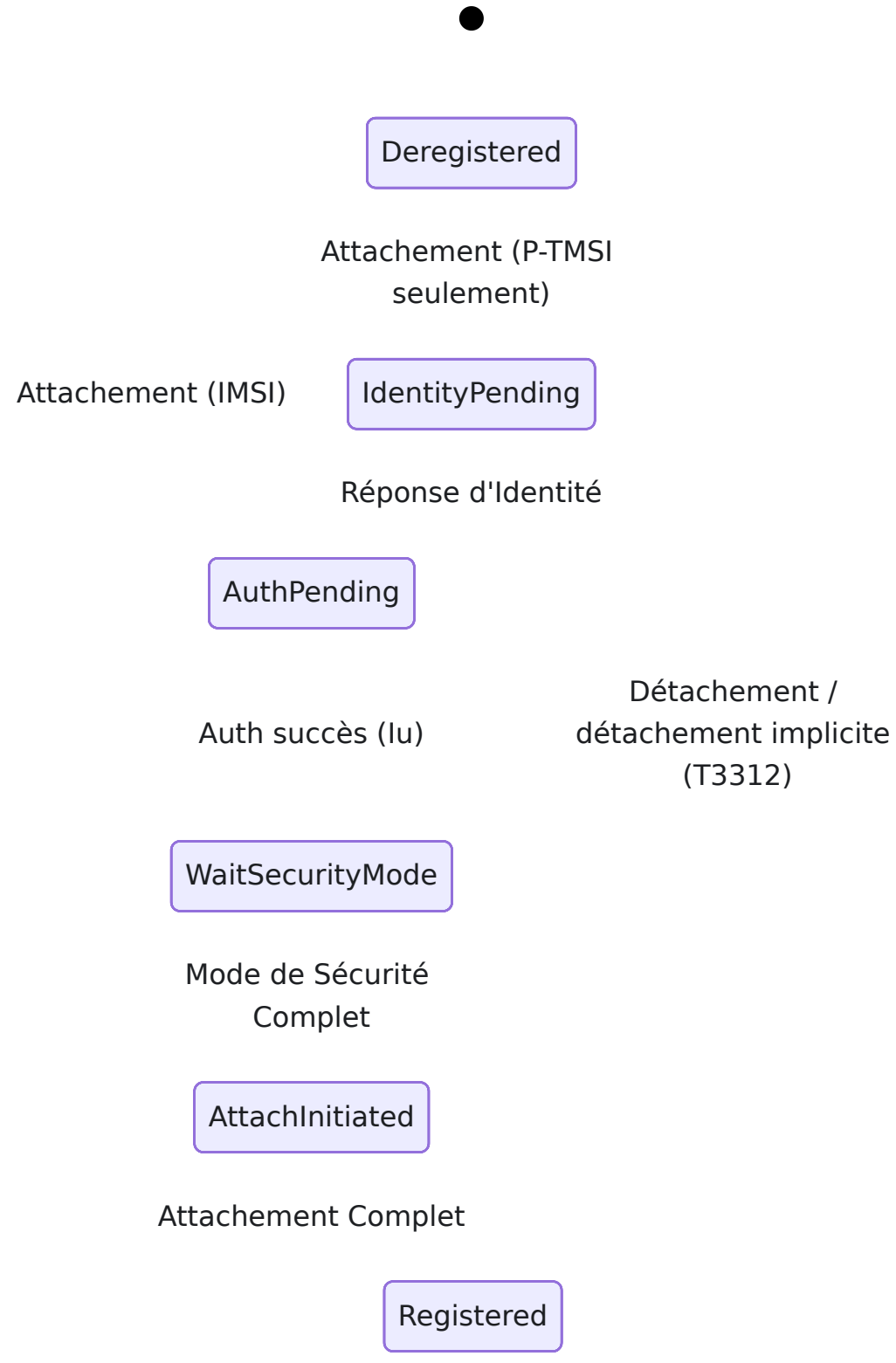
Paramètres de service GTP-C

Paramètre	Type	Obligatoire	Par défaut	Description
`name`	Atome	Oui	-	Nom du service ; `:s3` pour le serveur de mobilité SGSN.
`listen_ip`	Chaîne	Oui	-	Adresse de liaison pour le serveur GTPv2-C.
`listen_port`	Entier	Non	2123	Port UDP GTP-C (TS 29.274).
`control_module`	Module	Oui	-	`Omnimsc.Gtpc.Router` route les messages S3/S4 initiés par le pair dans le SGSN.
`t3`	Entier	Non	5000	Minuteur de retransmission de demande GTP-C (ms).
`n3`	Entier	Non	3	Tentatives maximales de retransmission GTP-C.

Lorsque les interfaces Sv (SRVCC) et GTPv2-C du SGSN fonctionnent sur un même hôte, liez-les à des points de terminaison IP/port distincts.

Gestion de Mobilité (GMM)

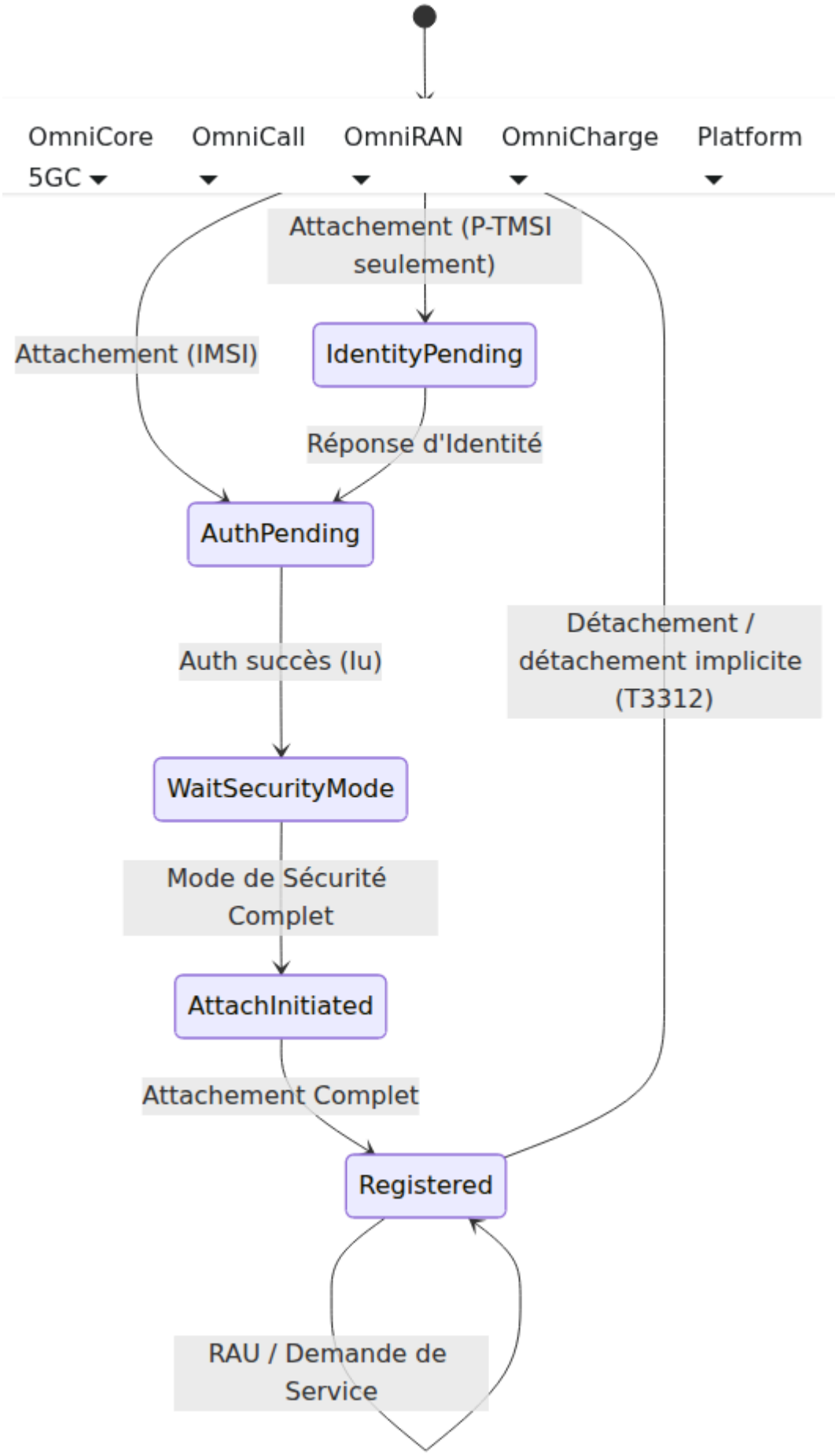
Le SGSN exécute une machine d'état GMM par UE (TS 24.008 §4.7).



Comportement GMM implémenté :

- **Attachement / RAU / Détachement / Demande de Service**, avec un attachement combiné (PS+CS) géré en interne avec le VLR.
- **Authentification UMTS AKA** avec validation RES contre XRES, y compris la resynchronisation AUTS.
- **Allocation P-TMSI** et une **signature P-TMSI** authentifiée lors d'un attachement/RAU ultérieur (TS 24.008 §10.5.5.8).
- **Minuteurs de retransmission** T3350/T3360/T3370 et le **minuteur mobile-atteignable** T3312 entraînant un détachement implicite.
- **ID Commun RANAP** envoyé au RNC après le Mode de Sécurité Complet (TS 25.413 §8.24).
- **Procédure d'identité** demandant l'IMEISV lors de l'attachement.
- **STATUT GMM** sur un message GMM inconnu ou erroné, et **causes de rejet par procédure** (pas une seule cause générique).
- **Demande de Détachement initiée par le réseau (MT)** afin que le réseau puisse détacher un UE et inciter à un nouvel attachement.
- **Gestion de l'état de Contexte PDP** sur RAU / Demande de Service afin que l'état PDP de la MS et du SGSN ne puisse pas diverger.
- **Libération Iu** après qu'une procédure uniquement de signalisation soit terminée, avec le minuteur de garde ci-dessus.

Gestion de Session (SM / PDP)



Comportement SM implémenté :

- **Activation de contexte PDP** avec négociation d'APN, QoS et adresse PDN.
- **Multiplexage NSAPI / contextes PDP secondaires** : un UE maintient plusieurs contextes concurrents identifiés par NSAPI (5-15) ; une collision de NSAPI en cours est résolue en désactivant localement le contexte en conflit selon TS 24.008 §6.1.3.1.4.
- **Négociation QoS** à partir de QoS demandée et souscrite dans le QoS de Porteur S4 et l'IE QoS NAS.
- **Types de PDP** IPv4, IPv6 et IPv4v6 de bout en bout.
- **Désactivation demandée par le réseau** avec minuteur de retransmission **T3395**.
- **Sélection d'APN et application d'abonnement** : valider l'APN demandé par rapport à l'abonnement, résoudre les APNs wildcard et par défaut, et rejeter un APN non abonné avec la cause SM correcte.
- **STATUT SM** et validation NSAPI sur erreurs de protocole, avec cause GTP-C mappée à la cause SM NAS.

Iu-PS et RANAP

Le gestionnaire Iu-PS possède la section orientée connexion SCCP par UE et relie NAS dans les deux sens via RANAP DirectTransfer.

- **InitialUE / pont DirectTransfer** transportant GMM/SM NAS dans chaque direction.
- **Attribution RAB** avec des paramètres dérivés du porteur/QoS souscrit, et réaction à la Réponse d'Attribution RAB **FailedList** (mappant la cause RANAP à un rejet SM) et modifications uniquement TEID (transmises au S-GW).
- **Libération Iu** après des procédures de signalisation, et sur libération SCCP entrante pour une connexion PS, avec le minuteur de garde.
- **RANAP RESET** d'un RNC purgeant les connexions Iu-PS obsolètes de ce RNC et accusant réception.
- **Indication d'Erreur RANAP** émise sur un PDU RANAP malformé / indécodable (TS 25.413 §8.27).

- **Signalisation de relocalisation SRNS** (TS 25.413 §8.6-8.9) : tous les six PDU de Relocalisation, entraînant la relocalisation intra-SGSN et la ré-ancrage du Tunnel Direct sur le RNC cible à l'achèvement. La relocalisation inter-SGSN via S3 est suivie comme un travail futur (voir Limitations).

S4 et GTP-C

- **Créer / Modifier / Supprimer Session** vers le S-GW, avec type RAT UTRAN et les F-TEIDs S4-SGSN.
- **Brokering de point de terminaison de Tunnel Direct**, et **retour en arrière descendant vers le SGSN sur PMM-IDLE** afin que le S-GW tamponne et déclenche la pagination au lieu d'envoyer à un RNC libéré.
- **Demande de Suppression / Mise à Jour de Porteur initiée par le pair** depuis le S-GW/P-GW : accusée et relayée à l'UE.
- **Gestion de chemin GTP-C** : Détection de Demande/Réponse Echo et de compteur de redémarrage de récupération pour invalider les sessions obsolètes (TS 23.007 §18).
- **Sélection P-GW/S-GW S-NAPTR DNS** par APN lorsque activée, avec un retour statique.
- **Pagination de données MT** : une Notification de Données Descendantes S4 déclenche la Pagination RANAP et est accusée (TS 29.274 §7.2.11).

Mobilité S3 (vers le MME)

- **Transfert de contexte en mode inactif** : Demande de Contexte / Réponse / **Accusé** (TS 29.274 §7.3.7).
- **Mode de sécurité de contexte MM** codé comme EPS (valeur 4) lors du transport d'un contexte KASME (TS 29.274 §8.38).
- **Conteneurs transparents de relocalisation Forward** (conteneurs RAN Source-à-Cible / Cible-à-Source) transportés de bout en bout afin que la radio cible puisse être configurée (TS 29.274 §7.3.1).

Gr MAP (Interface HLR)

- **UpdateGprsLocation** enregistrant le SGSN dans le HLR lors de l'Attachement GPRS (TS 23.060 §6.5.3).
- **Insert Subscriber Data** consommé dans le contexte d'abonné (APNs autorisés, QoS souscrite, APN-AMBR, facturation), alimentant l'application d'APN et la négociation de QoS.
- **Cancel Location** purgeant les contextes MM et PDP locaux et supprimant la session S4 ; **Purge MS** envoyé lorsque le SGSN supprime un abonné.

Le tour aller-retour Gr est conditionné par `gr_source` ; lorsqu'il n'est pas défini, l'attachement se poursuit sans enregistrement Gr afin que le laboratoire continue de fonctionner avec un quintet injecté.

Facturation (CDRs PS)

Le SGSN produit des enregistrements de détails d'appel du domaine PS routés vers le collecteur CDR partagé (TS 32.251, TS 32.298) :

- **S-CDR** (`SGSNPDPRecord`) ouvert lors de l'activation PDP et fermé lors de la désactivation.
- **M-CDR** (`SGSNMMRecord`) ouvert lors de l'Attachement Complet et fermé lors du Détachement, avec un conteneur de changement de localisation sur RAU.
- **Conteneurs de changement de condition de facturation** (QoS / RAT / tarif-temps / changement de Tunnel Direct) et **enregistrements partiels** avec un numéro de séquence incrémental.

Voir documentation CDR pour le collecteur et le format de sortie. Le comptage de volume sous Tunnel Direct dépend d'un flux de rapport d'utilisation S4 (voir Limitations).

CAMEL GPRS (Chargement et Contrôle en Ligne)

Un gprsSSF opt-in pilote le contrôle GPRS phase-3 CAMEL (TS 23.078, TS 29.078). Il est armé uniquement lorsque l'abonnement porte **GPRS-CSI** ; sans cela, l'attachement et l'activation PDP restent inchangés.

- **Modèles d'état gprsSSF** pour Attachement/Détachement et Contexte PDP, avec armement de point de détection et rapport d'événements.
- **InitialDPGPRS** déclenché aux points de détection Attachement et Établissement de Contexte PDP.
- **ApplyChargingGPRS / ApplyChargingReportGPRS** boucle de chargement en ligne.
- **Opérations de contrôle** Connecter/Continuer/Liberer/Annuler/Test d'Activité GPRS, le **minuteur Tssf** et **gestion par défaut GPRS** en cas d'erreur ou de délai d'attente gsmSCF.
- **FurnishChargingInformationGPRS** fusionné dans le S-CDR et **SendChargingInformationGPRS** capturé vers la couche SM.

Tables de Référence

Causes de Rejet GMM Communes (TS 24.008 §10.5.5.14)

Cause	Nom	Déclencheur typique
2	IMSI inconnu dans le HLR	Abonné non provisionné
7	Services GPRS non autorisés	L'abonnement interdit le service par paquet
9	L'identité MS ne peut pas être dérivée	RAU/Demande de Service P-TMSI non résoluble
11	PLMN non autorisé	Roaming / restriction PLMN
17	Échec du réseau	Pas de vecteurs d'authentification du HLR

Causes de Rejet SM (PDP) Communes (TS 24.008 §10.5.6.6)

Cause	Nom	Déclencheur typique
26	Ressources insuffisantes	S-GW a refusé de Créer la Session, ou aucun RAB n'a pu être attribué
27	APN manquant ou inconnu	L'APN demandé ne peut pas être résolu
31	Activation rejetée, non spécifiée	Échec de la configuration RAB RNC
33	Option de service demandée non souscrite	APN non dans l'abonnement

---

Métriques

Métrique : `omnimsc_sgsn_attach_count`
Type : Compteur
Description : Résultats d'attachement GPRS.
Étiquettes :

- `result` - Résultat de l'attachement (par exemple `accepted`, `rejected`).

Métrique : `omnimsc_sgsn_pdp_count`
Type : Compteur
Description : Résultats d'activation de contexte PDP.
Étiquettes :

- `result` - `active` ou `rejected`.

Exemples de requêtes :

```
# Taux d'acceptation d'attachement
sum(rate(omnimsc_sgsn_attach_count{result="accepted"}[5m]))
  / sum(rate(omnimsc_sgsn_attach_count[5m]))

# Taux de rejet PDP
sum(rate(omnimsc_sgsn_pdp_count{result="rejected"}[5m]))
```

Dépannage

Attachement rejeté avec cause 17 (échec du réseau)

Symptômes : L'UE ne peut pas s'attacher au domaine de paquet ; cause de rejet GMM Attachement 17.

Causes possibles :

- Aucun vecteur d'authentification retourné par le HLR via Gr.
- `quintet_source` non défini dans un laboratoire sans Gr actif.

Résolution :

1. Confirmer que le HLR retourne des vecteurs pour l'IMSI (SendAuthenticationInfo).
2. Dans un laboratoire, définir `quintet_source` pour injecter un quintet UMTS connu.

Activation PDP rejetée avec cause 26 (ressources insuffisantes)

Symptômes : Rejet de la Demande d'Activation de Contexte PDP cause 26.

Causes possibles :

- Le S-GW a refusé de Créer la Session (par exemple un ULI ou un APN-AMBR non nul qu'il rejette).
- Aucun RAB n'a pu être attribué par le RNC.

Résolution :

1. Vérifier que le S-GW accepte la Création de Session ; définir `default_apn_ambr` à `%{ul: 0, dl: 0}` pour les S-GWs qui rejettent une valeur non nulle.
2. Examiner la Réponse d'Attribution RAB pour une entrée FailedList.

Activation PDP rejetée avec cause 33 (option de service non souscrite)

Symptômes : Rejet de la Demande d'Activation de Contexte PDP cause 33.

Causes possibles :

- L'APN demandé n'est pas dans l'abonnement ou dans `subscribed_apns`.

Résolution :

1. Ajouter l'APN à l'abonnement HLR (Insert Subscriber Data) ou à `subscribed_apns`.
2. Définir `wildcard_apn: true` uniquement si tout APN doit être autorisé.

Aucune donnée descendante

Symptômes : Le lien montant fonctionne mais aucun paquet descendant n'arrive.

Causes possibles :

- Tunnel Direct non complété : la Modification de Porteur n'a pas transporté le F-TEID RNC.
- Le descendant est toujours ancré sur un RNC libéré après que l'UE soit devenue inactive.

Résolution :

1. Confirmer que la Modification de Porteur après l'attribution RAB a transporté le F-TEID RNC.
2. Confirmer que le retour en arrière descendant vers le SGSN a été déclenché sur PMM-IDLE afin que la pagination puisse ramener l'UE.

RAU non routé vers ce SGSN

Symptômes : Une Mise à Jour de Zone de Routage d'un UE atterrit sur le mauvais nœud.

Causes possibles :

- Le NRI P-TMSI ne correspond pas à `nri_bits` / allocation de pool de ce SGSN.

Résolution :

1. Aligner `nri_bits` avec la configuration du pool MSC/SGSN.

Limitations

Les éléments suivants sont implémentés comme seams ou chemins partiels et sont documentés afin que les opérateurs sachent ce qui n'est pas encore de bout en bout :

- **Comptage de volume sous Tunnel Direct** : le SGSN ne voit aucun plan utilisateur, donc les volumes S-CDR et de chargement en ligne CAMEL nécessitent un flux de rapport d'utilisation S4 qui n'est pas encore câblé. Les boucles d'enregistrement et de rapport sont complètes ; la diminution de volume en direct attend ce flux.
- **Conseil de Facturation CAMEL au MS** : SendChargingInformationGPRS est capturé vers la couche SM, mais la livraison AoC au terminal n'est pas encore construite.

- **Relocalisation Forward Inter-SGSN** : la signalisation de relocalisation intra-SGSN SRNS est complète ; la conduite du saut S3 vers un SGSN pair (achèvement du transfert PS en mode connecté) est suivie sous l'épopée de l'interface S3.

Trunking SIP-I

Ce document décrit l'interface de trunking SIP-I (SIP avec ISUP encapsulé) mise en œuvre par OmniMSC. SIP-I permet le transport transparent des messages ISUP au sein du signalement SIP, préservant ainsi l'intégralité des informations ISUP à travers les segments de trunk basés sur IP.

Pour le trunking SIP pur, voir Trunking SIP. Pour la configuration de routage, voir Configuration de Routage. Pour les paramètres de configuration, voir Référence de Configuration. Pour les opérations générales, voir Guide des Opérations.

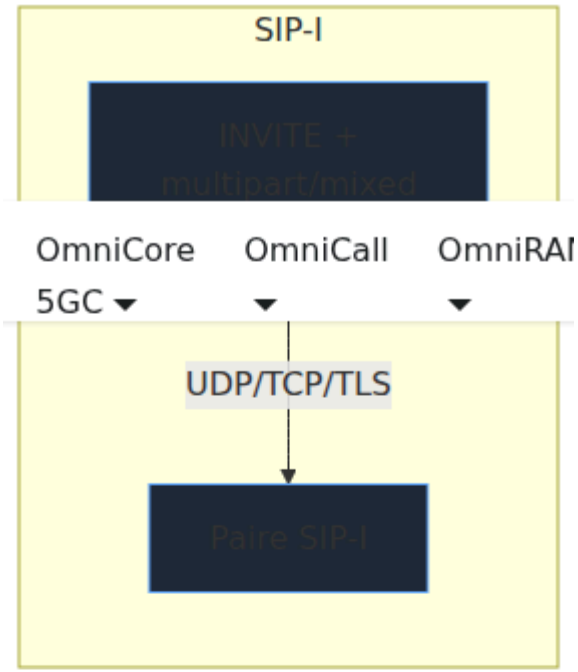
Qu'est-ce que SIP-I ?

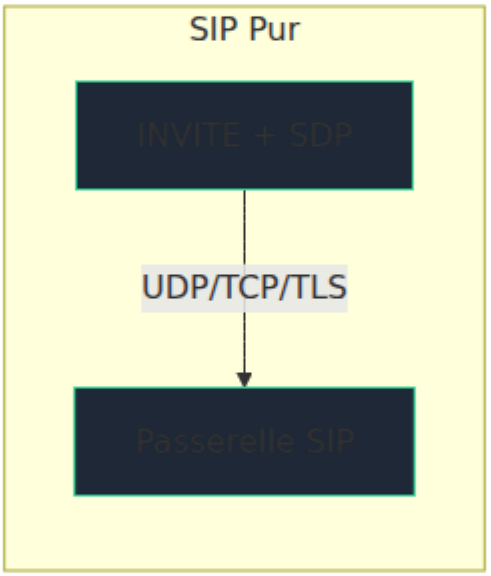
SIP-I (Session Initiation Protocol avec ISUP encapsulé) est défini par l'ITU-T Q.1912.5 et utilise le protocole SIP comme mécanisme de transport pour les messages ISUP. Contrairement au trunking SIP pur, qui mappe les paramètres ISUP aux en-têtes SIP (perdant potentiellement des informations), SIP-I inclut le message ISUP complet en tant que corps MIME aux c��tés du SDP, garantissant une interconnexion sans perte.

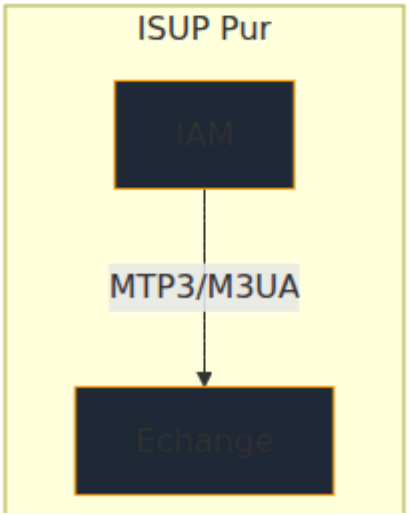
SIP-I est le protocole de trunking standard utilisé entre les serveurs MSC et les passerelles multimédias dans les réseaux de cœur basés sur IMS 3GPP et est largement déployé pour l'interconnexion PSTN.

Le corps ISUP est transporté selon la RFC 3204 (type de média MIME pour ISUP) et la RFC 3261 (SIP).

Comparaison des Protocoles


SIP-I
INVITE +
multipart/mixed
OmniCore
5GC
OmniCall
OmniRAI
UDP/TCP/TLS
Paire SIP-I


SIP Pur
INVITE + SDP
UDP/TCP/TLS
Passerelle SIP


ISUP Pur
IAM
MTP3/M3UA
Échange

Aspect	ISUP Pur	SIP Pur	SIP-I
Transport	MTP3/M3UA/SCTP	UDP/TCP/TLS	UDP/TCP/TLS
Informations de signalement	ISUP complet	Mappé aux en-têtes SIP	ISUP complet préservé
Description des médias	Capacité de transport dans IAM	SDP	SDP + capacité de transport ISUP
Perte d'information	Aucune	Possible (mappage de paramètres)	Aucune
Négociation de codec	TMR dans IAM	Offre/Réponse SDP	Offre/Réponse SDP
Cas d'utilisation	PSTN hérité	Interconnexion VoIP	MSC-MSC, passerelle PSTN

Format de Corps Multipart

Les messages SIP-I utilisent un corps MIME `multipart/mixed` contenant deux parties : l'offre/réponse SDP et le message ISUP encodé selon la RFC 3204.

```
Content-Type: multipart/mixed;boundary=boundary42

--boundary42
Content-Type: application/sdp

v=0
o=OmniMSC 12345 12345 IN IP4 203.0.113.10
s=OmniMSC
c=IN IP4 203.0.113.10
t=0 0
m=audio 10042 RTP/AVP 0 8
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000

--boundary42
Content-Type: application/ISUP;version=itu-t92+

<binary ISUP IAM>
--boundary42--
```

Le type de contenu `application/ISUP` est défini dans la RFC 3204. Le paramètre `version` identifie la variante ISUP (par exemple, `itu-t92+` pour ITU-T Q.767).

Configuration des Paires SIP-I

Les paires SIP-I sont configurées sous la clé `:sip_i`, séparément des paires SIP pures.

```
config :omnimsc, :sip_i,
  peers: [
    [name: "MSC-02-SIP-I",
     address: "10.2.1.100",
     port: 5060,
     transport: :tcp,
     isup_version: :itu_t92,
     codecs: [:pcmu, :pcma, :amr],
     max_channels: 100,
     trunk_group_id: "TG-InterMSC-01",
     point_code: [1, 2, 3]]
  ]
```

Paramètres des Paires SIP-I

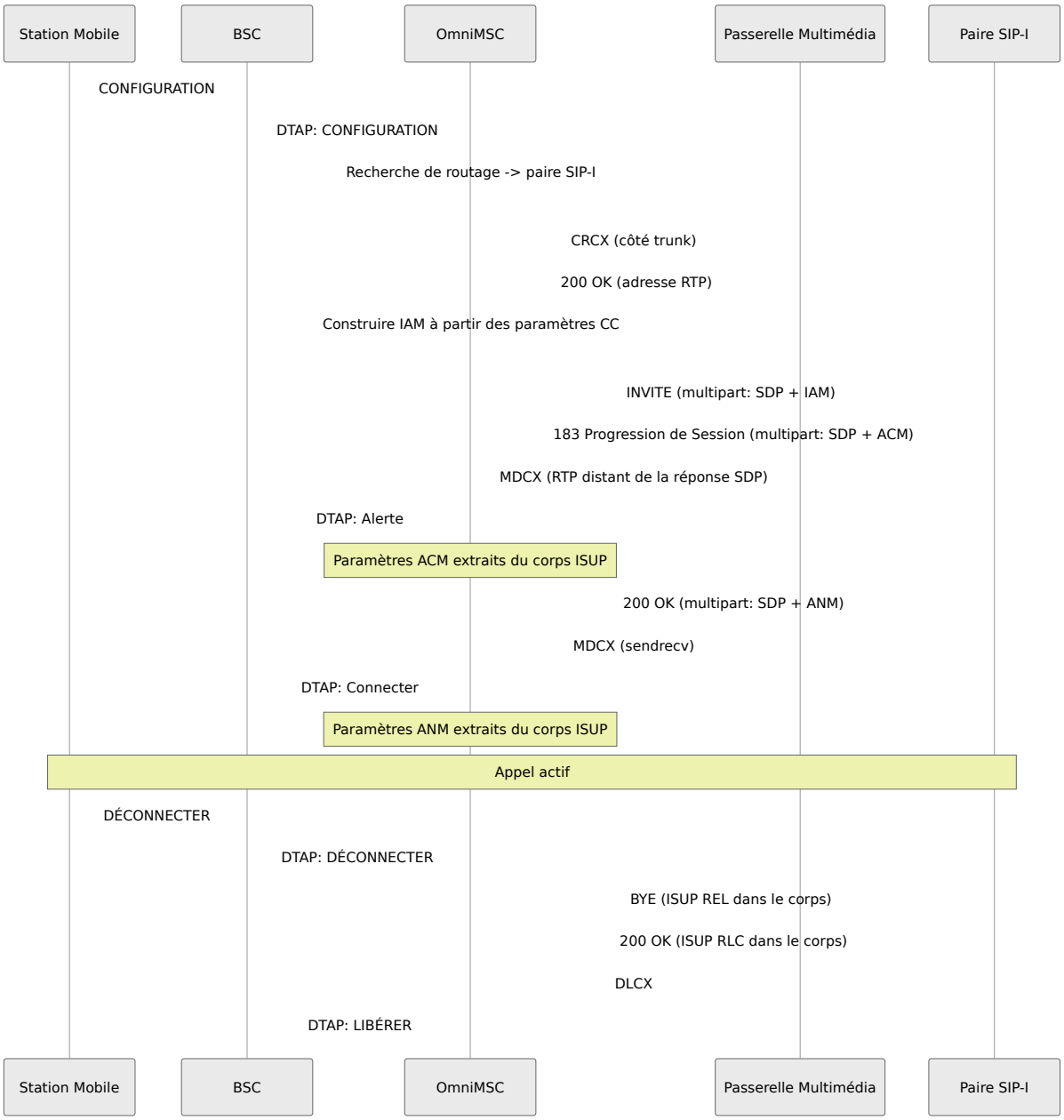
Paramètre	Type	Par défaut	Description
`name`	`string`	-- (obligatoire)	Nom logique de la paire. Référencé dans les entrées de table de routage avec le type `:sip_i`.
`address`	`string`	-- (obligatoire)	Adresse IP ou nom d'hôte de la paire.
`port`	`integer`	`5060`	Port SIP de la paire.
`transport`	`atom`	`:tcp`	Protocole de transport : `:udp`, `:tcp` ou `:tls`. TCP est recommandé pour SIP-I en raison de la taille plus importante des messages.
`isup_version`	`atom`	`:itu_t92`	Variante d'encodage ISUP : `:itu_t92` (ITU-T Q.767) ou `:ansi` (ANSI T1.113).
`codecs`	`list(atom)`	`[:pcmu, :pcma]`	Codecs audio pris en charge pour la partie SDP.
`max_channels`	`integer`	`100`	Nombre maximum d'appels simultanés vers cette paire.
`trunk_group_id`	`string` ou `nil`	`nil`	Identifiant du groupe de trunk utilisé pour le contexte de routage.

Paramètre	Type	Par défaut	Description
`point_code`	`list` ou `nil`	`nil`	Code de point SS7 distant sous la forme `[a, b, c]`, utilisé comme contexte de routage ISUP.

Les paires SIP-I n'ont pas de configuration de maintien d'OPTIONS.

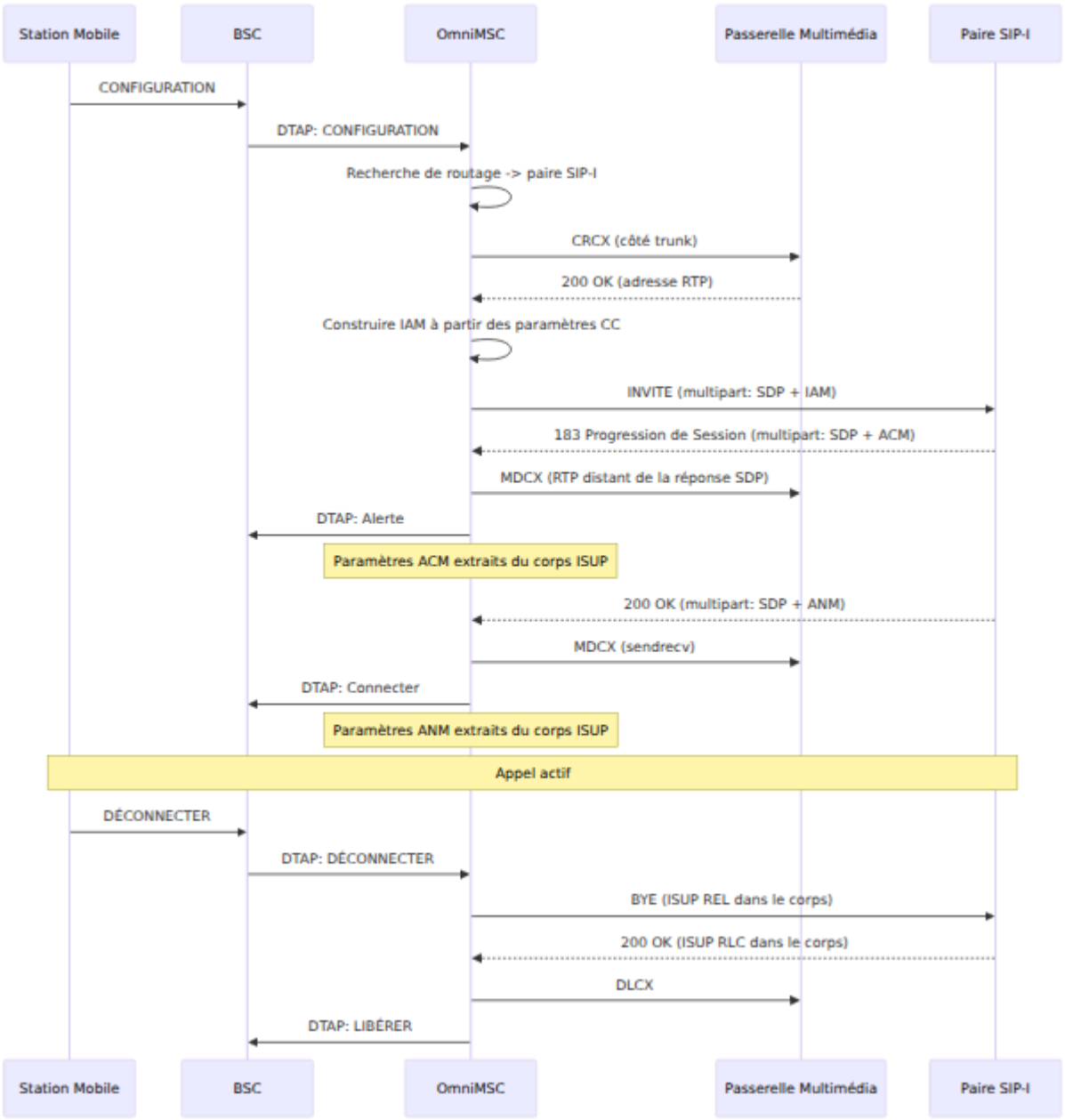
Appel Sortant (SIP-I)

Lorsque OmniMSC route un appel vers une paire SIP-I, il construit l'INVITE SIP avec un corps multipart contenant à la fois le SDP et l'ISUP IAM.



Appel Entrant (SIP-I)

Lorsqu'un INVITE arrive d'une paire SIP-I avec un corps multipart, OmniMSC extrait le message ISUP et l'utilise pour peupler les paramètres de la FSM CC.



Mappage des En-têtes ISUP-SIP

Lors de l'interconnexion entre le corps ISUP et les en-têtes SIP, OmniMSC applique le mappage suivant. Le corps ISUP est autoritaire ; les en-têtes SIP sont peuplés pour le bénéfice des intermédiaires uniquement SIP.

Paramètre ISUP (IAM)	En-tête SIP	Remarques
Numéro de la Partie Appelée	Request-URI, To	Format E.164 dans l'URI `tel:`
Numéro de la Partie Appelante	From, P-Asserted-Identity	L'indicateur de présentation contrôle l'en-tête `Privacy`
Indicateurs de Nature de Connexion	Via	Indicateur de saut par satellite
Indicateurs d'Appel Transféré	--	Encodé uniquement dans le corps ISUP
Catégorie de la Partie Appelante	P-Asserted-Identity	Catégorie d'opérateur/priorité
Exigence de Support de Transmission	Ligne `m=` SDP	Voix, audio 3,1 kHz, 64 k non restreint
Informations sur le Service Utilisateur	Lignes de codec SDP	Mappage des codecs et des débits
Indicateurs d'Appel Transféré Optionnels	Pris en charge	Indicateur d'accès ISDN

Paramètre ISUP (ACM/ANM)	Réponse SIP	Remarques
Indicateurs d'Appel Rétro	183/200	Indicateur de charge, drapeau d'interconnexion
Indicateurs de Cause (REL)	En-tête de Raison	Cause Q.850 selon la RFC 3326
Indicateurs d'Appel Rétro Optionnels	--	Encodé uniquement dans le corps ISUP

Référence de Mappage des Codes de Cause

SIP-I préserve le code de cause ISUP complet dans le corps ISUP. De plus, l'en-tête SIP `Reason` transporte la cause Q.850 pour les nœuds intermédiaires.

Pour la clôture d'appel, le message ISUP REL dans le corps BYE prend le pas sur l'en-tête de Raison SIP si les deux sont présents.

Références 3GPP et ITU-T

Référence	Titre	Pertinence
ITU-T Q.1912.5	Interconnexion entre SIP et Contrôle d'Appel Indépendant du Support (BICC) ou ISUP	Définition du protocole SIP-I
RFC 3204	Type de Média MIME pour les Objets ISUP et QSIG	Type de contenu `application/ISUP`
RFC 3261	SIP : Protocole d'Initiation de Session	Transport SIP
RFC 3264	Modèle Offre/Réponse avec SDP	Négociation SDP dans SIP-I
RFC 3326	Champ d'En-tête de Raison	Code de cause dans les réponses SIP
ITU-T Q.767	Application de l'ISUP	Encodage des messages ISUP
ITU-T Q.850	Utilisation de la Cause dans l'ISDN	Définitions des codes de cause
3GPP TS 29.163	Interconnexion entre le cœur commuté par circuit basé sur SIP-I et d'autres réseaux	Profil SIP-I 3GPP

Trunk SIP

Ce document couvre la configuration des pairs SIP, la surveillance des keepalives OPTIONS, la négociation des codecs SDP, le traitement des re-INVITE en cours de dialogue, les services en cours d'appel (mise en attente/reprise, transfert REFER, rafraîchissement UPDATE), les temporisateurs de session, le relais DTMF et les états d'appel des trunks SIP dans OmniMSC.

Pour le routage lié au SIP, voir Configuration de Routage. Pour le SIP avec ISUP encapsulé, voir Trunk SIP-I. Pour le dépannage des trunks SIP, voir Guide de Dépannage. Pour les séquences de flux d'appel montrant le signalement SIP dans le contexte, voir Diagrammes de Flux d'Appel. Pour la négociation des codecs des passerelles multimédias, voir Contrôle des Médias. Pour les paramètres de configuration des pairs SIP, voir Référence de Configuration.

Configuration des Pairs SIP

Chaque pair SIP représente un point de terminaison distant tel qu'une passerelle VoIP, un SBC, un nœud IMS ou un fournisseur de trunk SIP. Les pairs sont définis dans le bloc de configuration `:sip` et référencés par nom dans la table de routage.

Paramètre	Type	Par défaut	Description
`name`	`string`	-- (obligatoire)	Nom logique du pair. Référencé dans les entrées de la table de routage.
`address`	`string`	-- (obligatoire)	Adresse IP ou nom d'hôte du pair.
`port`	`integer`	`5060`	Port SIP du pair.
`transport`	`atom`	`:udp`	Protocole de transport : `:udp`, `:tcp` ou `:tls`.
`codecs`	`list(atom)`	`[:pcmu, :pcma]`	Codecs audio pris en charge pour la négociation SDP.
`max_channels`	`integer`	`100`	Nombre maximum d'appels simultanés vers ce pair.
`options_interval`	`integer` ou `nil`	`nil`	Intervalle en secondes pour les sondes de keepalive SIP OPTIONS.

OmniMSC s'identifie avec l'en-tête User-Agent `OmniMSC/0.1` dans toutes les requêtes et réponses SIP sortantes.

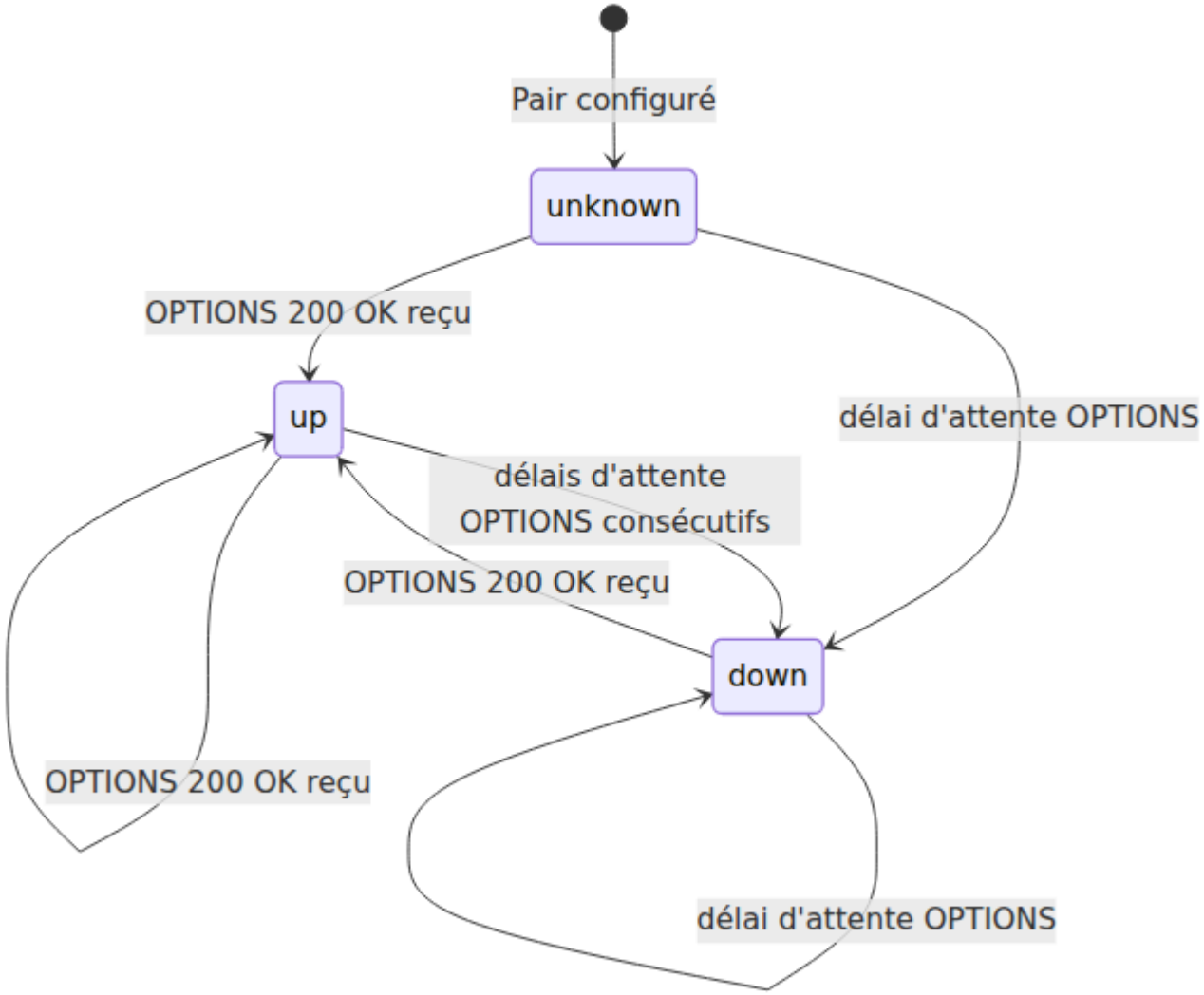
Keepalive SIP OPTIONS

Lorsque `options_interval` est configuré pour un pair, le Gestionnaire de Pairs SIP envoie des requêtes SIP OPTIONS périodiques pour surveiller la santé du

pair. L'état du pair détermine s'il est éligible pour le routage des appels.

États de Santé des Pairs

Chaque pair suit un état de `:up`, `:down` ou `:unknown`. Au démarrage, tous les pairs commencent dans l'état `:unknown`.

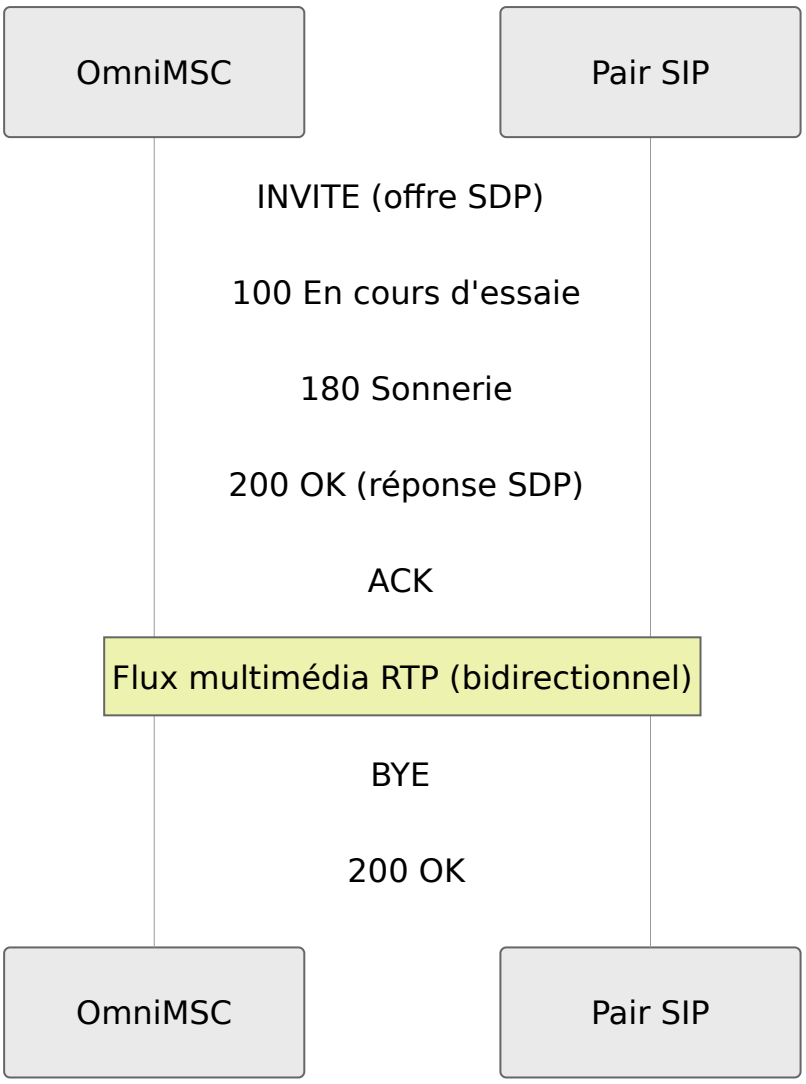


Événement	Transition	Effet
OPTIONS 200 OK reçu	Any -> up	Pair éligible pour le routage
Délais d'attente OPTIONS consécutifs	up/unknown -> down	Pair exclu du routage, alarme déclenchée
OPTIONS 200 OK après down	down -> up	Pair rééligible, alarme désactivée
`max_channels` atteint	up -> up (limite douce)	Nouveaux appels rejetés pour ce pair, appels existants non affectés

Pour la surveillance des pairs SIP dans le panneau de contrôle, voir Guide du Panneau de Contrôle.

Flux SIP d'Appel MO

Lorsque OmniMSC achemine un appel d'origine mobile vers un pair SIP, l'échange de signalement SIP suivant a lieu entre OmniMSC et le pair distant.



L'INVITE transporte une offre SDP avec des codecs basés sur la configuration du pair et les capacités du BSC. Le 200 OK contient la réponse SDP avec le codec sélectionné et l'adresse RTP distante. Après ACK, le chemin multimédia RTP est établi via la passerelle multimédia.

Traitement des Re-INVITE en Cours de Dialogue

Un pair SIP peut envoyer un re-INVITE dans un dialogue établi pour plusieurs raisons : mise en attente de l'appel, reprise, changement de codec ou rafraîchissement de session. OmniMSC accepte tout re-INVITE en cours de dialogue avec un 200 OK utilisant le SDP de session actuel. Si le re-INVITE transporte un corps SDP, le SDP distant est mis à jour à partir de celui-ci.

Le re-INVITE est répondu de la même manière, quelle que soit la raison (200 OK avec le SDP de session actuel). OmniMSC ne renvoie pas 488 Not Acceptable Here en réponse à un re-INVITE et ne renégocie pas le codec lors d'un re-INVITE. Le dialogue existant et la session multimédia restent en place. De plus, OmniMSC inspecte le SDP proposé pour une transition de mise en attente/reprise et le signale à la FSM de Contrôle d'Appel (CC) (voir Services en Cours d'Appel ci-dessous).

Services en Cours d'Appel

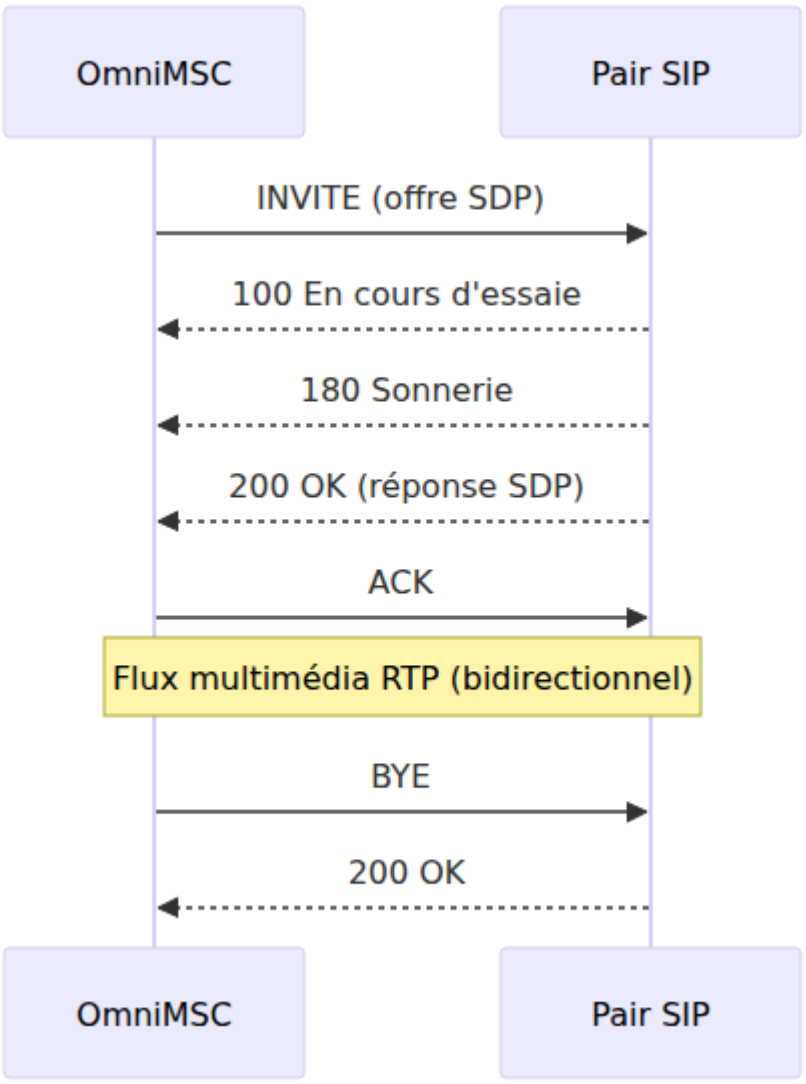
OmniMSC gère trois procédures en cours de dialogue sur une jambe de trunk SIP établie : mise en attente/reprise d'appel, transfert d'appel REFER et rafraîchissement de session UPDATE. Les trois ne s'appliquent que dans l'état d'appel `actif` ; les demandes reçues en dehors de `actif` sont ignorées ou rejetées selon le cas.

Mise en Attente et Reprise d'Appel

Un pair distant met l'appel en attente en envoyant un re-INVITE (ou UPDATE) dont le SDP marque le flux multimédia comme inactif. OmniMSC reconnaît à la fois les encodages de mise en attente modernes et hérités (section 5.1 de la RFC 3264, Annexe B de la TS 29.163) :

Encodage de Mise en Attente	Marqueur SDP	Remarques
Attribut de Direction	`a=sendonly` ou `a=inactive`	Préféré (RFC 3264). L'attribut au niveau multimédia remplace celui au niveau de session
Connexion à Zéro	`c=0.0.0.0`	Offre de mise en attente héritée de la RFC 2543
Reprise	`a=sendrecv` (ou pas d'attribut de direction) et un `c=` non nul	Rétablit le flux à actif

Lors d'une transition vers la mise en attente, OmniMSC répond par un 200 OK et signale `hold_ind` à la FSM CC ; la FSM marque l'appel comme en attente et propage la condition vers la station mobile (un NOTIFY avec un indicateur de mise en attente distante) et la couche MNCC. Lors d'une transition vers l'état actif, `retrieve_ind` est signalé et l'état de mise en attente est effacé. Les offres répétées avec une direction inchangée (par exemple, un rafraîchissement de session qui maintient l'appel en attente) sont idempotentes et ne signalent pas de transition.

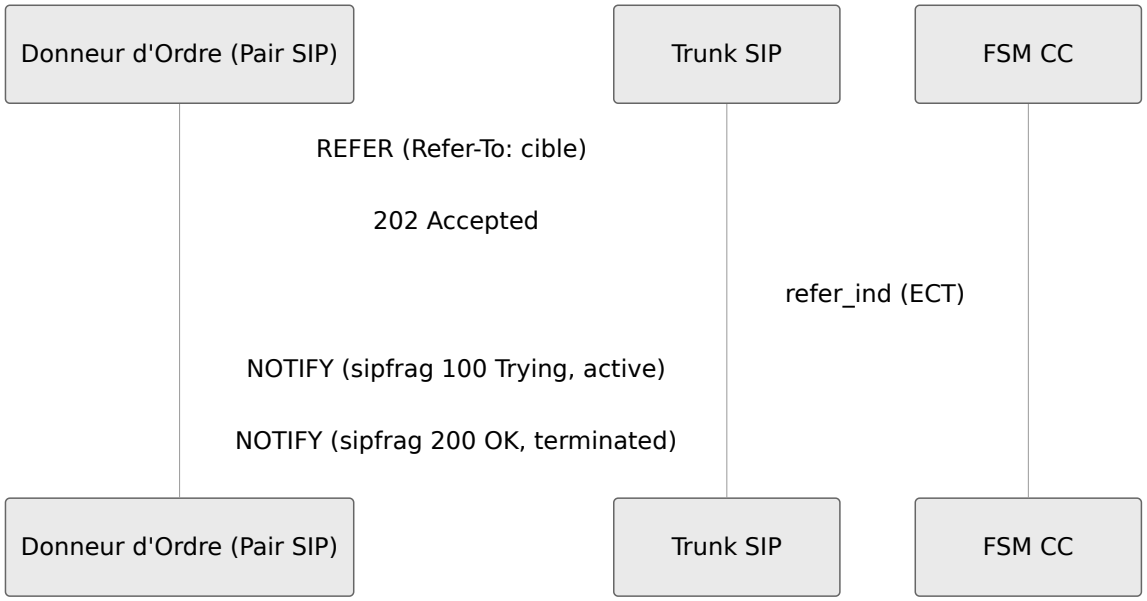


Transfert d'Appel REFER (RFC 3515)

Un pair peut transférer l'appel en envoyant un REFER en cours de dialogue dont l'en-tête `Refer-To` nomme la cible du transfert. OmniMSC accepte le REFER avec un 202 Accepted (établissant l'abonnement implicite à l'événement de référence), rapporte le transfert à la FSM CC comme une indication ECT (Transfert d'Appel Explicite, TS 24.091) portant l'URI `Refer-To`, et rapporte les progrès au donneur d'ordre via des messages NOTIFY sipfrag (section 2.4.5 de la RFC 3515). Un REFER sans `Refer-To` utilisable est rejeté avec 400 Bad Request.

Les NOTIFY de progression portent un corps `message/sipfrag` avec la ligne d'état de la transaction de l'autre côté et un en-tête `Subscription-State` :

NOTIFY	corps sipfrag	Subscription-State
Progress	`SIP/2.0 100 Trying`	`active`
Completion	`SIP/2.0 200 OK`	`terminated;reason=noresource`



Temporisateur de Session (RFC 4028)

OmniMSC prend en charge les temporisateurs de session SIP par la RFC 4028 pour détecter et nettoyer les sessions SIP orphelines. Les temporisateurs de session garantissent que les deux points de terminaison rafraîchissent périodiquement la session, empêchant ainsi un état d'appel obsolète après des pannes réseau.

Paramètre	Valeur	Description
Session-Expires	1800s (par défaut)	Temps maximum entre les rafraîchissements de session
Min-SE	90s	Valeur minimale acceptable pour Session-Expires
Refresher	UAC ou UAS	Déterminé lors de la négociation
session_refresh_method	`:invite` (par défaut) ou `:update`	Méthode utilisée pour envoyer le rafraîchissement périodique

Négociation du Temporisateur de Session

OmniMSC inclut les en-têtes `Session-Expires` et `Min-SE` dans les requêtes INVITE sortantes. Lorsque OmniMSC reçoit un 422 Session Interval Too Small en réponse à une INVITE sortante, il accuse réception du 422, extrait le Min-SE du pair et réessaie l'INVITE avec un Session-Expires mis à jour qui est au moins le minimum du pair.

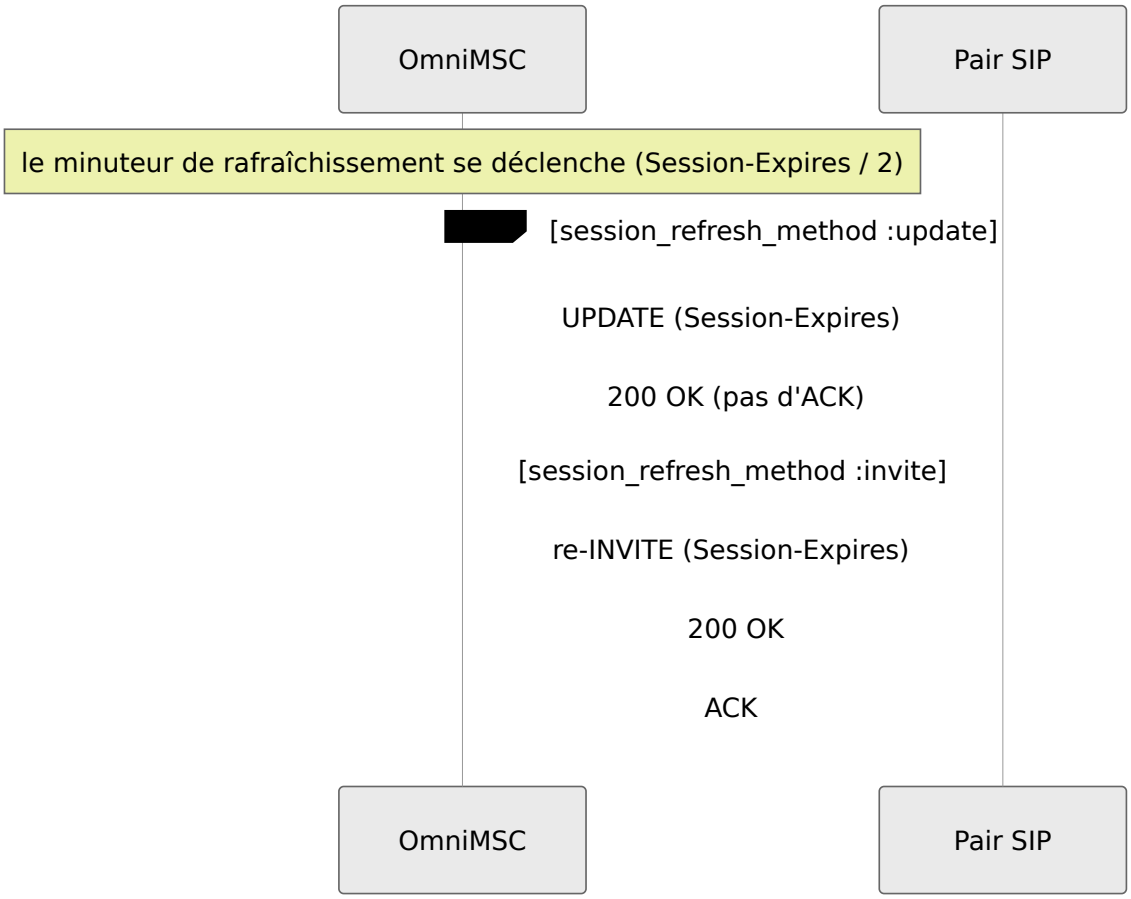
Le rafraîchissement est envoyé à la moitié de l'intervalle Session-Expires négocié. Si aucun rafraîchissement n'arrive avant l'expiration de la session, OmniMSC envoie BYE pour mettre fin à l'appel et libère toutes les ressources associées.

Méthode de Rafraîchissement : re-INVITE ou UPDATE (RFC 3311)

Par défaut, le rafraîchissement est envoyé sous forme de re-INVITE. Lorsqu'un trunk est configuré avec `session_refresh_method: :update`, OmniMSC rafraîchit la session avec un UPDATE (RFC 3311) à la place. L'UPDATE est plus léger : c'est une transaction autonome qui ne perturbe pas l'offre/réponse et ne nécessite pas d'ACK. Un 200 OK d'UPDATE n'est donc jamais accusé de

réception, tandis qu'un 200 OK de re-INVITE est accusé de réception comme d'habitude.

OmniMSC répond également à un UPDATE initié par le pair. Lorsque l'UPDATE transporte une offre SDP, OmniMSC renvoie son SDP actuel comme réponse ; le 200 OK annonce le `Session-Expires` négocié. Un UPDATE portant une offre de mise en attente entraîne le même signalement de mise en attente/reprise à la FSM CC qu'un re-INVITE.



Relais DTMF

OmniMSC relaie les tons DTMF en utilisant des messages SIP INFO selon le type de contenu `application/dtmf-relay`. Cette méthode est utilisée lorsque le pair ne prend pas en charge le type de charge utile RTP telephone-event de la RFC 2833 ou lorsque le DTMF hors bande est préféré.

Champ	Description	Exemple
Content-Type	Type MIME pour le relais DTMF	`application/dtmf-relay`
Signal	Chiffre DTMF (0-9, *, #, A-D)	`Signal=5`
Duration	Durée du ton en millisecondes	`Duration=160`

Lorsque des événements DTMF sont détectés du côté radio (via la passerelle multimédia), OmniMSC génère un message SIP INFO vers le pair SIP avec le signal et la durée correspondants. Dans la direction inverse, les événements DTMF SIP INFO entrants sont transférés à la passerelle multimédia pour être reproduits vers la station mobile.

Négociation des Codecs SDP

OmniMSC génère des offres SDP basées sur l'intersection de la liste de codecs configurée du pair et des capacités de codec vocal rapportées par le BSC. Les codecs sont offerts par ordre de préférence.

Codecs Pris en Charge

Codec	Type de Charge Utile RTP	Taux d'Horloge	Paramètres fmtp
PCMU	0	8000	--
PCMA	8	8000	--
AMR (narrowband)	dynamique (96)	8000	`octet-align=1`
AMR-WB (wideband)	dynamique (97)	16000	`octet-align=1`

La liste de codecs par défaut est `[:pcmu, :pcma]` (charge utile PCMU 0 et charge utile PCMA 8). L'AMR est proposé avec `octet-align=1` (RFC 4867) pour l'interopérabilité avec les réseaux d'accès 3GPP. La version de la parole GSM à débit complet est mappée sur PCMA (charge utile 8) du côté SIP. L'AMR et l'AMR-WB sont proposés lorsque le BSC indique le support de ces codecs dans la liste de versions vocales lors de l'attribution.

Sélection de Codec

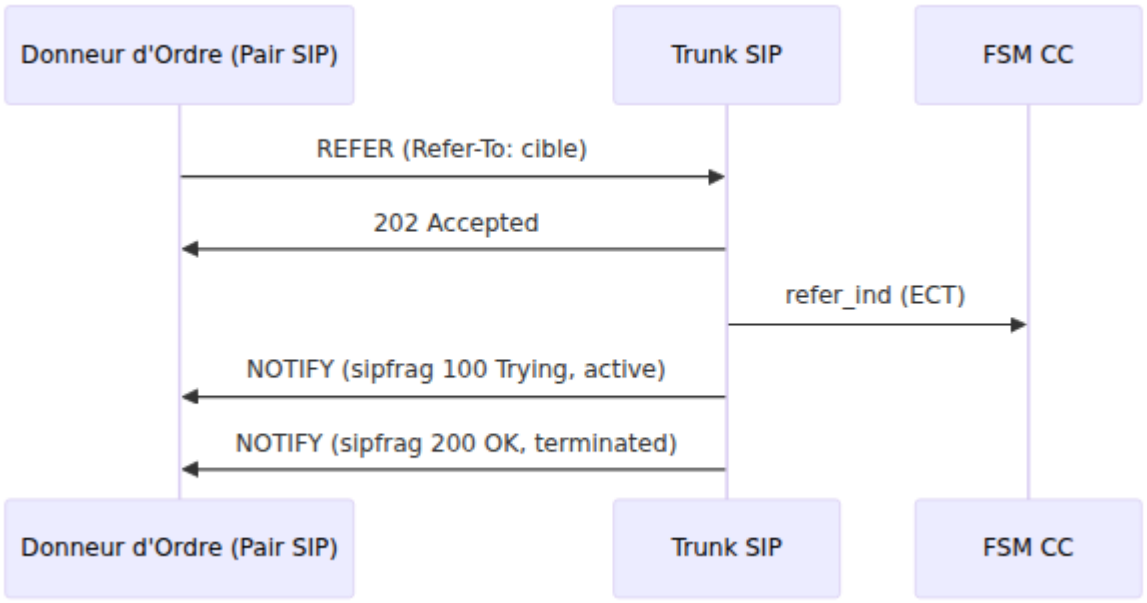
La sélection de codec suit le modèle Offre/Réponse SDP (RFC 3264) :

1. OmniMSC construit l'offre SDP à partir de la liste de codecs du pair, filtrée par les capacités vocales du BSC.
2. Le pair distant répond avec une réponse SDP contenant un ou plusieurs codecs acceptés.
3. OmniMSC sélectionne le premier codec commun dans l'ordre d'offre original.
4. La passerelle multimédia est instruite (via MDCX) avec le codec sélectionné et les paramètres RTP.

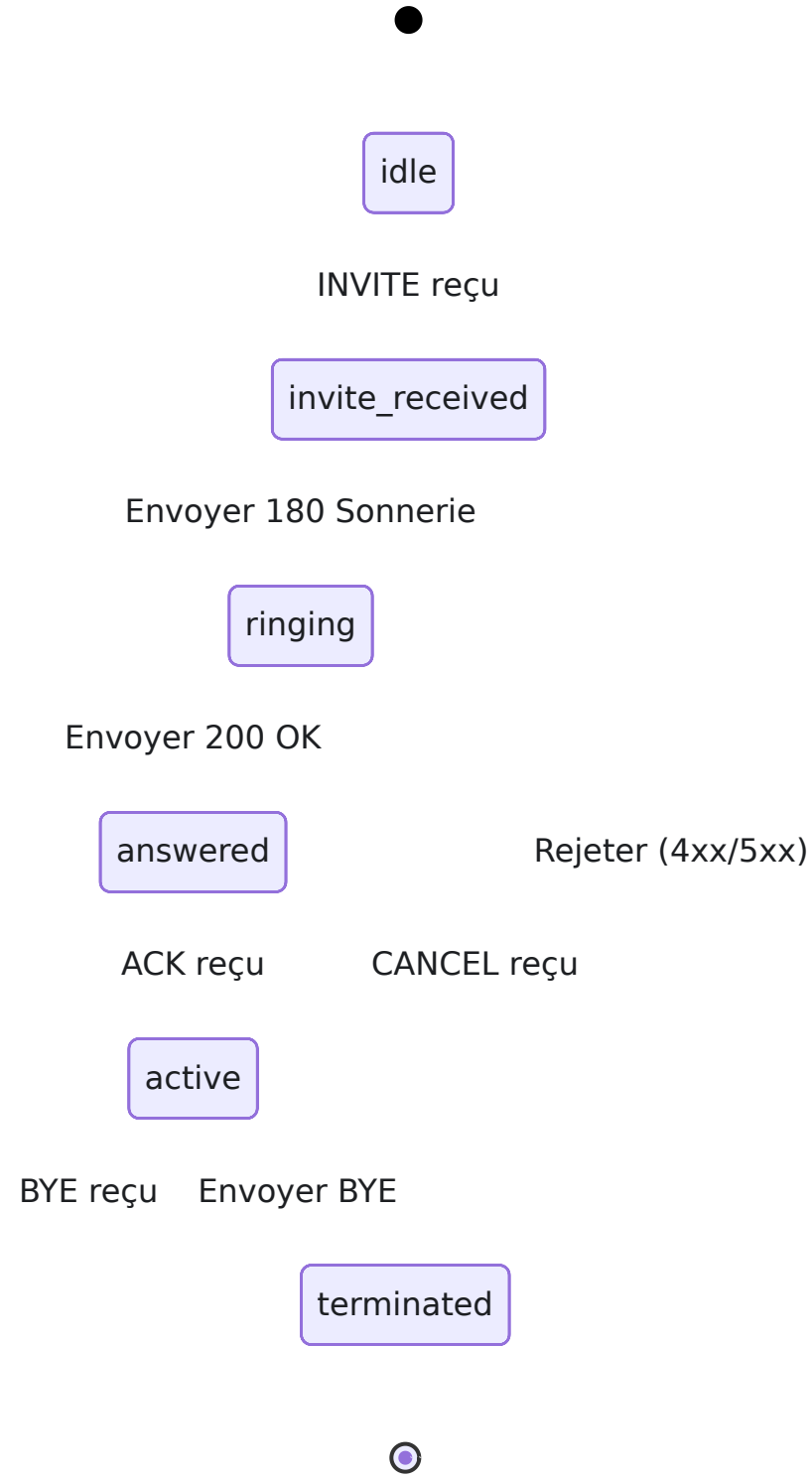
Si aucun codec commun n'existe, OmniMSC répond avec ou reçoit 488 Not Acceptable Here.

États d'Appel des Trunks SIP

États d'Appel Sortants



États d'Appel Entrants



Références

Référence	Titre	Pertinence
RFC 3261	SIP : Protocole d'Initiation de Session	Signalement SIP de base
RFC 4028	Temporisateurs de Session dans SIP	Session-Expires, Min-SE, mécanisme de rafraîchissement
RFC 3311	La Méthode SIP UPDATE	Rafraîchissement de session basé sur UPDATE
RFC 3515	La Méthode SIP Refer	Transfert d'appel REFER, progression NOTIFY sipfrag
RFC 2833	Charge Utile RTP pour les Chiffres DTMF	Type de charge utile RTP telephone-event
RFC 3264	Modèle Offre/Réponse avec SDP	Négociation des codecs SDP, marqueurs de mise en attente/reprise
RFC 4867	Format de Charge Utile RTP pour AMR et AMR-WB	Paramètre d'alignement octet AMR
RFC 3326	Champ d'En-tête de Raison	Code de cause dans BYE/CANCEL
TS 29.163	Interopérabilité entre les réseaux IMS et CS	Annexe B : interopérabilité mise en attente/reprise

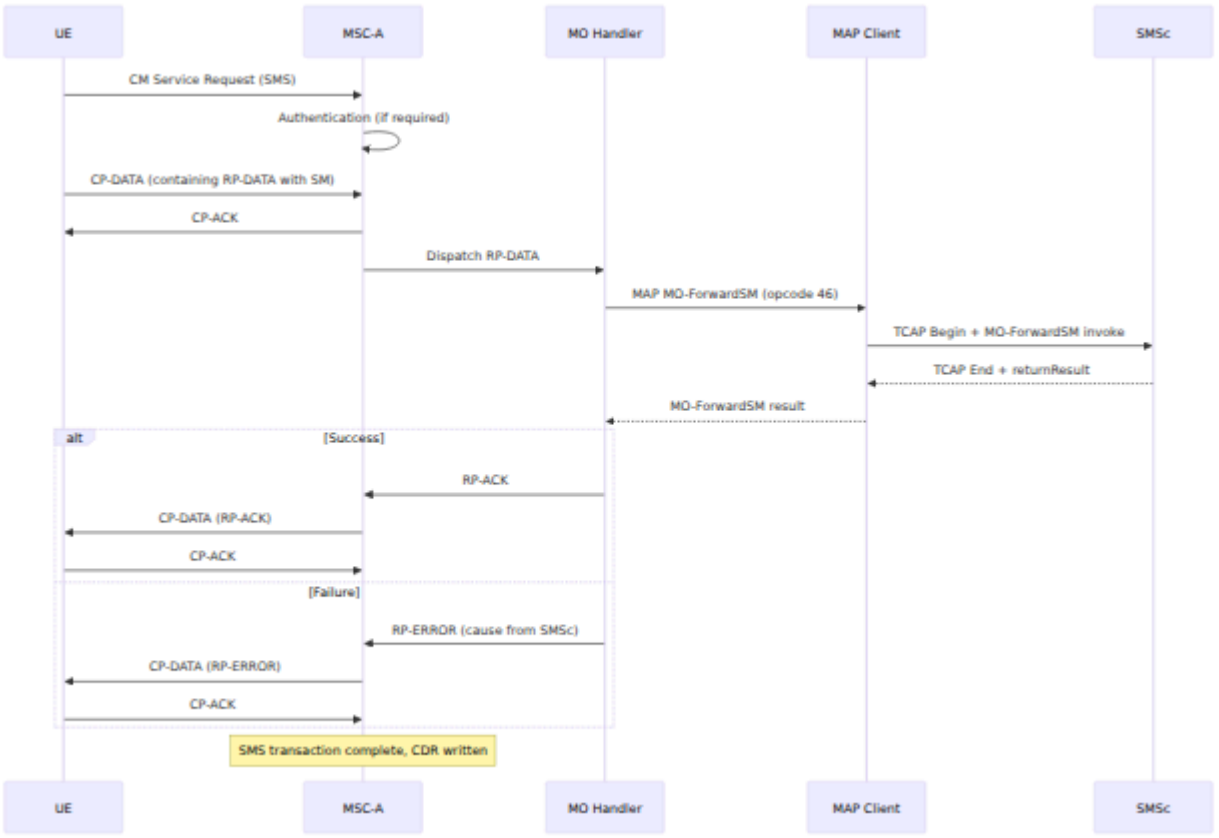
SMS

Ce document décrit l'implémentation du service de messages courts dans OmniMSC, couvrant les flux SMS d'origine mobile et de terminaison mobile, l'allocation des identifiants de transaction DTAP, la gestion du SAPI de l'interface A, le routage des réponses MAP et les couches de codec SMS.

Pour les diagrammes de flux d'appel qui incluent les SMS aux côtés de la voix, voir Diagrammes de flux d'appel. Pour les détails de l'interface MAP couvrant les opérations MO-ForwardSM et MT-ForwardSM, voir Opérations MAP. Pour la configuration de l'adresse SMSc et du code de point, voir Référence de configuration. Pour les problèmes de livraison de SMS courants, voir Dépannage — Problèmes de SMS.

MO-SMS (SMS d'origine mobile)

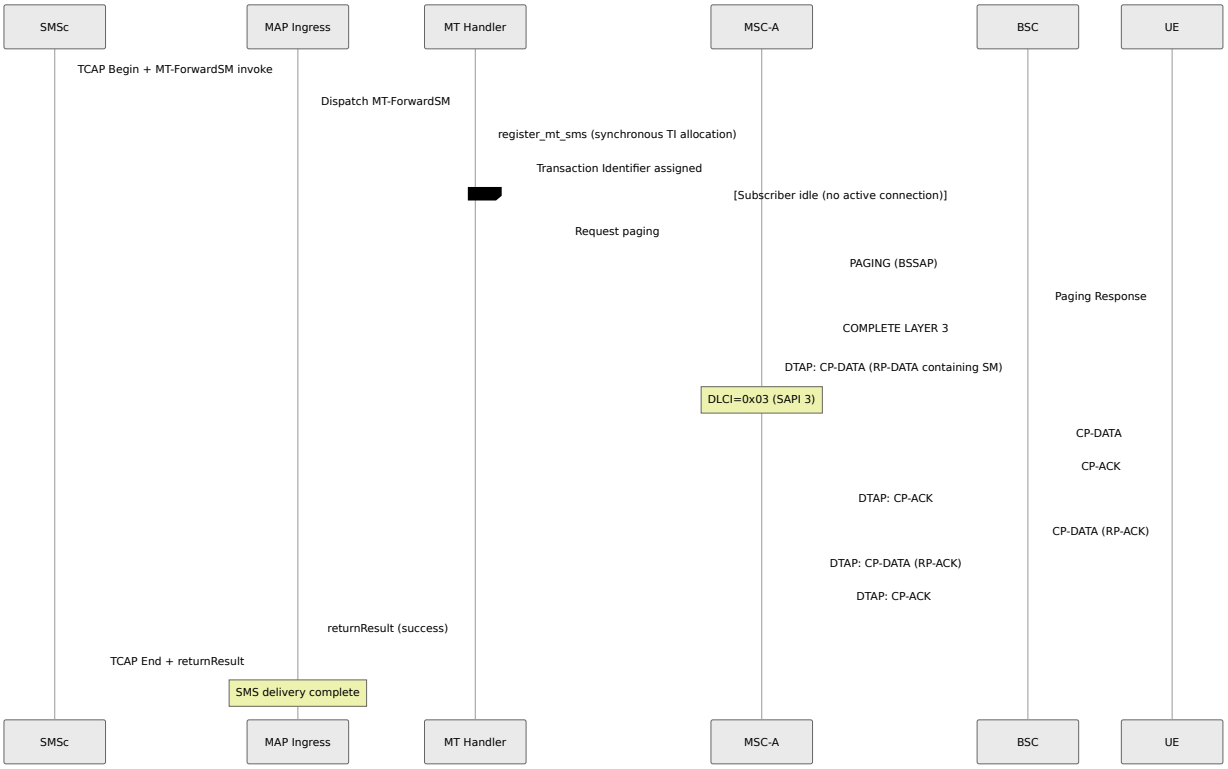
Un abonné envoie un message court via le MSC au Centre SMS (SMSc). Le MSC agit comme un relais, recevant le SM de l'interface radio et le transmettant au SMSc en utilisant MAP MO-ForwardSM.



Le MO Handler extrait le SM-RP-DA (adresse de destination, typiquement l'adresse SMSc) et le SM-RP-OA (adresse d'origine, le MSISDN de l'abonné) des RP-DATA, puis construit la requête MAP MO-ForwardSM. La réponse MAP détermine si le MSC envoie RP-ACK ou RP-ERROR au UE.

MT-SMS (SMS de terminaison mobile)

Le SMSc livre un message court à un abonné via le MSC. Le SMSc envoie un MAP MT-ForwardSM (opcode 44) au MSC, qui cherche l'abonné si nécessaire et livre le SM par l'interface radio.



Allocation TI synchrone

Le MT Handler appelle `register_mt_sms` sur le processus MSC-A comme une opération synchrone. Cela alloue un identifiant de transaction DTAP pour la livraison MT-SMS et empêche une condition de concurrence où deux livraisons MT-SMS simultanées au même abonné pourraient se voir attribuer le même TI. L'appel synchrone garantit que les valeurs TI sont uniques pour toutes les transactions SMS actives pour un abonné donné.

Identifiant de transaction DTAP

Pour le MT-SMS, le réseau alloue l'identifiant de transaction (TI). Selon la 3GPP TS 24.007, le drapeau TI distingue l'initiateur :

Direction	Drapeau TI	Signification
Réseau → UE (CP-DATA)	0	Le réseau a initié cette transaction
UE → Réseau (CP-ACK, RP-ACK)	1	UE répondant à une transaction initiée par le réseau

Le MSC définit le drapeau TI=0 dans le CP-DATA envoyé au UE. Le UE reflète la valeur TI mais définit le drapeau=1 dans toutes les réponses (CP-ACK, CP-DATA contenant RP-ACK). Cette convention permet aux deux parties de distinguer entre plusieurs transactions SMS simultanées.

SAPI 3

Les PDU NAS SMS (CP-DATA, CP-ACK, CP-ERROR) sont transportés sur SAPI 3 de l'interface A selon la 3GPP TS 48.006. Le byte DLCI (Identifiant de connexion de liaison de données) dans l'en-tête DTAP BSSAP est défini sur 0x03, indiquant SAPI=3.

Le SAPI 3 fournit un canal logique séparé du canal de signalisation principal (SAPI 0), qui transporte les messages CC et MM. Cette séparation permet la livraison de SMS de se produire simultanément avec un appel vocal actif sans interférer avec le signalement de contrôle d'appel.

Routage des réponses MAP

Lorsqu'un MT-ForwardSM arrive du SMSc, le MSC doit router la réponse TCAP End vers le bon code de point d'origine. Le module d'entrée capture l'OPC (Code de point d'origine) du message de transfert M3UA entrant et le stocke comme `routing_info[:opc]`.

Lors de la construction de la réponse TCAP End, le MSC utilise cet OPC stocké comme DPC (Code de point de destination) pour le message M3UA sortant. Cela garantit que la réponse atteint le bon SMSc, ce qui est important dans les réseaux où plusieurs instances de SMSc utilisent différents codes de point, ou où un STP route en fonction du code de point plutôt que du titre global SCCP.

L'échange OPC/DPC suit la convention standard M3UA : l'OPC de réponse est le code de point propre du MSC (le DPC entrant), et le DPC de réponse est le code de point du SMSc (l'OPC entrant).

Codec SMS

Le codec SMS gère deux couches de protocole selon la 3GPP TS 24.011 :

Couche CP (Sous-couche de gestion de connexion)

Message	Direction	Description
CP-DATA	Les deux	Transporte un message RP comme charge utile
CP-ACK	Les deux	Accuse réception de CP-DATA
CP-ERROR	Les deux	Signale une erreur de couche CP (valeur de cause incluse)

CP-DATA contient un seul PDU de couche RP. Chaque CP-DATA doit être accusé réception avec un CP-ACK avant que le prochain CP-DATA puisse être envoyé sur la même transaction.

Couche RP (Protocole de relais)

Message	Direction	Description
RP-DATA	Les deux	Transporte le SM-TP-DU (le message court réel) avec les adresses RP-DA et RP-OA
RP-ACK	Les deux	Confirme la livraison réussie de RP-DATA
RP-ERROR	Les deux	Signale une erreur de couche RP (valeur de cause provenant du tableau 8.4 de la TS 24.011)

Pour le MO-SMS, le RP-DATA du UE contient le SM-RP-DA (adresse SMSc) et le SM-RP-OA (adresse de l'abonné). Pour le MT-SMS, le MSC construit RP-DATA avec SM-RP-DA (IMSI de l'abonné) et SM-RP-OA (adresse SMSc).

Références

Spécification	Titre	Pertinence
TS 24.011	Support du service de messages courts point à point sur l'interface radio mobile	Couches de protocole CP et RP, formats de message, codes de cause
TS 29.002 Section 12	Spécification MAP - Procédures de service de messages courts	MAP MO-ForwardSM (opcode 46), MT-ForwardSM (opcode 44), informations de routage pour SM
TS 23.040	Réalisation technique de SMS	Encodage de la couche SM-TP, période de validité, rapports de statut
TS 48.006	Spécification du mécanisme de transport de signalisation pour l'interface BSC-MSC	Attribution DLCI/SAPI pour DTAP de l'interface A
TS 24.007	Signalisation de l'interface radio mobile couche 3 - Aspects généraux	Allocation de l'identifiant de transaction et conventions de drapeau TI

Services Complémentaires

Ce document décrit les services complémentaires mis en œuvre dans OmniMSC, couvrant le mécanisme de dispatch SS, le renvoi d'appel, le barring d'appel, l'attente d'appel, l'identification de ligne, la mise en attente d'appel, la conférence multi-parties et l'interaction avec le HLR. Pour les séquences de flux d'appel, voir Diagrammes de Flux d'Appel. Pour les paramètres de configuration, voir Référence de Configuration. Pour les fonctionnalités d'appel avancées telles que ECT et CCBS, voir Fonctionnalités d'Appel Avancées. Pour les opérations MAP utilisées pour relayer les changements SS au HLR (RegisterSS, ActivateSS), voir Opérations MAP. Pour les détails du pont de conférence MPTY au niveau média, voir Contrôle Média.

Vue d'Ensemble du Dispatch SS

Une station mobile interagit avec les services complémentaires en envoyant des messages DTAP du groupe de messages SS : SS REGISTER, SS FACILITY et SS RELEASE COMPLETE, comme défini dans 3GPP TS 24.010. Chaque message contient un élément d'information de service contenant des composants codés en ASN.1 avec un code d'opération et un code SS qui identifient le service cible. Les services complémentaires provisionnés pour chaque abonné, ainsi que leurs badges de statut, sont visibles sur la page des Abonnés du panneau de contrôle — voir Guide du Panneau de Contrôle.

Lorsque OmniMSC reçoit l'un de ces messages, le dispatcher CC/SS extrait le code SS de l'IE de service et achemine la demande vers le gestionnaire de service approprié. Le code SS est une valeur sur un octet définie dans 3GPP TS 29.002 qui identifie de manière unique le service complémentaire invoqué.

Opérations SS

Chaque service complémentaire prend en charge un sous-ensemble des cinq opérations standard :

Opération	Description
Enregistrer	Provisionner le service avec des paramètres (par exemple, numéro de renvoi, minuteur de non-réponse)
Effacer	Supprimer un service précédemment enregistré
Activer	Activer un service enregistré afin qu'il prenne effet
Désactiver	Désactiver un service actif sans supprimer l'enregistrement
Interroger	Interroger l'état actuel et les paramètres d'un service

Le MS encode ces opérations en utilisant des composants d'invocation au sein de l'IE de service. OmniMSC traite la demande, détermine si l'implication du HLR est requise, et renvoie un composant de résultat de retour ou d'erreur de retour dans la réponse.

Renvoi d'Appel

OmniMSC met en œuvre les quatre variantes de renvoi d'appel 3GPP définies dans TS 24.082. Chaque variante peut être provisionnée par abonné via MAP INSERT SUBSCRIBER DATA depuis le HLR, ou gérée par l'abonné en utilisant les opérations SS Register, Activate, Deactivate, Erase et Interrogate.

Variante	Code SS	Déclencheur	Référence 3GPP
Renvoi d'Appel Inconditionnel (CFU)	0x21	Tous les appels entrants	TS 24.082 Sec 4.1
Renvoi d'Appel en Cas d'Occupation (CFB)	0x29	Abonné appelé occupé	TS 24.082 Sec 4.2
Renvoi d'Appel en Cas de Non-Réponse (CFNRy)	0x2A	Pas de réponse dans le minuteur	TS 24.082 Sec 4.3
Renvoi d'Appel en Cas de Non Joignable (CFNRc)	0x2B	Abonné non joignable	TS 24.082 Sec 4.4

CFU (Renvoi d'Appel Inconditionnel)

Tous les appels à l'abonné sont renvoyés inconditionnellement au numéro de renvoi configuré. Lorsque CFU est actif, le MSC ne cherche pas à joindre l'abonné. CFU a la priorité sur toutes les autres variantes de renvoi.

CFB (Renvoi d'Appel en Cas d'Occupation)

Les appels sont renvoyés lorsque l'abonné est occupé (tous les canaux de trafic occupés ou utilisateur déterminé occupé). Le MSC détecte la condition d'occupation soit à partir de l'interface radio (UDUB) soit de l'état de la FSM CC.

CFNRy (Renvoi d'Appel en Cas de Non-Réponse)

Les appels sont renvoyés lorsque l'abonné ne répond pas dans un minuteur configurable (par défaut 20 secondes, plage 5-30 secondes selon 3GPP TS 24.082). Le minuteur de non-réponse commence lorsque la réponse de pagination ou l'indication d'alerte est reçue.

CFNRc (Renvoi d'Appel en Cas de Non Joignable)

Les appels sont renvoyés lorsque l'abonné ne peut pas être joint : IMSI détaché, pas de réponse de pagination, ou échec de lien radio. Le MSC détermine la joignabilité à partir de l'état de l'abonné VLR et du résultat de pagination.

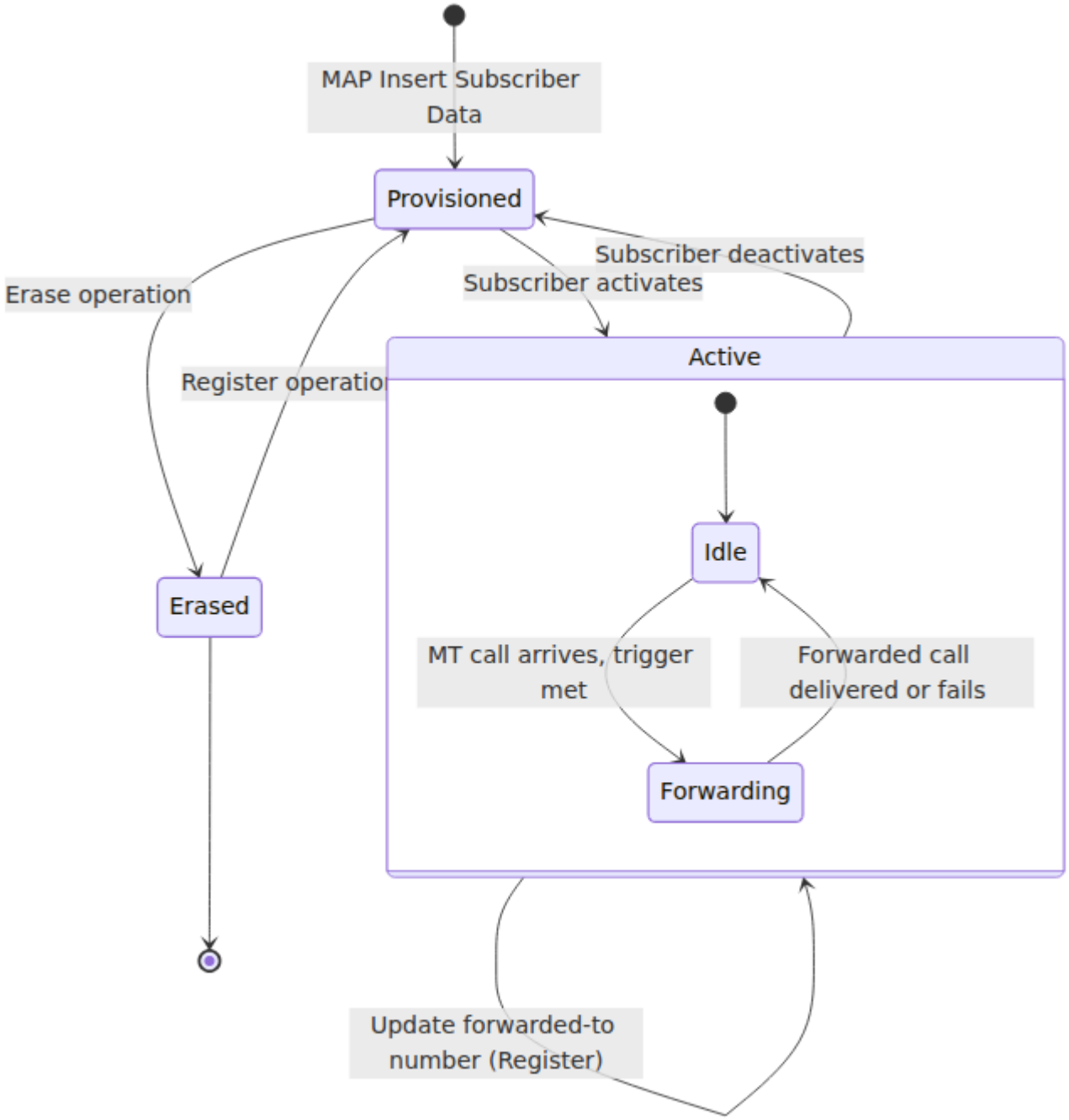
Opérations de Renvoi d'Appel

Un abonné gère le renvoi d'appel à travers les opérations SS standard :

Opération	Effet
Enregistrer	Stocker le numéro de renvoi et le minuteur de non-réponse optionnel ; active implicitement le service
Effacer	Supprimer le numéro de renvoi et désactiver le service
Activer	Activer une variante de renvoi précédemment enregistrée
Désactiver	Désactiver le renvoi sans supprimer le numéro enregistré
Interroger	Retourner l'état actuel (actif/inactif) et le numéro de renvoi

Les opérations d'enregistrement et d'effacement sont relayées au HLR via MAP, puisque les données de renvoi font partie du profil de l'abonné. L'activation, la désactivation et l'interrogation peuvent être gérées localement à partir des données VLR lorsque l'information est déjà disponible, ou relayées au HLR sinon.

Diagramme d'État de Renvoi d'Appel



Barring d'Appel

OmniMSC met en œuvre des services de barring d'appel selon 3GPP TS 24.088. Les catégories de barring sont provisionnées par le HLR via MAP INSERT SUBSCRIBER DATA et sont appliquées par le MSC lors de la configuration de l'appel. L'abonné ne peut pas annuler le barring provisionné par l'opérateur.

Le barring d'appel utilise l'espace de code SS MAP canonique défini dans 3GPP TS 29.002. Les catégories de barring individuelles et leurs codes de groupe englobants sont :

Catégorie	Code SS	Direction	Effet
Barring de Tous les Appels Sortants (BAOC)	0x92	MO	Bloquer tous les appels sortants
Barring des Appels Internationaux Sortants (BOIC)	0x93	MO	Bloquer les appels sortants internationaux
Barring des Appels Internationaux Sortants sauf vers le Pays d'Origine (BOIC-exHC)	0x94	MO	Bloquer les appels sortants internationaux sauf vers le pays PLMN d'origine
Barring de Tous les Appels Entrants (BAIC)	0x9A	MT	Bloquer tous les appels entrants
Barring des Appels Entrants lors de l'Itinérance (BicRoam)	0x9B	MT	Bloquer les appels entrants lorsque l'abonné est en itinérance en dehors de HPLMN

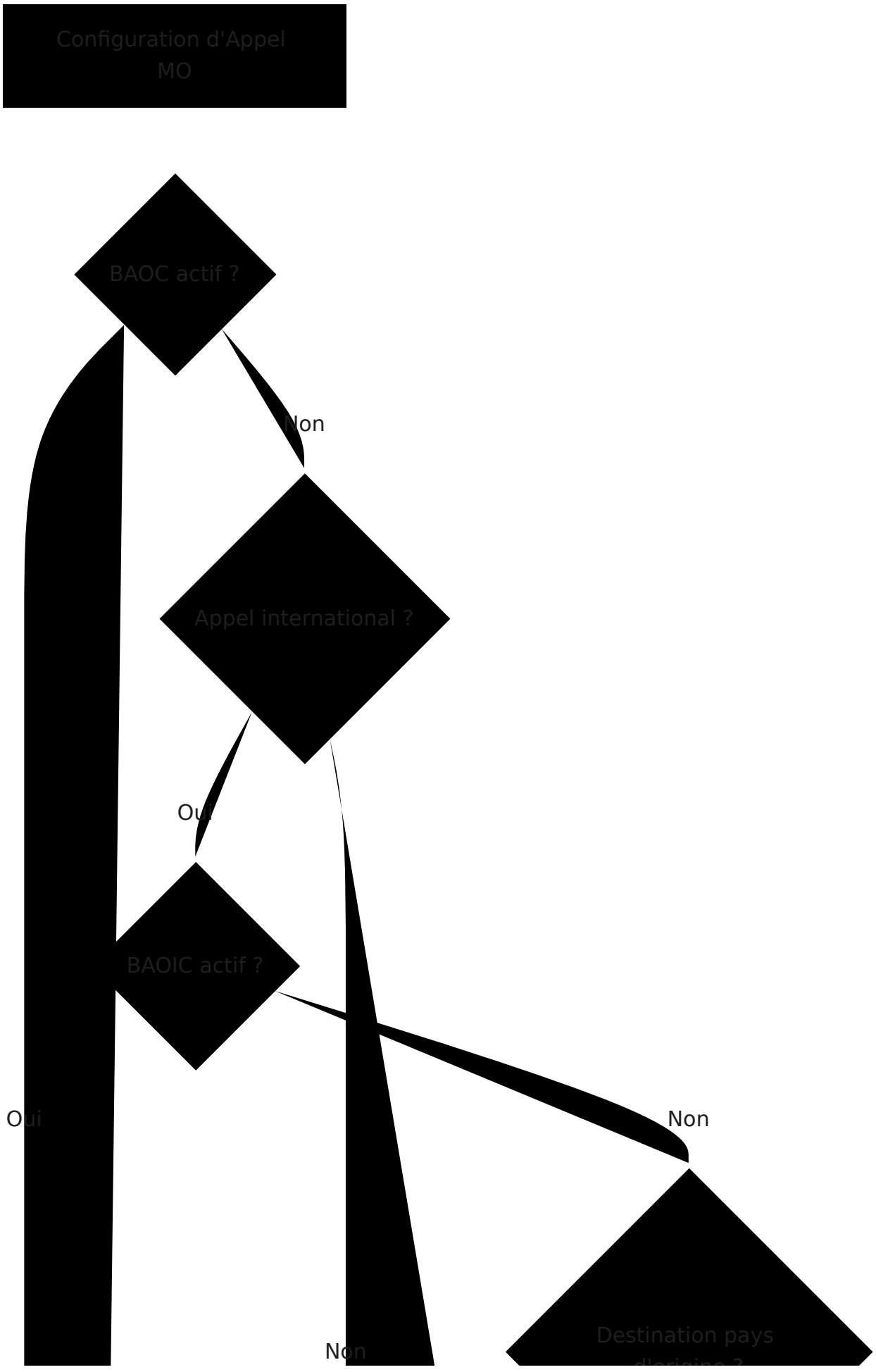
Les codes SS de groupe s'adressent à plusieurs catégories à la fois :

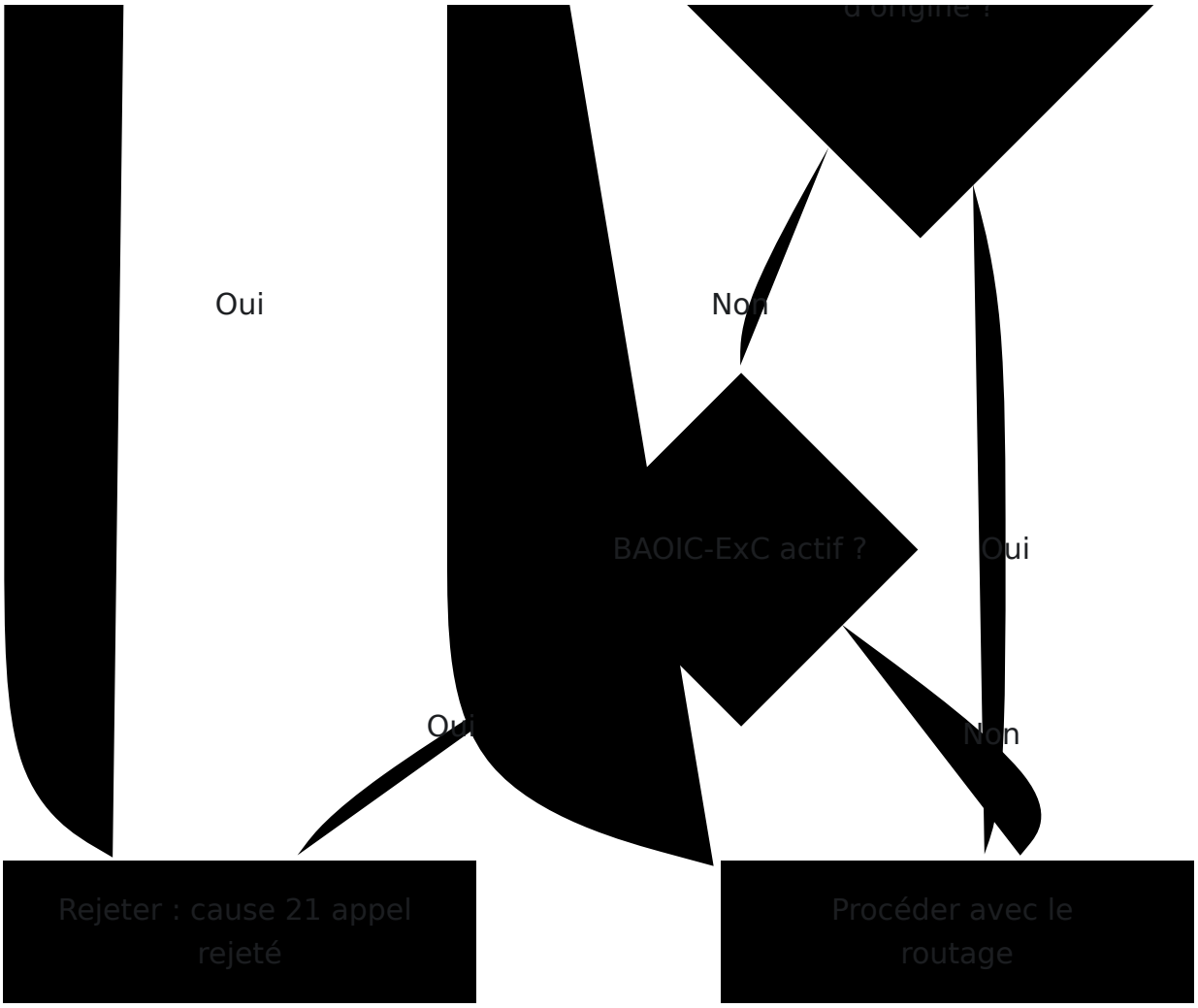
Groupe	Code SS	Couvre
Tous les Services de Barring	0x90	Tous les barrings sortants et entrants
Barring des Appels Sortants	0x91	BAOC, BOIC, BOIC-exHC
Barring des Appels Entrants	0x99	BAIC, BicRoam

Provisionnement de Barring

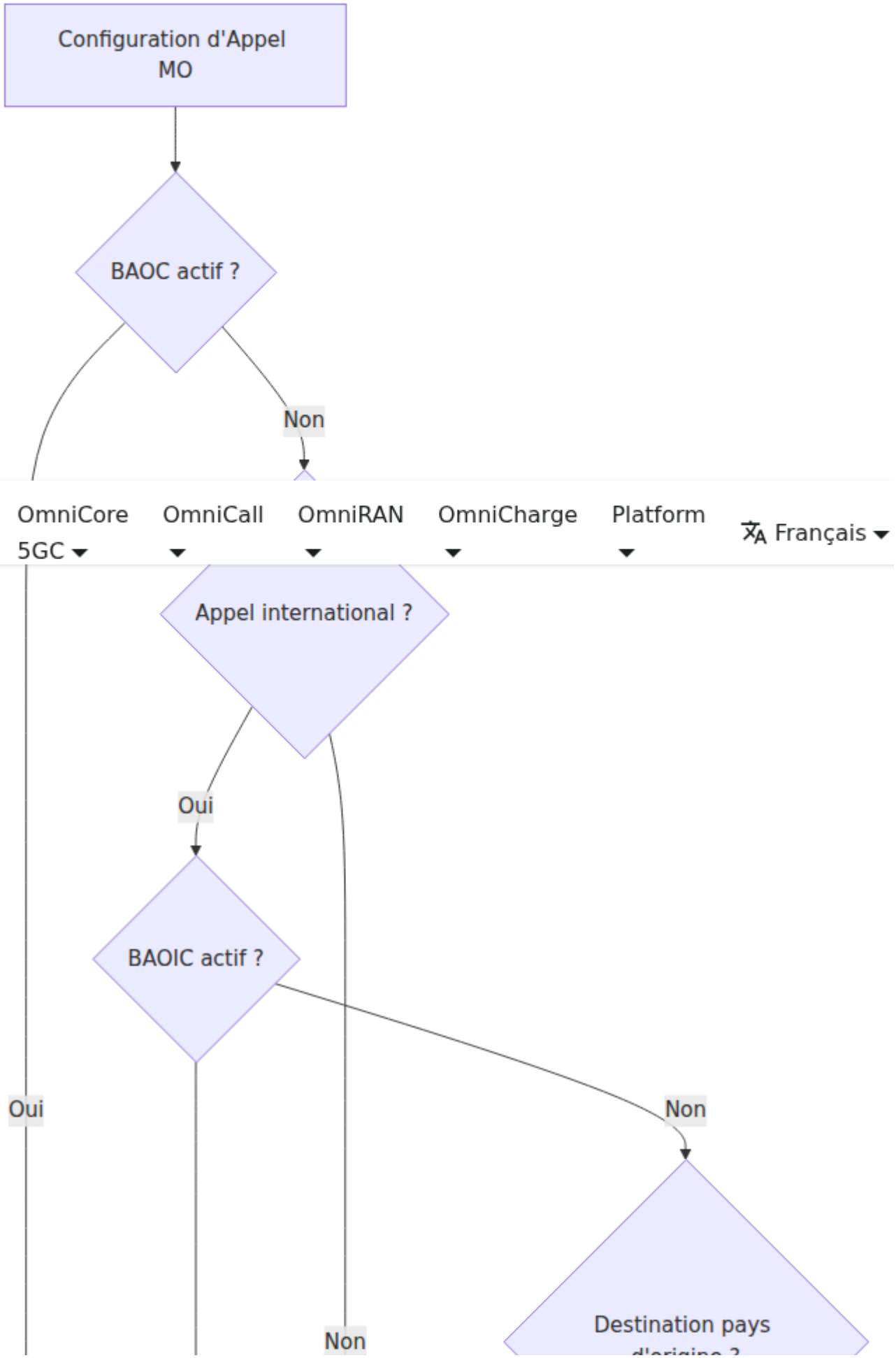
Les données de barring d'appel arrivent du HLR dans le cadre du profil de l'abonné lors de la mise à jour de localisation via l'opération MAP INSERT SUBSCRIBER DATA. Le VLR stocke les catégories de barring actives et le MSC les évalue au moment de la configuration de l'appel. Étant donné que le barring est contrôlé par l'opérateur, l'activation et la désactivation par l'abonné nécessitent une autorisation du HLR via un mot de passe de barring.

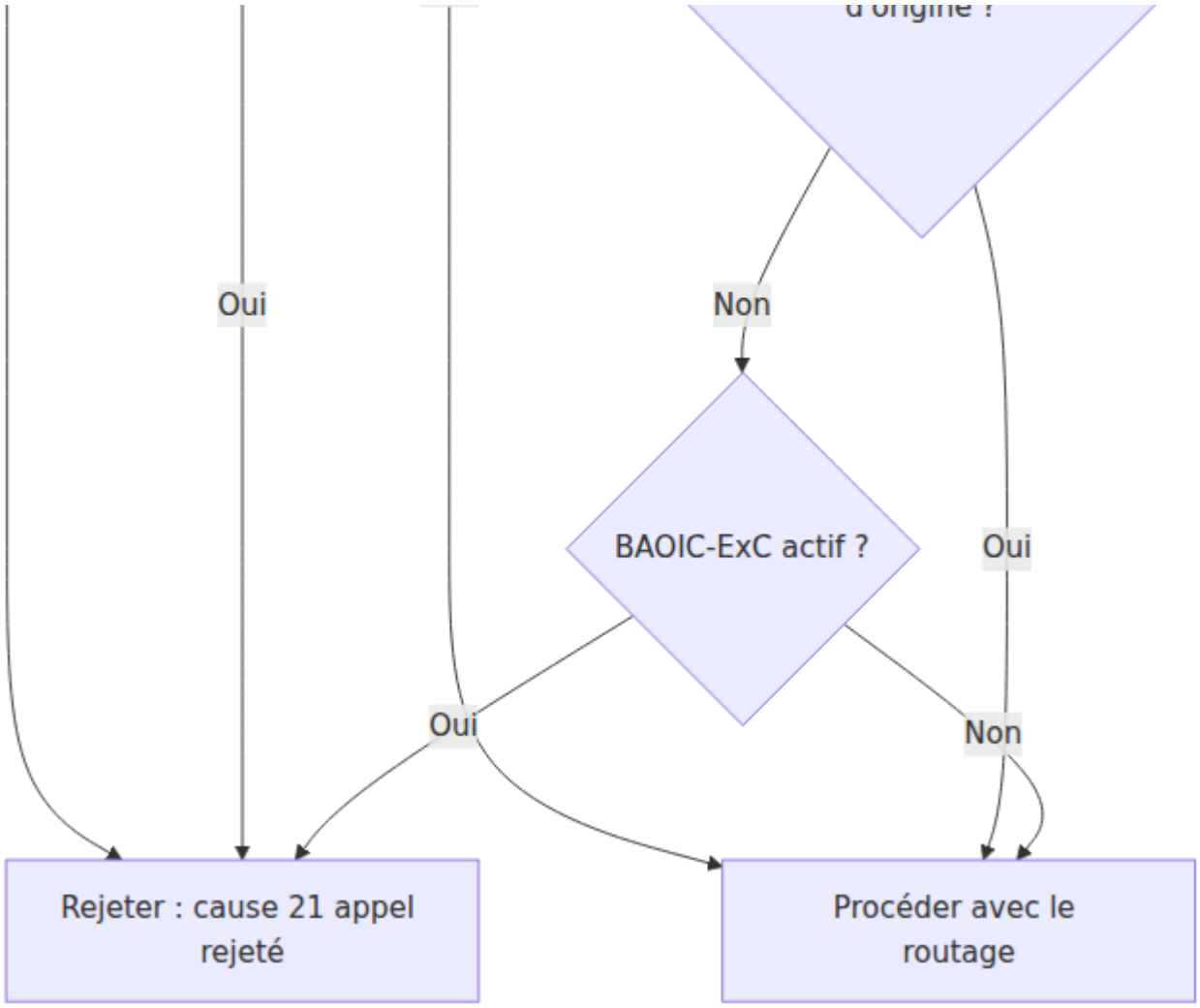
Évaluation du Barring -- Appels Sortants


Configuration d'Appel MO
BAOC actif ?
Non
Appel international ?
Oui
BAOIC actif ?
Oui
Non
Non
Destination pays



Évaluation du Barring -- Appels Entrants


Configuration d'Appel MO
BAOC actif ?
Non
OmniCore 5GC
OmniCall
OmniRAN
OmniCharge
Platform
Français
Appel international ?
Oui
BAOIC actif ?
Oui
Non
Non
Destination pays



Les services compl��mentaires de barring d'appel de l'abonné (BAOC/BOIC/BAIC) libèrent l'appel avec la cause GSM 21 (appel rejeté). Cela est distinct du barring déterminé par l'opérateur (ODB, TS 23.015), qui est évalué en premier et libère avec la cause GSM 8 (barring déterminé par l'opérateur).

Barring Déterminé par l'Opérateur et Groupe d'Utilisateurs Fermés lors de la Configuration MO

Au-delà des services de barring d'appel contrôlés par l'abonné ci-dessus, OmniMSC applique deux restrictions contrôlées par l'opérateur lors de la procédure d'appel mobile d'origine VLR (TS 23.018 Sec 7.1.2) : Barring Déterminé par l'Opérateur (ODB, TS 23.015) et Groupe d'Utilisateurs Fermés (CUG, TS 24.085). Les deux sont provisionnés par le HLR via MAP INSERT

SUBSCRIBER DATA, stockés sur l'abonné VLR, et vérifiés par le MSC lors de la CONFIGURATION MS avant que l'appel ne soit proposé au réseau. Un appel barré est libéré vers le MS avec RELEASE COMPLETE portant la cause GSM 04.08 appropriée et aucun enregistrement de facturation n'est créé pour un appel connecté.

Les trois vérifications sortantes sont appliquées dans un ordre fixe et la première qui barre libère l'appel :

1. Barring Déterminé par l'Opérateur (ODB)
2. Groupe d'Utilisateurs Fermés (CUG)
3. Services complémentaires de barring d'appel de l'abonné (BAOC/BOIC/BOIC-exHC)

Catégories de Barring Déterminé par l'Opérateur

Les catégories ODB sont stockées sur l'abonné sous `odb_categories`. Les catégories d'origine mobile suivantes sont appliquées à partir de l'analyse du numéro, toutes libérant avec la cause GSM 8 (barring déterminé par l'opérateur) :

Catégorie	Effet	Cause d Libérati
`barring_all_outgoing`	Bar tous les appels MO	8 (barring déterminé par l'opérate
`barring_outgoing_international`	Bar les appels MO vers des numéros internationaux	8 (barring déterminé par l'opérate
`barring_outgoing_international_except_home`	Bar les appels MO internationaux sauf vers le pays HPLMN	8 (barring déterminé par l'opérate
`barring_premium_rate_information`	Bar les appels MO vers un préfixe d'information à tarif premium configuré	8 (barring déterminé par l'opérate
`barring_premium_rate_entertainment`	Bar les appels MO vers un préfixe de divertissement à tarif premium configuré	8 (barring déterminé par l'opérate

Les préfixes à tarif premium sont spécifiques au réseau et n'ont pas de valeur par défaut. Configurez-les sous la clé `:odb` :

```
config :omnimsc, :odb,
  premium_rate_information_prefixes: ["1900"],
  premium_rate_entertainment_prefixes: ["1901"]
```

La catégorie `barring_outgoing_international_except_home` compare le code de pays E.164 composé avec le code de pays HPLMN fourni à la couche CC comme `home_country_code`. Sans code de pays d'origine configuré, la vérification except-home échoue (ne barre pas).

Groupe d'Utilisateurs Fermés

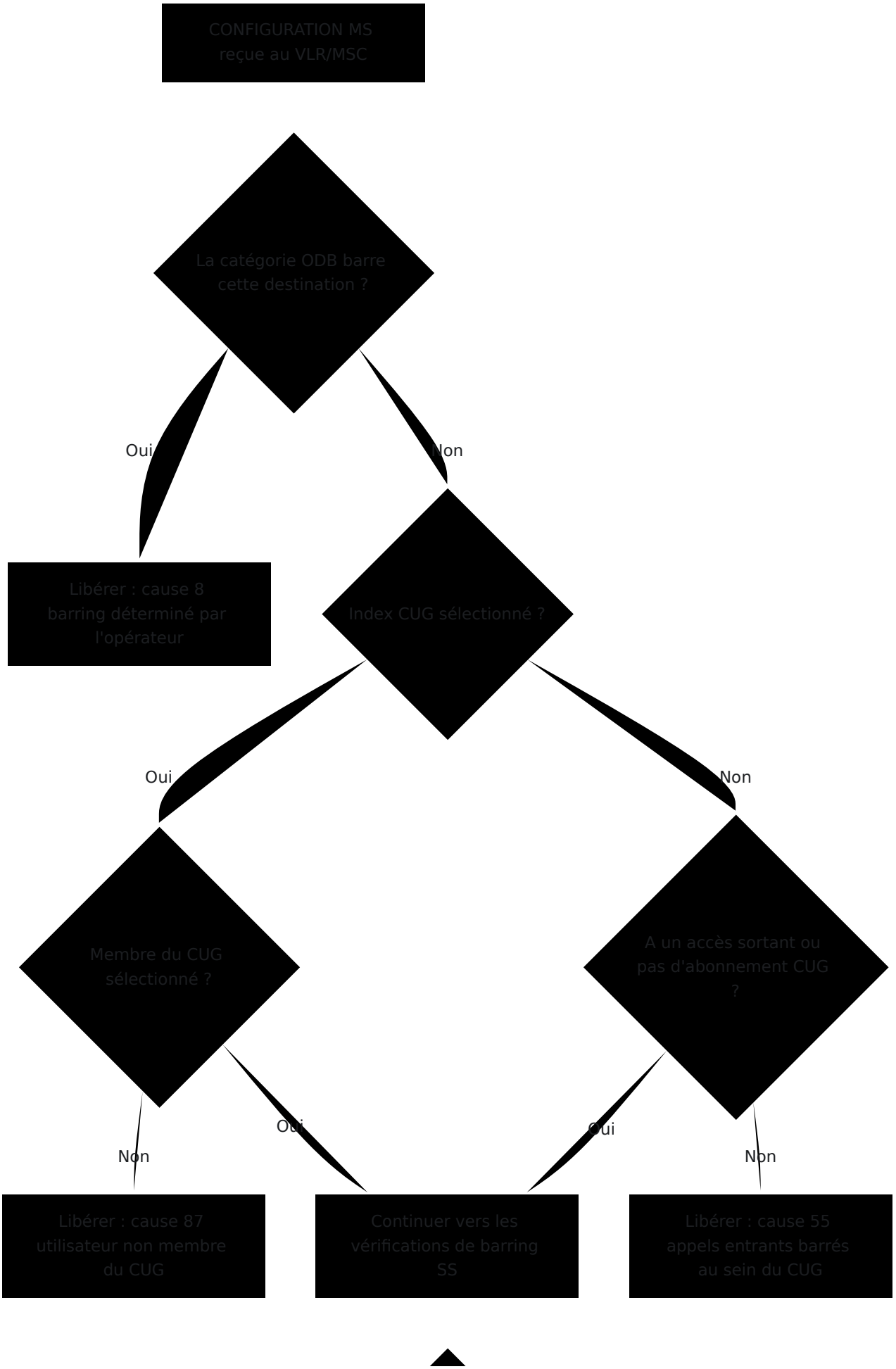
Le CUG restreint les destinations qu'un membre peut appeler. L'abonnement CUG de l'abonné est stocké sous `cug_info` :

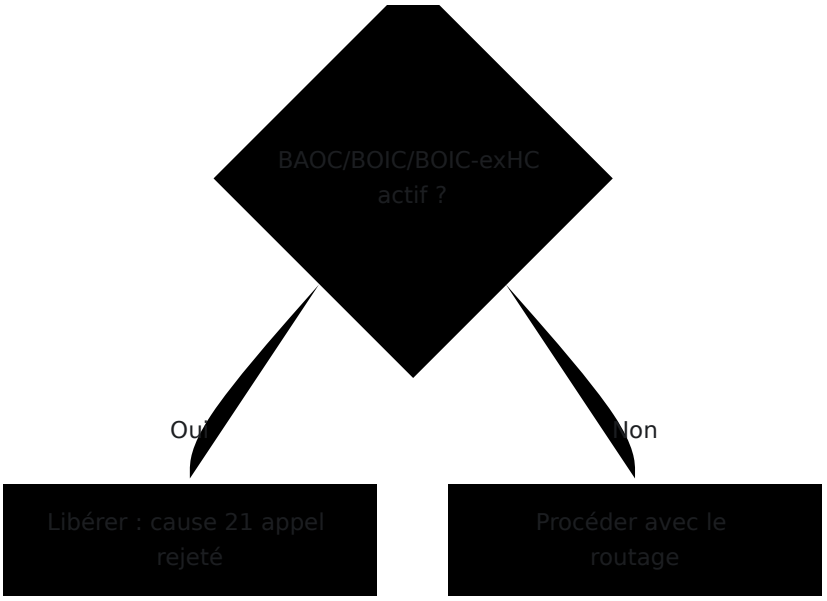
Champ	Description
`groups`	Liste des index CUG (codes d'interlock) dont l'abonné est membre
`outgoing_access`	Indique si l'abonné peut initier des appels en dehors de tout CUG (par défaut `false`)
`preferential_cug`	Index CUG utilisé lorsque le MS signale aucun index explicite (optionnel)

Lors d'une CONFIGURATION MS, le MS peut inclure un index CUG dans la fonctionnalité CUG (`cug_index`). Le VLR évalue l'appartenance et les droits d'accès :

Condition	Résultat	Cause de Libération
Pas d'abonnement CUG, appel simple (pas d'index)	Autorisé	--
Pas d'abonnement CUG, le MS sélectionne un index	Barré	87 (utilisateur non membre du CUG)
Le MS sélectionne un index dont l'abonné est membre	Autorisé	--
Le MS sélectionne un index dont l'abonné n'est pas membre	Barré	87 (utilisateur non membre du CUG)
Appel simple, l'abonné a un accès sortant	Autorisé	--
Appel simple, l'abonné n'a pas d'accès sortant	Barré	55 (appels entrants barrés au sein du CUG)

Flux de Vérification de Configuration MO


CONFIGURATION MS reçue au VLR/MSC
La catégorie ODB barre cette destination ?
Oui
Non
Libérer : cause 8 barring déterminé par l'opérateur
Index CUG sélectionné ?
Oui
Non
Membre du CUG sélectionné ?
A un accès sortant ou pas d'abonnement CUG ?
Non
Oui
Oui
Non
Libérer : cause 87 utilisateur non membre du CUG
Continuer vers les vérifications de barring SS
Libérer : cause 55 appels entrants barrés au sein du CUG

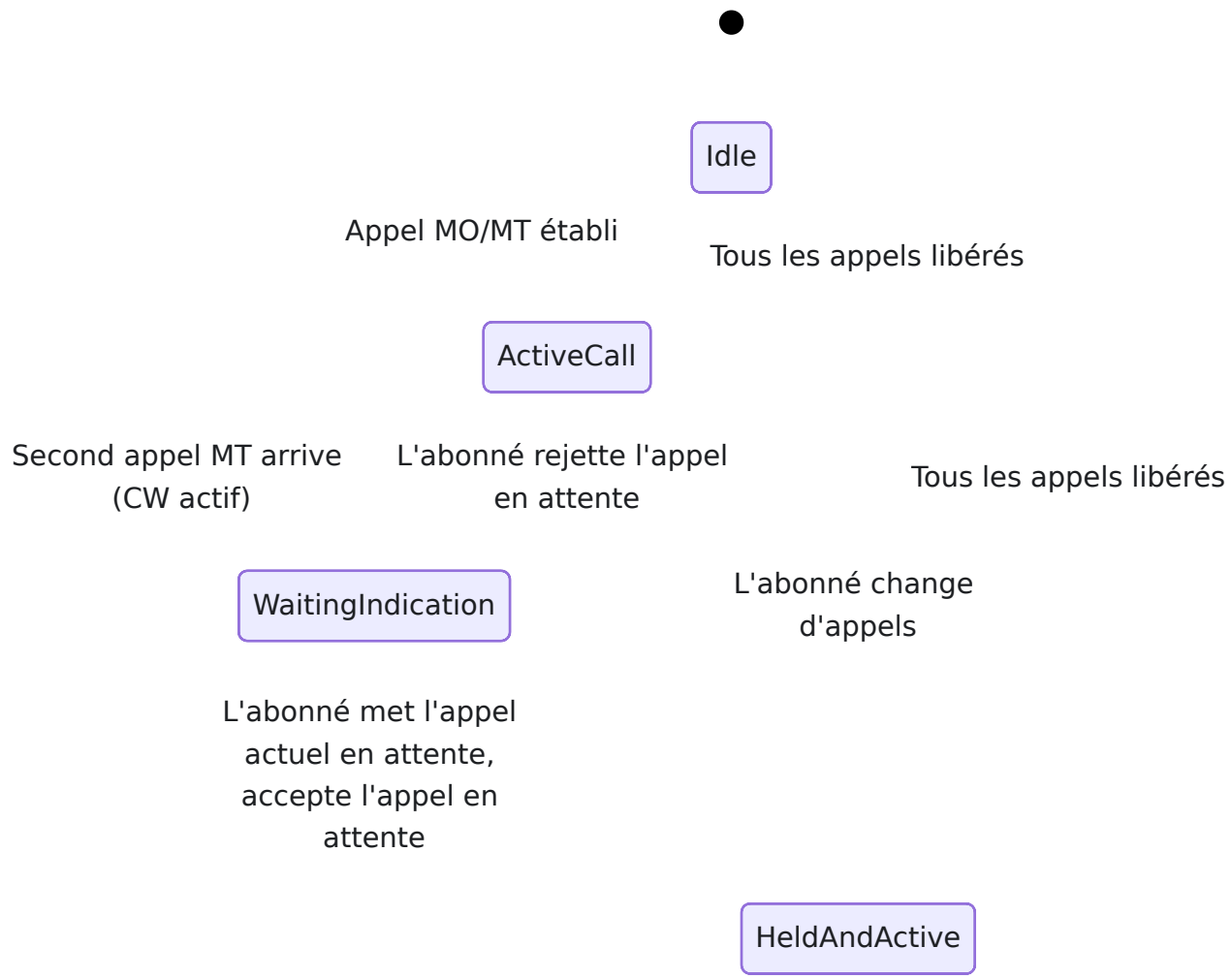


Attente d'Appel

OmniMSC met en œuvre l'Attente d'Appel (CW) selon 3GPP TS 24.083. L'Attente d'Appel a le code SS 0x41. L'abonné peut activer ou désactiver l'Attente d'Appel en utilisant les opérations SS standard Activer et Désactiver.

Lorsqu'un abonné avec CW actif est engagé dans un appel et reçoit un second appel entrant, le MSC inclut un élément d'information de Signal dans le message SETUP envoyé à la station mobile. L'IE Signal indique au MS de jouer un ton d'attente d'appel, alertant l'abonné de l'appel entrant. Sans CW actif, le MSC renvoie une indication d'occupation à la seconde partie appelante, ce qui peut déclencher CFB si configuré.

L'abonné peut alors accepter l'appel en attente en mettant l'appel actuel en attente (message HOLD) et en répondant au nouvel appel, ou rejeter l'appel en attente, ce qui se poursuit avec le traitement normal d'occupation.



Identification de Ligne

OmniMSC met en œuvre la Présentation de l'Identification de la Ligne Appelante (CLIP) et la Restriction de l'Identification de la Ligne Appelante (CLIR) selon 3GPP TS 24.081 et TS 24.083.

CLIP (Présentation de l'Identification de la Ligne Appelante) -- Code SS 0x11

CLIP fournit à la partie appelée le numéro de la partie appelante. Le MSC inclut le numéro appelant dans le message SETUP envoyé à la station mobile sur le segment MT, et dans l'IAM ou SIP INVITE sur le tronc sortant pour les appels MO. CLIP est un service provisionné par le réseau : lorsque CLIP est provisionné

pour l'abonné appelé, le réseau présente le numéro appelant sous réserve des restrictions CLIR de la partie appelante.

CLIR (Restriction de l'Identification de la Ligne Appelante) -- Code SS 0x12

CLIR permet à la partie appelante de restreindre la présentation de son numéro à la partie appelée. Le HLR provisionne le mode CLIR par défaut, et l'abonné peut invoquer des exceptions par appel lorsque cela est permis.

Mode	Comportement
Permanent	Le numéro est toujours restreint ; l'exception par appel n'est pas disponible
Temporaire (restreint par défaut)	Numéro restreint sauf si l'abonné invoque la présentation par appel
Temporaire (autorisé par défaut)	Numéro présenté sauf si l'abonné invoque la restriction par appel

Le MSC évalue le paramètre CLIR de l'abonné appelant lors de la population du Numéro de la Partie Appelante dans la signalisation sortante. Un contournement par l'opérateur du réseau peut forcer la présentation indépendamment du paramètre CLIR, pour des scénarios tels que l'interception légale et le rappel d'urgence.

Mise en Attente d'Appel

OmniMSC gère la Mise en Attente d'Appel selon 3GPP TS 24.083. La station mobile met un appel actif en attente en envoyant un message HOLD et le récupère en envoyant un message RETRIEVE. Les deux sont des messages CC gérés directement par la FSM CC au sein du MSC.

Lorsque le MSC reçoit un message HOLD, la FSM CC transitionne la branche d'appel vers l'état en attente, indique à la passerelle multimédia de régler la branche en attente en mode réception uniquement, et renvoie un accusé de réception HOLD au MS. Lors de RETRIEVE, la FSM CC inverse le processus : la branche de la passerelle multimédia revient en mode envoi-réception, et le MSC répond avec un accusé de réception RETRIEVE.

La Mise en Attente d'Appel est une condition préalable à plusieurs autres services complémentaires, y compris l'Attente d'Appel (acceptation d'un second appel), la conférence Multi-Parties (pontage des appels en attente et actifs), et le Transfert d'Appel Explicite (connexion des parties en attente et actives).

Conférence Multi-Parties (MPTY)

OmniMSC met en œuvre les appels Multi-Parties selon 3GPP TS 24.084. MPTY permet à un abonné de relier plusieurs appels dans une conférence. Le pont de conférence est hébergé sur la passerelle multimédia, le MSC contrôlant la participation par le biais d'échanges d'invocation et de résultat de retour CC FACILITY.

Opérations MPTY

Opération	Code SS	Description
BuildMPTY	0x51	Créer ou étendre la conférence en fusionnant les appels en attente et actifs
HoldMPTY	0x52	Mettre toute la conférence en attente
RetrieveMPTY	0x53	Récupérer une conférence en attente
SplitMPTY	0x54	Extraire une partie de la conférence dans un appel privé

Flux BuildMPTY

L'abonné établit d'abord deux appels (un actif, un en attente) en utilisant la configuration d'appel normale et la procédure HOLD, puis envoie une invocation BuildMPTY dans un message CC FACILITY. OmniMSC crée un contexte de conférence sur la passerelle multimédia, redirige toutes les branches d'appel vers le pont de conférence, et renvoie un résultat de retour BuildMPTY au MS. Des appels supplémentaires peuvent être ajoutés à la conférence en répétant le modèle de mise en attente et de numérotation suivi d'une autre invocation BuildMPTY.

HoldMPTY et RetrieveMPTY

HoldMPTY place toutes les branches de conférence en mode réception uniquement sur la passerelle multimédia, permettant à l'abonné de passer un appel privé en dehors de la conférence. RetrieveMPTY inverse cela, restaurant toutes les branches en mode envoi-réception et reconnectant l'abonné à la conférence.

SplitMPTY

SplitMPTY extrait une seule partie de la conférence dans un appel privé à deux parties avec l'abonné. Les participants restants à la conférence sont mis en attente. Le MS identifie la partie à séparer par référence d'appel dans l'invocation SplitMPTY.

Pont de Conférence sur MGW

La passerelle multimédia maintient le contexte de conférence avec une terminaison par participant. OmniMSC utilise CRCX pour créer des terminaisons et MDCX pour les ajouter ou les retirer du contexte de conférence. La passerelle effectue le mixage audio pour tous les participants dans le contexte.

Relais HLR

Plusieurs opérations SS nécessitent une interaction avec le HLR, puisque le profil de l'abonné est la source autorisée pour l'état du service complémentaire. Lorsque le MSC reçoit une opération SS qui modifie l'état persistant (Register, Erase, Activate, Deactivate pour le renvoi, vérification du mot de passe de barring), la demande est relayée au HLR via l'opération MAP appropriée. Le HLR traite la demande, met à jour le profil de l'abonné et renvoie le résultat, que le MSC transmet à la station mobile.

Les opérations relayées via MAP incluent :

- RegisterSS / EraseSS pour les numéros de renvoi d'appel
- ActivateSS / DeactivateSS pour les changements d'état de service qui doivent persister au-delà de l'enregistrement VLR actuel
- RegisterPassword pour la gestion du mot de passe de barring d'appel
- InterrogateSS lorsque le VLR ne détient pas les données demandées

---

Interrogation Locale

Lorsque le VLR détient déjà les données de service complémentaire actuelles (reçues lors de la mise à jour de localisation via INSERT SUBSCRIBER DATA), les demandes d'interrogation peuvent être répondues localement sans contacter le HLR. Cela réduit la charge de signalisation et le temps de réponse. Le MSC interroge l'enregistrement de l'abonné VLR pour le code SS demandé et renvoie l'état actuel directement à la station mobile.

L'interrogation locale est utilisée pour les requêtes d'état lorsque les données VLR sont connues pour être fraîches, comme immédiatement après une mise à jour de localisation ou après une opération Register/Activate/Deactivate réussie qui a mis à jour la copie locale du VLR.

Références de Spécification 3GPP

Spécification	Titre	Pertinence
TS 24.010	Couche 3 de l'Interface Radio Mobile -- Services Complémentaires	Structure des messages SS, IE de service, types de composants
TS 24.080	Spécification SS de la Couche 3 de l'Interface Radio Mobile -- Formats et Codage	Codage ASN.1 des opérations et composants SS
TS 24.081	Services Complémentaires d'Identification de Ligne	CLIP, CLIR
TS 24.082	Services Complémentaires de Renvoi d'Appel	CFU, CFB, CFNRy, CFNRc
TS 24.083	Services Complémentaires d'Attente d'Appel et de Mise en Attente	CW, HOLD, RETRIEVE
TS 24.084	Services Complémentaires Multi-Parties	BuildMPTY, HoldMPTY, RetrieveMPTY, SplitMPTY
TS 24.085	Services Complémentaires de Groupe d'Utilisateurs Fermés	Appartenance et droits d'accès CUG lors de la configuration MO
TS 24.088	Services Complémentaires de Barring d'Appel	BAOC, BAOIC, BAOIC-ExC, BAIC, BAIC-Roam
TS 23.015	Réalisation Technique du Barring Déterminé par l'Opérateur	Catégories ODB appliquées lors de la configuration d'appel

Spécification	Titre	Pertinence
TS 23.018	Gestion de Base des Appels	Procédure d'appel MO VLR (Sec 7.1.2), point d'application ODB/CUG
TS 29.002	Spécification MAP	Assignations de code SS, opérations MAP pour le provisionnement SS

Guide de dépannage

Ce document couvre les problèmes opérationnels courants rencontrés avec les déploiements d'OmniMSC et leurs étapes de résolution. Pour référence de configuration, voir Référence de configuration. Pour les métriques système et l'alerte, voir Référence des métriques. Pour le statut en temps réel et l'inspection des abonnés, voir Guide du panneau de contrôle.

Connectivité SS7

Lien STP hors service

Symptômes : Aucun nouvel appel n'est établi, les mises à jour de localisation ne se terminent pas, l'alarme `sctp_link_down` est déclenchée et `omnimsc_peer_status` affiche 0 pour le pair STP affecté.

Investigation : Vérifiez que l'association SCTP avec le STP est établie. Vérifiez que l'adresse IP distante et le port correspondent à la configuration du STP. Confirmez que le protocole SCTP 132 est autorisé à travers tous les pare-feu entre le MSC et le STP. Vérifiez que le contexte de routage STP correspond à la valeur configurée dans OmniMSC. Vérifiez que la machine d'état ASP M3UA a progressé à travers ASPUP et ASPAC jusqu'à l'état ACTIF. Si l'association est établie mais que M3UA n'atteint pas l'état ACTIF, vérifiez les journaux M3UA pour des morceaux ERR indiquant un contexte de routage ou un mode de trafic incompatible.

Résolution : Corrigez la configuration du point de terminaison SCTP (IP, port), les règles de pare-feu ou le contexte de routage M3UA comme indiqué par l'investigation. Une fois que l'association SCTP se rétablit et que M3UA atteint l'état ACTIF, l'alarme se désactive automatiquement et la signalisation reprend.

Délai d'attente du dialogue MAP

Symptômes : Les mises à jour de localisation se bloquent sans se terminer, la livraison de SMS échoue, l'alarme `hlr_unreachable` peut être déclenchée. Les opérations MAP expirent sans recevoir un TC-CONTINUE ou TC-END du HLR.

Investigation : Confirmez que le HLR est accessible au niveau du réseau. Vérifiez que les codes de point sont correctement configurés aux deux extrémités. Vérifiez que la traduction du titre global est correctement configurée si le routage SCCP basé sur GT est utilisé. Vérifiez que M3UA a une route active vers le code de point HLR. Inspectez les journaux pour des messages TC-BEGIN envoyés sans réponses TC-CONTINUE correspondantes.

Résolution : Corrigez la configuration du code de point ou du titre global si nécessaire. Si le HLR est accessible mais ne répond pas, le problème se situe du côté du HLR. Vérifiez que le HLR a une route de retour vers le code de point MSC.

DPC incorrect pour les réponses MAP

Symptômes : Le SMSc ne reçoit jamais l'accusé de réception MT-SMS. Les réponses MAP ForwardSM sont envoyées mais n'arrivent pas au SMSc d'origine. La livraison MT-SMS semble se terminer du point de vue du MSC mais le SMSc retransmet la demande.

Investigation : Vérifiez le code de point de destination (DPC) dans le message M3UA DATA portant la réponse MAP. Le DPC de réponse doit correspondre au code de point d'origine (OPC) de la demande MAP entrante, qui est le code de point du SMSc. Si la réponse est envoyée au code de point STP ou HLR au lieu du SMSc, le OPC de routing_info n'est pas utilisé pour le DPC de réponse.

Résolution : Assurez-vous que la réponse MAP utilise l'OPC de routing_info de la demande entrante comme DPC pour le message de retour. Cela garantit que la réponse atteint le bon code de point SMSc plutôt qu'une route par défaut.

Problèmes d'appel

Audio unidirectionnel

Symptômes : L'appel est établi (les deux parties entendent la sonnerie et répondent) mais l'audio ne circule que dans une seule direction, ou pas du tout.

Investigation : Vérifiez que les messages MGCP CRCX (Créer une connexion) et MDCX (Modifier la connexion) sont envoyés au passerelle multimédia et que la passerelle répond avec 200 OK. Vérifiez que le MGW est accessible et en bonne santé. Inspectez l'adresse de connexion SDP (ligne c=) dans le SIP 200 OK pour confirmer qu'elle contient une adresse IP routable, pas une adresse privée ou de boucle. Vérifiez que la clé de configuration SIP `signaling_address` est définie sur l'adresse que les pairs SIP distants doivent utiliser pour la signalisation et le contact SDP - le listener SIP annonce cette valeur comme adresse de signalisation dans les messages sortants. Confirmez que la plage de ports RTP est ouverte dans les deux sens à travers tous les pare-feu.

Résolution : Corrigez la connectivité MGW, la configuration de l'adresse SDP ou les règles de pare-feu comme identifié. Pour les déploiements où le MSC doit annoncer une adresse spécifique accessible, définissez la clé `signaling_address` dans la configuration SIP sur cette adresse.

SIP BYE non envoyé lors de la libération d'appel

Symptômes : Lorsque la connexion A-interface est libérée (par exemple, échec de lien radio, libération BSC), le pair SIP n'est pas informé. Le point de terminaison SIP distant maintient la session ouverte jusqu'à ce que son propre minuteur expire.

Investigation : Vérifiez que l'événement connection_lost est envoyé aux FSM CC lorsque le MSC-A libère la connexion. Chaque transaction d'appel active doit recevoir l'indication de libération afin que la FSM CC puisse déclencher SIP BYE sur la branche sortante.

Résolution : Assurez-vous que le gestionnaire de libération MSC-A itère toutes les transactions actives et délivre l'événement connection_lost. La FSM CC doit passer à l'état de libération et envoyer SIP BYE à la réception de cet événement.

Assignment Complete pour la mauvaise FSM CC

Symptômes : Un nouvel appel dans une connexion existante (par exemple, un second appel MO pendant que le premier est en attente) reçoit l'Assignment Complete pour la mauvaise transaction, provoquant une corruption de l'état de l'appel.

Investigation : Vérifiez que la référence active_trans est mise à jour lorsqu'un nouvel appel commence alors que la connexion est déjà dans l'état de communication. L'Assignment Complete est délivré à la transaction marquée comme active_trans au moment de la réception.

Résolution : Assurez-vous que le processus MSC-A met à jour active_trans avec la nouvelle transaction lors du traitement de la seconde demande de service CM ou de la configuration d'appel dans l'état de communication.

DTMF non fonctionnel

Symptômes : Les tonalités DTMF en cours d'appel ne sont pas reconnues par la partie distante ou le système IVR. L'abonné appuie sur des chiffres mais aucune action ne se produit.

Investigation : Vérifiez que des messages SIP INFO sont envoyés avec le type de contenu application/dtmf-relay lorsque des événements DTMF sont reçus du côté radio. Confirmez que le pair SIP prend en charge la méthode INFO pour le relais DTMF. Vérifiez la configuration du pair SIP pour les préférences de gestion DTMF.

Résolution : Assurez-vous que le relais DTMF basé sur SIP INFO est activé et que le pair est configuré pour l'accepter. Si le pair nécessite des paquets RTP telephone-event RFC 2833 au lieu de SIP INFO, ajustez la méthode de relais DTMF en conséquence.

Problèmes de SMS

Délai d'attente de livraison MT-SMS (TC1)

Symptômes : La livraison MT-SMS initiée par le SMSc expire. L'opération MAP ForwardSM ne se termine pas dans le délai du minuteur TC1. Le SMSc retransmettent la tentative de livraison.

Investigation : Vérifiez que l'opération register_mt_sms utilise un appel synchrone pour garantir que le DTAP CP-DATA est envoyé avant la réponse MAP. Vérifiez que l'identifiant de transaction DTAP (TI) est correctement alloué pour la direction MT. Confirmez que les PDU SMS sont envoyés sur SAPI 3 (le canal de signalisation dédié pour les SMS) plutôt que sur SAPI 0.

Résolution : Assurez-vous que l'enregistrement MT-SMS est synchrone, que l'allocation TI est correcte avec le drapeau TI défini pour les transactions d'origine réseau, et que SAPI 3 est utilisé pour les messages DTAP SMS.

Boucle de re-livraison MT-SMS

Symptômes : Le processus de gestion MT-SMS plante et redémarre de manière répétée, provoquant la re-livraison du même SMS en boucle. L'abonné peut recevoir des messages en double.

Investigation : Vérifiez le child_spec du processus de gestion MT-SMS dans l'arbre de supervision. Si la stratégie de redémarrage est définie sur permanent, le superviseur redémarrera le gestionnaire sans condition après chaque terminaison, y compris la complétion normale. Cela provoque une re-livraison car le gestionnaire redémarré réinitialise la livraison.

Résolution : Définissez le child_spec du gestionnaire MT-SMS sur restart: :temporary afin que la terminaison normale ne déclenche pas un redémarrage. Seules les pannes anormales devraient provoquer un redémarrage, et le SMSc gérera la re-livraison via son propre mécanisme de réessai.

Réponse MAP n'atteignant pas le SMSc

Symptômes : La livraison MT-SMS se termine du côté radio (l'abonné reçoit le message) mais le SMSc ne reçoit pas la réponse MAP ForwardSM. Le SMSc considère la livraison comme échouée et peut re-livrer.

Investigation : Vérifiez le DPC dans le message M3UA DATA portant la réponse MAP ForwardSM. Le DPC doit correspondre au code de point SMSc, qui est l'OPC de la demande MAP entrante (routing_info[:opc]). Si la réponse est routée vers le mauvais code de point, le SMSc ne la voit jamais.

Résolution : Assurez-vous que le DPC de réponse MAP est dérivé de routing_info[:opc] de la demande entrante, et non d'un code de point par défaut ou associé au HLR.

Authentification

Échec d'authentification -- Mismatch MAC

Symptômes : L'authentification de l'abonné échoue avec la raison mac_failure. L'UE envoie un échec d'authentification avec la cause "échec MAC" indiquant que la vérification d'authentification réseau a échoué sur le USIM.

Investigation : Cela indique un décalage entre la clé d'abonné (Ki/K) stockée dans le USIM et la clé stockée dans le HLR/AuC. Le vecteur d'authentification généré par l'AuC ne correspond pas à ce que le USIM calcule. Cela peut se produire après un remplacement de SIM, une migration HLR ou des erreurs de provisionnement.

Résolution : Vérifiez que la clé d'abonné dans le HLR/AuC correspond à la clé programmée dans le USIM. Re-provisionnez le profil d'abonné dans le HLR si nécessaire. Ce n'est pas un problème côté MSC -- le MSC relaie fidèlement les vecteurs du HLR.

Boucle de resynchronisation d'authentification

Symptômes : L'abonné entre dans un cycle de resynchronisation d'authentification qui se répète sans résolution. L'UE envoie un échec d'authentification avec la cause "échec SQN" et un paramètre AUTS. Le MSC relaie la resynchronisation au HLR, mais les tentatives d'authentification suivantes échouent également avec un échec SQN.

Investigation : OmniMSC permet un maximum de 2 tentatives de resynchronisation par cycle d'authentification. Vérifiez si le compte de resynchronisation a été dépassé. Vérifiez que le HLR traite correctement le paramètre AUTS et avance le SQN. Si le SQN HLR est significativement hors de portée du SQN USIM, une seule resynchronisation peut ne pas être suffisante.

Résolution : Si la boucle de resynchronisation persiste après 2 tentatives, l'abonné doit être re-provisionné dans le HLR. Le SQN HLR doit être réinitialisé pour s'aligner avec le SQN USIM. Contactez les opérations HLR pour résoudre la divergence de SQN.

Problèmes d'abonnés

TMSI inconnu sur la réponse de pagination

Symptômes : Un abonné répond à la pagination en utilisant un TMSI qui n'est pas reconnu par le MSC. Cela peut se produire après un redémarrage du MSC ou une corruption de la table TMSI.

Investigation : Lorsque le MSC reçoit une réponse de pagination avec un TMSI inconnu, il ne rejette pas l'abonné. Au lieu de cela, le MSC envoie une demande d'identité pour obtenir l'IMSI directement de la station mobile. C'est un comportement de récupération normal selon 3GPP TS 24.008.

Résolution : Aucune action requise. Le MSC résout automatiquement le TMSI inconnu en demandant l'IMSI de l'abonné. Si cela se produit fréquemment, vérifiez si la réallocation TMSI fonctionne correctement lors des mises à jour de localisation.

Demande de service CM pour IMSI inconnu

Symptômes : Un abonné envoie une demande de service CM mais n'est pas enregistré dans le VLR. Le MSC n'a pas de données d'abonné pour cet IMSI.

Investigation : OmniMSC déclenche une mise à jour de localisation implicite lorsqu'il reçoit une demande de service CM d'un abonné non enregistré. Le MSC initie la procédure complète de mise à jour de localisation (authentification, chiffrement, MAP UPDATE LOCATION vers le HLR) avant de procéder au service demandé.

Résolution : Aucune action requise. La mise à jour de localisation implicite est automatique. Si la mise à jour de localisation échoue elle-même (HLR inaccessible, échec d'authentification), la demande de service CM est rejetée et l'abonné doit réessayer.

Abonné bloqué dans le VLR

Symptômes : Un enregistrement d'abonné reste dans le VLR malgré que l'abonné soit inaccessible ou ait déménagé vers un autre MSC. Les tentatives de pagination pour cet abonné échouent systématiquement.

Investigation : Vérifiez si l'abonné a terminé une mise à jour de localisation dans un autre MSC (le HLR aurait envoyé un MAP CANCEL LOCATION, ce qui supprime l'enregistrement VLR). Si l'annulation a été manquée ou si l'enregistrement VLR est autrement obsolète, une suppression manuelle peut être nécessaire.

Résolution : Utilisez l'endpoint DELETE /api/subscribers/{id} pour purger l'enregistrement d'abonné du VLR. L'abonné se réenregistrera via une mise à jour de localisation lorsqu'il accédera à nouveau au réseau.

Performance

Rejet de surcharge

Symptômes : De nouveaux appels et mises à jour de localisation sont rejetés avec la cause GSM 42 (congestion de l'équipement de commutation). L'alarme `overload` est active.

Investigation : Vérifiez les seuils de surcharge actuels et les métriques système qui les dépassent. Les quatre métriques surveillées sont : appels actifs (maximum par défaut 10 000), abonnés enregistrés (maximum par défaut 50 000), nombre de processus BEAM (maximum par défaut 500 000), et taux de pagination (maximum par défaut 1 000/sec). Déterminez quelle métrique déclenche la condition de surcharge.

Résolution : Si les seuils sont appropriés pour le matériel, enquêtez sur la source de la surcharge : volume d'appels anormal, tempêtes de pagination ou fuites de processus. Si les seuils sont trop conservateurs pour le déploiement, augmentez-les dans la configuration de surcharge. Voir Référence de configuration.

Utilisation élevée de la mémoire

Symptômes : La consommation de mémoire BEAM augmente avec le temps ou connaît des pics inattendus. Le système peut devenir non réactif si la mémoire est épuisée.

Investigation : Vérifiez les tailles des tables ETS pour les principales stores en mémoire : table des abonnés VLR, contextes de conférence MPTY, et table des transactions TCAP. Un grand nombre d'entrées obsolètes dans l'une de ces tables peut provoquer une augmentation de la mémoire. Vérifiez également les fuites de processus - un nombre croissant de processus BEAM sans croissance correspondante des abonnés ou des appels indique des processus qui ne se terminent pas correctement.

Résolution : Identifiez et résolvez la source de la croissance. Les entrées VLR obsolètes peuvent être purgées via l'API des abonnés. Les délais d'expiration des transactions TCAP devraient nettoyer automatiquement les dialogues

abandonnés. Si des fuites de processus sont identifiées, enquêtez sur l'arbre de supervision pour des processus avec des stratégies de redémarrage incorrectes ou un traitement de délai d'expiration manquant.

Problèmes SIP

Pour la configuration des pairs SIP et les détails de maintien de vie OPTIONS, voir Trunking SIP.

Pair SIP affichant un statut INCONNU

Symptômes : Un pair SIP apparaît avec un statut INCONNU dans le panneau de contrôle ou les métriques, plutôt que UP ou DOWN.

Investigation : OmniMSC détermine le statut du pair SIP via des messages OPTIONS de maintien de vie périodiques. Si le maintien de vie OPTIONS n'est pas configuré pour le pair, ou si le pair n'a jamais répondu à une demande OPTIONS, le statut reste INCONNU. Vérifiez si la configuration du pair inclut des paramètres de maintien de vie. Vérifiez que le pair est accessible et répond aux SIP OPTIONS avec 200 OK.

Résolution : Activez le maintien de vie OPTIONS pour le pair dans la configuration SIP. Si le maintien de vie est activé mais que le pair ne répond pas, enquêtez sur la connectivité réseau et confirmez que le pair prend en charge la méthode OPTIONS.

retransmissions re-INVITE du pair

Symptômes : Un pair SIP envoie des demandes re-INVITE pendant un appel établi (pour renégociation de codec, rafraîchissement de session ou mise en attente/reprise) et les retransmet car le MSC ne répond pas. Le pair peut finalement terminer l'appel en raison de la re-INVITE sans réponse.

Investigation : Vérifiez que la pile SIP du MSC gère les messages re-INVITE en dialogue lorsque l'appel est dans l'état actif. Si la re-INVITE arrive pendant une

transition d'état ou n'est pas associée au bon dialogue, elle peut être silencieusement abandonnée.

Résolution : Assurez-vous que la couche de transaction SIP associe correctement la re-INVITE en dialogue à la branche d'appel existante et que la FSM CC traite la re-INVITE dans l'état actif. Le MSC doit répondre avec 200 OK contenant une réponse SDP mise à jour.

Expiration du minuteur de session

Symptômes : Les appels établis sont déconnectés de manière inattendue après un intervalle fixe (généralement 1800 secondes). Le pair SIP envoie BYE avec la raison "Expiration du minuteur de session."

Investigation : Les minuteurs de session SIP (RFC 4028) nécessitent une re-INVITE ou UPDATE périodique pour maintenir la session active. Vérifiez la négociation de l'en-tête Session-Expires lors de la configuration de l'appel. Vérifiez que le MSC respecte la valeur Min-SE (Minimum Session Expires) proposée par le pair. Si le MSC est le rafraîchisseur, confirmez qu'il envoie re-INVITE ou UPDATE avant l'expiration du minuteur de session.

Résolution : Assurez-vous que le MSC participe à la négociation du minuteur de session et effectue un rafraîchissement de session comme requis par le rôle négocié (rafraîchisseur ou rafraîchi). Si les minuteurs de session ne sont pas nécessaires dans le déploiement, le pair peut devoir être configuré pour ne pas les exiger.

Références de spécification 3GPP

Spécification	Titre	Pertinence
TS 24.008	Couche 3 de l'interface radio mobile	Authentification, identité, procédures DTAP
TS 29.002	Spécification MAP	Opérations HLR, routage par code de point
TS 48.008	Interface MSC-BSS (BSSMAP)	Assignment, mode de chiffrement, pagination
TS 23.018	Procédures de transfert	Transfert inter-MSC
TS 22.101	Principes de service	Appel d'urgence, surcharge

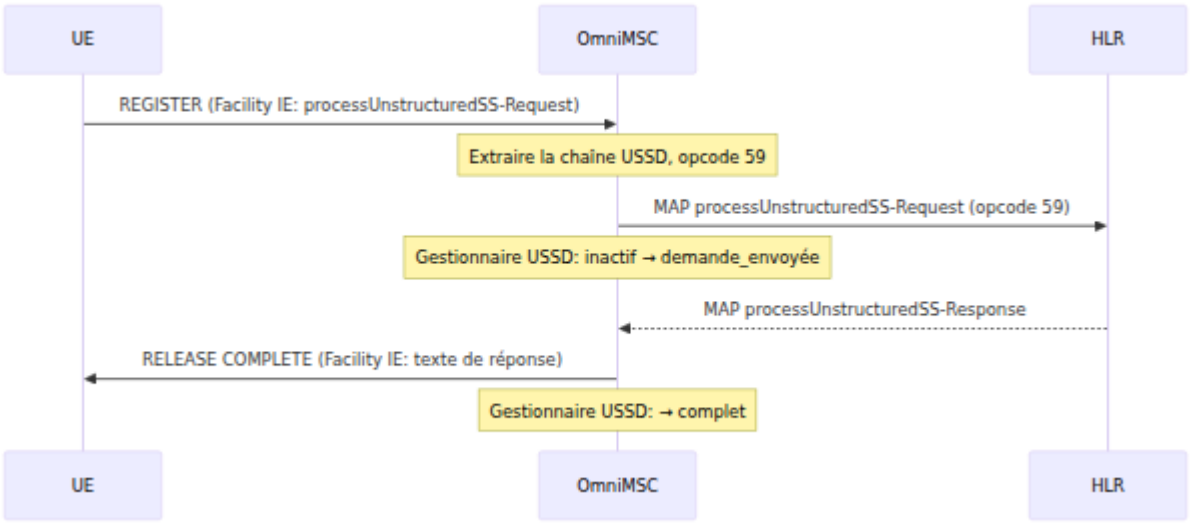
USSD

Ce document décrit l'implémentation des Données de Service Supplémentaires Non Structurées (USSD) dans OmniMSC, couvrant le relais HLR, le traitement local, le menu de diagnostic easter egg, le codec USSD et le flux de messages SS.

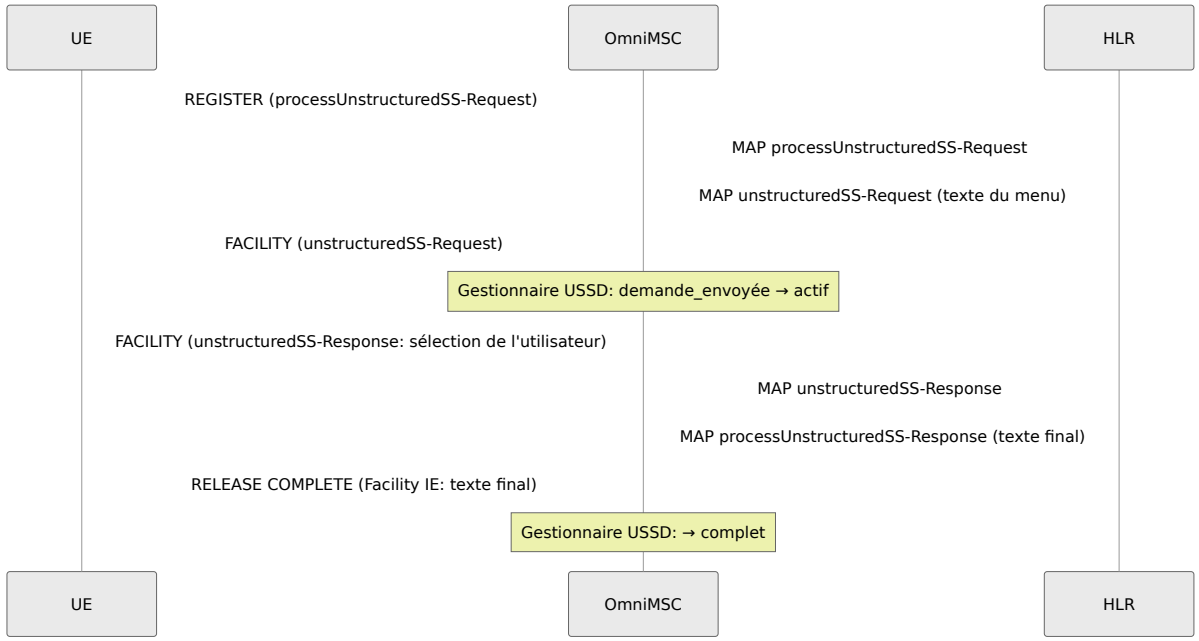
Pour les codes de service supplémentaires gérés via USSD (codes MMI de renvoi d'appel, barrages d'appel, attente d'appel), voir Services Supplémentaires. Pour l'opération MAP ProcessUnstructuredSS-Request et la gestion du dialogue, voir Opérations MAP. Pour les métriques Prometheus liées à l'USSD, voir Métriques et Surveillance. Pour la configuration de la passerelle USSD, voir Référence de Configuration. Pour le dépannage des problèmes USSD, voir Dépannage.

Relais USSD vers HLR

Lorsqu'un abonné envoie une chaîne USSD qui n'est pas traitée localement par le MSC, la demande est relayée au HLR via MAP. Le MS envoie un message REGISTER contenant un Facility IE avec un processUnstructuredSS-Request (opcode 59). Le MSC extrait la chaîne USSD et transmet la demande au HLR en utilisant la même opération MAP.



Pour les sessions interactives à plusieurs étapes, le HLR répond avec un unstructuredSS-Request (opcode 60) au lieu d'une réponse finale. Le MSC relaie cela à l'UE sous forme de message FACILITY, et la réponse de l'UE est renvoyée au HLR. Ce dialogue se poursuit jusqu'à ce que le HLR envoie un processUnstructuredSS-Response final.



Traitement Local USSD

Le MSC peut traiter certains codes USSD localement sans les transmettre au HLR ou à une passerelle externe. Le traitement local est utilisé pour :

- Codes d'activation/désactivation de services supplémentaires (CFU, CFB, CFNR, CFNRC, CLIP, CLIR, Barrage d'Appel, Attente d'Appel) utilisant le format MMI standard défini dans 3GPP TS 22.030
- Codes de diagnostic définis par l'opérateur gérés en interne par le MSC

Lorsqu'une chaîne USSD correspond à un code de service traité localement, le Gestionnaire USSD l'achemine vers le Gestionnaire SS ou le module interne approprié. La réponse est envoyée directement à l'UE sans signalisation MAP.

Pour les codes non traités localement, le module Passerelle USSD achemine la demande vers une passerelle USSD externe. Le routage est purement basé sur

le préfixe : chaque passerelle configurée déclare une liste de préfixes `codes`, et la première passerelle dont la liste de préfixes correspond au code de service traite la demande. Une passerelle configurée avec `codes: :all` agit comme une passerelle par défaut/catch-all, recevant tout code non correspondant à une passerelle plus spécifique. Si aucune passerelle ne correspond et qu'aucun `:all` par défaut n'est configuré, la demande est rejetée.

Easter Egg : Menu de Diagnostic Système

OmniMSC inclut un menu de diagnostic caché accessible en composant `*#6664#` (qui s'écrit `*#OMNI#` sur un clavier de téléphone). Le MSC reconnaît plusieurs variantes de ce code sur le clavier et répond avec un menu USSD interactif.

Le menu principal propose les options suivantes :

Touche	Élément de Menu	Informations Affichées
1	État du Système	Temps de fonctionnement, abonnés enregistrés, connexions actives, appels actifs, utilisation de la mémoire, nombre de planificateurs
2	VLR	Nombre d'abonnés enregistrés, FSM LU actives, FSM Auth actives
3	Appels Actifs	Compte et résumé des appels actifs (direction, numéros appelants/appelés)
4	Pile SS7	Nombre de connexions SCCP, nombre de transactions TCAP, demandes de pagination en attente
5	BEAM VM	Nombre de processus/limite, profondeur de la file d'attente d'exécution, nombre de réductions, répartition de la mémoire (total, ETS, binaire)
6	À Propos	Informations sur la version d'OmniMSC, version OTP, marque Omnitouch Network Services
9	Demande de Vente	Informations de contact
0	Sortie	Met fin à la session

Chaque sous-menu affiche une option "0. Retour" qui renvoie au menu principal. Les données de diagnostic sont collectées à partir des métriques système en direct au moment de la demande.

L'easter egg est entièrement géré au sein du MSC sans aucune signalisation MAP. Le Gestionnaire USSD détecte le code magique, l'achemine vers le module EasterEgg et gère le dialogue du menu à plusieurs étapes en utilisant des messages unstructuredSS-Request initiés par le réseau vers l'UE.

Codec USSD

Le codec USSD gère l'encodage et le décodage des éléments de protocole USSD selon 3GPP TS 24.080 et TS 24.090.

Structure de l'IE Facility

L'IE Facility (tag 0x1C) encapsule un composant encodé en ASN.1 BER :

Type de Composant	Tag ASN.1	Utilisation
Invoke	0xA1	Transporte une demande (processUnstructuredSS-Request, unstructuredSS-Request, unstructuredSS-Notify)
ReturnResultLast	0xA2	Transporte une réponse (processUnstructuredSS-Response, unstructuredSS-Response)

Chaque composant contient un ID d'invocation, un code d'opération et un paramètre SEQUENCE optionnel avec le schéma de codage des données USSD et la chaîne USSD.

Codes d'Opération MAP

Opcode	Opération	Direction
59	processUnstructuredSS-Request	MO: UE → MSC → HLR
60	unstructuredSS-Request	MT: HLR → MSC → UE (étape de menu interactif)
61	unstructuredSS-Notify	MT: HLR → MSC → UE (notification, aucune réponse attendue)

Encodage GSM 7 bits

Les chaînes USSD sont encodées en utilisant l'alphabet par défaut GSM 7 bits défini dans 3GPP TS 23.038. Chaque caractère est représenté comme un septet de 7 bits, et les septets sont regroupés en octets (8 septets tiennent dans 7 octets). Le byte de schéma de codage des données (DCS=0x0F) indique l'encodage GSM 7 bits.

Pour les chaînes nécessitant des caractères en dehors de l'alphabet GSM 7 bits, l'encodage UCS-2 (DCS=0x48) est utilisé, où chaque caractère occupe deux octets en UTF-16 big-endian.

La longueur maximale de la chaîne USSD est de 182 caractères pour l'encodage GSM 7 bits (160 octets empaquetés) ou 80 caractères pour UCS-2 (160 octets).

Flux de Messages SS REGISTER et RELEASE COMPLETE

Les sessions USSD utilisent les types de messages de Service Supplémentaire (SS) définis dans 3GPP TS 24.010 :

Message	Direction	But
REGISTER	UE → MSC	Initie une nouvelle transaction SS. Contient un Facility IE avec la demande USSD.
FACILITY	Les deux	Transporte des données en cours de session (étapes de menu interactif). Utilisé pour les dialogues USSD à plusieurs étapes.
RELEASE COMPLETE	Les deux	Met fin à la transaction SS. Peut contenir un Facility IE avec la réponse finale.

Une simple demande-réponse USSD utilise REGISTER (de l'UE) suivi de RELEASE COMPLETE (du MSC). Une session interactive à plusieurs étapes utilise REGISTER, puis un ou plusieurs échanges FACILITY, puis RELEASE COMPLETE.

La session a un délai de garde configurable (par défaut 30 secondes). Si ni l'UE ni la passerelle ne répondent dans cette fenêtre, le MSC termine la session avec RELEASE COMPLETE.

Références

Spécification	Titre	Pertinence
TS 24.090	Données de Service Supplémentaires Non Structurées (USSD)	Procédures USSD, gestion de session
TS 29.002 Section 14	Spécification MAP - opérations de service supplémentaire	MAP processUnstructuredSS-Request (opcode 59), unstructuredSS-Request (opcode 60), unstructuredSS-Notify (opcode 61)
TS 24.080	Spécification de l'interface radio mobile couche 3 SS - Formats et codage	Structure de l'IE Facility, encodage des composants
TS 23.038	Alphabets et informations spécifiques à la langue	Alphabet par défaut GSM 7 bits, empaquetage de septets
TS 22.030	Interface Homme-Machine (MMI)	Format de code de service, syntaxe de chaîne USSD
TS 24.010	Spécification de l'interface radio mobile couche 3 SS - Aspects généraux	Types de messages REGISTER, FACILITY, RELEASE COMPLETE

Service d'Appel de Groupe Vocal et Service de Diffusion Vocale

Ce document décrit le Service d'Appel de Groupe Vocal (VGCS) et le Service de Diffusion Vocale (VBS) pour le contrôle des appels de groupe et de diffusion mis en œuvre dans OmniMSC par Omnitouch. VGCS suit la norme 3GPP TS 43.068 et VBS suit la norme 3GPP TS 43.069. Les opérations d'appel de groupe MAP échangées avec le Registre d'Appels de Groupe (GCR) et les MSC relais suivent la clause 17.6.7 de la norme 3GPP TS 29.002.

Pour le contrôle des appels point à point, voir Flux d'Appels. Pour les procédures MAP et TCAP sous-jacentes, voir Opérations MAP. Pour les services de précedence et de préemption Multi-Niveaux améliorés utilisés pour prioriser les interlocuteurs, voir Services Supplémentaires. Pour les paramètres de configuration, voir Référence de Configuration.

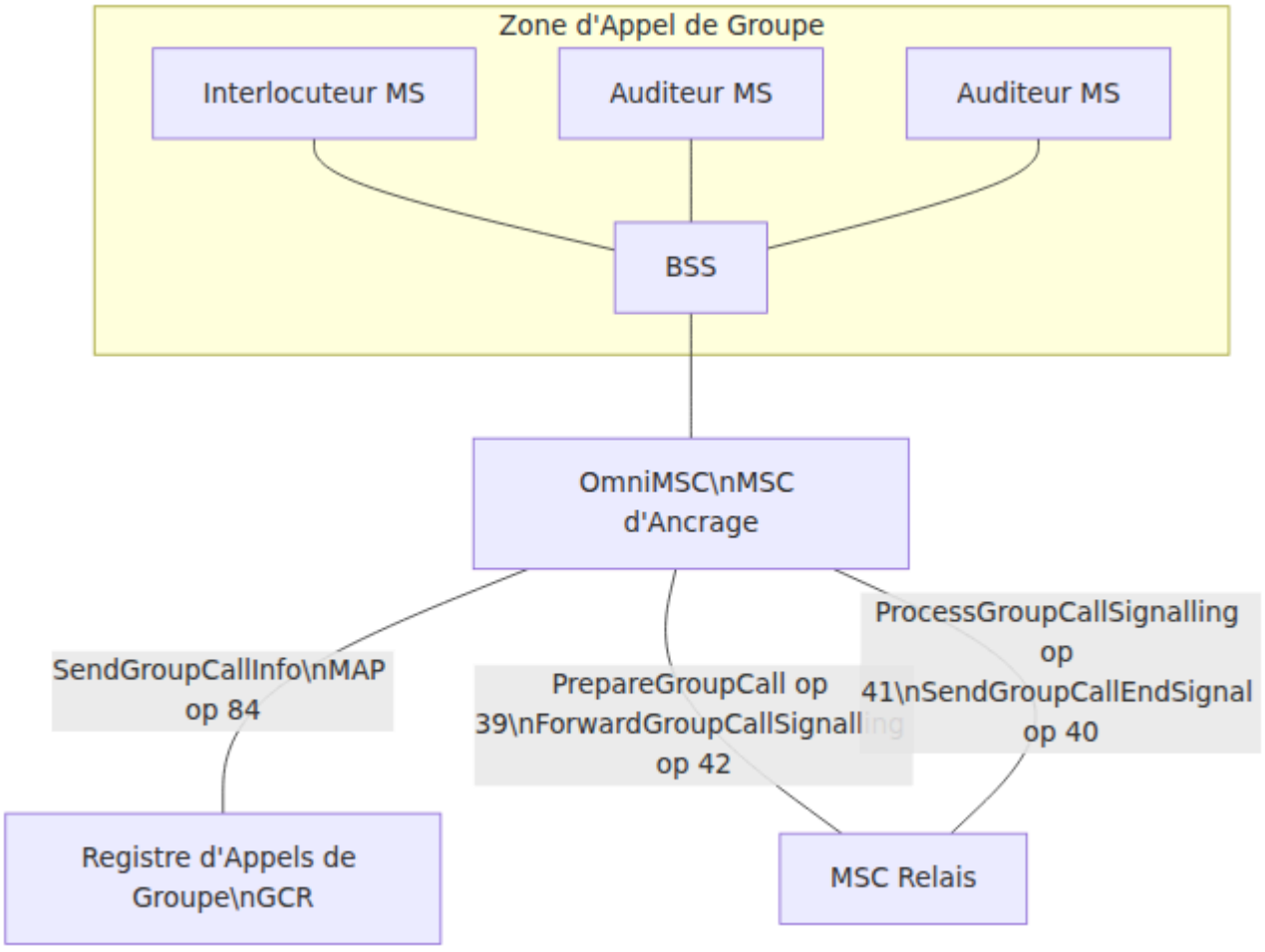
Aperçu

VGCS et VBS sont des services ASCI (Advanced Speech Call Items) utilisés principalement dans les réseaux ferroviaires (GSM-R) et de sécurité publique. Ils permettent à un seul interlocuteur d'être entendu par de nombreux auditeurs dans une ou plusieurs zones d'appel de groupe.

- VGCS (TS 43.068) est un appel de groupe bidirectionnel. Tout abonné au service dans la zone d'appel de groupe peut devenir l'interlocuteur en saisissant le lien montant. Un seul interlocuteur détient le lien montant à la fois.
- VBS (TS 43.069) est une diffusion unidirectionnelle. Seul l'initiateur de la diffusion (un répartiteur ou un abonné désigné) transmet sur le lien

descendant. Il n'y a pas de contention sur le lien montant.

Un appel de groupe ou de diffusion est ancré à un MSC de service, le MSC d'ancrage. Le MSC d'ancrage interroge le Registre d'Appels de Groupe (GCR) pour résoudre les attributs de groupe et la référence d'appel ASCI, puis prépare les canaux d'appel de groupe dans les cellules pertinentes via les MSC relais. Le groupe est identifié par un Id de Groupe (VGCS) ou un Id de Groupe de diffusion (VBS).



Opérations d'Appel de Groupe MAP

OmniMSC met en œuvre les cinq opérations d'appel de groupe MAP de la clause 17.6.7 de la norme TS 29.002. Les opérations sont effectuées en TCAP sur SCCP en utilisant le codec ASN.1 compilé (module `MAP-Group-Call-Operations` et types de données `MAP-GR-DataTypes`).

Opération	Opcode	Direction	Confirmé	Objecti
SendGroupCallInfo	84	MSC d'Ancrage vers GCR	Oui	Interroger le Registr d'Appels d Groupe pour l'adresse MSC d'ancrage et la référence d'appel ASCI
PrepareGroupCall	39	MSC d'Ancrage vers MSC relais	Oui	Demande à un MSC relais d'allouer des ressource de canal d'appel de groupe et de retourner numéro d'appel de groupe
SendGroupCallEndSignal	40	MSC relais vers MSC d'ancrage	Oui	Libérer ur liaison d'appel de groupe
ForwardGroupCallSignalling	42	MSC d'Ancrage	Non	Transmett des

Opération	Opcode	Direction	Confirmé	Objecti
		vers MSC relais		command de contrô du lien descenda (accord, rejet, sais libération
ProcessGroupCallSignalling	41	MSC relais vers MSC d'ancrage	Non	Transmett des indication de contrô du lien montant (demande de lien montant, libération de lien montant, libération d'appel)

Le code de téléservice distingue le service. VGCS utilise voiceGroupCall (0x91) et VBS utilise voiceBroadcastCall (0x92), selon la norme TS 22.003 et le module MAP-TS-Code.

Priorité de l'interlocuteur

Les opérations de contrôle du lien montant portent une priorité d'interlocuteur (TS 43.068 et le type MAP TalkerPriority) :

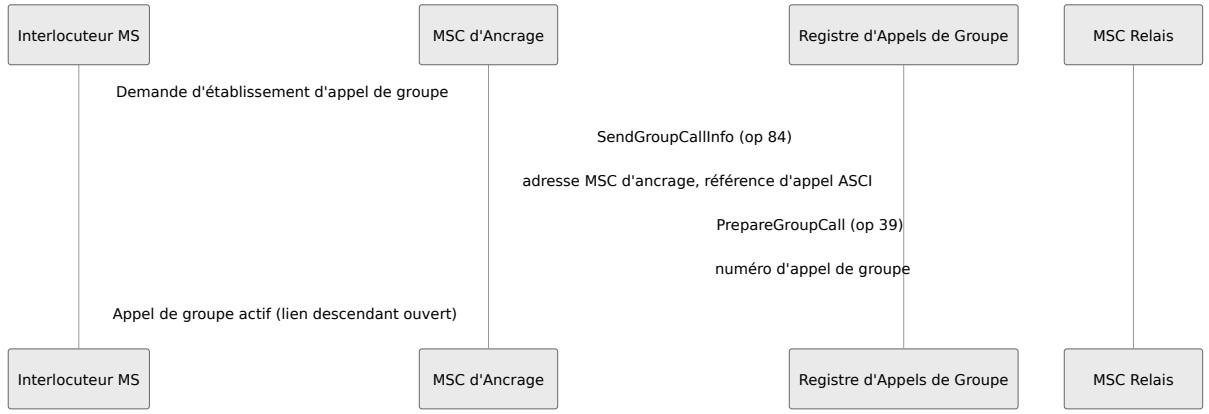
Priorité	Valeur	Signification
normal	0	Abonné de service standard
privilégié	1	Abonné privilégié, peut préempter les interlocuteurs normaux
urgence	2	Interlocuteur d'urgence, la plus haute précedence

Machine d'État de Contrôle d'Appel de Groupe

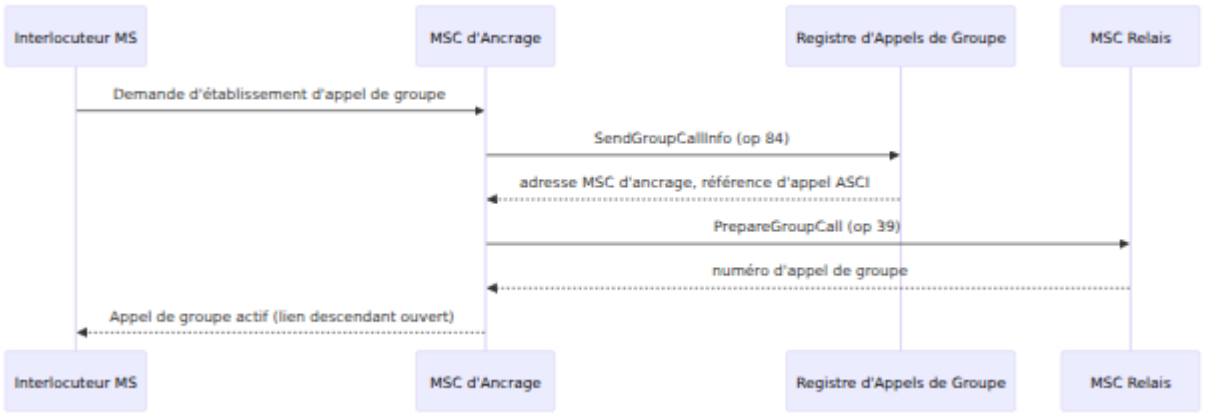
Le contrôle d'appel de groupe du MSC d'ancrage est une machine d'état (`Omnimsc.VGCS.FSM`) qui reflète la FSM de contrôle d'appel point à point. Elle gère un seul appel de groupe ou de diffusion à travers l'établissement, la phase active, la contention du lien montant VGCS, et la libération.

État	Signification
null	Aucun appel de groupe en cours
établissement	Une demande d'établissement a été acceptée ; le GCR est en cours d'interrogation (SendGroupCallInfo)
group_channel_setup	Le MSC d'ancrage prépare les canaux d'appel de groupe dans les MSC relais (PrepareGroupCall)
actif	L'appel de groupe ou de diffusion est établi ; le lien descendant est ouvert. Pour VGCS, le lien montant est initialement libre
uplink_busy	VGCS seulement. Un interlocuteur a saisi le lien montant. D'autres demandes de lien montant sont rejetées jusqu'à ce que le lien montant soit libéré
release	L'appel est en cours de démantèlement (SendGroupCallEndSignal) avant de revenir à null

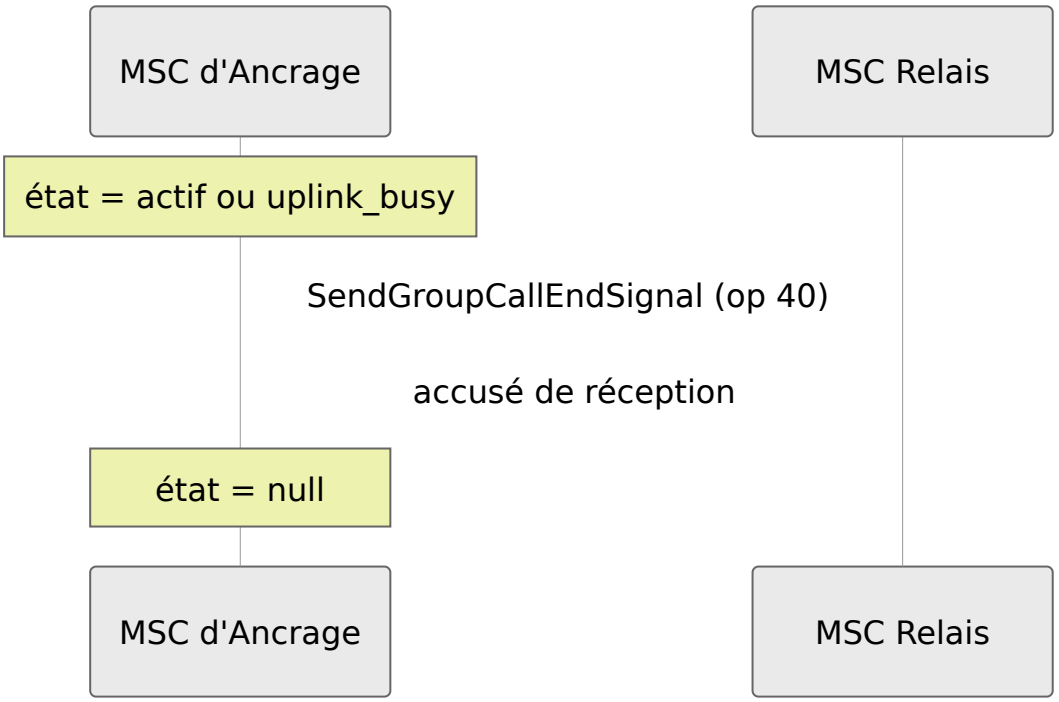
Flux d'établissement



Flux de contrôle du lien montant VGCS



Flux de libération



Configuration

La couche de contrôle d'appel de groupe fonctionne sous `Omnimsc.VGCS.Supervisor` et ne nécessite aucune configuration obligatoire pour accepter les opérations d'appel de groupe entrantes. Les paramètres optionnels suivants ajustent le comportement du MSC relais.

Paramètre	Emplacement	Par défaut	Description
group_call_number	`config :omnimsc, Omnimsc.VGCS.Handler`	titre global MSC	Numéro E.164 retourné dans la réponse PrepareGroupCall lorsqu'il agit en tant que MSC relais
global_title	`config :omnimsc, :msc`	aucun	Adresse MSC d'ancrage annoncée dans la réponse SendGroupCallInfo

Exemple :

```
config :omnimsc, Omnimsc.VGCS.Handler,
  group_call_number: "14155559000"
```

Implémenté et Différé

Les éléments suivants sont implémentés dans cette version.

- Machine d'état de contrôle d'appel de groupe pour VGCS et VBS, couvrant l'établissement, la phase active, la saisie, le rejet et la libération du lien montant VGCS, et la libération d'appel, avec un filet de sécurité de temporisation de garde.
- Encodeurs pour les cinq opérations de demande d'appel de groupe MAP (SendGroupCallInfo, PrepareGroupCall, SendGroupCallEndSignal, ForwardGroupCallSignalling, ProcessGroupCallSignalling), chacun produisant un message TCAP complet via le codec ASN.1 compilé.

- Décodeurs qui normalisent les arguments d'opération d'appel de groupe en représentations OmniMSC.
- Routage d'entrée des opérations d'appel de groupe entrantes (opcodes 39, 40, 41, 42, 84) vers le gestionnaire d'appels de groupe, qui les corrèle à la machine d'état d'appel de groupe en cours par Id de Groupe et répond aux opérations confirmées avec un accusé de réception TCAP.

Les éléments suivants sont différés.

- Encodage des corps de résultats d'opération confirmée (le numéro d'appel de groupe dans la réponse PrepareGroupCall et l'adresse MSC d'ancrage et la référence d'appel ASCI dans la réponse SendGroupCallInfo). Le codec TCAP compilé dans la dépendance SS7 connecte les arguments d'opération d'appel de groupe à son ensemble d'objets Invokable ROS mais ne connecte pas les résultats à l'ensemble d'objets Returnable. En conséquence, ces réponses sont actuellement envoyées sous la forme d'un TCAP returnResult vide (uniquement invokeId), ce qui est un accusé de réception valide selon la définition ReturnResult de ROS (la séquence de résultats est optionnelle), mais ne transporte pas la charge utile du résultat. Les opérations de direction de demande, le décodage des arguments et les décodeurs de résultats côté pair ne sont pas affectés. Cela est suivi contre la dépendance SS7 exposant les résultats d'appel de groupe dans Returnable.
- L'établissement de canal d'appel de groupe côté radio dans le BSS (le canal VGCS/VBS et les procédures de notification des normes TS 44.068 et TS 44.069) est hors du champ d'application pour la couche de contrôle du réseau central décrite ici.

Documentation Connexe

- Flux d'Appels pour les séquences d'appels vocaux point à point
- Opérations MAP pour le transport MAP et TCAP
- Services Supplémentaires pour la précedence et la préemption eMLPP
- Référence de Configuration pour tous les paramètres de configuration