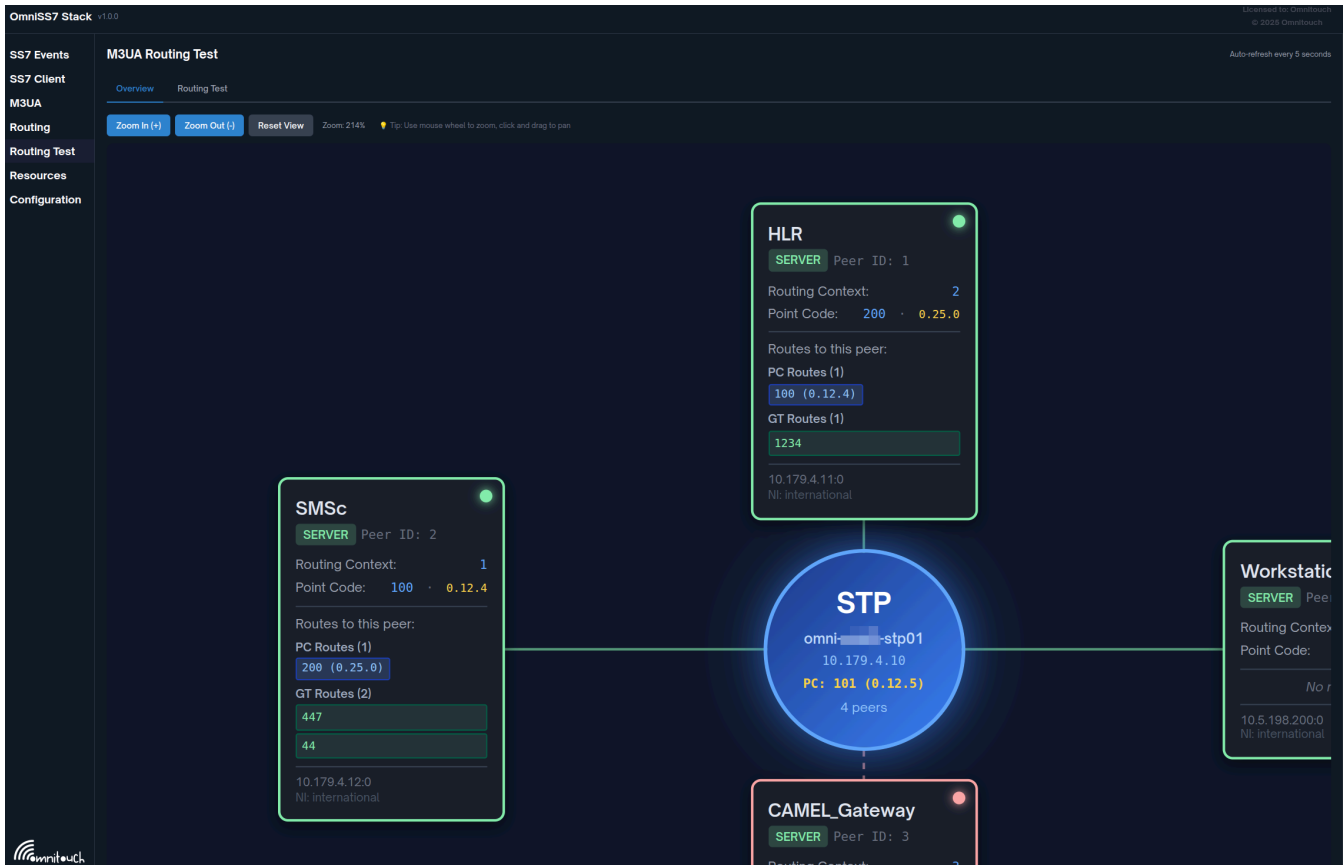




OmniSS7 - Guide de l'utilisateur

OmniSS7 par Omnitouch Network Services est une pile de signalisation SS7 complète et polyvalente qui offre une fonctionnalité flexible des éléments de réseau.



Aperçu de la documentation

Cette documentation est organisée par rôle d'élément de réseau. Choisissez le guide qui correspond à votre déploiement :

Guides de configuration

- Guide STP** - Configuration du Point de Transfert de Signal
 - Routeage du trafic SS7 entre les pairs de réseau
 - Routeage par code de point et titre global
 - Équilibrage de charge et dissimulation de topologie
 - Utilisez ceci si vous routez le trafic SS7 entre les réseaux
- Guide Client MAP** - Configuration du Client MAP
 - Connectez-vous en tant que client M3UA pour envoyer des requêtes MAP
 - Requêtes HLR, authentification, informations de routage
 - Support du protocole MAP générique
 - Utilisez ceci si vous envoyez des requêtes MAP aux éléments de réseau
- Guide Centre SMS** - Configuration du Centre SMS (SMSc)
 - Routeage et livraison de messages SMS
 - Mise en file d'attente de messages avec base de données
 - Auto-flush et rapports de livraison
 - Utilisez ceci si vous exploitez un Centre SMS
- Guide HLR** - Configuration du Registre de Localisation Abonné
 - Gestion de la base de données des abonnés
 - Génération de vecteurs d'authentification
 - Mises à jour de localisation et informations de routage
 - Utilisez ceci si vous exploitez un HLR/HSS
- Guide Passerelle CAMEL** - Configuration de la Passerelle CAMEL
 - Services de réseau intelligent (CAP/CAMEL)
 - Contrôle d'appel en temps réel et facturation
 - Intégration OCS pour la facturation
 - Générateur de requêtes interactif et surveillance de session
 - Utilisez ceci si vous fournissez des services IN ou une facturation en temps réel

Fonctionnalités communes

- Guide des fonctionnalités communes** - Composants partagés
 - Aperçu et configuration de l'interface utilisateur Web
 - Documentation API
 - Surveillance et métriques (Prometheus)
 - Meilleures pratiques et dépannage

Documentation de référence

- Annexe** - Référence technique
 - Spécifications du protocole SS7
 - Codes d'opération MAP
 - Flux de transactions TCAP
 - Encodages et formats de caractères

Démarrage rapide

1. Aperçu du système

OmniSS7 peut fonctionner en différents modes selon vos besoins réseau :

3. Configuration

OmniSS7 peut fonctionner en 5 modes opérationnels différents. Le fichier de configuration config/runtime.exs contient des exemples complets et prêts à l'emploi.

Pour changer de mode :

- Ouvrez config/runtime.exs
- Décommentez la section de configuration souhaitée (STP, HLR, SMSc ou CAMEL GW)
- Commentez les autres sections
- Mettez à jour les adresses IP et les URL API si nécessaire
- Redémarrez l'application

→ Voir les guides spécifiques au mode ci-dessous pour des instructions de configuration complètes

Exemples de configurations dans runtime.exs :

Mode STP :

```
config :omniss7,
  map_client_enabled: true,
  hlr_mode_enabled: false,
  smsc_mode_enabled: false,
  camelgw_mode_enabled: false,
  map_client_m3ua: %{}
```

Mode HLR :

```
config :omniss7,
  map_client_enabled: false,
  hlr_mode_enabled: true,
  smsc_mode_enabled: false,
  camelgw_mode_enabled: false,
  hlr_api_base_url: "...",
  map_client_m3ua: %{}
```

Mode SMSc :

```
config :omniss7,
  map_client_enabled: true,
  hlr_mode_enabled: false,
  smsc_mode_enabled: true,
  camelgw_mode_enabled: false,
  smsc_api_base_url: "...",
  auto_flush_enabled: true,
  map_client_m3ua: %{}
```

Mode Passerelle CAMEL :

```
config :omniss7,
  cap_client_enabled: true,
  camelgw_mode_enabled: true,
  ocs_enabled: true,
  ocs_url: "http://your-ocs-server/api/charging",
  cap_version: :v2, # Version CAP : :v1, :v2, :v3, ou :v4
  cap_client_m3ua: %{}
```

4. Accéder à l'interface Web

Naviguez vers <http://localhost> (ou votre nom d'hôte configuré)

Architecture du système

Matrice des fonctionnalités

Fonctionnalité	Mode STP	Client MAP	Mode SMSc	Mode HLR	Passerelle CAMEL
Routing par code de point	☑	☑	☑	☑	☑
Routing par titre global	☑	☑	☑	☑	☑
Réécriture de SSN	☑	☑	☑	☑	☑
Support multi-pair	☑	☑	☑	☑	☑
Requêtes MAP (Envoyer)	☑	☑	☑	☑	☑
Réponses MAP (Recevoir)	☑	☑	☑	☑	☑
Gestion de file d'attente SMS	☑	☑	☑	☑	☑
Auto-flush SMS	☑	☑	☑	☑	☑
Base de données des abonnés	☑	☑	☑	☑	☑
Vecteurs d'authentification	☑	☑	☑	☑	☑
Mises à jour de localisation	☑	☑	☑	☑	☑
Support CAP/CAMEL	☑	☑	☑	☑	☑
Facturation en temps réel	☑	☑	☑	☑	☑
Contrôle d'appel (Services IN)	☑	☑	☑	☑	☑
Interface Web	☑	☑	☑	☑	☑
API REST	☑	☑	☑	☑	☑
Métriques Prometheus	☑	☑	☑	☑	☑

Opérations courantes

Accès à l'interface Web

- URL : <http://localhost> (ou nom d'hôte configuré)
- API Swagger : <http://localhost/swagger>
- Métriques : <http://localhost/metrics>

Surveillance

```
# Vérifier l'état des pairs M3UA
curl http://localhost/api/m3ua-status
```

```
# Voir les métriques Prometheus
curl http://localhost/metrics
```

```
# Vérifier la santé de l'application
curl http://localhost/api/health
```

Journaux

```
# Configurer le niveau de journalisation dans config/runtime.exs
config :logger,
  level: :debug # Options : :debug, :info, :warning, :error
```

Capacités clés

- Support complet du protocole MAP** - Opérations MAP Phase 2/3
- Support du protocole CAP/CAMEL** - CAP v1/v2/v3/v4 pour des services de réseau intelligent
- Signalisation M3UA/CTCP** - Transport SS7 basé sur IP
- Facturation en temps réel** - Intégration OCS pour la facturation prépayée/postpayée
- File d'attente de messages en temps réel** - Livraison de SMS avec base de données
- Générateur de requêtes interactif** - Interface Web pour les tests CAMEL/CAP
- Surveillance de session** - Suivi des sessions d'appel CAMEL en temps réel
- Documentation API interactive** - Interface Swagger pour les tests
- Métriques Prometheus** - Observabilité complète
- Configuration multi-rôle** - STP, Client MAP, SMSc, HLR, Passerelle CAMEL

Aperçu de la pile de protocoles

Exemples de cas d'utilisation

Passerelle réseau (STP)

Routing du trafic SS7 entre différents réseaux mobiles

- Connecter les réseaux d'opérateurs
- Passerelle SS7 internationale
- Équilibrage de charge entre HLR
- Traduction de titre global
- NAT SCTP (Réutilisation intelligente de titre global)
- [Guide STP](#)

Centre SMS (SMSc)

Livrer des messages SMS aux abonnés mobiles

- Livraison MT-SMS
- Origine MO-SMS
- Routing domicile SMS
- Masquage IMSI
- Pare-feu SMS
- Gestion de file d'attente de messages
- Rapports de livraison
- Intègre dans OmniMessage pour gérer tous les SMS MAP
- [Guide Centre SMS](#)

Client MAP

Interagir avec n'importe quel élément de réseau via MAP en utilisant une API RESTful simple

- PRN / SRI / ATI / etc
- Construisez vos propres applications SS7/MAP en utilisant des API RESTful
- Passerelles USSD
- Requêtes de vecteurs d'authentification
- Recherches IMSI/MSISDN
- Requêtes d'informations de routage
- [Guide Client MAP](#)

Base de données des abonnés (HLR)

Gérer les données des abonnés et l'authentification

- Mises à jour de localisation
- Génération d'authentification
- Provisionnement d'informations de routage
- Intégration complète dans OmniHSS
- → [Guide HLR](#)

Plateforme de réseau intelligent (Passerelle CAMEL)

Contrôle d'appel en temps réel et facturation pour les opérateurs de télécommunications

- Facturation d'appels prépayée/postpayée
- Contrôle d'appel (connexion, libération, routage)
- Gestion de session et génération de CDR
- Générateur de requêtes interactif pour les tests
- → [Guide Passerelle CAMEL](#)

Support et ressources

Documentation

Guides de configuration de base :

- [Guide de configuration STP](#) - Routage du Point de Transfert de Signal
- [Guide de configuration Client MAP](#) - Client du protocole MAP
- [Guide de configuration Centre SMS](#) - Routage et livraison de SMS
- [Guide de configuration HLR](#) - Base de données des abonnés
- [Guide de configuration Passerelle CAMEL](#) - Réseau intelligent & facturation

Intégration & Référence :

- [Guide du générateur de requêtes CAMEL](#) - Outil de test interactif
- [Guide des fonctionnalités communes](#) - Composants partagés & Interface Web
- [Référence technique](#) - Spécifications du protocole

Informations de contact

Produit : OmniSS7

Fabricant : Omnitouch Network Services

Version de la documentation : 2.0

Dernière mise à jour : 2025

Pour un support technique, une assistance à l'implémentation ou des demandes de vente, veuillez contacter Omnitouch Network Services.

Cette documentation couvre l'opération en temps réel d'OmniSS7 et la fonctionnalité utilisateur finale. Pour l'installation, le développement ou la configuration avancée, veuillez vous référer à la documentation technique.



Guide de l'API REST

[← Retour à la documentation principale](#)

Ce guide fournit une documentation complète pour l'**API REST** d'OmniSS7 et l'**interface Swagger**.

Table des matières

1. [Aperçu](#)
2. [Configuration du serveur HTTP](#)
3. [Swagger UI](#)
4. [Points de terminaison de l'API](#)
5. [Authentification](#)
6. [Formats de réponse](#)
7. [Gestion des erreurs](#)
8. [Métriques \(Prometheus\)](#)
9. [Exemples de requêtes](#)

Aperçu

OmniSS7 fournit une API REST pour un accès programmatique aux opérations MAP (Mobile Application Part). L'API vous permet de :

- Envoyer des requêtes MAP (SRI, SRI-for-SM, UpdateLocation, etc.)
- Récupérer des réponses MAP
- Surveiller les métriques système via Prometheus

Architecture de l'API

Configuration du serveur HTTP

Détails du serveur

Paramètre	Valeur	Configurable
Protocole	HTTP	Non
Adresse IP	0.0.0.0 (toutes les interfaces)	Via code uniquement
Port	8080	Via code uniquement
Transport	Plug.Cowboy	Non

URL d'accès : http://[server-ip]:8080

Activation/Désactivation du serveur HTTP

Contrôlez si le serveur HTTP démarre :

```
config :omniss7,  
  start_http_server: true  # Mettre à false pour désactiver
```

Par défaut : true (activé)

Lorsqu'il est désactivé : Le serveur HTTP ne démarrera pas, et l'API REST/l'interface Swagger ne sera pas disponible.

Swagger UI

L'API comprend une **Swagger UI** pour la documentation interactive de l'API et les tests.

Accéder à Swagger UI

URL : http://[server-ip]:8080/swagger

Fonctionnalités :

- Documentation interactive de l'API
- Fonctionnalité d'essai pour tester les points de terminaison
- Schémas de requête/réponse
- Charges utiles d'exemple

Swagger JSON

La spécification OpenAPI est disponible à :

URL : http://[server-ip]:8080/swagger.json

Cas d'utilisation :

- Importer dans Postman ou d'autres clients API
 - Générer des bibliothèques clientes
 - Automatisation de la documentation de l'API
-

Points de terminaison de l'API

Tous les points de terminaison des opérations MAP suivent le modèle : POST

/api/{operation}

Résumé des points de terminaison

Point de terminaison	Méthode	But	Délai d'attente
/api/sri	POST	Envoyer des informations de routage	10s
/api/sri-for-sm	POST	Envoyer des informations de routage pour SM	10s
/api/send-auth-info	POST	Envoyer des informations d'authentification	10s
/api/MT-forwardSM	POST	SMS Mobile Terminé Forward SM	10s
/api/forwardSM	POST	Forward SM	10s
/api/updateLocation	POST	Mettre à jour la localisation	10s
/api/prn	POST	Fournir un numéro de roaming	10s
/metrics	GET	Métriques Prometheus	N/A
/swagger	GET	Swagger UI	N/A
/swagger.json	GET	Spécification OpenAPI	N/A

Remarque : Toutes les requêtes MAP ont un **délai d'attente de 10 secondes codé en dur**.

SendRoutingInfo (SRI)

Récupérer des informations de routage pour établir un appel à un abonné mobile.

Point de terminaison : POST /api/sri

Corps de la requête :

```
{
  "msisdn": "1234567890",
  "gmsc": "5551234567"
}
```

Paramètres :

Champ	Type	Requis	Description
msisdn	String	Oui	MSISDN de la partie appelée
gmsc	String	Oui	Titre global du MSC de passerelle

Réponse (200 OK) :

```
{
  "result": {
    "imsi": "001001234567890",
    "msrn": "5551234999",
    "vlr_number": "5551234800",
    ...
  }
}
```

Erreur (504 Gateway Timeout) :

```
{
  "error": "timeout"
}
```

Exemple cURL :

```
curl -X POST http://localhost:8080/api/sri \
-H "Content-Type: application/json" \
-d '{
  "msisdn": "1234567890",
  "gmsc": "5551234567"
}'
```

SendRoutingInfoForSM (SRI-for-SM)

Récupérer des informations de routage pour livrer un SMS à un abonné mobile.

Point de terminaison : POST /api/sri-for-sm

Corps de la requête :

```
{
  "msisdn": "1234567890",
  "service_center": "5551234567"
}
```

Paramètres :

Champ	Type	Requis	Description
msisdn	String	Oui	MSISDN de destination
service_center	String	Oui	Titre global du centre de services

Réponse (200 OK) :

```
{
  "result": {
```

```

    "imsi": "001001234567890",
    "msc_number": "5551234800",
    "location_info": {...},
    ...
  }
}

```

Exemple cURL :

```

curl -X POST http://localhost:8080/api/sri-for-sm \
-H "Content-Type: application/json" \
-d '{
  "msisdn": "1234567890",
  "service_center": "5551234567"
}'

```

SendAuthenticationInfo

Demander des vecteurs d'authentification pour un abonné.

Point de terminaison : POST /api/send-auth-info

Corps de la requête :

```

{
  "imsi": "001001234567890",
  "vectors": 3
}

```

Paramètres :

Champ	Type	Requis	Description
imsi	String	Oui	IMSI de l'abonné
vectors	Integer	Oui	Nombre de vecteurs d'authentification à générer

Réponse (200 OK) :

```

{
  "result": {
    "authentication_sets": [
      {
        "rand": "0123456789ABCDEF...",
        "xres": "...",
        "ck": "...",
        "ik": "...",
        "autn": "..."
      }
    ]
  }
}

```



```
    ],  
    ...  
  }  
}
```

Exemple cURL :

```
curl -X POST http://localhost:8080/api/send-auth-info \  
-H "Content-Type: application/json" \  
-d '{  
  "imsi": "001001234567890",  
  "vectors": 3  
}'
```

MT-ForwardSM

Livrer un SMS Mobile Terminé à un abonné.

Point de terminaison : POST /api/MT-forwardSM

Corps de la requête :

```
{  
  "imsi": "001001234567890",  
  "destination_service_centre": "5551234567",  
  "originating_service_center": "5551234568",  
  "smsPDU": "0001000A8121436587F900001C48656C6C6F20576F726C64"  
}
```

Paramètres :

	Champ	Type Requis	Description
imsi		StringOui	IMSI de l'abonné de destination
destination_service_centre		StringOui	GT du centre de services de destination
originating_service_center		StringOui	GT du centre de services d'origine
smsPDU		StringOui	SMS TPDU au format hexadécimal

Remarque : smsPDU doit être une chaîne encodée en hexadécimal (majuscule ou minuscule).

Réponse (200 OK) :

```
{  
  "result": {  
    "delivery_status": "success",  
    ...  
  }  
}
```

```
}  
}
```

Exemple cURL :

```
curl -X POST http://localhost:8080/api/MT-forwardSM \  
-H "Content-Type: application/json" \  
-d '{  
  "imsi": "001001234567890",  
  "destination_service_centre": "5551234567",  
  "originating_service_center": "5551234568",  
  "smsPDU": "0001000A8121436587F900001C48656C6C6F20576F726C64"  
}'
```

ForwardSM

Transférer un message SMS (MO-SMS de l'abonné).

Point de terminaison : POST /api/forwardSM

Corps de la requête : Identique à MT-ForwardSM

Exemple cURL :

```
curl -X POST http://localhost:8080/api/forwardSM \  
-H "Content-Type: application/json" \  
-d '{  
  "imsi": "001001234567890",  
  "destination_service_centre": "5551234567",  
  "originating_service_center": "5551234568",  
  "smsPDU": "0001000A8121436587F900001C48656C6C6F20576F726C64"  
}'
```

UpdateLocation

Notifier le HLR du changement de localisation de l'abonné (enregistrement VLR).

Point de terminaison : POST /api/updateLocation

Corps de la requête :

```
{  
  "imsi": "001001234567890",  
  "vlr": "5551234800"  
}
```

Paramètres :

Champ	Type	Requis	Description
imsi	String	Oui	IMSI de l'abonné
vlr	String	Oui	Adresse du titre global du VLR

Réponse (200 OK) :

```
{
  "result": {
    "hlr_number": "5551234567",
    "subscriber_data": {...},
    ...
  }
}
```

Remarque : En mode HLR, cela déclenche la séquence InsertSubscriberData (ISD) avec un délai d'attente de 10 secondes par ISD.

Exemple cURL :

```
curl -X POST http://localhost:8080/api/updateLocation \
-H "Content-Type: application/json" \
-d '{
  "imsi": "001001234567890",
  "vlr": "5551234800"
}'
```

ProvideRoamingNumber (PRN)

Demander le MSRN (Mobile Station Roaming Number) pour le routage des appels vers un abonné en itinérance.

Point de terminaison : POST /api/prn

Corps de la requête :

```
{
  "msisdn": "1234567890",
  "gmsc": "5551234567",
  "msc_number": "5551234800",
  "imsi": "001001234567890"
}
```

Paramètres :

Champ	Type	Requis	Description
msisdn	String	Oui	MSISDN de l'abonné
gmsc	String	Oui	GT du MSC de passerelle
msc_number	String	Oui	Numéro MSC pour l'abonné
imsi	String	Oui	IMSI de l'abonné

Réponse (200 OK) :

```
{
  "result": {
    "msrn": "5551234999",
    ...
  }
}
```

Exemple cURL :

```
curl -X POST http://localhost:8080/api/prn \
-H "Content-Type: application/json" \
-d '{
  "msisdn": "1234567890",
  "gmsc": "5551234567",
  "msc_number": "5551234800",
  "imsi": "001001234567890"
}'
```

Authentification

État actuel : L'API ne nécessite pas d'authentification.

Considérations de sécurité :

- L'API est destinée à un usage sur un réseau interne/de confiance
- Envisagez d'utiliser des règles de pare-feu pour restreindre l'accès
- Pour les déploiements en production, envisagez de mettre en œuvre un middleware d'authentification

Formats de réponse

Toutes les réponses utilisent le format **JSON**.

Réponse de succès

Statut HTTP : 200 OK

Structure :

```
{
  "result": {
    // Données de réponse spécifiques à l'opération
  }
}
```

Réponse d'erreur

Statut HTTP :

- 400 Bad Request - Corps de requête invalide
- 504 Gateway Timeout - Délai d'attente de la requête MAP (10 secondes)
- 404 Not Found - Point de terminaison invalide

Structure :

```
{
  "error": "timeout"
}
```

ou

```
{
  "error": "invalid request"
}
```

Gestion des erreurs

Erreurs courantes

Erreur	Code HTTP	Description	Solution
JSON invalide	400	Le corps de la requête n'est pas un JSON valide	Vérifiez la syntaxe JSON
Champs manquants	400	Champs requis manquants	Incluez tous les paramètres requis
Délai d'attente	504	La requête MAP a dépassé le délai d'attente de 10s	Vérifiez la connectivité M3UA, la disponibilité HLR/VLR
Non trouvé	404	Point de terminaison invalide	Vérifiez l'URL du point de terminaison

Comportement de délai d'attente

Toutes les requêtes MAP ont un **délai d'attente de 10 secondes codé en dur** :

1. Requête envoyée au MapClient GenServer
2. Attend une réponse jusqu'à 10 secondes
3. Si aucune réponse → retourne 504 Gateway Timeout
4. Si réponse reçue → retourne 200 OK avec résultat

Dépannage des délais d'attente :

- Vérifiez l'état de la connexion M3UA (Web UI → page M3UA)
 - Vérifiez que l'élément réseau (HLR/VLR/MS) est accessible
 - Vérifiez la configuration de routage
 - Consultez les journaux d'événements SS7 pour les erreurs
-

Métriques (Prometheus)

L'API expose des métriques Prometheus pour la surveillance.

Point de terminaison des métriques

URL : `http://[server-ip]:8080/metrics`

Format : Format texte Prometheus

Exemple de sortie :

```
# HELP map_requests_total Total MAP requests
# TYPE map_requests_total counter
map_requests_total{operation="sri"} 42
map_requests_total{operation="sri_for_sm"} 158
map_requests_total{operation="updateLocation"} 23

# HELP cap_requests_total Total CAP requests
# TYPE cap_requests_total counter
cap_requests_total{operation="initialDP"} 87
cap_requests_total{operation="requestReportBCSMEEvent"} 91

# HELP map_request_duration_milliseconds Duration of MAP request/
responses in ms
# TYPE map_request_duration_milliseconds histogram
map_request_duration_milliseconds_bucket{operation="sri",le="10"} 5
map_request_duration_milliseconds_bucket{operation="sri",le="50"} 12
map_request_duration_milliseconds_bucket{operation="sri",le="100"} 35
...

# HELP map_pending_requests Number of pending MAP TID waiters
# TYPE map_pending_requests gauge
map_pending_requests 3
```

Métriques disponibles

Métrique	Type	Étiquettes	Description
map_requests_total	Compteur	operation	Nombre total de requêtes MAP par type d'opération
cap_requests_total	Compteur	operation	Nombre total de requêtes CAP par type d'opération
map_request_duration_milliseconds	Histogramme	operation	Durée de la requête en millisecondes
map_pending_requests	Jauge	-	Nombre de transactions MAP en attente

Configuration de Prometheus

Ajoutez à votre `prometheus.yml` :

```
scrape_configs:
  - job_name: 'omniss7'
    static_configs:
      - targets: ['server-ip:8080']
    metrics_path: '/metrics'
    scrape_interval: 15s
```

Exemples de requêtes

Exemple Python

```
import requests
import json

# Requête SRI-for-SM
url = "http://localhost:8080/api/sri-for-sm"
payload = {
    "msisdn": "1234567890",
    "service_center": "5551234567"
}

response = requests.post(url, json=payload, timeout=15)

if response.status_code == 200:
```

```

    result = response.json()
    print(f"Succès : {result}")
elif response.status_code == 504:
    print("Délai d'attente - aucune réponse du réseau")
else:
    print(f"Erreur : {response.status_code} - {response.text}")

```

Exemple JavaScript

```

const axios = require('axios');

async function sendSRI() {
  try {
    const response = await axios.post('http://localhost:8080/api/sri', {
      msisdn: '1234567890',
      gmsc: '5551234567'
    }, {
      timeout: 15000
    });

    console.log('Succès :', response.data);
  } catch (error) {
    if (error.code === 'ECONNABORTED') {
      console.error('Délai d\'attente - aucune réponse du réseau');
    } else {
      console.error('Erreur :', error.response?.data || error.message);
    }
  }
}

sendSRI();

```

Exemple Bash/cURL

```

#!/bin/bash

# Requête UpdateLocation
response=$(curl -s -w "\n%{http_code}" -X POST http://localhost:8080/api/updateLocation \
  -H "Content-Type: application/json" \
  -d '{
    "imsi": "001001234567890",
    "vlr": "5551234800"
  }')

http_code=$(echo "$response" | tail -n 1)

```



```
body=$(echo "$response" | sed '$d')

if [ "$http_code" -eq 200 ]; then
    echo "Succès : $body"
elif [ "$http_code" -eq 504 ]; then
    echo "Délai d'attente - aucune réponse du réseau"
else
    echo "Erreur $http_code : $body"
fi
```

Diagrammes de flux

Flux de requête API

Résumé

L'API REST d'OmniSS7 fournit :

- ❖ **Opérations MAP** - Support complet pour SRI, SRI-for-SM, UpdateLocation, livraison SMS, authentification
- ❖ **Swagger UI** - Documentation interactive de l'API et tests
- ❖ **Métriques Prometheus** - Surveillance et observabilité
- ❖ **Délai d'attente codé en dur** - Délai d'attente de 10 secondes pour toutes les requêtes MAP
- ❖ **Serveur HTTP** - Fonctionne sur le port 8080 (configurable via `start_http_server`)

Pour l'accès à l'interface Web, consultez le [Guide de l'interface Web](#).

Pour les détails de configuration, consultez la [Référence de configuration](#).



Référence Technique (Annexe)

[← Retour à la Documentation Principale](#)

Référence technique pour les protocoles SS7 et l'implémentation d'OmniSS7.

Pile de Protocoles SS7

Codes d'Opération MAP

Opération	Opcode	But
updateLocation	2	Enregistrer la localisation de l'abonné
cancelLocation	3	Désenregistrer du VLR
provideRoamingNumber	4	Demander MSRN
sendRoutingInfo	22	Interroger le routage des appels
mt-forwardSM	44	Livrer un SMS à l'abonné
sendRoutingInfoForSM	45	Interroger le routage des SMS
mo-forwardSM	46	Transférer un SMS de l'abonné
sendAuthenticationInfo	56	Demander des vecteurs d'authentification

Types de Messages TCAP

- **BEGIN** - Démarrer la transaction
 - **CONTINUE** - Milieu de transaction
 - **END** - Réponse finale
 - **ABORT** - Annuler la transaction
-

Addressage SCCP

Formats de Titre Global

- **E.164** - Numéro de téléphone international (par exemple, 447712345678)
- **E.212** - Format IMSI (par exemple, 234509876543210)
- **E.214** - Format de code de point

Numéros de Sous-Système (SSN)

- **SSN 6**: HLR

- **SSN 7:** VLR
 - **SSN 8:** MSC/SMSC
 - **SSN 9:** GMLC
 - **SSN 10:** SGSN
-

TPDU SMS

Types de Messages

- **SMS-DELIVER** (MT) - Réseau vers mobile
- **SMS-SUBMIT** (MO) - Mobile vers réseau
- **SMS-STATUS-REPORT** - Statut de livraison
- **SMS-COMMAND** - Commande à distance

Encodages de Caractères

- **GSM7** - Alphabet GSM 7 bits (160 caractères par SMS)
 - **UCS2** - Unicode 16 bits (70 caractères par SMS)
 - **8-bit** - Données binaires (140 octets par SMS)
-

États M3UA

- **DOWN** - Pas de connexion SCTP
 - **CONNECTING** - Connexion SCTP en cours
 - **ASPUP_SENT** - En attente de l'ACK ASPUP
 - **INACTIVE** - ASP actif mais non opérationnel
 - **ASPAC_SENT** - En attente de l'ACK ASPAC
 - **ACTIVE** - Prêt pour le trafic
-

Codes de Point SS7 Communs

Les codes de point sont généralement des valeurs de 14 bits (UIT) ou de 24 bits (ANSI).

Format d'Exemple (UIT) :

- Réseau : 3 bits
 - Cluster : 8 bits
 - Membre : 3 bits
-

Codes d'Erreur SCCP

- **0** - Pas de traduction pour l'adresse
 - **1** - Pas de traduction pour une adresse spécifique
 - **2** - Congestion du sous-système
 - **3** - Échec du sous-système
 - **4** - Utilisateur non équipé
 - **5** - Échec MTP
 - **6** - Congestion du réseau
 - **7** - Non qualifié
 - **8** - Erreur dans le transport du message
-

Codes d'Erreur MAP

Code	Erreur	Description
1	unknownSubscriber	Abonné non présent dans le HLR
27	absentSubscriber	Abonné non joignable
34	systemFailure	Échec du réseau
35	dataMissing	Données requises non disponibles
36	unexpectedDataValue	Valeur de paramètre invalide

Documentation Connexe

- [← Retour à la Documentation Principale](#)
 - [Guide STP](#)
 - [Guide Client MAP](#)
 - [Guide Centre SMS](#)
 - [Guide HLR](#)
 - [Fonctionnalités Communes](#)
-

OmniSS7 par Omnitouch Network Services



Guide de Configuration du Passerelle CAMEL

Vue d'ensemble

Le mode **Passerelle CAMEL (CAMELGW)** transforme OmniSS7 en une plateforme de Réseau Intelligent (IN) qui fournit des services de contrôle d'appel et de facturation en temps réel en utilisant le protocole CAMEL Application Part (CAP).

OmniSS7 Stack CAMEL GW

Download to Omnicloud
© 2025 Omnicloud

SS7 Events

SS7 Client

M3UA

CAP Sessions

CAP Requests

Resources

Configuration

CAMEL Sessions

Active: 0

Auto-refresh every 2 seconds

Call ID	State	IMSI	Calling Number	Called Number	Service Key	Duration	Start Time	OTID
<div><div></div><div>No Active CAMEL Sessions</div><div>Sessions will appear here when calls are initiated</div></div>								
Total Sessions								
0								
Initiated								
0								
Answered								
0								
<div><div>About CAMEL Sessions</div><div>This page displays active CAMEL (Customized Applications for Mobile network Enhanced Logic) sessions managed by the gsmSCF (Service Control Function).</div><div>Initiated - Call setup in progress</div><div>answered - Call is active</div><div>terminated - Call ended (cleanup pending)</div></div>								

Qu'est-ce que CAMEL ?

CAMEL (Applications Personnalisées pour la Logique Améliorée des Réseaux Mobiles) est un ensemble de normes conçu pour fonctionner sur un réseau de cœur GSM ou UMTS. Il permet aux opérateurs de fournir des services nécessitant un contrôle en temps réel des appels, tels que :

- **Appels prépayés** - Vérification et facturation en temps réel du solde
- **Services à tarif premium** - Facturation spéciale pour les services à valeur ajoutée
- **Contrôle du routage des appels** - Routage dynamique des destinations en fonction du temps/emplacement
- **Réseaux privés virtuels** - Plans de numérotation d'entreprise
- **Filtrage des appels** - Autoriser/bloquer les appels en fonction de critères

Versions du Protocole CAP

OmniSS7 CAMELGW prend en charge plusieurs versions de CAP :

Version	Phase	Fonctionnalités
CAP v1	Phase CAMEL 1	Contrôle d'appel de base, opérations limitées
CAP v2	Phase CAMEL 2	Opérations améliorées, support SMS
CAP v3	Phase CAMEL 3	Support GPRS, opérations supplémentaires
CAP v4	Phase CAMEL 4	Fonctionnalités avancées, support multimédia

Par défaut : CAP v2 (le plus largement déployé)

Architecture

Exemple de Flux d'Appel

Configuration

Prérequis

- OmniSS7 installé et en cours d'exécution
- Connectivité M3UA avec MSC/GMSC (gsmSSF)
- Système de Facturation en Ligne (OCS) avec point de terminaison API (optionnel, pour la facturation en temps réel)

Activer le Mode Passerelle CAMEL

Modifiez config/runtime.exe et configurez la section Passerelle CAMEL :

```
config :omniss7,  
# Drapeaux de mode - Activer les fonctionnalités CAP/CAMEL  
cap_client_enabled: true,  
camelgw_mode_enabled: true,  
  
# Désactiver d'autres modes  
map_client_enabled: false,  
hlr_mode_enabled: false,  
smc_mode_enabled: false,  
  
# Configuration de la Version CAP/CAMEL  
# Détermine quelle version CAP utiliser pour les requêtes sortantes et le dialogue  
# Options : :v1, :v2, :v3, :v4  
cap_version: :v2,  
  
# Intégration OCS (pour la facturation en temps réel)  
ocs_enabled: true,  
ocs_url: "http://your-ocs-server/api/charging",  
ocs_timeout: 5000, # millisecondes  
ocs_auth_token: "your-api-token" # Optionnel, si OCS nécessite une authentification  
  
# Configuration de la Connexion M3UA pour CAMEL  
# Se connecter en tant qu'ASP (Application Server Process) pour les opérations CAP  
cap_client_m3ua: %(  
  mode: "ASP",  
  callback: (CapClient, :handle_payload, []),  
  process_name: :camelgw_client_asp,  
  
# Point de terminaison local (système CAMELGW)  
local_ip: {18, 179, 4, 13},  
local_port: 2905,
```

```
# Point de terminaison distant (MSC/GMSC - gsmSSF)
remote_ip: {10, 179, 4, 10},
remote_port: 2965,

# Paramètres M3UA
routing_context: 1,
network_appearance: 0,
asp_identifiant: 13
}
```

Configurer les Pages de l'Interface Web

L'Interface Web comprend des pages spécialisées pour les opérations CAMEL :

```
config :control_panel,
  use_additional_pages: [
    {S57.Web.EventsLive, "/events", "Événements S57"},
    {S57.Web.TestClientLive, "/client", "Client S57"},
    {S57.Web.M3UAStatusLive, "/m3ua", "M3UA"},
    {S57.Web.CAMELSessionsLive, "/camel_sessions", "Sessions CAP"},
    {S57.Web.CAMELRequestLive, "/camel_request", "Requêtes CAP"},
  ],
  page_order: ["/events", "/client", "/m3ua", "/camel_sessions",
    "/camel_request", "/application", "/configuration"]
```

Opérations CAP Supportées

Opérations Entrantes (de gsmSSF → gsmSCF)

Opération	Opcode	Description	Gestionnaire
InitialDP	0	Point de Détection Initial - notification de mise en place d'appel	handle_initial_dp/1
EventReportBCSM	6	Événement du Modèle d'Etat d'Appel de Base (réponse, déconnexion, etc.)	handle_event_report_bcsml
ApplyChargingReport	71	Rapport de facturation de gsmSSF	handle_apply_charging_report/1
AssistRequestInstructions	16	Demande d'assistance de gsmSRF	handle_assist_request_instructions/1

Opérations Sortantes (de gsmSCF → gsmSSF)

Opération	Opcode	Description	Générateur
Connect	20	Connecter l'appel au numéro de destination	CapRequestGenerator.connect_request/2
Continue	31	Continuer le traitement de l'appel sans modification	CapRequestGenerator.continue_request/1
ReleaseCall	22	Libérer/terminer l'appel	CapRequestGenerator.release_call_request/2
RequestReportBCSMEvent	23	Demandeur une notification des événements d'appel	CapRequestGenerator.request_report_bcsml_event_request/2
ApplyCharging	35	Appliquer la facturation à l'appel	CapRequestGenerator.apply_charging_request/3

Fonctionnalités de l'Interface Web

Page des Sessions CAMEL

URL : http://localhost/camel_sessions

Surveillance en temps réel des sessions d'appel CAMEL actives :

Fonctionnalités :

- **Liste des sessions en direct** - Se rafraichit automatiquement toutes les 2 secondes
- **Détails de la session** - OTID, ID d'appel, Etat, Durée
- **Version CAP** - Affiche la version du protocole (CAP v1/v2/v3/v4) détectée à partir de l'InitialDP
- **Informations sur l'appel** - IMSI, Numéro A, Numéro B, Clé de Service
- **Suivi de l'état** - Initié, Répondu, Terminé
- **Chronomètre de durée** - Affichage de la durée d'appel en temps réel

Colonnes du tableau :

- ID d'appel, Etat, Version, IMSI, Numéro appelant, Numéro appelé, Clé de Service, Durée, Heure de début, OTID

États de la session :

- **Initié** - InitialDP reçu, en attente de réponse
- **Répondu** - Appel répondu, facturation en cours
- **Terminé** - Appel terminé, CDR généré

Détection de la Version CAP : Le système détecte automatiquement la version du protocole CAP à partir de la portion de dialogue de l'InitialDP et l'affiche dans la colonne Version. Cela aide à identifier quelle version CAP chaque MSC utilise.

Constructeur de Requêtes CAMEL

URL : http://localhost/camel_request

Outil interactif pour construire et envoyer des requêtes CAP :

Fonctionnalités :

- **Sélecteur de type de requête** - InitialDP, Connect, ReleaseCall, etc.
- **Champs de formulaire dynamiques** - S'adapte au type de requête sélectionné
- **Options SCCP/M3UA** - Configuration d'adressage avancée
- **Historique des requêtes** - Dernières 20 requêtes avec statut
- **Suivi de session** - Maintient l'OTID pour les requêtes de suivi
- **Retour d'information en temps réel** - Messages de succès/erreur

Types de Requêtes :

1. **InitialDP** - Démarrer une nouvelle session d'appel
 - Clé de Service (entier)
 - Numéro appelant (A-partie)
 - Numéro appelé (B-partie)
2. **Connect** - Routage de l'appel vers la destination
 - Numéro de destination
3. **ReleaseCall** - Terminer l'appel
 - Code de Cause (16=Normal, 17=Occupé, 31=Non spécifié)
4. **RequestReportBCSMEvent** - Demander des notifications d'événements
 - Événements : oAnswer, oDisconnect, tAnswer, tDisconnect
5. **Continue** - Continuer l'appel sans modification
 - Aucun paramètre requis
6. **ApplyCharging** - Appliquer des limites de durée d'appel
 - Durée (secondes, 1-864000)
 - Libération sur Timeout (booléen)
 - Voir [Guide du Constructeur de Requêtes CAMEL](#) pour une utilisation détaillée

Options SCCP Avancées :

- Titre Global de la Partie Appelée
- Titre Global de la Partie Appelante
- SSN Appelée (par défaut : 146 = gsmSSF)
- SSN Appelante (par défaut : 146)

Options M3UA :

- OPC (Code de Point d'Origine, par défaut : 5013)
- DPC (Code de Point de Destination, par défaut : 5011)

Intégration avec OCS

Cycle de Vie de l'Appel avec Facturation

1. Initiation de l'Appel (InitialDP)

Lorsque le MSC envoie l'InitialDP, CAMELGW :

1. **Détecte la version CAP** - Examine la portion de dialogue pour identifier CAP v1/v2/v3/v4
2. **Décode le message CAP** - Extraie l'IMSI, les numéros appelant/appelé
3. **Appelle OCS** - API InitiateSession
4. **Reçoit l'autorisation** - MaxUsage (par exemple, 30 secondes)
5. **Stocke la session** - Dans SessionStore (table ETS) avec la version CAP
6. **Répond au MSC** - RequestReportBCSMEvent + Continue (en utilisant la même version CAP)

Exemple :

```
# Données InitialDP décodées
%{
  imsi: "310150123456789",
  calling_party_number: "14155551234",
  called_party_number: "14155556789",
  service_key: 1,
  msc_address: "19216800123",
  cap_version: :v2 # Détecté à partir du dialogue
}

# Réponse OCS
{:ok, %{max_usage: 30}} # 30 secondes autorisées
```

```
# Entrée SessionStore
%(
  call_id: "CAMEL-48080173",
  initial_dp_data: %(.),
  cap_version: v2, # Stocké pour la génération de réponse
  start_time: 1730246400,
  state: :initiated
)
```

2. Réponse à l'Appel (EventReportBCSM - oAnswer)

Lorsque l'appel est répondu :

1. **Reçoit l'événement oAnswer** - Du MSC
2. **Met à jour OCS** - UpdateSession avec usage=0
3. **Démarrs la boucle de débit** - OCS commence la facturation
4. **Met à jour l'état de la session** - :answered dans SessionStore
5. **Continue l'appel** - Envoie Continue au MSC

3. Mises à Jour Périodiques (Optionnel)

Pour les appels longs, demander un crédit supplémentaire :

```
# Toutes les 30 secondes
OCS.Client.update_session(call_id, %{}), current_usage)
```

Si MaxUsage retourne 0, l'abonné n'a pas de crédit → Envoyer ReleaseCall

4. Terminaison de l'Appel (EventReportBCSM - oDisconnect)

Lorsque l'appel se termine :

1. **Reçoit l'événement oDisconnect** - Du MSC
2. **Calcule la durée totale** - À partir de l'heure de début de la session
3. **Termine la session OCS** - API TerminateSession
4. **CDR généré** - Par OCS avec le coût final
5. **Nettoie la session** - Supprime de SessionStore
6. **Envoie ReleaseCall** - Confirme la terminaison au MSC

Analyse des CDR

Les CDR sont générés par votre OCS et incluent généralement :

Champs CDR de CAMEL :

- Account - IMSI ou numéro appelant
- Destination - Numéro de la partie appelée
- OriginID - Identifiant d'appel unique (CAMEL-OTID)
- Usage - Durée totale de l'appel (secondes)
- Cost - Coût calculé
- IMSI - IMSI de l'abonné
- CallingPartyNumber - A-partie
- CalledPartyNumber - B-partie
- MSAddress - Code de point MSC servant
- ServiceKey - Clé de service CAMEL

Tests

Test Manuel avec le Constructeur de Requêtes

1. Naviguer vers le Constructeur de Requêtes :

http://localhost/camel_request

2. Envoyer InitialDP :

- Sélectionner "InitialDP" dans le menu déroulant
- Clé de Service : 100
- Numéro Appelant : 14155551234
- Numéro Appelé : 14155556789
- Cliquer sur "Envoyer la Requête InitialDP"
- Noter l'OTID généré

3. Surveiller la Session :

- Ouvrir un nouvel onglet : http://localhost/camel_sessions
- Voir la session active avec l'état "Initié"

4. Simuler la Réponse à l'Appel :

- Retourner au Constructeur de Requêtes
- Sélectionner "EventReportBCSM"
- Type d'Événement : oAnswer
- Cliquer sur "Envoyer la Requête EventReportBCSM"
- L'état de la session change en "Répondu"

5. Terminer l'Appel :

- Sélectionner "ReleaseCall"
- Code de Cause : 16 (Normal)
- Cliquer sur "Envoyer la Requête ReleaseCall"
- L'état de la session change en "Terminé"

Test avec un MSC Réel

Configurer le Service CAMEL du MSC

Sur votre MSC/VLR, configurez le service CAMEL :

```
# Exemple de configuration MSC Huawei
ADD CAMELSERVICE:
  SERVICEID=1,
  SERVICEKEY=100,
  GSMSCFADRN="55512341234", # Titre Global CAMEL
  DEFAULTCALLHANDLING=CONTINUE;
```

```
ADD CAMELSUBSCRIBER:
  IMSI="310150123456789",
  SERVICEID=1,
  TRIGGERTYPE=TERMCALL;
```

Surveiller les Journaux

Regardez les journaux CAMELGW pour les messages CAP entrants :

```
# Voir les journaux en temps réel
tail -f /var/log/omniss7/omniss7.log
```

```
# Filtrer pour les événements CAP
grep "CAP:" /var/log/omniss7/omniss7.log
```

```
# Voir le journal des événements (format JSON)
curl http://localhost/api/events | jq '.[] | select(.map_event | startswith("CAP:"))'
```

Test de Charge

Utilisez le Constructeur de Requêtes dans une boucle pour les tests de charge :

```
# Envoyer 100 requêtes InitialDP
for i in {1..100}; do
  curl -X POST http://localhost/api/camel/initial_dp \
    -H "Content-Type: application/json" \
    -d '{
      "service_key": 100,
      "calling_number": "14155551234",
      "called_number": "14155556789"
    }'
  sleep 0.1
done
```

Surveillance & Opérations

Métriques Prometheus

CAMELGW expose des métriques à <http://localhost:8080/metrics> :

Métriques spécifiques à CAP :

- `cap_requests_total{operation}` - Total des requêtes CAP par type d'opération (par exemple, initialDP requestReportBCSMEvent)

Métriques MAP/API supplémentaires :

- `map_requests_total{operation}` - Total des requêtes MAP par type d'opération
- `map_request_duration_milliseconds{operation}` - Histogramme de durée des requêtes
- `map_pending_requests` - Nombre de transactions MAP en attente

Métriques STP M3UA (si le mode STP est activé) :

- `m3ua_stp_messages_received_total{peer_name,point_code}` - Messages reçus des pairs
- `m3ua_stp_messages_sent_total{peer_name,point_code}` - Messages envoyés aux pairs
- `m3ua_stp_routing_failures_total{reason}` - Échecs de routage par raison

Exemples de requêtes :

```
# Requêtes CAP
curl http://localhost:8080/metrics | grep cap_requests_total

# Total des InitialDP recus
curl http://localhost:8080/metrics | grep 'cap_requests_total{operation="initialDP"}'

# Requêtes MAP en attente
curl http://localhost:8080/metrics | grep map_pending_requests
```

Vérifications de Santé

```
# Vérifier la connectivité M3UA
curl http://localhost/api/m3ua-status

# Vérifier la connectivité OCS
curl http://localhost/api/ocs-status

# Vérifier les sessions actives
curl http://localhost/api/camel/sessions/count
```

Configuration des Journaux

Ajustez le niveau de journalisation dans config/runtime.exs :

```
config :logger,
  level: :info # Options : :debug, :info, :warning, :error

# Activer la journalisation de débogage CAP
config :logger, :console,
  metadata: [:cap_operation, :otid, :call_id]
```

Dépannage

Problème : Aucun message CAP reçu

Symptômes : Le Constructeur de Requêtes fonctionne, mais le MSC n'envoie pas l'InitialDP

Vérifiez :

- 1. État du lien M3UA : curl http://localhost/api/m3ua-status
- 2. Configuration du service CAMEL du MSC (Clé de Service, adresse gsmSCF)
- 3. Routage SSCP (Le Titre Global doit router vers CAMELWG)
- 4. Règles de pare-feu (autoriser le port SCTP 2905)

Solution :

```
# Vérifier la connectivité M3UA
tcpdump -i eth0 sctp

# Vérifier si le MSC peut atteindre CAMELWG
ss -tln | grep 2905
```

Problème : Erreurs OCS

Symptômes : INSUFFICIENT_CREDIT ou erreurs de délai d'attente

Vérifiez :

- 1. OCS est accessible : curl http://your-ocs-server/api/health
- 2. Le compte a un solde dans OCS
- 3. Plan de tarification configuré dans OCS
- 4. Connectivité réseau vers OCS
- 5. Le jeton d'authentification est valide (si requis)

Solution :

- Vérifiez la configuration de l'URL OCS dans runtime.exs
- Vérifiez les journaux OCS pour des erreurs
- Testez l'API OCS manuellement avec curl
- Vérifiez que les règles de pare-feu permettent la connectivité

Problème : Session non trouvée

Symptômes : EventReportBCSM échoue avec "Session non trouvée"

Cause : Mismatch d'OTID ou session expirée

Solution :

- 1. Vérifiez l'OTID dans les journaux
- 2. Vérifiez le délai d'expiration de la session (par défaut : pas d'expiration)
- 3. Assurez-vous que le DTID correspond à l'OTID dans les messages Continue/End

```
# Vérifier les sessions actives
iex> CAMELWG.SessionStore.list_sessions()
```

Problème : Erreurs de décodage

Symptômes : Failed to decode InitialDP dans les journaux

Cause : Mismatch de version CAP ou message malformé

Solution :

- 1. Vérifiez que la configuration de la version CAP correspond au MSC
- 2. Vérifiez que l'encodage ASN.1 est correct
- 3. Capturez PCAP et analysez avec Wireshark

```
# Capturez les messages CAP
tcpdump -i eth0 -w cap_trace.pcap sctp port 2905

# Analysez avec Wireshark (filtre : m3ua)
wireshark cap_trace.pcap
```

Configuration Avancée

Plusieurs Versions CAP

Supportez différentes versions CAP par clé de service :

```
config :omniess7,
  cap_version_map: %{
    100 => :v2, # La clé de service 100 utilise CAP v2
    200 => :v3, # La clé de service 200 utilise CAP v3
    300 => :v4 # La clé de service 300 utilise CAP v4
  },
  cap_version: :v2 # Par défaut
```

Résumé

Le mode Passerelle CAMEL permet à OmniSS7 de fonctionner comme une plateforme complète de Réseau Intelligent avec :

- ◊ **Support complet du protocole CAP** (v1/v2/v3/v4)
- ◊ **Facturation en temps réel** via l'intégration OCS
- ◊ **Opérations de contrôle d'appel** (Connect, Release, Continue)
- ◊ **Gestion des sessions** avec stockage ETS
- ◊ **Tests interactifs** via le Constructeur de Requêtes de l'Interface Web
- ◊ **Surveillance en direct** des sessions d'appel actives
- ◊ **Génération de CDR** pour la facturation et l'analyse
- ◊ **Performance et fiabilité prêtes pour la production**

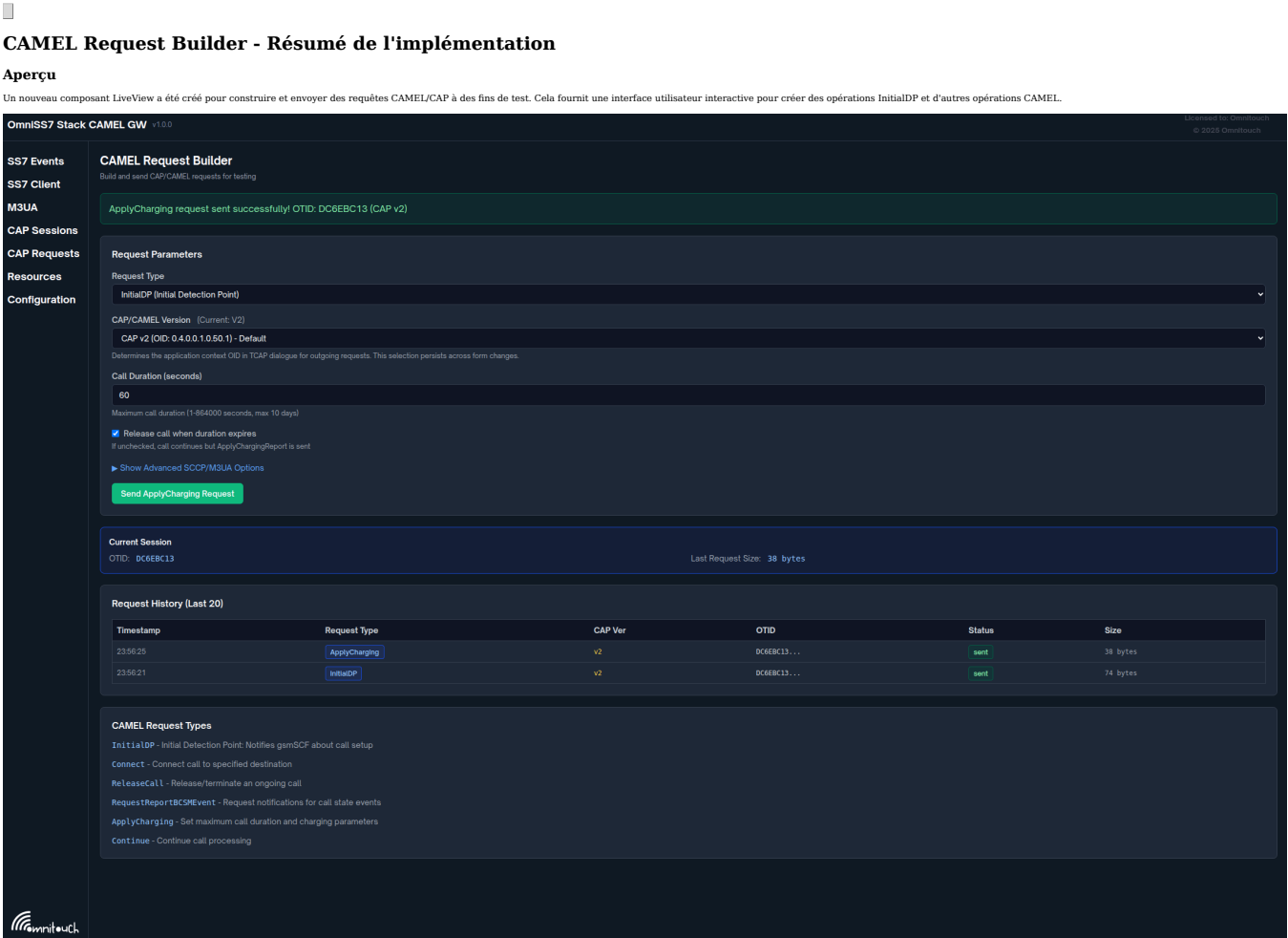
Pour des informations supplémentaires :

- [Documentation du Constructeur de Requêtes CAMEL](#)
- [Référence Technique - Opérations CAP](#)

Produit : Passerelle CAMEL OmniSS7

Versión de la Documentation : 1.0

Dernière Mise à Jour : 2025-10-26



Nouveaux composants

1. CAMEL Request Builder LiveView

Fonctionnalités :

- Interface utilisateur interactive basée sur un formulaire pour construire des requêtes CAMEL
- Support pour plusieurs types de requêtes :
 - InitialDP** - Point de Détection Initiale (notification de configuration d'appel)
 - Connect** - Connecter l'appel à la destination
 - ReleaseCall** - Libérer/terminer l'appel
 - RequestReportBCSMEvent** - Demander des notifications d'événements
 - Continue** - Continuer le traitement de l'appel
 - ApplyCharging** - Appliquer des limites de facturation/durée aux appels

Capacités clés :

- Menu déroulant de sélection du type de requête
- Champs de formulaire dynamiques en fonction du type de requête sélectionné
- Options SCCP/M3UA avancées (section réductible)
 - Titres globaux de la partie appelée/appelante
 - Configuration du SSN (Numéro de sous-système)
 - Paramètres OPC/DPC (Code de point)
- Historique des requêtes en temps réel (20 dernières requêtes)
- Suivi de session via OTID
- Retour d'information sur le succès/erreur
- Suivi de la taille de la requête

Route : /camel_request

2. Journal d'événements amélioré avec support CAMEL

Nouvelles fonctions :

- paklog_camel/2 - Journalisation dédiée des messages CAMEL/CAP
- lookup_cap_opcode_name/1 - Recherche du code d'opération CAP
- find_cap_opcode/1 - Extraire le code d'opération CAP à partir de JSON
- extract_cap_tids/1 - Extraire OTID/DTID des messages CAP
- format_cap_to_json/1 - Convertir les PDU CAP en format JSON

Codes d'opération CAP pris en charge :

```
0 => "initialDP"
5 => "connect"
6 => "releaseCall"
7 => "requestReportBCSMEvent"
8 => "eventReportBCSM"
10 => "continue"
13 => "furnishChargingInformation"
35 => "applyCharging"
... (47 opérations au total)
```

Fonctionnalités :

- Journalisation JSON de toutes les requêtes/réponses CAMEL
- Détection automatique des actions TCAP (Début/Continuer/Fin/Abandon)
- Extraction d'adressage SCCP
- Gestion des erreurs pour les messages malformés
- Traitement des tâches en arrière-plan (non-bloquant)
- Événement préfixé par "CAP:" pour un filtrage facile

3. CapClient mis à jour

Modifications :

- Ajout d'appels paklog_camel/2 pour les messages entrants et sortants
- Journalisation double : MAP (paklog) et CAP (paklog_camel) pour la compatibilité
- Messages sortants journalisés dans sccp_m3ua_maker/2
- Messages entrants journalisés dans handle_payload/1

Configuration

Les nouvelles pages LiveView ont été ajoutées à la configuration d'exécution :

Fichier : config/runtime.exs

```
config :control_panel,
  use_additional_pages: [
    {S57.Web.EventsLive, "/events", "Événements S57"},
    {S57.Web.TestClientLive, "/client", "Client S57"},
    {S57.Web.M3UAStatusLive, "/m3ua", "M3UA"},
    {S57.Web.HlrLinksLive, "/hlr_links", "Liens HLR"},
    {S57.Web.CAMELSessionsLive, "/camel_sessions", "Sessions CAMEL"},
    {S57.Web.CAMELRequestLive, "/camel_request", "Constructeur de requêtes CAMEL"}
  ],
  page_order: ["/events", "/client", "/m3ua", "/hlr_links",
               "/camel_sessions", "/camel_request",
               "/application", "/configuration"]
```

Utilisation

Accéder au Constructeur de Requêtes

1. Naviguez vers : https://your-server:8087/camel_request
2. Sélectionnez le type de requête dans le menu déroulant
3. Remplissez les paramètres requis
4. Optionnellement, développez "Options SCCP/M3UA Avancées" pour un réglage fin
5. Cliquez sur "Envoyer [RequestType] Requête"

Flux de Requête

InitialDP (Nouvel Appel)

1. Définir la Clé de Service (par exemple, 100)
2. Définir le Numéro Appelant (A-Party)
3. Définir le Numéro Appelé (B-Party)
4. Envoyer la requête → Génère un nouvel OTID
5. OTID stocké dans la session pour les requêtes de suivi

Requêtes de Suivi (Connect, ReleaseCall, etc.)

1. Doit avoir un OTID actif de l'InitialDP
2. La requête utilise automatiquement l'OTID stocké
3. Avertissement affiché si aucun OTID actif

Paramètres de Requête

InitialDP :

- Clé de Service (entier)
- Numéro Appelant (format ISDN)
- Numéro Appelé (format ISDN)

Connect :

- Numéro de Destination (où acheminer l'appel)

ReleaseCall :

- Code de Cause (16 = Normal, 17 = Occupé, 31 = Non spécifié)

RequestReportBCSMEvent :

- Événements BCSM (séparés par des virgules : oAnswer, oDisconnect, etc.)

Continue :

- Aucun paramètre (utilise l'OTID actif)

ApplyCharging :

- Durée (secondes, 1-864000) - Durée maximale de l'appel avant action
- Libérer en cas de dépassement de délai (booléen) - Si l'appel doit être libéré lorsque la durée expire

Options Avancées

Adressage SCCP :

- GT de la Partie Appelée (Titre Global)
- GT de la Partie Appelante
- SSN Appelé (par défaut 146 = gsmSSF)
- SSN Appelant (par défaut 146)

Codes de Point M3UA :

- OPC (Code de Point d'origine, par défaut 5013)
- DPC (Code de Point de destination, par défaut 5011)

Journalisation JSON

Tous les messages CAMEL sont désormais journalisés au format JSON dans le journal des événements avec :

- **Direction** : entrant/sortant
- **Action TCAP** : Début/Continuer/Fin/Abandon
- **Opération CAP** : par exemple, "CAP:initialDP", "CAP:connect"
- **Adressage SCCP** : Informations sur la Partie Appelée/Appelante
- **TID** : OTID/OTID pour la corrélation
- **Message Complet** : PDU CAP encodé en JSON

Exemple d'Entrée de Journal

```
{
  "map_event": "CAP:initialDP",
  "direction": "outgoing",
  "tcap_action": "Begin",
  "otid": "A1B2C3D4",
  "sccp_called": {
    "SSN": 146,
    "GlobalTitle": {
      "Digits": "55512341234",
      "NumberingPlan": "isdn_tele",
      "NatureOfAddress_Indicator": "International"
    }
  },
  "event_message": "{ ... full CAP PDU ... }"
}
```

Historique des Requêtes

L'interface utilisateur affiche les 20 dernières requêtes avec :

- Horodatage
- Type de requête (avec badge codé par couleur)
- OTID (premiers 8 caractères hexadécimaux)
- Statut (envoyé/erreur)
- Taille du message en octets

Suivi de Session

Panneau d'Informations de Session Actuelle :

- Affiche l'OTID actif
- Montre la taille du dernier message en octets
- Visible uniquement lorsque la session est active

Flux de Travail de Test

1. Démarrer un Nouvel Appel :

- Envoyer InitialDP → Obtenir OTID
- Le système crée une session

2. Contrôler l'Appel :

- Envoyer RequestReportBCSMEvent → Demander des notifications
- Envoyer ApplyCharging → Définir la limite de durée de l'appel (par exemple, 290 secondes)
- Envoyer Connect → Acheminer vers la destination
- OU Envoyer ReleaseCall → Terminer

3. Voir les Résultats :

- Vérifier l'historique des requêtes
- Surveiller la page des Sessions CAMEL
- Examiner les journaux d'événements avec le préfixe "CAP :"

ApplyCharging - Contrôle de Durée d'Appel

Aperçu

L'opération ApplyCharging vous permet de définir une durée maximale d'appel et éventuellement de libérer l'appel lorsque cette durée expire. Cela est généralement utilisé pour des scénarios de facturation prépayée ou pour imposer des limites de temps sur les appels.

Cas d'Utilisation

- **Facturation Prépayée** : Limiter la durée d'appel en fonction du solde de l'abonné
- **Facturation Basée sur le Temps** : Imposer des intervalles de facturation périodiques

- **Gestion des Ressources** : Empêcher les appels de se prolonger indéfiniment
- **Intégration OCS** : Coordonner avec les systèmes de facturation en ligne pour le contrôle de crédit en temps réel

Paramètres

Durée (maxCallPeriodDuration)

- **Type** : Entier (1-864000 secondes)
- **Description** : Nombre maximum de secondes que l'appel peut durer avant que le minuteur expire
- **Exemples** :
 - 60 = 1 minute
 - 290 = 4 minutes 50 secondes (valeur de test courante)
 - 3600 = 1 heure
 - 86400 = 24 heures

Libérer en cas de dépassement de délai (releaseIfDurationExceeded)

- **Type** : Booléen (vrai/faux)
- **Par défaut** : vrai
- **Description** : Que se passe-t-il lorsque la durée expire :
 - vrai : Libérer/déconnecter automatiquement l'appel
 - Faux : Envoyer une notification mais garder l'appel actif (permet à gsmSCF d'agir)

Structure du Message

Le message ApplyCharging est encodé en tant que TCAP Continue avec :

- **TCAP** : Message Continue (utilise la transaction existante)
- **Opcode** : 35 (applyCharging)
- **Paramètres** : ApplyChargingArg contenant :
 - aChBillingChargingCharacteristics : Informations de facturation basées sur le temps
 - TimeDurationCharging : Durée maximale et indicateur de libération
 - partyToCharge : Quelle partie est facturée (par défaut : sendingSideID)

Exemple d'Utilisation

Scénario : Appel prépayé avec limite de 5 minutes

1. Envoyer **InitialDP** pour commencer la surveillance de l'appel

```
Clé de Service : 100
Appelant : 447700900123
Appelé : 447700900456
→ OTID : A182C3D4
```

2. Envoyer **ApplyCharging** pour définir la limite de 5 minutes

```
Durée : 300 (secondes)
Libérer en cas de dépassement de délai : vrai
→ Utilise OTID : A182C3D4
```

3. Envoyer **Connect** pour compléter l'appel

```
Destination : 447700900456
→ Utilise OTID : A182C3D4
```

4. Après 5 minutes (300 secondes) :

- L'appel est automatiquement libéré par le réseau
- gsmSCF reçoit une notification de déconnexion

Meilleures Pratiques

1. **Envoyer toujours ApplyCharging AVANT Connect**

- Assure que la facturation est active lorsque l'appel se connecte
- Empêche les segments d'appel non facturés

2. **Utiliser avec RequestReportBCSMEvent**

- Demander les événements oAnswer et oDisconnect
- Permet de suivre la durée réelle de l'appel
- Permet de réappliquer la facturation si nécessaire

3. **Définir des durées raisonnables**

- Trop court : Opérations de facturation fréquentes, mauvaise expérience utilisateur
- Trop long : Risque de perte de revenus sur les appels prépayés
- Typique : 60-300 secondes pour prépayé, plus long pour postpayé

4. **Gérer le dépassement de délai de manière élégante**

- Si release=false, être prêt à gérer les notifications d'expiration du minuteur
- Implémenter une logique pour prolonger la durée ou libérer l'appel

Gestion des Erreurs

Problèmes courants :

- **Aucun OTID actif** : Doit envoyer InitialDP d'abord
- **Durée invalide** : Doit être de 1 à 864000 secondes
- **Support réseau** : Certaines implémentations SSF peuvent ne pas prendre en charge ApplyCharging
- **Précision du minuteur** : La résolution du minuteur réseau est généralement de 1 seconde, mais peut varier

Surveillance

Suivre les opérations ApplyCharging via :

- **Historique des Requêtes** : Montre les requêtes ApplyCharging envoyées
- **Journal des Événements** : Rechercher "CAP:applyCharging"
- **Sessions CAMEL** : Surveiller les sessions actives avec facturation appliquée
- **Trace TCAP** : Débugger les problèmes d'encodage/décodage

Détails de l'Implémentation

Gestion de l'État

- LiveView assigne l'état du formulaire de suivi
- OTID stocké dans les assignations de socket
- Historique des requêtes limité à 20 entrées
- Actualisation automatique désactivée (envoi manuel uniquement)

Génération de Requêtes

- Utilise le module existant CapRequestGenerator
- Construit les structures TCAP/CAP appropriées
- Encode avec le code: TCAPMessages
- Enveloppe dans SCCP via CapClient.sccp_m3ua_maker/2

Mécanisme d'Envoi

- Envoie via M3UA à : camelgw_client_osp
- Utilise le contexte de routage 1
- Encapsulation automatique SCCP/M3UA

Gestion des Erreurs

- Validation du formulaire avec retour d'information utilisateur
- Gestion élégante de l'OTID manquant
- Erreurs d'analyse affichées dans l'interface utilisateur
- Échecs d'encodage journalisés

Améliorations Futures

Ajouts potentiels :

1. Modèles/prunets de requêtes
2. Corrélation et affichage des réponses
3. Visualisation du flux d'appel
4. Détails de session en profondeur
5. Exporter l'historique des requêtes
6. Tests de charge (requêtes en masse)
7. Export PCAP des messages générés
8. Validation des paramètres CAP

Notes d'Intégration

- Compatible avec la journalisation MAP existante (pak.log)
- Partage la base de données de journal d'événements avec les événements MAP
- Utilise la même infrastructure SCCP/M3UA
- Fonctionne avec CAMELSessionsLive pour la surveillance
- S'intègre avec le routage M3UA existant

Fichiers Modifiés

- config/runtime.exs - MIS À JOUR

Dépendances

- CapRequestGenerator existant
- CapClient pour l'envoi M3UA
- M3UA.Server pour la transmission de paquets

- EventLog pour la journalisation des messages
- Cadre Phoenix LiveView
- Panneau de Contrôle pour l'infrastructure de l'interface utilisateur



Guide des Fonctionnalités Communes

[-- Retour à la Documentation Principale](#)

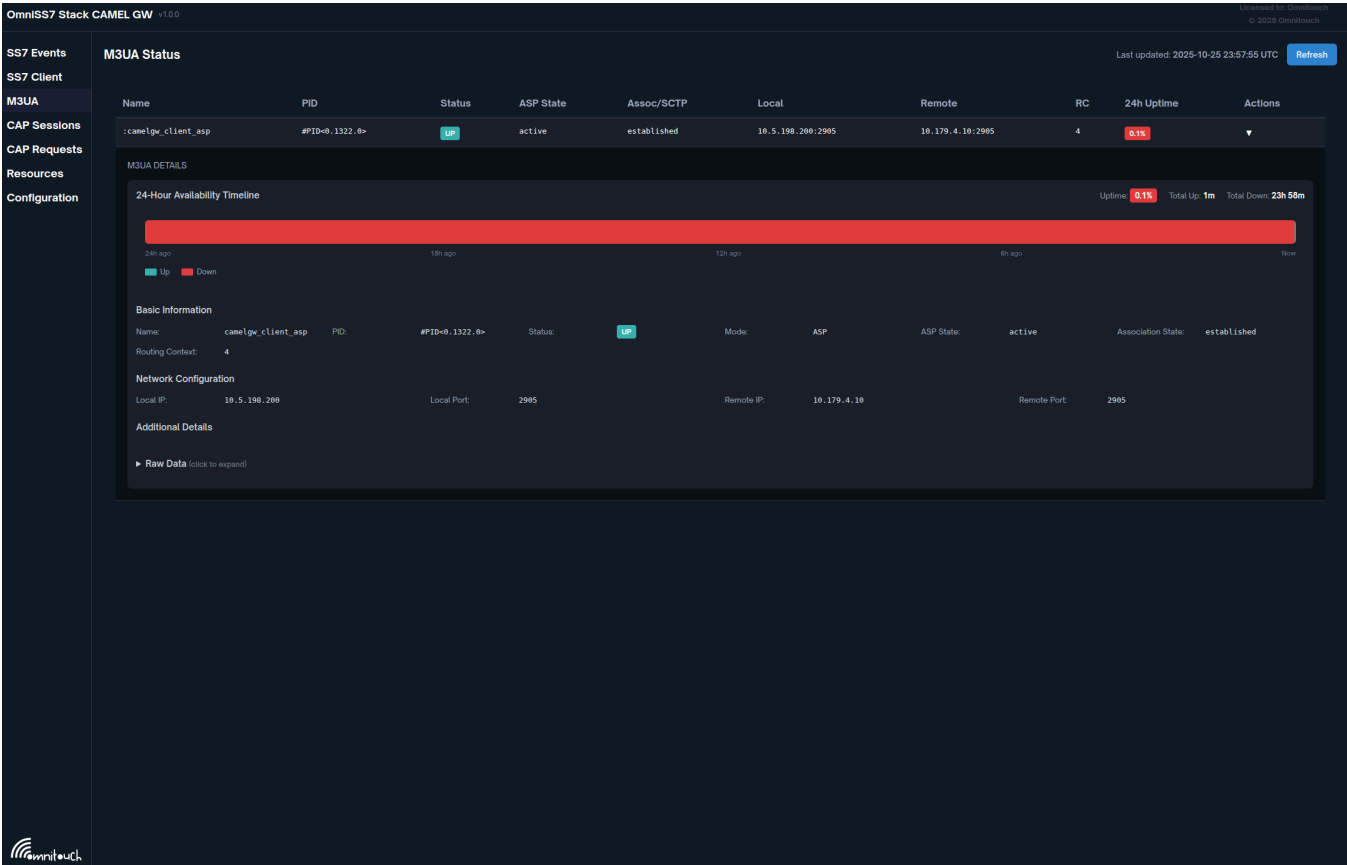
Ce guide couvre les fonctionnalités communes à tous les modes de fonctionnement d'OmniSS7.

Table des Matières

- 1. [Aperçu de l'Interface Web](#)
- 2. [Documentation de l'API](#)
- 3. [Surveillance et Métriques](#)
- 4. [Meilleures Pratiques](#)

Aperçu de l'Interface Web

L'interface Web est accessible via l'adresse de votre serveur web configuré.



Navigation Principale

- **Événements** - Événements de signalisation SS7 en temps réel et journaux de messages
- **Application** - État de l'application et informations d'exécution
- **Configuration** - Visualiseur de configuration du système
- **État M3UA** - Connexions de pairs M3UA (mode STP)
- **File d'attente SMS** - Messages SMS sortants (mode SMSc)

Accéder à l'Interface Web

1. Ouvrez votre navigateur web
2. Naviguez vers le nom d'hôte configuré (par exemple, <http://localhost>)
3. Consultez le tableau de bord de l'état du système

Documentation de l'API Swagger

Documentation API interactive :

<http://your-server/swagger>

Configuration de l'Interface Web

Configurer dans `config/runtime.exs` :

```
config :control_panel,
  # Ordre des pages dans le menu de navigation
  page_order: ["/events", "/application", "/configuration"],

  # Paramètres du serveur web
  web: %{
    listen_ip: "0.0.0.0", # IP à lier (0.0.0.0 pour toutes les interfaces)
    port: 80, # Port HTTP (443 pour HTTPS)
    hostname: "localhost", # Nom d'hôte du serveur pour la génération d'URL
    enable_tls: false, # Mettre vrai pour activer HTTPS
    tls_cert: "cert.pem", # Chemin vers le fichier de certificat TLS
    tls_key: "key.pem" # Chemin vers le fichier de clé privée TLS
  }
```

Paramètres de Configuration :

Paramètre	Type	Par Défaut	Description
page_order	Liste	["/events", "/application", "/configuration"]	Ordre des pages dans le menu de navigation
listen_ip	Chaîne	"0.0.0.0"	Adresse IP à lier au serveur web
port	Entier	80	Port HTTP (utiliser 443 pour HTTPS)
hostname	Chaîne	"localhost"	Nom d'hôte du serveur pour la génération d'URL
enable_tls	Booléen	false	Activer HTTPS avec TLS
tls_cert	Chaîne	"cert.pem"	Chemin vers le certificat TLS (lorsque TLS activé)
tls_key	Chaîne	"key.pem"	Chemin vers la clé privée TLS (lorsque TLS activé)

Configuration du Logger

Configurer le niveau de journalisation dans `config/runtime.exs` :

```
config :logger,
  level: :debug # Options : :debug, :info, :warning, :error
```

Niveaux de Journalisation :

- `:debug` - Informations détaillées de débogage
- `:info` - Messages d'information généraux
- `:warning` - Messages d'avertissement pour des problèmes potentiels

- `error` - Messages d'erreur uniquement

Documentation de l'API

URL de Base de l'API

http://your-server/api

Codes de Réponse

- **200** - Succès
- **400** - Mauvaise Demande
- **504** - Délai d'Attente de la Passerelle

Spécification OpenAPI

http://your-server/swagger.json

Surveillance et Métriques

Point de Terminalson des Métriques Prometheus

http://your-server/metrics

Catégories de Métriques Clés

Métriques M3UA/SCTP :

- Changements d'état d'association SCTP
- Transitions d'état ASP M3UA
- Unités de données de protocole envoyées/reçues

Métriques M2PA :

- Transitions d'état de lien (DOWN → ALIGNMENT → PROVING → READY)
- Messages et octets envoyés/reçus par lien
- Erreurs spécifiques au lien (décodage, encodage, SCTP)

Métriques STP :

- Messages reçus/envoyés par pair
- Échecs de routage par raison
- Distribution du trafic entre les pairs

Métriques Client MAP :

- Requêtes MAP par type d'opération
- Histogrammes de durée des requêtes
- Jauge des transactions en attente

Métriques CAP :

- Requêtes CAP par type d'opération
- Opérations de passerelle CAMEL

Métriques SMSc :

- Profondeur de la file d'attente
- Taux de livraison
- Messages échoués

Intégration Grafana

Les métriques d'OmniSS7 sont compatibles avec Prometheus et Grafana.

Meilleures Pratiques

Recommandations de Sécurité

- Isolation du Réseau**
 - Déployer dans un VLAN dédié
 - Règles de pare-feu pour restreindre l'accès
 - Autoriser SCTP uniquement à partir d'adresses connues
- Sécurité de l'Interface Web**
 - Activer TLS pour la production
 - Utiliser un proxy inverse avec authentification
 - Restreindre aux IPs de gestion
- Sécurité de l'API**
 - Mettre en œuvre une limitation de débit
 - Utiliser des clés API ou OAuth
 - Journaliser toutes les requêtes pour audit

Optimisation des Performances

- Limites TPS**
 - Configurer un TPS approprié
 - Surveiller la charge du système
 - Ajuster les tampons SCTP
- Optimisation de la Base de Données**
 - Ajouter des index
 - Archiver les anciens messages
 - Surveiller le pool de connexions
- Ajustement M3UA**
 - Ajuster les intervalles de battement SCTP
 - Configurer les valeurs de délai d'attente
 - Utiliser plusieurs liens pour la redondance

Surveillance et Alerte

Métriques Clés :

- État de connexion M3UA
- Taux de réussite des requêtes MAP
- Temps de réponse de l'API
- Profondeur de la file d'attente de messages

Seuils d'Alerte :

- M3UA hors service > 1 minute
- Taux de délai d'attente MAP > 10%
- Profondeur de la file d'attente > 1000
- Taux d'erreur de l'API > 5%

Référence Complète de Configuration

Tous les Paramètres de Configuration

Cette section fournit une référence complète de tous les paramètres de configuration disponibles dans tous les modes de fonctionnement.

Configuration du Logger (:logger)

```
config :logger,
  level: :debug # :debug | :info | :warning | :error
```

Configuration de l'Interface Web (:control_panel)

```
config :control_panel,
  page_order: ["/events", "/application", "/configuration"],
  web: %{
    listen_ip: "0.0.0.0",
    port: 80,
    hostname: "localhost",
    enable_tls: false,
    tls_cert: "cert.pem",
    tls_key: "key.pem"
  }
```

Paramètre	Type	Requis	Par Défaut	Description
page_order	Liste de Chaînes	Non	["/events", "/application", "/configuration"]	Ordre des pages du menu de navigation
web.listen_ip	Chaîne	Oui	"0.0.0.0"	Adresse IP à lier au serveur web
web.port	Entier	Oui	80	Numéro de port HTTP/HTTPS
web.hostname	Chaîne	Oui	"localhost"	Nom d'hôte du serveur
web.enable_tls	Booléen	Non	false	Activer HTTPS
web.tls_cert	Chaîne	Si TLS activé	"cert.pem"	Chemin vers le certificat TLS
web.tls_key	Chaîne	Si TLS activé	"key.pem"	Chemin vers la clé privée TLS

Configuration STP M3UA (:omiss7)

```
config :omiss7,
  m3ua_stp: %{
    enabled: false,
    local_ip: (127, 0, 0, 1),
    local_port: 2905
  },
  enable_gt_routing: true,
  m3ua_peers: [...],
  m3ua_routes: [...],
  m3ua_gt_routes: [...]
```

Paramètre	Type	Requis	Par Défaut	Description
m3ua_stp.enabled	Boolean	Oui	false	Activer le mode STP au démarrage
m3ua_stp.local_ip	Tuple	Oui	(127, 0, 0, 1)	IP à lier pour M3UA entrant
m3ua_stp.local_port	Entier	Oui	2905	Port SCTP pour M3UA
enable_gt_routing	Boolean	Non	false	Activer le routage de titre global

Paramètres de Pair M3UA :

Paramètre	Type	Requis	Description
peer_id	Entier	Oui	Identifiant unique du pair
name	Chaine	Oui	Nom descriptif du pair
role	Atome	Oui	:client ou :server
local_ip	Tuple	Si :client	IP locale à lier
local_port	Entier	Si :client	Port local (0 pour dynamique)
remote_ip	Tuple	Oui	IP du pair distant
remote_port	Entier	Si :client	Port du pair distant
routing_context	Entier	Oui	Contexte de routage M3UA
point_code	Entier	Oui	Code de point SS7
network_indicator	Atome	Non	:international ou :national

Paramètres de Route M3UA :

Paramètre	Type	Requis	Description
dest_pc	Entier	Oui	Code de point de destination
peer_id	Entier	Oui	Pair à travers lequel router
priority	Entier	Oui	Priorité de la route (plus bas = plus haute priorité)
network_indicator	Atome	Non	:international ou :national

Paramètres de Route GT M3UA :

Paramètre	Type	Requis	Description
gt_prefix	Chaine	Oui	Préfixe de Titre Global à correspondre
peer_id	Entier	Oui	Pair de destination
priority	Entier	Oui	Priorité de la route
description	Chaine	Non	Description de la route pour journalisation
source_ssn	Entier	Non	Correspondre uniquement si SSN source correspond
dest_ssn	Entier	Non	Réécrite le SSN de destination à cette valeur

Configuration Client MAP (:omiss7)

```
config :omiss7,
  map_client_enabled: false,
  map_client_m3ua: %{
    mode: "ASP",
    callback: (MapClient, :handle_payload, []),
    process_name: :map_client_asp,
    local_ip: (10, 0, 0, 100),
    local_port: 2905,
    remote_ip: (10, 0, 0, 1),
    remote_port: 2905,
    routing_context: 1
  }
```

Paramètre	Type	Requis	Par Défaut	Description
map_client_enabled	Boolean	Oui	false	Activer le mode client MAP
map_client_m3ua.mode	Chaine	Oui	"ASP"	Mode de connexion M3UA ("ASP" ou "SGP")
map_client_m3ua.callback	Tuple	Oui	(MapClient, :handle_payload, [])	Gestionnaire de rappel de message
map_client_m3ua.process_name	Atome	Oui	:map_client_asp	Nom de processus enregistré
map_client_m3ua.local_ip	Tuple	Oui	-	Adresse IP locale
map_client_m3ua.local_port	Entier	Oui	2905	Port SCTP local
map_client_m3ua.remote_ip	Tuple	Oui	-	IP STP/SGP distante
map_client_m3ua.remote_port	Entier	Oui	2905	Port SCTP distant
map_client_m3ua.routing_context	Entier	Oui	-	Contexte de routage M3UA

Configuration du Centre SMS (:omiss7)

```
config :omiss7,
  auto_flush_enabled: false,
  auto_flush_interval: 10_000,
  auto_flush_dest_smsc: nil,
  auto_flush_tps: 10
```

Paramètre	Type	Requis	Par Défaut	Description
auto_flush_enabled	Boolean	Non	false	Activer le vidage automatique de la file d'attente SMS
auto_flush_interval	Entier	Non	10000	Intervalle de sondage de la file d'attente (millisecondes)
auto_flush_dest_smsc	Chaine	nil	nil	Filtrer par SMSC de destination (nil = tous)
auto_flush_tps	Entier	Non	10	Transactions maximales par seconde

Configuration de l'API HTTP (:omiss7)

Le backend SMS utilise maintenant l'API HTTP au lieu de connexions directes à la base de données.

```
config :omiss7,
  smsc_api_base_url: "https://10.5.198.200:8443",
  frontend_name: "omni-smsc01" # Optionnel : par défaut au nom d'hôte_SMSC
```

Paramètres de l'API :

Paramètre	Type	Requis	Par Défaut	Description
smsc_api_base_url	Chaine	Oui	"https://10.5.198.200:8443"	URL de base pour l'API backend SMS
frontend_name	Chaine	Non	"{hostname}_SMSc"	Identifiant de frontend pour l'enregistrement

Points de Terminaison de l'API Utilisés :

- POST /api/frontends - Enregistrer cette instance de frontend avec le backend
- POST /api/messages_raw - Insérer de nouveaux messages SMS
- GET /api/messages - Récupérer la file d'attente de messages (avec l'en-tête smsc)
- PATCH /api/messages/{id} - Marquer le message comme livré
- PUT /api/messages/{id} - Mettre à jour l'état du message
- POST /api/events - Ajouter le suivi des événements
- GET /api/status - Point de terminaison de vérification de santé

Enregistrement du Frontend :

Le système s'enregistre automatiquement auprès de l'API backend au démarrage et se réenregistre toutes les 5 minutes. L'enregistrement inclut :

- Nom et type de frontend (SMSc)
- Nom d'hôte
- Temps de fonctionnement en secondes
- Détails de configuration (format JSON)

Remarques de Configuration :

- La vérification SSL est désactivée par défaut pour les certificats auto-signés
- Les requêtes HTTP expirent après 5 secondes
- Tous les horodatages sont au format ISO 8601
- L'API utilise JSON pour les corps de requête/réponse

Documentation Connexe

- [← Retour à la Documentation Principale](#)
- [Guide STP](#)
- [Guide Client MAP](#)
- [Guide Centre SMS](#)
- [Guide HLIR](#)



Référence de Configuration

[← Retour à la Documentation Principale](#)

Ce document fournit une référence complète pour tous les paramètres de configuration d'OmniSS7.

Table des Matières

1. [Aperçu](#)
2. [Drapeaux de Mode Opérationnel](#)
3. [Paramètres de Mode HLR](#)
4. [Paramètres de Mode SMSc](#)
5. [Paramètres de Mode STP](#)
6. [Paramètres de NAT de Titre Global](#)
7. [Paramètres de Connexion M3UA](#)
8. [Paramètres du Serveur HTTP](#)
9. [Paramètres de Base de Données](#)
10. [Valeurs Codées en Dur](#)

Aperçu

La configuration d'OmniSS7 est gérée via `config/runtime.exs`. Le système prend en charge trois modes opérationnels :

- **Mode STP** - Point de Transfert de Signal pour le routage
- **Mode HLR** - Registre de Localisation Domiciliaire pour la gestion des abonnés
- **Mode SMSc** - Centre SMS pour la livraison de messages

Fichier de Configuration : `config/runtime.exs`

Drapeaux de Mode Opérationnel

Contrôle quelles fonctionnalités sont activées.

Paramètre	Type	Par Défaut	Description	Modes
<code>map_client_enabled</code>	Boolean	false	Activer le client MAP et la connectivité M3UA	Tous
<code>hlr_mode_enabled</code>	Boolean	false	Activer les fonctionnalités spécifiques au HLR	HLR
<code>smsc_mode_enabled</code>	Boolean	false	Activer les fonctionnalités spécifiques au SMSc	SMSc

Exemple :

```
config :omniss7,  
  map_client_enabled: true,  
  hlr_mode_enabled: true,  
  smsc_mode_enabled: false
```

Paramètres de Mode HLR

Configuration pour le mode HLR (Registre de Localisation Domiciliaire).

Configuration de l'API HLR

Paramètre	Type	Par Défaut	Requis	Description
hlr_api_base_url	String	-	Oui	URL du point de terminaison de l'API HLR backend (vérification SSL codée en dur désactivée)
hlr_service_center_gt_address	String	-	Oui	Adresse de Titre Global HLR retournée dans les réponses UpdateLocation
smsc_service_center_gt_address	String	-	Oui	Adresse GT SMSc retournée dans les réponses SRI-for-SM

Exemple :

```
config :omniss7,  
  hlr_api_base_url: "https://10.180.2.140:8443",  
  hlr_service_center_gt_address: "55512341111",  
  smsc_service_center_gt_address: "55512341112"
```

Mapping MSISDN ↔ IMSI

Configuration pour la génération d'IMSI synthétiques à partir de MSISDN. Pour une explication technique détaillée de l'algorithme de mapping, voir [Mapping MSISDN ↔ IMSI dans le Guide HLR](#).

Paramètre	Type	Par Défaut	Requis	Description
hlr_imsi_plmn_prefix	String	"50557"	Non	Préfixe PLMN (MCC+MNC) pour la génération d'IMSI synthétiques
hlr_msisdn_country_code	String	"61"	Non	Préfixe de code pays pour le mapping inverse IMSI→MSISDN
hlr_msisdn_nsn_offset	Integer	0	Non	Décalage dans le MSISDN où commence le NSN (typiquement la longueur du code pays)
hlr_msisdn_nsn_length	Integer	9	Non	Longueur du Numéro d'Abonné National à extraire du MSISDN

Exemple (code pays à 2 chiffres) :

```
config :omniss7,  
  hlr_imsi_plmn_prefix: "50557",      # MCC 505 + MNC 57  
  hlr_msisdn_country_code: "99",      # Exemple de code pays à 2 chiffres  
  hlr_msisdn_nsn_offset: 2,           # Ignorer le code pays à 2 chiffres  
  hlr_msisdn_nsn_length: 9            # Extraire le NSN à 9 chiffres
```

Exemple (code pays à 3 chiffres) :

```
config :omniss7,  
  hlr_imsi_plmn_prefix: "50557",      # MCC 505 + MNC 57  
  hlr_msisdn_country_code: "999",      # Exemple de code pays à 3 chiffres  
  hlr_msisdn_nsn_offset: 3,           # Ignorer le code pays à 3 chiffres  
  hlr_msisdn_nsn_length: 8            # Extraire le NSN à 8 chiffres
```

Important : Définissez `nsn_offset` sur la longueur de votre code pays pour extraire correctement le NSN. Par exemple :

- Code pays "9" (1 chiffre) → `nsn_offset: 1`
- Code pays "99" (2 chiffres) → `nsn_offset: 2`
- Code pays "999" (3 chiffres) → `nsn_offset: 3`

Configuration InsertSubscriberData (ISD)

Configuration pour les données de provisionnement des abonnés envoyées aux VLR lors de UpdateLocation. Pour une explication détaillée de la séquence ISD et du flux de messages, voir [Configuration InsertSubscriberData dans le Guide HLR](#).

Paramètre	Type	Par Défaut	Requis	Description
isd_network_access_mode	Atom	:packetAndCircuit	Non	Type d'accès réseau : :packetAndCircuit, :packetOnly, ou :circuitOnly
isd_send_ss_data	Boolean	true	Non	Envoyer ISD #2 avec les données des Services Supplémentaires
isd_send_call_barring	Boolean	true	Non	Envoyer ISD #3 avec les données de Blocage d'Appels

Exemple :

```
config :omniss7,  
  isd_network_access_mode: :packetAndCircuit,  
  isd_send_ss_data: true,  
  isd_send_call_barring: true
```

Configuration CAMEL

Configuration pour le routage d'appels intelligents basé sur CAMEL. Pour une explication détaillée de l'intégration CAMEL et des clés de service, voir [Intégration CAMEL dans le Guide HLR](#).

Paramètre	Type	Par Défaut	Requis	Description
camel_service_key	Integer	11_110	Non	Clé de service CAMEL pour les réponses SRI
camel_trigger_detection_point	Atom	:termAttemptAuthorized	Non	Point de déclenchement CAMEL : :termAttemptAuthorized, :tBusy, :tNoAnswer, :tAnswer
camel_gsmSCF_gt_address	String	(utilise le GT appelé)	Non	Titre Global gsmSCF par défaut pour les réponses CAMEL (peut être remplacé par GT NAT)

Exemple :

```
config :omniss7,  
  camel_service_key: 11_110,  
  camel_trigger_detection_point: :termAttemptAuthorized
```

Préfixes VLR Domiciliaires

Configuration pour distinguer les abonnés domiciliés des abonnés en itinérance. Pour une explication détaillée de la détection domicile/itinérance et des opérations PRN, voir [Gestion des Abonnés en Itinérance dans le Guide HLR](#).

Paramètre	Type	Par Défaut	Requis	Description
home_vlr_prefixes	List	["5551231"]	Non	Préfixes GT VLR considérés comme réseau "domiciliaire"

Exemple :

```
config :omniss7,
```

```
home_vlr_prefixes: ["5551231", "5551234"]
```

Paramètres de Mode SMSc

Configuration pour le mode Centre SMS.

Configuration de l'API SMSc

Paramètre	Type	Par Défaut	Requis	Description
smsc_api_base_url	String-		Oui	URL du point de terminaison de l'API SMSc backend (vérification SSL codée en dur désactivée)
smsc_name	String	"{hostname}_SMSc"	Non	Identifiant SMSc pour l'enregistrement backend
smsc_service_center_gt_address	String-		Oui	Adresse de Titre Global du Centre de Service

Exemple :

```
config :omniss7,  
  smsc_api_base_url: "https://10.179.3.219:8443",  
  smsc_name: "ipsmgw",  
  smsc_service_center_gt_address: "55512341112"
```

Remarque : L'enregistrement frontend a lieu toutes les **5 minutes** (codé en dur) via le module SMS.FrontendRegistry.

Configuration d'Auto-Vidage

Paramètre	Type	Par Défaut	Requis	Description
auto_flush_enabled	Boolean	true	Non	Activer le traitement automatique de la file d'attente SMS
auto_flush_interval	Integer	10_000	Non	Intervalle de traitement de la file d'attente en millisecondes
auto_flush_dest_smsc	String	-	Oui	Nom du SMSc de destination pour l'auto-vidage
auto_flush_tps	Integer	10	Non	Taux de traitement des messages (transactions/seconde)

Exemple :

```
config :omniss7,  
  auto_flush_enabled: true,  
  auto_flush_interval: 10_000,  
  auto_flush_dest_smsc: "ipsmgw",  
  auto_flush_tps: 10
```

Paramètres de Mode STP

Configuration pour le mode Point de Transfert de Signal M3UA. Pour une configuration de routage détaillée et des exemples, voir le [Guide de Configuration STP](#).

Serveur STP Autonome

Paramètre	Type	Par Défaut	Requis	Description
m3ua_stp.enabled	Boolean	false	Non	Activer le serveur STP M3UA autonome
m3ua_stp.local_ip	Tuple	{127, 0, 0, 1}	Non	Adresse IP pour écouter les connexions
m3ua_stp.local_port	Integer	2905	Non	Port à écouter
m3ua_stp.point_code	Integer	-	Oui (si activé)	Code de point SS7 de ce STP

Exemple :

```
config :omniss7,  
  m3ua_stp: %{  
    enabled: true,  
    local_ip: {10, 179, 4, 10},  
    local_port: 2905,  
    point_code: 100  
  }  
}
```

Routing par Titre Global

Paramètre	Type	Par Défaut	Requis	Description
enable_gt_routing	Boolean	false	Non	Activer le routage par GT en plus du routage par PC

Exemple :

```
config :omniss7,  
  enable_gt_routing: true
```

Paramètres de NAT de Titre Global

La Traduction d'Adresse de Réseau de Titre Global permet des GT de réponse différents en fonction du préfixe de la partie appelante. Pour une explication détaillée et des exemples, voir le [Guide de NAT de Titre Global](#).

Paramètre	Type	Par Défaut	Requis	Description
gt_nat_enabled	Boolean	false	Non	Activer/désactiver la fonctionnalité de NAT GT
gt_nat_rules	List of Maps	[]	Oui (si activé)	Liste des mappings préfixe-à-GT

Format de Règle : Chaque règle dans gt_nat_rules doit être une carte avec :

- calling_prefix: Préfixe de chaîne à faire correspondre avec le GT appelant
- response_gt: Titre Global à utiliser dans les réponses

Exemple :

```
config :omniss7,  
  gt_nat_enabled: true,  
  gt_nat_rules: [  
    # Lorsqu'appelé depuis un GT commençant par "8772", répondre avec "55512341112"  
    %{calling_prefix: "8772", response_gt: "55512341112"},  
    # Lorsqu'appelé depuis un GT commençant par "8773", répondre avec "55512341111"  
    %{calling_prefix: "8773", response_gt: "55512341111"},  
    # Fallback par défaut (préfixe vide correspond à tous)  
    %{calling_prefix: "", response_gt: "55512311555"}  
  ]
```

Voir Aussi : [Guide de NAT GT](#) pour une utilisation détaillée et des exemples.

Paramètres de Connexion M3UA

Configuration de connexion M3UA pour le mode client MAP. Pour une utilisation détaillée et des exemples, voir le [Guide Client MAP](#).

Paramètre	Type	Par Défaut	Requis	Description
map_client_m3ua.mode	String	-	Oui	Mode de connexion : "ASP" ou "SGP"
map_client_m3ua.callback	Tuple	-	Oui	Module/fonction de rappel : {MapClient, :handle_payload, []}
map_client_m3ua.process_name	Atom	-	Oui	Nom du processus pour l'enregistrement
map_client_m3ua.local_ip	Tuple	-	Oui	Adresse IP locale à lier
map_client_m3ua.local_port	Integer	2905	Oui	Port SCTP local
map_client_m3ua.remote_ip	Tuple	-	Oui	Adresse IP STP/SGW distante
map_client_m3ua.remote_port	Integer	2905	Oui	Port SCTP distant
map_client_m3ua.routing_context	Integer	-	Oui	ID de contexte de routage M3UA

Exemple :

```
config :omniss7,  
  map_client_m3ua: %{  
    mode: "ASP",  
    callback: {MapClient, :handle_payload, []},  
    process_name: :hmr_client_asp,  
    local_ip: {10, 179, 4, 11},  
    local_port: 2905,  
    remote_ip: {10, 179, 4, 10},  
    remote_port: 2905,  
    routing_context: 1  
  }  
}
```

Paramètres du Serveur HTTP

Configuration pour le serveur HTTP de l'API REST.

Paramètre	Type	Par Défaut	Requis	Description
start_http_server	Boolean	true	Non	Activer/désactiver le serveur HTTP (port 8080)

Valeurs Codées en Dur (non configurables) :

- **IP** : 0.0.0.0 (toutes les interfaces)
- **Port** : 8080
- **Transport** : Plug.Cowboy

Exemple :

```
config :omniss7,  
  start_http_server: true # Définir sur false pour désactiver
```

Points de Terminaison de l'API :

- API REST : [http://\[server-ip\]:8080/api/*](http://[server-ip]:8080/api/*)
- Swagger UI : [http://\[server-ip\]:8080/swagger](http://[server-ip]:8080/swagger)
- Métriques Prometheus : [http://\[server-ip\]:8080/metrics](http://[server-ip]:8080/metrics)

Voir [Guide de l'API](#) pour plus de détails.

Paramètres de Base de Données

Configuration pour la persistance de la base de données Mnesia.

Paramètre	Type	Par Défaut	Requis	Description
mnesia_storage_type	Atom	:disc_copies	Non	Type de stockage Mnesia : :disc_copies ou :ram_copies

Exemple :

```
config :omniss7,  
  mnesia_storage_type: :disc_copies # Production  
  # mnesia_storage_type: :ram_copies # Test uniquement
```

Types de Stockage :

- :disc_copies - Stockage persistant sur disque (survit aux redémarrages) - **Recommandé pour la production**
- :ram_copies - Seulement en mémoire (perdu lors du redémarrage) - Pour test uniquement

Tables Mnesia :

- m3ua_peer - Connexions de pairs M3UA
- m3ua_route - Routes de Code de Point
- m3ua_gt_route - Routes de Titre Global

Emplacement : Répertoire Mnesia.{node_name}/

Valeurs Codées en Dur

Les valeurs suivantes sont **codées en dur dans le code source** et ne peuvent pas être modifiées via la configuration.

Délais

Valeur	Impact	Solution de Contournement
Délai de demande MAP : 10 secondes	Toutes les opérations MAP expirent après 10s	Modifier le code source
Délai ISD : 10 secondes	Chaque message ISD expire après 10s	Modifier le code source

Serveur HTTP

Valeur	Impact	Solution de Contournement
IP HTTP : 0.0.0.0	Le serveur écoute sur toutes les interfaces	Modifier le code source
Port HTTP : 8080	L'API REST fonctionne sur le port 8080	Modifier le code source

Vérification SSL

Valeur	Impact	Solution de Contournement
API HLR SSL : désactivé	Vérification SSL toujours désactivée	Modifier le code source
API SMS Sc SSL : désactivé	Vérification SSL toujours désactivée	Modifier le code source

Intervalles d'Enregistrement

Valeur	Impact	Solution de Contournement
Enregistrement frontend : 5 minutes	Le SMSc s'enregistre avec le backend toutes les 5 min	Modifier le code source

Actualisation Automatique de l'Interface Web

Page	Intervalle
Gestion du Routage	5 secondes
Abonnés Actifs	2 secondes

Exemples de Configuration

Configuration HLR Minimale

```
config :omniss7,  
    map_client_enabled: true,  
    hlr_mode_enabled: true,  
    smsc_mode_enabled: false,  
  
    hlr_api_base_url: "https://10.180.2.140:8443",  
    hlr_service_center_gt_address: "55512341111",  
    smsc_service_center_gt_address: "55512341112",  
  
    map_client_m3ua: %{\br/>        mode: "ASP",  
        callback: {MapClient, :handle_payload, []},  
        process_name: :hlr_client_asp,  
        local_ip: {10, 179, 4, 11},  
        local_port: 2905,  
        remote_ip: {10, 179, 4, 10},  
        remote_port: 2905,  
        routing_context: 1  
    }  
}
```

Configuration SMSc Minimale

```
config :omniss7,  
    map_client_enabled: true,  
    hlr_mode_enabled: false,  
    smsc_mode_enabled: true,  
  
    smsc_api_base_url: "https://10.179.3.219:8443",  
    smsc_name: "ipsmgw",  
    smsc_service_center_gt_address: "55512341112",  
  
    auto_flush_enabled: true,  
    auto_flush_interval: 10_000,  
    auto_flush_dest_smsc: "ipsmgw",  
    auto_flush_tps: 10,  
  
    map_client_m3ua: %{\br/>        mode: "ASP",  
        callback: {MapClient, :handle_payload, []},  
        process_name: :stp_client_asp,  
        local_ip: {10, 179, 4, 12},  
    }  
}
```

```
    local_port: 2905,  
    remote_ip: {10, 179, 4, 10},  
    remote_port: 2905,  
    routing_context: 1  
}
```

STP avec Serveur Autonome

```
config :omniss7,  
  map_client_enabled: true,  
  hlr_mode_enabled: false,  
  smsc_mode_enabled: false,  
  
  enable_gt_routing: true,  
  mnesia_storage_type: :disc_copies,  
  
  m3ua_stp: %{  
    enabled: true,  
    local_ip: {10, 179, 4, 10},  
    local_port: 2905,  
    point_code: 100  
  },  
  
  map_client_m3ua: %{  
    mode: "ASP",  
    callback: {MapClient, :handle_payload, []},  
    process_name: :stp_client_asp,  
    local_ip: {10, 179, 4, 10},  
    local_port: 2906,  
    remote_ip: {10, 179, 4, 11},  
    remote_port: 2905,  
    routing_context: 1  
  }  
}
```

Résumé

Total des Paramètres de Configuration : 32

Par Catégorie :

- Mode Opérationnel : 3 paramètres
- Mode HLR : 13 paramètres
- Mode SMSc : 7 paramètres
- Mode STP : 5 paramètres
- Connexion M3UA : 8 paramètres
- Serveur HTTP : 1 paramètre
- Base de Données : 1 paramètre

Paramètres Requis (doivent être définis) :

- hlr_api_base_url (mode HLR)
 - hlr_service_center_gt_address (mode HLR)
 - smsc_api_base_url (mode SMSc)
 - smsc_service_center_gt_address (mode SMSc/HLR)
 - Tous les paramètres map_client_m3ua.*
 - m3ua_stp.point_code (si STP activé)
-

Documentation Connexe

- [Guide HLR](#) - Configuration spécifique au HLR
- [Guide SMSc](#) - Configuration spécifique au SMSc
- [Guide STP](#) - Configuration de routage STP
- [Guide de l'API](#) - Référence de l'API REST
- [Guide de l'Interface Web](#) - Documentation de l'interface web



Guide de NAT de Titre Global

Vue d'ensemble

La traduction d'adresse de titre global (GT NAT) est une fonctionnalité qui permet à OmniSS7 de répondre avec différentes adresses de titre global en fonction du préfixe GT de la partie appelante, du préfixe GT de la partie appelée, ou d'une combinaison des deux. Cela est essentiel lors de l'opération avec plusieurs titres globaux et de la nécessité de s'assurer que les réponses utilisent le bon GT en fonction du réseau ou du pair qui appelle et/ou du GT qu'ils ont appelé.

Quoi de neuf (GT NAT amélioré)

La fonctionnalité GT NAT a été améliorée avec de nouvelles capacités puissantes :

Nouvelles fonctionnalités

1. **Correspondance de préfixe de partie appelée** : Les règles peuvent désormais correspondre sur `called_prefix` en plus de `calling_prefix`
2. **Correspondance combinée** : Les règles peuvent correspondre à la fois sur les préfixes appelants ET appelés simultanément
3. **Priorisation basée sur le poids** : Les règles utilisent désormais un champ `weight` (plus bas = priorité plus élevée) au lieu de simplement la longueur du préfixe
4. **Correspondance flexible** : Vous pouvez désormais créer des règles avec :
 - Seulement le préfixe appelant
 - Seulement le préfixe appelé
 - Les préfixes appelants et appelés
 - Aucun (règle de secours)

Nouveau format de règle

Champs requis :

- `weight` : Priorité entière (plus bas = priorité plus élevée)
- `response_gt` : Le GT à utiliser pour la réponse

Champs optionnels (au moins un recommandé pour une correspondance spécifique) :

- `calling_prefix` : Correspondre au préfixe GT de la partie appelante
- `called_prefix` : Correspondre au préfixe GT de la partie appelée

Exemple :

```
gt_nat_rules: [  
  # Règle spécifique avec les deux préfixes - priorité la plus élevée  
  %{calling_prefix: "8772", called_prefix: "555", weight: 1,  
  response_gt: "111111"},  
  
  # Règles spécifiques - priorité moyenne  
  %{calling_prefix: "8772", weight: 10, response_gt: "222222"},  
  %{called_prefix: "555", weight: 10, response_gt: "333333"},  
  
  # Règle de secours wildcard - priorité la plus basse  
  %{weight: 100, response_gt: "999999"}  
]
```

Cas d'utilisation

Opération multi-réseaux

Lorsque vous avez plusieurs réseaux pairs et que chacun s'attend à des réponses d'un GT spécifique :

- **Réseau A** appelle votre GT 111111 et s'attend à des réponses de 111111
- **Réseau B** appelle votre GT 222222 et s'attend à des réponses de 222222

Sans GT NAT, vous auriez besoin d'instances séparées ou de routage complexe. Avec GT NAT, une seule instance d'OmniSS7 peut gérer cela intelligemment.

Scénarios de roaming

Lorsque vous opérez en tant qu'HLR ou SMSc avec des accords de roaming :

- Les abonnés du **réseau domestique** utilisent le GT 555000
- Le **partenaire de roaming 1** utilise le GT 555001
- Le **partenaire de roaming 2** utilise le GT 555002

GT NAT garantit que chaque partenaire reçoit des réponses du bon GT auquel ils sont configurés pour router.

Tests et migration

Lors des migrations de réseau ou des tests :

- Migrer progressivement le trafic de l'ancien GT vers le nouveau GT
- Maintenir les deux GT pendant la période de transition
- Router les réponses en fonction du GT utilisé par l'appelant

Comment ça fonctionne

Flux de traduction d'adresse

1. **Demande entrante** : OmniSS7 reçoit un message SCCP avec :
 - GT de la partie appelée : 55512341112 (votre GT)
 - GT de la partie appelante : 877234567 (leur GT)
2. **Recherche GT NAT** : Le système vérifie le GT appelant 877234567 par rapport aux règles de préfixe configurées
3. **Correspondance de préfixe** : Trouve le préfixe correspondant le plus long (par exemple, 8772 correspond à 877234567)
4. **Sélection du GT de réponse** : Utilise `response_gt` de la règle correspondante (par exemple, 55512341112)
5. **Réponse envoyée** : La réponse SCCP utilise :
 - GT de la partie appelée : 877234567 (inversé - leur GT)
 - GT de la partie appelante : 55512341112 (GT NAT)

Types de réponses affectés

GT NAT s'applique à plusieurs couches de la pile SS7 :

Couche SCCP (Toutes les réponses)

- Adresses GT appelées/appelantes SCCP dans tous les messages de réponse
- Accusés de réception ISD (InsertSubscriberData)
- Réponses UpdateLocation
- Réponses d'erreur

Couche MAP (Opération spécifique)

- **Réponses SRI-for-SM** : `networkNode-Number` (adresse GT SMS) Sc)
- **UpdateLocation** : `hlr-Number` dans les réponses
- **InsertSubscriberData** : GT HLR dans les messages ISD

Configuration

Configuration de base

Ajoutez à `config/runtime.exs` :

```

config :omniss7,
  # Activer GT NAT
  gt_nat_enabled: true,

  # Définir les règles GT NAT
  gt_nat_rules: [
    # Règle 1 : Les appels du préfixe "8772" obtiennent une réponse
    du "55512341112"
    %{calling_prefix: "8772", response_gt: "55512341112"},

    # Règle 2 : Les appels du préfixe "8773" obtiennent une réponse
    du "55512341111"
    %{calling_prefix: "8773", response_gt: "55512341111"},

    # Règle par défaut (préfixe vide correspond à tout)
    %{calling_prefix: "", response_gt: "55512311555"}
  ]

```

Paramètres de configuration

Pour une référence complète de configuration, voir [Paramètres de Titre Global NAT dans la Référence de Configuration](#).

Paramètre	Type	Requis	Description
gt_nat_enabled	Booléen	Oui	Activer/désactiver la fonctionnalité GT NAT
gt_nat_rules	Liste de Maps	Oui (si activé)	Liste des règles de correspondance de préfixes

Format de règle

Chaque règle est une carte avec les clés suivantes :

```

%{
  calling_prefix: "8772",      # (Optionnel) Préfixe à faire
  correspondre avec le GT appelant
  called_prefix: "555",       # (Optionnel) Préfixe à faire
  correspondre avec le GT appelé
  weight: 10,                 # (Requis) Valeur de priorité (plus
  bas = priorité plus élevée)
  response_gt: "55512341112"  # (Requis) GT à utiliser dans les
  réponses
}

```

Champs de règle :

- **calling_prefix** (Optionnel) : Préfixe de chaîne à faire correspondre avec le GT appelant entrant

- La correspondance se fait par `String.starts_with?/2`
- La chaîne vide "" ou nil agit comme un wildcard (correspond à n'importe quel GT appelant)
- Peut être omis pour correspondre à n'importe quel GT appelant
- **called_prefix** (Optionnel) : Préfixe de chaîne à faire correspondre avec le GT appelé entrant
 - La correspondance se fait par `String.starts_with?/2`
 - La chaîne vide "" ou nil agit comme un wildcard (correspond à n'importe quel GT appelé)
 - Peut être omis pour correspondre à n'importe quel GT appelé
- **weight** (Requis) : Valeur de priorité entière
 - Poids inférieur = priorité plus élevée (traité en premier)
 - Doit être ≥ 0
 - Utilisé comme critère de tri principal pour les règles de correspondance
- **response_gt** (Requis) : L'adresse de Titre Global à utiliser dans les réponses
 - Doit être une chaîne de numéro valide E.164
 - Doit correspondre à l'un de vos GT configurés

Au moins l'un de `calling_prefix` ou `called_prefix` doit être spécifié pour un routage spécifique. Les deux peuvent être omis pour une règle wildcard/ de secours.

Logique de correspondance de règle

Les règles sont évaluées par **poids d'abord (croissant)**, puis par **spécificité de préfixe combinée** :

Algorithme de correspondance :

1. Filtrer les règles où tous les préfixes spécifiés correspondent
 - Si `calling_prefix` est défini, il doit correspondre au GT appelant
 - Si `called_prefix` est défini, il doit correspondre au GT appelé
 - Si les deux sont définis, les deux doivent correspondre
 - Si aucun n'est défini, la règle agit comme un wildcard
2. Trier les règles correspondantes par :
 - **Primaire** : Poids (croissant - valeurs plus basses d'abord)
 - **Secondaire** : Longueur de préfixe combinée (décroissante - plus long = plus spécifique)
3. Retourner la première règle correspondante

Exemples :

```
# Exemples de règles
gt_nat_rules: [
  # Poids 1 : Priorité la plus élevée - correspond aux deux préfixes
  %{calling_prefix: "8772", called_prefix: "555", weight: 1,
  response_gt: "111111"},

  # Poids 10 : Priorité moyenne - règles spécifiques
  %{calling_prefix: "8772", weight: 10, response_gt: "222222"}, #
  Appelant seulement
  %{called_prefix: "555", weight: 10, response_gt: "333333"}, #
  Appelé seulement

  # Poids 100 : Priorité la plus basse - wildcard de secours
  %{weight: 100, response_gt: "444444"} # Correspond à tout
]

# Exemples de correspondance :
# Appelant : "877234567", Appelé : "555123" -> "111111" (poids 1, les
deux correspondent)
# Appelant : "877234567", Appelé : "999999" -> "222222" (poids 10,
appellant seulement)
# Appelant : "999999999", Appelé : "555123" -> "333333" (poids 10,
appelé seulement)
# Appelant : "999999999", Appelé : "888888" -> "444444" (poids 100,
wildcard)
```

Exemples

Exemple 1 : Deux partenaires réseau

Scénario : Vous exploitez un SMSc avec deux partenaires réseau. Chacun s'attend à des réponses d'un GT différent.

```
config :omniss7,
  gt_nat_enabled: true,

  # GT SMSc par défaut (utilisé lorsque GT NAT est désactivé ou
aucune règle ne correspond)
  smsc_service_center_gt_address: "5551000",

  # Règles GT NAT pour les partenaires
  gt_nat_rules: [
    # Partenaire A (préfixe 4412) s'attend à des réponses du GT
5551001
    %{calling_prefix: "4412", weight: 10, response_gt: "5551001"},

    # Partenaire B (préfixe 4413) s'attend à des réponses du GT
5551002
```

```
%{calling_prefix: "4413", weight: 10, response_gt: "5551002"},  
  
# Par défaut : utiliser le GT SMS standard (wildcard de secours)  
%{weight: 100, response_gt: "5551000"}  
]
```

Flux de trafic :

SRI-for-SM entrant de 44121234567 :
GT appelé : 5551001 (votre GT que le Partenaire A utilise)
GT appelant : 44121234567 (GT du Partenaire A)

Recherche GT NAT :
"44121234567" correspond au préfixe "4412"
GT de réponse sélectionné : "5551001"

Réponse SRI-for-SM à 44121234567 :
GT appelé : 44121234567 (inversé)
GT appelant : 5551001 (NAT'd)
networkNode-Number : 5551001 (dans la réponse MAP)

Exemple 2 : HLR avec GT régionaux

Scénario : HLR national avec différents GT par région.

```
config :omniss7,  
  gt_nat_enabled: true,  
  hlr_service_center_gt_address: "555000", # GT HLR par défaut  
  
  gt_nat_rules: [  
    # VLRs de la région nord (préfixe 5551)  
    %{calling_prefix: "5551", weight: 10, response_gt: "555100"},  
  
    # VLRs de la région sud (préfixe 5552)  
    %{calling_prefix: "5552", weight: 10, response_gt: "555200"},  
  
    # VLRs de la région ouest (préfixe 5553)  
    %{calling_prefix: "5553", weight: 10, response_gt: "555300"},  
  
    # Par défaut pour d'autres régions (wildcard)  
    %{weight: 100, response_gt: "555000"}  
  ]
```

Exemple 3 : Scénario de migration

Scénario : Migration progressive de l'ancien GT vers le nouveau GT.

```
config :omniss7,
```



```

    gt_nat_enabled: true,
    hlr_service_center_gt_address: "123456789", # Ancien GT (par
défaut)

    gt_nat_rules: [
        # Réseaux migrés (ont déjà mis à jour leurs configurations)
        %{calling_prefix: "555", weight: 10, response_gt: "987654321"},
# Nouveau GT
        %{calling_prefix: "666", weight: 10, response_gt: "987654321"},
# Nouveau GT

        # Tout le monde utilise encore l'ancien GT (wildcard)
        %{weight: 100, response_gt: "123456789"} # Ancien GT
    ]

```

Exemple 4 : Correspondance de préfixe de partie appelée (NOUVEAU)

Scénario : Vous avez plusieurs GT pour différents services et souhaitez répondre avec le bon GT en fonction de quel GT a été appelé.

```

config :omniss7,
    gt_nat_enabled: true,

    gt_nat_rules: [
        # Lorsqu'ils appellent votre GT SMS (5551xxx), répondez avec ce
GT
        %{called_prefix: "5551", weight: 10, response_gt: "555100"},

        # Lorsqu'ils appellent votre GT Voix (5552xxx), répondez avec ce
GT
        %{called_prefix: "5552", weight: 10, response_gt: "555200"},

        # Lorsqu'ils appellent votre GT Données (5553xxx), répondez avec
ce GT
        %{called_prefix: "5553", weight: 10, response_gt: "555300"},

        # Règle de secours par défaut
        %{weight: 100, response_gt: "555000"}
    ]

```

Flux de trafic :

Demande entrante au GT appelé : 555100 (votre GT SMS)
 GT appelant : 441234567 (n'importe quel appelant)

Recherche GT NAT :
 GT appelé "555100" correspond au préfixe "5551"

GT de réponse sélectionné : "555100"

La réponse utilise le GT appelant : 555100 (correspond à ce qu'ils ont appelé)

Exemple 5 : Correspondance combinée de préfixes appelants + appelés (AVANCÉE)

Scénario : Différents partenaires appellent différents GT, et vous souhaitez un contrôle précis.

```
config :omniss7,  
  gt_nat_enabled: true,  
  
  gt_nat_rules: [  
    # Partenaire A appelant votre GT SMS - priorité la plus élevée  
    (poids 1)  
    %{calling_prefix: "4412", called_prefix: "5551", weight: 1,  
    response_gt: "555101"},  
  
    # Partenaire B appelant votre GT SMS - priorité la plus élevée  
    (poids 1)  
    %{calling_prefix: "4413", called_prefix: "5551", weight: 1,  
    response_gt: "555102"},  
  
    # Quiconque appelant votre GT SMS - priorité moyenne (poids 10)  
    %{called_prefix: "5551", weight: 10, response_gt: "555100"},  
  
    # Partenaire A appelant n'importe quel GT - priorité moyenne  
    (poids 10)  
    %{calling_prefix: "4412", weight: 10, response_gt: "555200"},  
  
    # Règle de secours par défaut - faible priorité (poids 100)  
    %{weight: 100, response_gt: "555000"}  
  ]
```

Exemples de correspondance :

```
# Partenaire A appelle le GT SMS  
Appelant : "441234567", Appelé : "555100"  
→ Correspond à la règle de poids 1 (les deux préfixes) → "555101"  
  
# Partenaire A appelle le GT Voix  
Appelant : "441234567", Appelé : "555200"  
→ Correspond à la règle de poids 10 (appelant seulement) → "555200"  
  
# Appelant inconnu appelle le GT SMS  
Appelant : "999999999", Appelé : "555100"
```

→ Correspond à la règle de poids 10 (appelé seulement) → "555100"

Appelant inconnu appelle le GT Voix

Appelant : "999999999", Appelé : "555200"

→ Correspond à la règle de poids 100 wildcard → "555000"

Modes opérationnels

GT NAT fonctionne dans tous les modes opérationnels d'OmniSS7 :

Mode HLR

GT NAT affecte :

- Réponses UpdateLocation (GT HLR dans la réponse)
- Messages InsertSubscriberData (GT HLR en tant que partie appelante)
- Réponses SendAuthenticationInfo
- Réponses Cancel Location

Pour plus d'informations sur les opérations HLR, voir le [Guide de Configuration HLR](#).

Configuration :

```
config :omniss7,  
  hlr_mode_enabled: true,  
  hlr_service_center_gt_address: "5551234567", # GT HLR par défaut  
  
  gt_nat_enabled: true,  
  gt_nat_rules: [  
    %{calling_prefix: "331", weight: 10, response_gt: "5551234568"},  
# France  
    %{calling_prefix: "44", weight: 10, response_gt: "5551234569"},  
# Royaume-Uni  
    %{weight: 100, response_gt: "5551234567"} # Wildcard par défaut  
  ]
```

Mode SMSc

GT NAT affecte :

- Réponses SRI-for-SM (champ networkNode-Number) - voir [Détails SRI-for-SM](#)
- Accusés de réception MT-ForwardSM

Pour plus d'informations sur les opérations SMSc, voir le [Guide de Configuration SMSc](#).

Configuration :

```
config :omniss7,
  smsc_mode_enabled: true,
  smsc_service_center_gt_address: "5559999", # GT SMS Sc par défaut

  gt_nat_enabled: true,
  gt_nat_rules: [
    %{calling_prefix: "1", weight: 10, response_gt: "5559991"}, #
    Amérique du Nord
    %{calling_prefix: "44", weight: 10, response_gt: "5559992"}, #
    Royaume-Uni
    %{calling_prefix: "86", weight: 10, response_gt: "5559993"}, #
    Chine
    %{weight: 100, response_gt: "5559999"} # Wildcard par défaut
  ]
```

Mode Passerelle CAMEL

GT NAT affecte :

- Toutes les réponses au niveau SCCP (GT gsmSCF en tant que partie appelante)
- Réponses des opérations CAMEL/CAP (InitialDP, EventReportBCSM, etc.)
- Accusés de réception RequestReportBCSMEvent
- Réponses ApplyCharging
- Réponses Continue

Configuration :

```
config :omniss7,
  camelgw_mode_enabled: true,
  camel_gsmSCF_gt_address: "55512341112", # GT gsmSCF par défaut

  gt_nat_enabled: true,
  gt_nat_rules: [
    %{calling_prefix: "555", weight: 10, response_gt: "55512341111"},
    # Réseau A
    %{calling_prefix: "666", weight: 10, response_gt: "55512311555"},
    # Réseau B
    %{weight: 100, response_gt: "55512341112"} # Wildcard par défaut
  ]
```

Cas d'utilisation : Lorsque vous opérez en tant que gsmSCF (Service Control Function) pour plusieurs réseaux, chaque gsmSSF de réseau peut s'attendre à des réponses d'un GT gsmSCF spécifique. GT NAT garantit que le bon GT est utilisé en fonction de quel gsmSSF appelle.

Journalisation et Débogage

Activer la journalisation GT NAT

GT NAT inclut la journalisation automatique de toutes les traductions :

```
# Dans les journaux, vous verrez :  
[info] GT NAT [réponse SRI-for-SM] : GT appelant 877234567 -> GT de  
réponse 55512341112  
[info] GT NAT [UpdateLocation ISD] : GT appelant 331234567 -> GT de  
réponse 55512341111  
[info] GT NAT [réponse MAP BEGIN] : GT appelant 441234567 -> GT de  
réponse 55512311555
```

Le champ de contexte montre où le NAT a été appliqué :

- "réponse SRI-for-SM" - Dans le gestionnaire SRI-for-SM
- "UpdateLocation ISD" - Dans les messages InsertSubscriberData
- "UpdateLocation END" - Dans la réponse UpdateLocation END
- "réponse MAP BEGIN" - Réponses MAP BEGIN génériques
- "ISD ACK" - Accusé de réception ISD
- "réponse d'erreur HLR" - Réponse d'erreur de l'HLR
- "réponse CAMEL" - Réponses d'opérations CAMEL/CAP (gsmSCF)

Validation

Le système valide la configuration GT NAT au démarrage :

```
# Vérifier la config GT NAT  
iex> GtNat.validate_config()  
{:ok, [  
  %{calling_prefix: "8772", weight: 10, response_gt: "55512341112"},  
  %{calling_prefix: "8773", weight: 10, response_gt: "55512341111"}  
]}
```

```
# Vérifier si activé  
iex> GtNat.enabled?()  
true
```

```
# Obtenir toutes les règles  
iex> GtNat.get_rules()  
[  
  %{calling_prefix: "8772", weight: 10, response_gt: "55512341112"},  
  %{calling_prefix: "8773", weight: 10, response_gt: "55512341111"}  
]
```

Tester GT NAT

Testez la logique GT NAT de manière programmatique :

```
# Tester la traduction avec uniquement le GT appelant (called_gt est nil)
iex> GtNat.translate_response_gt("877234567", nil, "default_gt")
"55512341112"

# Tester la traduction avec les deux GT appelant et appelé
iex> GtNat.translate_response_gt("877234567", "555123", "default_gt")
"55512341112"

# Tester avec journalisation (GT appelé nil)
iex> GtNat.translate_response_gt_with_logging("877234567", nil,
"default_gt", "test")
# Journaux : GT NAT [test] : GT appelant 877234567 -> GT de réponse
55512341112
"55512341112"

# Tester avec journalisation (les deux GT)
iex> GtNat.translate_response_gt_with_logging("877234567", "555123",
"default_gt", "test")
# Journaux : GT NAT [test] : GT appelant 877234567, GT appelé 555123
-> GT de réponse 55512341112
"55512341112"

# Tester sans correspondance (retourne par défaut)
iex> GtNat.translate_response_gt("999999999", "888888", "default_gt")
"default_gt"
```

Dépannage

Problème : GT NAT ne fonctionne pas

Vérification 1 : Est-il activé ?

```
iex> Application.get_env(:omniss7, :gt_nat_enabled)
true # Devrait être vrai
```

Vérification 2 : Les règles sont-elles configurées ?

```
iex> Application.get_env(:omniss7, :gt_nat_rules)
[%{calling_prefix: "8772", response_gt: "55512341112"}, ...] #
Devrait retourner une liste
```

Vérification 3 : Vérifiez les journaux Recherchez "GT NAT" dans les journaux pour voir si des traductions se produisent.

Problème : Mauvais GT dans les réponses

Symptôme : Les réponses utilisent une adresse GT inattendue

Cause : La correspondance de préfixe de règle pourrait être trop large ou la règle par défaut attrape le trafic

Solution : Réviser les poids et les préfixes des règles :







```
# MAUVAIS : Wildcard avec un poids bas (attrape tout en premier)
gt_nat_rules: [
    %{weight: 1, response_gt: "111111"},          # Cela
    correspond à tout en premier !
    %{calling_prefix: "8772", weight: 10, response_gt: "222222"} #
    Jamais atteint
]

# BON : Règles spécifiques avec un poids inférieur, wildcard avec un
poids plus élevé
gt_nat_rules: [
    %{calling_prefix: "8772", weight: 10, response_gt: "222222"}, #
    Spécifique, poids bas
    %{weight: 100, response_gt: "111111"} # Wildcard, poids élevé
    (secours)
]
```

Problème : GT NAT non appliqué à un type de message spécifique

Symptôme : Certaines réponses utilisent le GT NAT'd, d'autres non

Couverture actuelle :

-  GT appelant SCCP (toutes les réponses)
-  Réponses SRI-for-SM (networkNode-Number)
-  Messages ISD UpdateLocation (GT HLR)
-  Réponses UpdateLocation END
-  Accusés de réception ISD
-  Réponses MAP BEGIN

Si un type de message spécifique n'utilise pas GT NAT, il se peut qu'il ne soit pas encore implémenté. Vérifiez le code source ou contactez le support.

Considérations de performance

Performance de recherche

GT NAT utilise une correspondance de préfixe simple avec une complexité $O(n)$ où n est le nombre de règles.

Conseils de performance :

- Gardez le nombre de règles en dessous de 100 pour la meilleure performance
- Utilisez des préfixes spécifiques pour réduire le nombre de règles
- La règle par défaut (préfixe vide) doit être la dernière

Benchmark (système typique) :

- 10 règles : $< 1\mu s$ par recherche
- 50 règles : $< 5\mu s$ par recherche
- 100 règles : $< 10\mu s$ par recherche

Utilisation de la mémoire

Chaque règle nécessite ~ 100 octets de mémoire :

- 10 règles ≈ 1 Ko
- 100 règles ≈ 10 Ko

Meilleures pratiques

1. Inclure toujours une règle de secours wildcard

```
gt_nat_rules: [  
  {%calling_prefix: "8772", weight: 10, response_gt: "111111"},  
  {%calling_prefix: "8773", weight: 10, response_gt: "222222"},  
  {%weight: 100, response_gt: "default_gt"} # Avoir toujours un  
wildcard avec un poids élevé  
]
```

2. Utiliser des préfixes et des poids significatifs

```
# BON : Préfixes clairs et spécifiques avec des poids appropriés  
{%calling_prefix: "331", weight: 10, response_gt: "..."} # France  
{%calling_prefix: "44", weight: 10, response_gt: "..."} # Royaume-  
Uni  
  
# MAUVAIS : Préfixes trop larges ou poids déroutants  
{%calling_prefix: "3", weight: 5, response_gt: "..."} # Trop de
```



```
pays
%{calling_prefix: "331", weight: 100, response_gt: "..."} # Le poids
devrait être plus bas pour les règles spécifiques
```

3. Documentez vos règles

```
gt_nat_rules: [
  # Partenaire XYZ - réseau britannique (plage GT : 4412xxxxxxx)
  # Poids 10 : Priorité standard du partenaire
  %{calling_prefix: "4412", weight: 10, response_gt: "5551001"},

  # Partenaire ABC - réseau français (plage GT : 33123xxxxxx)
  # Poids 10 : Priorité standard du partenaire
  %{calling_prefix: "33123", weight: 10, response_gt: "5551002"}
]
```

4. Testez avant le déploiement

```
# Testez dans iex avant de déployer
iex> GtNat.translate_response_gt("44121234567", nil, "default")
"5551001" # Résultat attendu

# Testez avec le GT appelé
iex> GtNat.translate_response_gt("44121234567", "555123", "default")
"5551001" # Résultat attendu
```

5. Surveillez les journaux

Activez la journalisation de niveau INFO pour voir toutes les traductions GT NAT en production.

Intégration avec d'autres fonctionnalités

Mode STP

GT NAT fonctionne indépendamment du routage STP. Le STP route en fonction des codes de point et des GT de destination, tandis que GT NAT gère l'adressage des réponses.

Pour plus d'informations sur le routage STP, voir le [Guide de Configuration STP](#).

Intégration CAMEL

GT NAT est **entièrement intégré** avec les opérations CAMEL/CAP :

Couche SCCP :

- GT de la partie appelante dans toutes les réponses CAMEL
- Appliqué automatiquement en fonction du GT gsmSSF entrant

Configuration :

- camel_gsmscf_gt_address - GT gsmSCF par défaut (optionnel)
- Si non configuré, utilise le GT de la partie appelée de la demande entrante
- Les règles GT NAT remplacent le défaut en fonction du préfixe de la partie appelante

Exemple :

```
# Lorsque gsmSSF 555123456 appelle votre gsmSCF
# Entrant : Appelé=55512341112, Appelant=555123456
# Recherche GT NAT : "555" -> response_gt="55512341111"
# Réponse : Appelé=555123456, Appelant=55512341111
```

Équilibrage de charge

GT NAT peut être combiné avec l'équilibrage de charge M3UA pour une gestion avancée du trafic.

Guide de migration

Activer GT NAT sur un système existant

1. Préparer la configuration

```
# Ajouter à runtime.exs (garder désactivé au départ)
config :omniss7,
  gt_nat_enabled: false, # Commencer désactivé
  gt_nat_rules: [
    # Vos règles ici avec des poids
    %{calling_prefix: "877", weight: 10, response_gt: "111111"},
    %{weight: 100, response_gt: "999999"} # Wildcard de secours
  ]
```

2. Tester la configuration

```
# Valider que la config compile
mix compile

# Tester dans iex
iex -S mix
iex> GtNat.validate_config()
```

3. Activer en staging

```
gt_nat_enabled: true # Changer à vrai
```

4. Surveiller les journaux

```
tail -f log/omniss7.log | grep "GT NAT"
```

5. Déployer en production

- Déployer pendant la fenêtre de maintenance
- Surveiller les 24 premières heures de près
- Avoir un plan de retour prêt (définir `gt_nat_enabled: false`)

Support

Pour des problèmes ou des questions :

- Vérifiez les journaux pour les messages "GT NAT"
- Validez la config avec `GtNat.validate_config()`
- Consultez la section de dépannage de ce guide
- Contactez le support OmniSS7 avec des extraits de journaux



Guide de Configuration HLR

[-- Retour à la Documentation Principale](#)

Ce guide fournit la configuration pour utiliser OmniSS7 comme un **Home Location Register (HLR/HSS)** avec **OmniHSS** comme base de données d'abonnés en backend.

Intégration OmniHSS

Le mode HLR d'OmniSS7 fonctionne comme un frontend de signalisation SS7 qui interagit avec **OmniHSS**, un serveur d'abonnés à domicile (HSS) complet. Cette architecture sépare les préoccupations :

- **OmniSS7 (Frontend HLR)** : Gère toute la signalisation du protocole SS7/MAP, le routage SCCP et la communication réseau
- **OmniHSS (Backend HSS)** : Gère les données des abonnés, l'authentification, le provisioning et les fonctionnalités avancées

Pourquoi OmniHSS ?

OmniHSS fournit une gestion des abonnés de qualité opérateur avec des fonctionnalités incluant :

- **Support Multi-IMSI** : Chaque abonné peut avoir plusieurs IMSI associés à un seul MSISDN pour le roaming international, le changement de réseau et le provisioning eSIM
- **Authentication Flexible** : Support pour les algorithmes d'authentification Milenage (3G/4G/5G) et COMP128 (2G)
- **Suivi des Sessions Circuits & Paquets** : Suivi indépendant des enregistrements réseau CS (circuit-switched) et PS (packet-switched)
- **Provisioning Avancé** : Profils de service personnalisables, services supplémentaires et données d'abonnement CAMEL
- **Conception API-First** : API HTTP RESTful pour l'intégration avec les systèmes de facturation, CRM et provisioning
- **Mises à Jour en Temps Réel** : Suivi de localisation, gestion de session et génération de vecteurs d'authentification

Toutes les données des abonnés, les informations d'authentification et les configurations de service sont stockées et gérées dans OmniHSS. OmniSS7 interroge OmniHSS via des appels API HTTPS pour répondre aux opérations MAP comme UpdateLocation, SendAuthenticationInfo et SendRoutingInfo.

Important : Le mode HLR d'OmniSS7 est un **frontend de signalisation uniquement**. Toute la logique de gestion des abonnés, les algorithmes d'authentification, les règles de provisioning et les opérations de base de données sont gérées par OmniHSS. Ce guide couvre la configuration du protocole SS7/MAP dans OmniSS7. Pour des informations sur le provisioning des abonnés, la configuration de l'authentification, les profils de service et les opérations administratives, **reportez-vous à la documentation d'OmniHSS**.

Support Multi-IMSI

OmniHSS prend en charge nativement les configurations **Multi-IMSI**, permettant à un seul abonné (identifié par MSISDN) d'avoir plusieurs IMSI. Cela permet :

- **Profils de Roaming International** : Différents IMSI pour différentes régions afin de réduire les coûts de roaming
- **eSIM Multi-Profile** : Plusieurs profils réseau sur un seul appareil compatible eSIM
- **Changement de Réseau** : Changement transparent entre les réseaux sans changer de MSISDN
- **Coordination Dual SIM** : Coordination entre plusieurs SIM physiques ou virtuelles
- **Tests & Développement** : Plusieurs IMSI de test pointant vers le même abonné

Comment ça fonctionne :

- Chaque IMSI a ses propres informations d'authentification (Ki, OPc, algorithme)
- Chaque IMSI peut avoir des enregistrements de session circuits et paquets indépendants
- Les services et profils des abonnés peuvent être partagés ou personnalisés par IMSI
- OmniSS7 interroge OmniHSS par IMSI, et OmniHSS retourne les données appropriées de l'abonné
- Les systèmes de facturation peuvent suivre l'utilisation par IMSI tout en associant tous les IMSI à un seul compte

Exemple de scénario Multi-IMSI :

Abonné MSISDN : +1-555-123-4567
|-- IMSI 1 : 310260123456789 (Réseau National US - Authentification Milenage)
~~666~~-- IMSI 2 : 208011234567890 (Profil de Roaming France - Authentification Milenage)
|-- IMSI 3 : 440201234567891 (Profil de Roaming UK - Authentification COMP128)

Tous les trois IMSI peuvent être utilisés indépendamment pour l'enregistrement réseau, mais ils appartiennent tous au même compte d'abonné. OmniHSS gère la correspondance IMSI-abonné et assure une authentification et un provisioning appropriés pour chaque IMSI.

OmniSS7 Stack v1.0.0

Download by Omnitouch © 2025 Omnitouch

SS7 Events

SS7 Client

M3UA

HLR Links

Active Subscribers

Resources

Configuration

Active Subscribers

Total: 0 Auto-refresh every 2 seconds

Active Subscribers: Subscribers who have sent an UpdateLocation request and have not yet sent a CancelLocation. This table shows the IMSI, current VLR, MSC, registration time, and duration for each active subscriber.

Clear All Subscribers

IMSI	VLR Number	MSC Number	Updated At	Duration
<div><div>No Active Subscribers</div><div>Subscribers will appear here when they send UpdateLocation requests.</div></div>				

Table des Matières

1. [Intégration OmniHSS](#)
2. [Support Multi-IMSI](#)
3. [Qu'est-ce que le Mode HLR ?](#)
4. [Activation du Mode HLR](#)
5. [Base de Données des Abonnés](#)
6. [Vecteurs d'Authentification](#)
7. [Mises à Jour de Localisation](#)
8. [Intégration CAMEL](#)
9. [Gestion des Abonnés en Roaming](#)
10. [Opérations HLR](#)

- [Mapping des Champs de Réponse](#)
 - [SendRoutingInfo \(SRU\)](#)
 - [UpdateLocation \(LSU\)](#)
 - [SendRoutingInfoForSM](#)
- [Résumé des Sources de Champs](#)

Qu'est-ce que le Mode HLR ?

Le **Mode HLR** permet à OmniSS7 de fonctionner comme un Home Location Register pour :

- **Gestion des Abonnés** : Stocker et gérer les données des abonnés
- **Authentification** : Gérer des vecteurs d'authentification pour l'accès au réseau
- **Suivi de Localisation** : Traiter les mises à jour de localisation provenant des VLR
- **Informations de Routage** : Fournir des informations de routage pour les appels et les SMS

Architecture HLR

Activation du Mode HLR

OmniSS7 peut fonctionner en différents modes. Pour l'utiliser comme HLR, vous devez activer le mode HLR dans la configuration.

Changement vers le Mode HLR

Le fichier `config/runtime.exs` d'OmniSS7 contient trois modes opérationnels préconfigurés. Pour activer le mode HLR :

1. **Ouvrez** `config/runtime.exs`
2. **Trouvez** les trois sections de configuration (lignes 53-174) :
 - Configuration 1 : Mode STP (lignes 53-85)
 - Configuration 2 : Mode HLR (lignes 87-123)
 - Configuration 3 : Mode SMS (lignes 125-174)
3. **Commentez** la configuration actuellement active (ajoutez # à chaque ligne)
4. **Décommentez** la configuration HLR (supprimez # des lignes 87-123)
5. **Personnalisez** les paramètres de configuration selon vos besoins
6. **Redémarrez** l'application : `iex -S mix`

Configuration du Mode HLR

La configuration HLR complète ressemble à ceci :

```
config :omniSS7,
  # Flags de mode - Activer uniquement les fonctionnalités HLR
  map_client_enabled: true,
  hlr_mode_enabled: true,
  smsc_mode_enabled: false,

  # Configuration de l'API Backend OmniHSS
  hlr_api_base_url: "https://10.180.2.140:8443",

  # Adresse GT du Centre de Service HLR pour les opérations SMS
  hlr_service_center_gt_address: "1234567890",

  # Configuration de Mapping MSISDN => IMSI
  # Voir : section Mapping MSISDN => IMSI pour les détails
  hlr_imsi_plan_prefix: "50557",
  hlr_msisdn_country_code: "61",
  hlr_msisdn_nsn_offset: 0,
  hlr_msisdn_nsn_length: 9,

  # Configuration InsertSubscriberData
  # Mode d'Accès Réseau : :packetAndCircuit, :packetOnly, ou :circuitOnly
  isd_network_access_mode: :packetAndCircuit,

  # Envoyer ISD #2 (données de Services Supplémentaires)
  isd_send_ss_data: true,

  # Envoyer ISD #3 (données de Barrage d'Appels)
  isd_send_call_barring: true,

  # Configuration CAMEL (pour les réponses SendRoutingInfo)
  # Clé de Service pour l'initiation de service CAMEL
  camel_service_key: 11_110,

  # Point de Détection de Déclenchement CAMEL
  # Options : :termAttemptAuthorized, :tBusy, :tNoAnswer, :tAnswer
  camel_trigger_detection_point: :termAttemptAuthorized,

  # Préfixes VLR à Domicile
  # Liste des préfixes d'adresses VLR considérés comme réseau "domestique"
  # Si le VLR de l'abonné commence par l'un de ces préfixes, utilisez la réponse SRI standard
  # Sinon, l'abonné est en roaming et nous devons envoyer PRN pour obtenir MSRN
  home_vlr_prefixes: ["123456"],

  # Configuration de Connexion MSUA
  # Se connecter en tant qu'ASP pour recevoir les opérations MAP (UpdateLocation, SendAuthInfo, etc.)
  map_client_m3ua: %{
    mode: "ASP",
    callback: (MapClient, :handle_payload, []),
    process_name: :hlr_client_asp,
    # Point de terminaison local (système HLR)
    local_ip: {10, 179, 4, 11},
    local_port: 2905,
    # Point de terminaison STP distant
    remote_ip: {10, 179, 4, 10},
    remote_port: 2905,
    routing_context: 1
  }
}
```

OmniSS7 Stack

SS7 Events

SS7 Client

M3UA

HLR Links

Active

Subscribers

Resources

Configuration

HLR API Connection Status

HLR HTTP API

Latency

46.14 ms

Version/Role

—

Host

https://10.180.2.140:8443

Details

{:tls_alert, {:bad_certificate, ~c"TLS client: In state wait_cert.cr at ssl_handshake.erl:2178 generated CLIENT ALERT: Fatal - Bad Certificate\n selfsigned_peer"}}}

DOWN

Subscriber Lookup

Lookup Type

IMSI

IMSI Value

e.g. 001010000000001

Lookup

Generate Authentication Vectors

IMSI

e.g. 001010000000001

Generate

Paramètres de Configuration à Personnaliser

Pour une référence complète de tous les paramètres de configuration, voir la [Référence de Configuration](#).

Paramètre	Type	Par Défaut	Description	Exemple
hlr_api_base_url	String	Requis	OmniHSS point d'API backend	"https://10.179.3.219:8443"
hlr_service_center_gt_address	String	Requis	Adresse GT HLR utilisée dans les réponses UpdateLocation	"5551234568"
smsc_service_center_gt_address	String	Requis	Adresse GT SMSC retournée dans les réponses SRI-for-SM	"5551234567"
hlr_smsc_alert_gts	Liste	[1]	Liste des GTs SMSC pour envoyer alertServiceCenter après UpdateLocation	["15559876543", "15559876544"]
hlr_alert_location_expiry_seconds	Integer	172800	Temps d'expiration de localisation (secondes) lorsque le SMSc reçoit alertServiceCenter	86400
hlr_imsi_plmn_prefix	String	"50557"	Préfixe PLMN (MCC+MNC) pour le mapping MSISDN→IMSI (voir MSISDN→IMSI Mapping)	"001001"
hlr_msisdn_country_code	String	"61"	Préfixe de code pays pour le mapping inverse IMSI→MSISDN (voir MSISDN→IMSI Mapping)	"1"
hlr_msisdn_nsn_offset	Integer	0	Décalage dans MSISDN pour l'extraction NSN (voir MSISDN→IMSI Mapping)	0
hlr_msisdn_nsn_length	Integer	9	Longueur du Numéro d'Abonné National à extraire (voir MSISDN→IMSI Mapping)	10
isd_network_access_mode	Atom	:packetAndCircuit	Mode d'accès réseau pour InsertSubscriberData	:packetOnly
isd_send_ss_data	Boolean	true	Envoyer ISD #2 avec des données de Services Supplémentaires	false
isd_send_call_barring	Boolean	true	Envoyer ISD #3 avec des données de Barrière d'Appels	false
camel_service_key	Integer	11_110	Clé de service CAMEL pour les réponses SendRoutingInfo	100
camel_trigger_detection_point	Atom	:termAttemptAuthorized	Point de détection de déclenchement CAMEL	:tBusy
home_vlr_prefixes	Liste	["5551231"]	Liste des préfixes d'adresses VLR considérés comme réseau "domestique"	["555123"]
local_ip	Tuple	Requis	Adresse IP de votre système HLR	{10, 179, 4, 12}
local_port	Integer	2905	Port SCTP local	2905
remote_ip	Tuple	Requis	Adresse IP STP pour la connectivité SS7	{10, 179, 4, 10}
remote_port	Integer	2905	Port SCTP distant	2905
routing_context	Integer	1	ID de contexte de routage M3UA	1

Paramètres de Configuration à Personnaliser

Pour une référence complète de tous les paramètres de configuration, voir la [Référence de Configuration](#).

Paramètre	Type	Par Défaut	Description	Exemple
hlr_api_base_url	String	Requis	OmniHSS point d'API backend	"https://10.179.3.219:8443"
hlr_service_center_gt_address	String	Requis	Adresse GT HLR utilisée dans les réponses UpdateLocation	"5551234568"
smsc_service_center_gt_address	String	Requis	Adresse GT SMSC retournée dans les réponses SRI-for-SM	"5551234567"
hlr_smsc_alert_gts	Liste	[1]	Liste des GTs SMSC pour envoyer alertServiceCenter après UpdateLocation	["15559876543", "15559876544"]
hlr_alert_location_expiry_seconds	Integer	172800	Temps d'expiration de localisation (secondes) lorsque le SMSc reçoit alertServiceCenter	86400
hlr_imsi_plmn_prefix	String	"50557"	Préfixe PLMN (MCC+MNC) pour le mapping MSISDN→IMSI (voir MSISDN→IMSI Mapping)	"001001"
hlr_msisdn_country_code	String	"61"	Préfixe de code pays pour le mapping inverse IMSI→MSISDN (voir MSISDN→IMSI Mapping)	"1"
hlr_msisdn_nsn_offset	Integer	0	Décalage dans MSISDN pour l'extraction NSN (voir MSISDN→IMSI Mapping)	0
hlr_msisdn_nsn_length	Integer	9	Longueur du Numéro d'Abonné National à extraire (voir MSISDN→IMSI Mapping)	10
isd_network_access_mode	Atom	:packetAndCircuit	Mode d'accès réseau pour InsertSubscriberData	:packetOnly
isd_send_ss_data	Boolean	true	Envoyer ISD #2 avec des données de Services Supplémentaires	false
isd_send_call_barring	Boolean	true	Envoyer ISD #3 avec des données de Barrière d'Appels	false
camel_service_key	Integer	11_110	Clé de service CAMEL pour les réponses SendRoutingInfo	100
camel_trigger_detection_point	Atom	:termAttemptAuthorized	Point de détection de déclenchement CAMEL	:tBusy
home_vlr_prefixes	Liste	["5551231"]	Liste des préfixes d'adresses VLR considérés comme réseau "domestique"	["555123"]
local_ip	Tuple	Requis	Adresse IP de votre système HLR	{10, 179, 4, 12}
local_port	Integer	2905	Port SCTP local	2905
remote_ip	Tuple	Requis	Adresse IP STP pour la connectivité SS7	{10, 179, 4, 10}
remote_port	Integer	2905	Port SCTP distant	2905
routing_context	Integer	1	ID de contexte de routage M3UA	1

Que se Passe-t-il Lorsque le Mode HLR est Activé

Lorsque hlr_mode_enabled: true, l'interface web affichera :

- **Événements SS7** - Journalisation des événements
- **Client SS7** - Test des opérations MAP
- **M3UA** - Etat de la connexion
- **Liens HLR** - Etat de l'API HLR + gestion des abonnés ~ *Spécifique au HLR*
- **Ressources** - Surveillance du système
- **Configuration** - Visualiseur de configuration

Les onglets **Routage**, **Test de Routage** et **Liens SMSc** seront cachés.

Notes Importantes

- **Configuration Requis** : Le paramètre hlr_service_center_gt_address est **obligatoire**. L'application échouera à démarrer s'il n'est pas configuré.
- **Backend OmniHSS** : L'API OmniHSS doit être accessible à l'URL hlr_api_base_url configurée.
- **Délai d'Attente des Requêtes API** : Toutes les requêtes API OmniHSS ont un **délai d'attente codé en dur de 5 secondes**
- **Délai d'Attente des Requêtes MAP** : Toutes les requêtes MAP (SRI, UpdateLocation, SendAuthInfo, etc.) ont un **délai d'attente codé en dur de 10 secondes**
- **Délai d'ISD** : Chaque message InsertSubscriberData (ISD) dans une séquence UpdateLocation a un **délai d'attente codé en dur de 10 secondes**
- La connexion M3UA au STP est requise pour recevoir les opérations MAP
- Après avoir changé de modes, vous devez redémarrer l'application pour que les modifications prennent effet
- **Interface Web** : Voir le [Guide de l'Interface Web](#) pour des informations sur l'utilisation de l'interface web
- **Accès API** : Voir le [Guide API](#) pour la documentation de l'API REST et l'accès à Swagger UI

Base de Données des Abonnés

OmniHSS gère toutes les données des abonnés y compris les identités, les informations d'authentification, les profils de service et les informations de localisation. OmniSS7 récupère ces données via des appels API RESTful.

Modèle d'Abonné OmniHSS

OmniHSS stocke des informations complètes sur les abonnés :

- **Plusieurs IMSI par abonné** : Support pour les configurations Multi-IMSI (eSIM, profils de roaming, changement de réseau)
- **Informations d'authentification** : Sélection de KI, Opc et algorithme (Milenage ou COMP128)
- **Profils de service** : Catégorie d'abonné, services autorisés, paramètres QoS
- **Suit de localisation** : Suivi indépendant de l'information de localisation actuelle VLR/MSC (session circuit) et SGSN/CGSN (session paquet)
- **Données d'abonnement CAMEL** : Clés de service, points de déclenchement et adresses gsmSCF
- **Services supplémentaires** : Transfert d'appels, barrages, attente, configurations CLIP/CLIR
- **Etat administratif** : Activé/désactivé, restrictions de service, dates d'expiration

Vecteurs d'Authentification

Générer des Vecteurs d'Authentification

OmniHSS génère des vecteurs d'authentification en utilisant les algorithmes Milenage ou COMP128 en fonction de la méthode d'authentification configurée pour chaque abonné. Lorsque OmniSS7 reçoit des requêtes MAP **sendAuthenticationInfo** :

1. OmniSS7 extrait l'IMSI de la requête MAP
2. OmniSS7 appelle l'API OmniHSS pour générer des vecteurs d'authentification
3. OmniHSS récupère les informations d'authentification Ki et Opc de l'abonné
4. OmniHSS génère le nombre demandé de vecteurs (RAND, XRES, CK, IK, AUTN)
5. OmniSS7 encode les vecteurs au format MAP et les retourne au VLR/SGSN demandeur

Intégration de l'API OmniHSS

OmniSS7 communique avec OmniHSS via l'API REST HTTPS pour récupérer des informations sur les abonnés, mettre à jour les données de localisation et générer des vecteurs d'authentification :

```
config :omniSS7,
  hlr_api_base_url: "https://omnihss-server:8443"
```

Lorsque OmniSS7 reçoit des opérations MAP du réseau SS7, il interroge OmniHSS pour :

- **Récupérer les données de l'abonné** par IMSI ou MSISDN
- **Générer des vecteurs d'authentification** en utilisant les informations Ki/OpC stockées
- **Mettre à jour la localisation de la session circuit** lorsque les abonnés effectuent UpdateLocation
- **Vérifier l'état de l'abonné** et les droits de service

Mises à Jour de Localisation

Traitement de la Mise à Jour de Localisation

Lors de la réception des requêtes MAP **updateLocation**, OmniSS7 coordonne avec OmniHSS pour enregistrer l'abonné à un nouveau VLR :

1. **Extraire les informations de localisation** de la requête UpdateLocation (IMSI, nouveau GT VLR, nouveau GT MSC)
2. **Interroger OmniHSS** pour vérifier que l'abonné existe et est activé
3. **Mettre à jour la session circuit** dans OmniHSS avec la nouvelle localisation VLR/MSC
4. **Envoyer des messages InsertSubscriberData (ISD)** pour provisionner l'abonné au nouveau VLR
5. **Retourner la réponse UpdateLocation** au VLR (inclut le GT HLR de hlr_service_center_gt_address)
6. **Envoyer alertServiceCenter** aux Gts SMSc configurés (si hlr_smc_alert_gts est peuplé)

Remarque : Le paramètre de configuration hlr_service_center_gt_address spécifie le Global Title du HLR qui est retourné dans les réponses UpdateLocation. Cela permet au VLR/MSC d'identifier et de router les messages de retour 📡 ce HLR.

Intégration du Centre de Service d'Alerte

Après une mise à jour de localisation réussie, le HLR peut automatiquement notifier les systèmes SMSc qu'un abonné est maintenant joignable en envoyant des messages **alertServiceCenter** (opcode MAP 64). Pour des informations sur la façon dont le SMSc gère ces alertes, voir [Gestion du Centre de Service d'Alerte dans le Guide SMSc](#).

Configuration

Configurez la liste des Global Titles SMSc à notifier :

```
config :omniSS7,
  # Liste des Gts SMSc pour envoyer alertServiceCenter après UpdateLocation
  hlr_smc_alert_gts: [
    "15559878543",
    "15559878544"
  ],

  # Temps d'expiration de localisation lorsque le SMSc reçoit alertServiceCenter (par défaut : 48 heures)
  hlr_alert_location_expiry_seconds: 172800
```

Diagramme de Flux

Comportement

Lorsqu'un abonné effectue une mise à jour de localisation :

1. Le HLR envoie alertServiceCenter à **chaque** GT SMSc dans la liste hlr_smc_alert_gts
2. Le message inclut le MSISDN de l'abonné
3. Le HLR utilise hlr_service_center_gt_address comme GT de l'appelant
4. Adressage SCCP : SSN appelant=6 (HLR), SSN appelé=8 (SMSc)

Le SMSc reçoit l'alerte et :

- **Supprime le préfixe TON/NPI** du MSISDN (par exemple, "19123123213" → "123123213")
- Marque l'abonné comme joignable dans sa base de données de localisation (via POST à /api/location)
- **Définit le champ user_agent** sur le GT HLR lors de l'appel à l'API (pour le suivi de quel HLR a envoyé l'alerte)
- Définit le temps d'expiration de localisation basé sur hlr_alert_location_expiry_seconds
- Suit l'abonné dans le Tracker d'Abonnés du SMSc pour la surveillance

Tests

Utilisez la page **Abonnés Actifs** dans l'interface Web pour envoyer manuellement des messages alertServiceCenter pour les tests :

1. Accédez à l'onglet "Abonnés Actifs"
2. Trouvez la section "Tester le Centre de Service d'Alerte"
3. Entrez MSISDN, GT SMSc et GT HLR (les valeurs par défaut sont pré-remplies à partir de la config)
 - GT SMSc par défaut est la première entrée dans hlr_smc_alert_gts
 - GT HLR par défaut est hlr_service_center_gt_address
4. Cliquez sur "Envoyer alertServiceCenter"

Ceci est utile pour tester la gestion des alertes SMSc sans nécessiter un flux complet de mise à jour de localisation. Le formulaire utilise la validation phx-blur pour éviter d'afficher des erreurs pendant la saisie.

Configuration InsertSubscriberData (ISD)

Après une mise à jour de localisation réussie, le HLR envoie des données de provisioning des abonnés au VLR en utilisant des messages **InsertSubscriberData** (ISD). La configuration ISD vous permet de personnaliser quelles données sont envoyées et comment.

Pour la référence des paramètres de configuration, voir [Configuration ISD dans la Référence de Configuration](#).

Séquence ISD

Le HLR peut envoyer jusqu'à 3 messages ISD séquentiels :

1. **ISD #1** (Toujours envoyé) - Données de base de l'abonné :
 - IMSI
 - MSISDN
 - Catégorie d'abonné
 - État de l'abonné (serviceGranted)
 - Liste des services de support
 - Liste des téléservices
 - Mode d'accès réseau
2. **ISD #2** (Optionnel) - Données des Services Supplémentaires (SS) :
 - Paramètres de transfert d'appels (inconditionnel, occupé, pas de réponse, non joignable)
 - Appel en attente
 - Mise en attente d'appel
 - Service multi-parties
 - État et fonctionnalités des services supplémentaires
3. **ISD #3** (Optionnel) - Données de Barrage d'Appels :
 - Barrage de tous les appels sortants (BAOC)
 - Barrage des appels internationaux sortants (BOIC)
 - Données de restriction d'accès

Options de Configuration

```
# Configuration InsertSubscriberData
# Mode d'Accès Réseau : :packetAndCircuit, :packetOnly, ou :circuitOnly
isd_network_access_mode: :packetAndCircuit,

# Envoyer ISD #2 (données de Services Supplémentaires)
isd_send_ss_data: true,

# Envoyer ISD #3 (données de Barrage d'Appels)
isd_send_call_barring: true,
```

Mode d'Accès Réseau

Le paramètre isd_network_access_mode contrôle quel type d'accès réseau l'abonné est autorisé :

Valeur	Description	Cas d'Utilisation
:packetAndCircuit	À la fois commuté par paquets (GPRS/LTE) et commuté par circuits (voix)	Par défaut - Abonnés à service complet
:packetOnly	Commuté par paquets uniquement (données/LTE)	Cartes SIM uniquement pour données, appareils IoT
:circuitOnly	Commuté par circuits uniquement (voix/SMS)	Appareils anciens, plans uniquement vocaux

Contrôle des Messages ISD

Vous pouvez contrôler quels messages ISD sont envoyés en fonction de vos besoins réseau :

Envoyer tous les ISD (Par défaut - Ensemble de fonctionnalités complet) :

```
isd_send_ss_data: true,
isd_send_call_barring: true,
```

Envoyer uniquement les données de base de l'abonné (Provisioning minimal) :

```
isd_send_ss_data: false,
isd_send_call_barring: false,
```

Envoyer de base + services supplémentaires (Pas de barrage d'appels) :

```
isd_send_ss_data: true,
isd_send_call_barring: false,
```

Exemple de Flux ISD

Lorsqu'une mise à jour de localisation est reçue :

```
HLR → HLR: UpdateLocation (DÉBUT)
HLR → VLR: InsertSubscriberData #1 (CONTINUER) - Données de base
HLR → HLR: ISD #1 ACK (CONTINUER)
```

HLR → VLR: InsertSubscriberData #2 (CONTINUER) - Données SS [si activé]
VLR → HLR: ISD #2 ACK (CONTINUER)
HLR → VLR: InsertSubscriberData #3 (CONTINUER) - Barrage d'appels [si activé]
VLR → HLR: ISD #3 ACK (CONTINUER)
HLR → VLR: Réponse UpdateLocation (FIN)

Si `isd_send_ss_data` ou `isd_send_call_barring` sont définis sur `false`, ces messages ISD sont ignorés, et la FIN de la mise à jour de localisation est envoyée plus tôt.

Melleures Pratiques

- **Configuration par Défaut** : Utilisez `packetAndCircuit` et activez tous les ISD pour une compatibilité maximale
- **IoT/M2M** : Utilisez `packetOnly` et désactivez les données SS/barrage d'appels pour les appareils uniquement pour données
- **Interopérabilité** : Certains VLR plus anciens peuvent ne pas prendre en charge tous les services supplémentaires - désactivez `isd_send_ss_data` si vous rencontrez des problèmes
- **Performance** : Désactiver les ISD inutilisés réduit la surcharge des messages et accélère les mises à jour de localisation

Intégration CAMEL

Configuration CAMEL pour SendRoutingInfo

Lors de la réponse aux requêtes **SendRoutingInfo** (SRI) d'un GMSC (Gateway MSC), le HLR peut demander au GMSC d'invoquer des services CAMEL pour un routage d'appels intelligent et un contrôle de service.

Pour la référence des paramètres de configuration, voir [Configuration CAMEL dans la Référence de Configuration](#).

Qu'est-ce que CAMEL ?

CAMEL (Applications Personnalisées pour la Logique Améliorée des Réseaux Mobiles) est un protocole qui permet des services réseau intelligents dans les réseaux GSM/UMTS. Il permet aux opérateurs de réseau de mettre en œuvre des services à valeur ajoutée tels que :

- Facturation prépayée
- Filtrage et barrage d'appels
- Réseaux Privés Virtuels (VPN)
- Services à tarif premium
- Transfert d'appels avec logique personnalisée
- Services basés sur la localisation

Options de Configuration

```
# Configuration CAMEL (pour les réponses SendRoutingInfo)
# Clé de Service pour l'initiation de service CAMEL
camel_service_key: 11_110,

# Point de Détection de Déclenchement CAMEL
# Options : :termAttemptAuthorized, :tBusy, :tNoAnswer, :tAnswer
camel_trigger_detection_point: :termAttemptAuthorized,
```

Clé de Service

La `camel_service_key` identifie quel service CAMEL doit être invoqué au `gsmSCF` (Service Control Function). Il s'agit d'un identifiant numérique configuré dans votre réseau :

Clé de Service	Cas d'Utilisation Typique
11_110	Contrôle des appels entrants prépayés (par défaut)
100	Service prépayé d'origine
200	Transfert d'appels avec logique personnalisée
300	Réseau Privé Virtuel (VPN)
Personnalisé	Services spécifiques à l'opérateur

Exemple de Configuration :

```
# Pour le contrôle des appels entrants prépayés
camel_service_key: 11_110,

# Pour le service VPN
camel_service_key: 300,
```

Point de Détection de Déclenchement

Le `camel_trigger_detection_point` spécifie quand le service CAMEL doit être déclenché lors de la configuration de l'appel :

Point de Détection	Description	Quand Déclenché
:termAttemptAuthorized	Tentative d'appel autorisée (par défaut)	Avant que l'appel ne soit routé vers l'abonné
:tBusy	Occupé à la terminaison	Lorsque l'abonné est occupé
:tNoAnswer	Pas de réponse à la terminaison	Lorsque l'abonné ne répond pas
:tAnswer	Réponse à la terminaison	Lorsque l'abonné répond à l'appel

Exemples de Configuration :

Contrôle prépayé standard (déclenchement avant le routage) :

```
camel_trigger_detection_point: :termAttemptAuthorized,
```

Gestion personnalisée des occupations (déclenchement lorsque occupé) :

```
camel_trigger_detection_point: :tBusy,
```

Facturation basée sur la réponse (déclenchement à la réponse) :

```
camel_trigger_detection_point: :tAnswer,
```

Réponse SRI avec CAMEL

Lorsqu'il est configuré, les réponses **SendRoutingInfo** incluent des informations d'abonnement CAMEL :

```
GMSC → HLR: SendRoutingInfo (DÉBUT)
HLR → GMSC: Réponse SRI (FIN) avec :
- IMSI
- Numéro VLR
- État de l'abonné
- Infos de routage CAMEL :
  * Clé de Service : 11_110
  * Adresse gsmSCF : <adresse configurée>
  * Point de Détection de Déclenchement : termAttemptAuthorized
  * Gestion des Appels par Défaut : continueCall
```

Le GMSC contacte `gsmSCF` au point de déclenchement pour exécuter le service CAMEL.

Melleures Pratiques

- **Réseaux de Production** : Utilisez des clés de service standardisées convenues avec votre fournisseur `gsmSCF`
- **Tests** : Utilisez `:termAttemptAuthorized` pour des tests les plus complets
- **Services Prépayés** : La clé de service `11_110` est une norme industrielle courante pour les appels entrants prépayés
- **Gestion de Repli** : `defaultCallHandling: :continueCall` garantit que les appels se poursuivent si le `gsmSCF` est injoignable

Gestion des Abonnés en Roaming

Détection VLR à Domicile vs VLR en Roaming

Lorsque le HLR reçoit une requête **SendRoutingInfo** (SRI), il doit déterminer si l'abonné est sur un VLR "domestique" (dans votre réseau) ou sur un VLR en roaming (visite d'un autre réseau). Le comportement diffère en fonction de cette détermination :

Pour la référence des paramètres de configuration, voir [Préfixes VLR à Domicile dans la Référence de Configuration](#).

- **VLR à Domicile** : Retourner une réponse SRI standard avec des informations de routage CAMEL
- **VLR en Roaming** : Envoyer une requête **Provide Roaming Number** (PRN) pour obtenir un MSRN, puis le retourner dans la réponse SRI

Configuration

```
# Préfixes VLR à Domicile
# Liste des préfixes d'adresses VLR considérés comme réseau "domestique"
# Si l'adresse VLR de l'abonné commence par l'un de ces préfixes, utilisez la réponse SRI standar
# Sinon, l'abonné est en roaming et nous devons envoyer PRN pour obtenir MSRN
home_vlr_prefixes: ["55123"],
```

Exemple de Configuration :

```
# Un seul opérateur de réseau domestique
home_vlr_prefixes: ["55123"],

# Plusieurs opérateurs de réseau domestique (par exemple, différentes régions ou filiales)
home_vlr_prefixes: ["55123", "55124", "55125"],
```

Comment Ça Fonctionne

1. Flux Abonné à Domicile (Standard)

Lorsque l'adresse VLR de l'abonné commence par un préfixe domestique configuré :

```
GMSC → HLR: SendRoutingInfo (MSISDN: "1234567890")
HLR interroge l'API backend pour les données de l'abonné
HLR vérifie l'adresse VLR : "551234567"
HLR détermine : VLR commence par "55123" → Réseau domestique
HLR → GMSC: Réponse SRI avec infos de routage CAMEL :
- IMSI
- Numéro VLR : "551234567"
- Adresse gsmSCF (MSC) : "551234501"
- Clé de service CAMEL : 11_110
- Point de détection de déclenchement : termAttemptAuthorized
```

2. Flux Abonné en Roaming (PRN Requis)

Lorsque l'adresse VLR de l'abonné ne correspond à aucun préfixe domestique :


```
GMSC → HLR: SendRoutingInfo (MSISDN: "1234567890")
HLR interroge l'API backend pour les données de l'abonné
HLR vérifie l'adresse VLR : "49170123456"
HLR détermine : VLR ne commence pas par "555123" → Roaming
HLR → MSC: ProvideRoamingNumber (PRN) :
- MSISDN : "1234567890"
- IMSI : "999999876543210"
- Numéro MSC : "49170123456"
- Adresse GMSC : "5551234567"
MSC → HLR: Réponse PRN avec MSRN : "49170999888777"
HLR → GMSC: Réponse SRI avec infos de routage :
- IMSI
- Numéro VLR : "49170123456"
- Numéro en Roaming (MSRN) : "49170999888777"
```

Différences de Structure de Réponse

Réponse SRI Abonné à Domicile

```
{
  imsi: "999999876543210",
  extendedRoutingInfo: {
    :camelRoutingInfo: {
      gsmCamelSubscriptionInfo: {
        "t-CSI": {
          serviceKey: 11 110,
          "gsmSCF-Address": "5551234501",
          defaultCallHandling: :continueCall,
          "t-BcmTriggerDetectionPoint": :termAttemptAuthorized
        }
      }
    }
  },
  subscriberInfo: {
    locationInformation: {v"vlr-number": "5551234567"},
    subscriberState: {notProvidedFromVLR, :NULL}
  }
}
```

Réponse SRI Abonné en Roaming

```
{
  imsi: "999999876543210",
  extendedRoutingInfo: {
    :routingInfo: {
      roamingNumber: "49170999888777" # MSRN de PRN
    }
  },
  subscriberInfo: {
    locationInformation: {v"vlr-number": "49170123456"},
    subscriberState: {notProvidedFromVLR, :NULL}
  }
}
```

Opération Provide Roaming Number (PRN)

Structure de la Requête PRN

La requête PRN envoyée au MSC/VLR contient :

	Champ	Source	Description
MSISDN		Requête SRI	Numéro de téléphone de l'abonné
IMSI		API HLR	IMSI de l'abonné
Numéro MSC		API HLR	MSC servant l'abonné en roaming (serving_msc)
Adresse GMSC		Requête SRI	GMSC effectuant la requête SRI originale
Numéro de Référence d'Appel		Statique	Identifiant de référence d'appel
Phases CAMEL Supportées		Statique	Phases CAMEL prises en charge par le GMSC

Gestion de la Réponse PRN

Le HLR attend une réponse PRN contenant :

- MSRN** (Numéro de Roaming de la Station Mobile) : Un numéro temporaire alloué par le réseau visité pour le routage de l'appel

Gestion des Erreurs :

- Si le PRN expire → Retourne l'erreur 27 (Abonné Absent) dans la réponse SRI
- Si le PRN échoue → Retourne l'erreur 27 (Abonné Absent) dans la réponse SRI
- Si le MSRN ne peut pas être extrait → Retourne l'erreur 27 (Abonné Absent) dans la réponse SRI

Exemples de Configuration

Opérateur de Réseau Domestique Unique

```
# Tous les adresses VLR commençant par "555123" sont considérées comme domestiques
home_vlr_prefixes: ["555123"],
```

- VLR 5551234567 → Domicile (réponse CAMEL)
- VLR 5551235001 → Domicile (réponse CAMEL)
- VLR 49170123456 → Roaming (PRN + réponse MSRN)

Opérateur Multi-Région

```
# Plusieurs réseaux domestiques dans différentes régions
home_vlr_prefixes: ["555123", "555124", "555125"],
```

- VLR 5551234567 → Domicile (région 1)
- VLR 5552341234 → Domicile (région 2)
- VLR 5553411111 → Domicile (région 3)
- VLR 44201234567 → Roaming (international)

Configuration de Test

Pour tester la fonctionnalité PRN, définissez une liste vide pour traiter tous les VLR comme en roaming :

```
# Tous les VLR sont traités comme en roaming (pour tester le flux PRN)
home_vlr_prefixes: [],
```

Meilleures Pratiques

- Sélection de Préfixe** : Utilisez le préfixe unique le plus court qui identifie les VLR de votre réseau (par exemple, code pays + code réseau)
- Multiples Préfixes** : Incluez tous les préfixes VLR de votre réseau, y compris différentes régions et filiales
- Accords de Roaming** : Assurez-vous que le PRN est correctement pris en charge par les réseaux partenaires en roaming
- Tests** : Testez à la fois les scénarios domestiques et en roaming de manière approfondie avant le déploiement en production
- Surveillance** : Surveillez les taux de délai d'attente du PRN pour identifier les problèmes de connectivité avec les partenaires en roaming

Dépannage

Symptôme : Tous les abonnés traités comme en roaming

- Cause** : `home_vlr_prefixes` non configuré ou préfixes ne correspondant pas aux adresses VLR
- Solution** : Vérifiez les adresses VLR dans votre base de données et mettez à jour les préfixes en conséquence

Symptôme : Les requêtes PRN expirant

- Cause** : Problèmes de connectivité réseau vers le MSC/VLR partenaire en roaming
- Solution** : Vérifiez le routage M3UA/SCCP vers les adresses MSC distantes

Symptôme : MSRN invalide dans la réponse SRI

- Cause** : Format de réponse PRN du partenaire en roaming ne correspondant pas à la structure attendue
- Solution** : Examinez les journaux de réponse PRN et ajustez `extract_msrn_from_prn/1` si nécessaire

Opérations HLR

Opérations MAP Supportées

- `updateLocation` (Opcode 2) - Enregistrer la localisation VLR
- `sendAuthenticationInfo` (Opcode 56) - Générer des vecteurs d'auth
- `sendRoutingInfo` (Opcode 22) - Fournir MSRN pour les appels avec support CAMEL
- `sendRoutingInfoForSM` (Opcode 45) - Fournir GT MSC pour SMS
- `cancelLocation` (Opcode 3) - Désenregistrer du VLR ancien
- `insertSubscriberData` (Opcode 7) - Pousser le profil de l'abonné

Mapping des Champs de Réponse

Cette section détaille d'où provient chaque champ dans les réponses HLR.

Réponse `SendRoutingInfo` (SRI)

But : Fournit des informations de routage pour les appels entrants vers un abonné.

Le HLR fournit deux types de réponses différents en fonction de si l'abonné est sur un VLR domestique ou en roaming :

Réponse Abonné à Domicile (Routage CAMEL)

Utilisé lorsque l'adresse VLR de l'abonné commence par une valeur configurée dans `home_vlr_prefixes`.

Structure de Réponse :

Champ	Source	Description	Exemple
IMSI	API OmniHSS	IMSI de l'abonné provenant de la base de données OmniHSS	"999999876543210"
Numéro VLR	API OmniHSS	VLR actuel servant l'abonné (circuit_session.assigned_vlr)	"5551234567"
Etat de l'Abonné	Statique	Toujours notProvidedFromVLR	:notProvidedFromVLR
extendedRoutingInfo	-	Type : camelRoutingInfo	-
Adresse gsmSCF	API OmniHSS	MSC servant l'abonné (circuit_session.assigned_msc)	"5551234501"
Cle de Service	runtime.exs	Identifiant de service CAMEL (camel_service_key)	11_110
Point de Détection de Déclenchement	runtime.exs	Quand déclencher CAMEL (camel_trigger_detection_point)	:termAttemptAuthorized
Gestion des Capacités CAMEL	Statique	Niveau de support de phase CAMEL	3
Gestion des Appels par Défaut	Statique	Repli si gsmSCF injoignable	:continueCall

Réponse Abonné en Roaming (Routage MSRN)

Utilisé lorsque l'adresse VLR de l'abonné ne correspond à aucun préfixe home_vlr_prefixes configuré.

Structure de Réponse :

Champ	Source	Description	Exemple
IMSI	API OmniHSS	IMSI de l'abonné provenant de la base de données OmniHSS	"999999876543210"
Numéro VLR	API OmniHSS	VLR actuel servant l'abonné (circuit_session.assigned_vlr)	"49170123456"
Etat de l'Abonné	Statique	Toujours notProvidedFromVLR	:notProvidedFromVLR
extendedRoutingInfo	-	Type : routingInfo	-
Numéro en Roaming (MSRN)	Réponse PRN	MSRN obtenu de la requête ProvideRoamingNumber	"49170999888777"

Logique de Décision de Routage :

- OmniSS7 reçoit la requête SendRoutingInfo
- OmniSS7 interroge les données de l'abonné depuis l'API OmniHSS
- OmniSS7 vérifie l'adresse VLR par rapport aux home_vlr_prefixes :

Si le VLR commence par un préfixe domestique :
- Retourner les infos de routage CAMEL (flux abonné domestique)

Si le VLR ne correspond à aucun préfixe domestique :
- Envoyer ProvideRoamingNumber (PRN) au MSC
- Extraire le MSRN de la réponse PRN
- Retourner les infos de routage avec MSRN (flux abonné en roaming)

Flux de Données :

- OmniSS7 interroge OmniHSS pour les informations sur l'abonné
- OmniHSS retourne IMSI, localisation actuelle VLR/MSC et état de l'abonné
- OmniSS7 utilise ces données pour construire la réponse MAP

Exigences de Configuration :

```
# Dans runtime.exs
home_vlr_prefixes: ["555123"], # Liste des préfixes VLR à domicile
```

Réponses d'Erreur :

- Si serving_vlr et serving_msc sont null : Retourne l'erreur 27 (Abonné Absent)
- Si l'abonné n'est pas trouvé : Retourne l'erreur 1 (Abonné Inconnu)
- Si la requête PRN expire (cas en roaming) : Retourne l'erreur 27 (Abonné Absent)
- Si la réponse PRN est invalide (cas en roaming) : Retourne l'erreur 27 (Abonné Absent)

Réponse UpdateLocation avec InsertSubscriberData

But : Enregistre l'abonné à un nouveau VLR et provisionne les données de l'abonné.

Réponse UpdateLocation FIN

Champ	Source	Description	Exemple
Numéro HLR	runtime.exs	Global Title de ce HLR (hlr_service_center_gt_address)	"5551234568"
Type de Message TCAP	Statique	Réponse finale après tous les ISD	FIN

InsertSubscriberData #1 (Données de Base de l'Abonné)

Champ	Source	Description	Exemple
IMSI	Requête	Provenant de la requête UpdateLocation	"999999876543210"
MSISDN	API OmniHSS	Numéro de téléphone de l'abonné provenant d'OmniHSS	"555123456"
Catégorie	Statique	Catégorie d'abonné	"A" (00A)
Etat de l'Abonné	Statique	Etat de service	:serviceGranted
Liste des Services de Support	Statique	Services de support pris en charge	[<<31>>]
Liste des Téléservices	Statique	Téléservices pris en charge	[<<17>>, "1", "\"]
Mode d'Accès Réseau	runtime.exs	Accès par paquet/circuit (isd_network_access_mode)	:packetAndCircuit

InsertSubscriberData #2 (Services Supplémentaires) - Optionnel

Champ	Source	Description	Contrôlé Par
SS Provisionnés	Statique	Données des services supplémentaires	isd_send_ss_data: true
Transfert d'Appels	Statique	Configurations de transfert (inconditionnel, occupé, pas de réponse, non joignable)	Config activé
Appel en Attente	Statique	Etat du service d'appel en attente	Config activé
Service Multi-Parties	Statique	Support d'appel conférence	Config activé

ISD #2 Inclut :

- Transfert d'appels inconditionnel (code SS 21)
- Transfert d'appels en cas d'occupation (code SS 41)
- Transfert d'appels en cas de non réponse (code SS 42)
- Transfert d'appels en cas de non joignabilité (code SS 62)
- Appel en attente (code SS 43)
- Service multi-parties (code SS 51)
- Services CLIP/CLIR

InsertSubscriberData #3 (Barrage d'Appels) - Optionnel

Champ	Source	Description	Contrôlé Par
Infos de Barrage d'Appels	Statique	Configurations de barrage d'appels	isd_send_call_barring: true
BAOC	Statique	Barrage de tous les appels sortants (code SS 146)	Config activé
BOIC	Statique	Barrage des appels internationaux sortants (code SS 147)	Config activé
Données de Restriction d'Accès	Statique	Restrictions d'accès au réseau	Config activé

Contrôle de Séquence ISD :

- ISD #1 : **Toujours envoyé** - Contient les données essentielles de l'abonné
- ISD #2 : Envoyé uniquement si isd_send_ss_data: true dans runtime.exs
- ISD #3 : Envoyé uniquement si isd_send_call_barring: true dans runtime.exs

Réponse SendRoutingInfoForSM (SRI-for-SM)

But : Fournit des informations de routage MSC/SMSC pour la livraison de SMS. Lorsqu'un SMSc doit livrer un SMS à un abonné, il envoie une requête SRI-for-SM au HLR pour déterminer où router le message.

Structure de Réponse :

Champ	Source	Description	Comment Généré	Exemple
IMSI	Calculé	IMSI synthétique dérivé de MSISDN	PLMN_PREFIX + zero_padded_MSISDN	"001001555123456"
Numéro de Noeud Réseau	runtime.exs	Adresse GT SMSC pour le routage SMS	smc_service_center_gt_address	"5551234567"

Paramètres de Configuration (depuis runtime.exs) :

```
# Adresse GT du Centre de Service (retournée dans les réponses SRI-for-SM)
# Cela indique au SMSc demandeur d'envoyer les messages MT-ForwardSM
smc_service_center_gt_address: "5551234567", # Requis
```

```
# Configuration de Mapping MSISDN -> IMSI
# Préfixe PLMN : MCC (001 = Réseau de Test) + MNC (01 = Opérateur de Test)
hlr_imsi_plmn_prefix: "001001", # Seul paramètre de config nécessaire !
```

Mapping MSISDN ↔ IMSI

Paramètres de Configuration :

Ces paramètres contrôlent comment OmniSS7 génère des IMSI synthétiques à partir des MSISDN pour les réponses SRI-for-SM :

- hlr_imsi_plmn_prefix : Le préfixe MCC+MNC à utiliser lors de la construction des IMSI synthétiques (par exemple, "50557" pour MCC=505, MNC=57)
- hlr_imsi_plmn_prefix : Code de pays à préfixer lors du mapping inverse IMSI→MSISDN (par exemple, "61" pour l'Australie, "1" pour les Etats-Unis/Canada)
- hlr_imsi_plmn_offset : Position du caractère où commence le Numéro d'Abonné National (NSN) dans le MSISDN (typiquement 0 si le MSISDN n'inclut pas le code pays, ou longueur du code pays s'il l'inclut)
- hlr_imsi_plmn_length : Nombre de chiffres à extraire du MSISDN comme NSN

Pour des détails supplémentaires sur la configuration, voir [Mapping MSISDN ↔ IMSI dans la Référence de Configuration](#).

Pourquoi le Mapping MSISDN vers IMSI est-il Nécessaire ?

Le protocole MAP pour **SendRoutingInfoForSM** (SRI-for-SM) exige que le HLR retourne un **IMSI** (Identité Internationale d'Abonné Mobile) dans sa réponse. Cependant, le SMSc demandeur ne connaît que le **MSISDN** (numéro de téléphone).

Dans un réseau traditionnel :

- Le SMSc envoie SRI-for-SM avec le MSISDN de destination (par exemple, "5551234567")
- Le HLR doit rechercher l'abonné dans sa base de données pour trouver son IMSI
- Le HLR retourne l'IMSI dans la réponse SRI-for-SM
- Le SMSc utilise ensuite cet IMSI lors de l'envoi de MT-ForwardSM au MSC/VLR

Approche d'OmniSS7 - IMSIs Synthétiques :

Au lieu de maintenir une base de données complète des abonnés avec des mappings MSISDN vers IMSI, OmniSS7 utilise un schéma d'encodage simple pour **calculer** des IMSI synthétiques directement à partir des MSISDN. Cette approche offre deux avantages clés :

1. **Confidentialité** : Les véritables IMSI des abonnés stockés dans la base de données HLR ne sont jamais exposés dans les réponses SRI-for-SM envoyées sur le réseau SS7
2. **Simplicité** : Pas besoin d'interroger la base de données HLR pour les recherches IMSI lors des opérations SRI-for-SM - l'IMSI est calculé à la volée à partir du MSISDN

Comment Ça Fonctionne :

Les MSISDN sont encodés directement dans la portion d'abonné de l'IMSI (les chiffres après MCC+MNC) :

IMSI = PLMN_PREFIX + zero_padded_MSISDN

Où :

- **PLMN_PREFIX** : MCC + MNC (par exemple, "001001" pour Réseau de Test)
- **MSISDN** : Tous les chiffres numériques du numéro de téléphone
- **Zero Padding** : Complété par des zéros à gauche pour remplir l'IMSI à exactement 15 chiffres

Exemple Étape par Étape :

```
# Configuration
plmn_prefix = "001001" # MCC 001 + MNC 01

# Entrée : MSISDN de la requête SRI-for-SM (décodé TBDC)
msisdn = "555123456" # 9 chiffres

# Étape 1 : Calculer l'espace disponible pour le numéro d'abonné
subscriber_digits = 15 - String.length("001001") # = 9 chiffres

# Étape 2 : Compléter le MSISDN avec des zéros pour remplir la portion d'abonné
padded_msisdn = String.pad_left("555123456", 9, "0") # = "555123456" (pas de remplissage nécessaire)

# Étape 3 : Concaténer le préfixe PLMN + MSISDN complété
imsi = "001001" <-> "555123456" # = "001001555123456" (exactement 15 chiffres)
```

Exemples Complets :

MSISDN d'Entrée	Préfixe PLMN	Chiffres d'Abonné Disponibles	MSISDN Complété	IMSI Final	Remarques
"555123456"	"001001" (6)	9	"555123456"	"001001555123456"	Ajustement exact, pas de remplissage
"99"	"001001" (6)	9	"000000099"	"001001000000099"	Complété par des zéros
"999999999"	"001001" (6)	9	"999999999"	"001001999999999"	Ajustement exact
"91123456789"	"001001" (6)	9	"555123456"	"001001555123456"	Trop long, les 9 chiffres de droite sont conservés

Gestion des Cas Limites :

- **MSISDN Courts** : Complétés par des zéros à gauche (par exemple, "99" → "000000099")
- **MSISDN Longs** : Les chiffres de droite sont conservés, les chiffres de gauche sont tronqués (par exemple, "91123456789" → "555123456")
- **Longueur de l'IMSI** : Toujours exactement 15 chiffres

Mapping Inverse (IMSI → MSISDN) :

Le SMSc peut inverser ce mapping pour convertir les IMSIs en MSISDN :

```
# Entrée : IMSI de la réponse SRI-for-SM
imsi = "001001555123456"

# Étape 1 : Supprimer le préfixe PLMN
plmn_prefix = "001001"
subscriber_portion = String.slice(imsi, 6, 9) # = "555123456"

# Étape 2 : Supprimer Les zéros à gauche pour obtenir le MSISDN réel
msisdn = String.replace_leading(subscriber_portion, "0", "") # = "555123456"
```

Exemples de Mapping Inverse :

IMSI d'Entrée	Préfixe PLMN	Portion d'Abonné	Supprimer les Zéros à Gauche	MSISDN Final
"001001555123456"	"001001"	"555123456"	"555123456"	"555123456"
"001001000000099"	"001001"	"000000099"	"09"	"99"
"001001999999999"	"001001"	"999999999"	"999999999"	"999999999"

Propriétés de Ce Mapping :

- **Déterministe** : Le même MSISDN produit toujours le même IMSI
- **Récupérable** : Peut être converti en retour de IMSI à MSISDN
- **Configuration Minimale** : Nécessite uniquement hlr_imsi_plmn_prefix
- **Préservation de la Confidentialité** : Les véritables IMSI ne sont jamais exposés
- **Aucune Recherche dans la Base de Données** : Calcul rapide, aucun appel API nécessaire
- **Toujours 15 Chiffres** : L'IMSI est toujours exactement de 15 chiffres

Gestion des Entrées MSISDN :

Lorsque le HLR reçoit une requête SRI-for-SM, le MSISDN subit un décodage TBDC :

1. **Décodage TBDC** : Convertir TBDC binaire en chaîne (peut inclure un préfixe TON/NPI comme "91")
2. **Extraire les Chiffres** : Conserver uniquement les chiffres numériques, supprimer tout caractère non numérique
3. **Normaliser** : Si plus long que l'espace disponible, prendre les chiffres de droite ; si plus court, compléter par des zéros
4. **Encoder** : Concaténer le préfixe PLMN + MSISDN normalisé

Considérations de Sécurité :

Les IMSIs synthétiques retournés dans les réponses SRI-for-SM sont uniquement à des fins de routage. Ils ne sont PAS les véritables IMSIs stockés dans la base de données des abonnés HLR. Cela fournit une couche supplémentaire de protection de la vie privée, car les véritables IMSIs des abonnés ne sont exposés que lorsque cela est absolument nécessaire (par exemple, lors des opérations UpdateLocation ou SendAuthenticationInfo qui nécessitent de véritables vecteurs d'authentification).

Flux de Réponse :

1. SMSc → HLR: Requête SRI-for-SM
- MSISDN (TBDC) : "91123456789" (inclut TON/NPI)
2. Traitement HLR :
- Décodage TBDC : "91123456789"
- Extraire les chiffres : "91123456789" (11 chiffres)
- Adapter à 9 chiffres : "555123456" (9 chiffres de droite)
- Ajouter PLMN : "001001" + "555123456" = "001001555123456"
- Obtenir GT SMSc depuis la config : "5551234567"
3. HLR → SMSc: Réponse SRI-for-SM
- IMSI : "001001555123456" (synthétique, toujours 15 chiffres)
- Numéro de Noeud Réseau : "5551234567" (où envoyer MT-ForwardSM)
4. SMSc envoie MT-ForwardSM à "5551234567" avec IMSI "001001555123456"

Configuration :

Les paramètres suivants sont utilisés dans runtime.exs :

```
# Préfixe PLMN : MCC (001 = Réseau de Test) + MNC (01 = Opérateur de Test)
hlr_imsi_plmn_prefix: "001001",

# Extraction NSN (si les MSISDN incluent le code pays)
hlr_msisdn_country_code: "1", # Utilisé pour le mapping inverse (IMSI→MSISDN)
hlr_msisdn_nsn_offset: 1, # Ignorer 1 chiffre du code pays
hlr_msisdn_nsn_length: 10 # Extraire 10 chiffres NSN
```

Configuration d'Extraction NSN :

Si vos MSISDN incluent le code pays (par exemple, "68988000088" au lieu de simplement "88000088"), vous devez configurer l'extraction NSN :

- **hlr_msisdn_nsn_offset** : Position où commence le NSN (typiquement la longueur de votre code pays)
- **hlr_msisdn_nsn_length** : Nombre de chiffres dans le NSN

Exemples :

Exemple	Code Pays	MSISDN	Exemple_nsn_offset	nsn_length	NSN Extraît
Code Pays à 1 Chiffre "9"	"9"	"95551234567"	1	10	"5551234567"
Code Pays à 2 Chiffres "99"	"99"	"99412345678"	2	9	"412345678"
Code Pays à 3 Chiffres "999"	"999"	"99988000088"	3	8	"88000088"

Comment Ça Fonctionne :

1. **MSISDN → IMSI** : Extraire le NSN du MSISDN, compléter par des zéros, concaténer avec le préfixe PLMN

```
MSISDN : "99988000088"
NSN : String.slice("99988000088", 3, 8) = "88000088"
MSISDN Complété : "088000088" (9 chiffres)
IMSI : "547050" + "088000088" = "54705088000088"
```

2. **IMSI → MSISDN** : Supprimer le préfixe PLMN, supprimer les zéros à gauche, préfixer le code pays

```
IMSI : "54705088000088"
Portion d'Abonné : "088000088"
Supprimer les zéros : "88000088"
MSISDN : "+999" + "88000088" = "+99988000088"
```

Exigences de l'API : Aucune - SRI-for-SM utilise des valeurs calculées et la config uniquement. Aucun appel à la base de données n'est requis.

Résumé des Sources de Champs

Type de Source	Description	Exemples
API OmniHSS	Données dynamiques provenant de la base de données des abonnés OmniHSS	IMSI, MSISDN, VLR/MSC servant depuis circuit_session
runtime.exs	Paramètres de configuration OmniSS7	smsc_service_center_gt_address, camel_service_key, isd_network_access_node
Statique	Valeurs codées en dur dans le générateur de réponse	État de l'abonné, services de support, codes SS
Requête	Champs extraits de la requête MAP entrante	IMSI de UpdateLocation, MSISDN de SRI
Calculé	Valeurs dérivées utilisant la logique	IMSI synthétique dans SRI-for-SM (hlr_imsi_prefix + NSN)

Dépendances de Configuration

Requis dans runtime.exs :

- hlr_service_center_gt_address - Utilisé dans les réponses UpdateLocation
- smsc_service_center_gt_address - Utilisé dans les réponses SRU-for-SM (où les MT-ForwardSM doivent être routés)

Optionnel dans runtime.exs (avec valeurs par défaut) :

- camel_service_key - Par défaut : 11_110
- camel_trigger_detection_point - Par défaut : :termAttemptAuthorized
- isd_network_access_mode - Par défaut : :packetAndCircuit
- isd_send_ss_data - Par défaut : true
- isd_send_call_barring - Par défaut : true
- hlr_imsi_plmn_prefix - Par défaut : "001001" (préfixe PLMN pour le mapping MSISDN→IMSI)

Requis de la part d'OmniHSS :

OmniHSS doit fournir des points d'API REST pour :

- Recherche d'abonné par IMSI et MSISDN
- Mises à jour de localisation de session circuit (assignation VLR/MSC)
- Génération de vecteurs d'authentification
- Requêtes sur l'état de l'abonné et les profils de service

Documentation Connexe

Documentation OmniSS7 :

- [= Retour à la Documentation Principale](#)
- [Guide des Fonctionnalités Communes](#)
- [Guide Client MAP](#)
- [Référence Technique](#)
- [Référence de Configuration](#)

Documentation OmniHSS : Pour la gestion des abonnés, le provisioning, la configuration de l'authentification et les opérations administratives, reportez-vous à la **documentation produit OmniHSS**. OmniHSS contient toute la logique de base de données des abonnés, les algorithmes d'authentification, les règles de provisioning de service et les capacités de gestion Multi-IMSI.

OmniSS7 par Omnitouch Network Services

Guide de Configuration du Client MAP

[-- Retour à la Documentation Principale](#)

Ce guide fournit une configuration détaillée pour utiliser OmniSS7 en tant que **Client MAP** pour envoyer des requêtes du protocole MAP aux éléments du réseau.

OmniSS7 Stack v1.0.0

Changelog to OmniSS7
© 2024 OmniTouch

SS7 Events

SS7 Client

M3UA

Routing

Routing Test

SMSc Links

Resources

Configuration

MAP Test Client

SendRoutingInfo

PRN

SendRoutingInfoForSM

SendAuthenticationInfo

MT-forwardSM

ForwardSM

UpdateLocation

CancelLocation

AnyTimeUpdate

SendSM

SMS-Deliver-PDU

mslscn

123456789

gmsc

Submit

Got response in 0 seconds

RESPONSE

```
{
  "components": [
    {
      "type": "BasicRMS",
      "value": {
        "action": "returnError",
        "errorCode": 27,
        "severity": 0
      }
    }
  ],
  "id": "B75ABF93",
  "type": "end"
}
```




Table des Matières

- 1. [Qu'est-ce que le Mode Client MAP ?](#)
- 2. [Activation du Mode Client MAP](#)
- 3. [Opérations MAP Disponibles](#)
- 4. [Envoi de Requetes via l'API](#)
- 5. [Métriques et Surveillance](#)
- 6. [Dépannage](#)

Qu'est-ce que le Mode Client MAP ?

Mode Client MAP permet à OmniSS7 de se connecter en tant que **Processus Serveur d'Application (ASP)** à un pair M3UA (STP ou SGP) et d'envoyer/recevoir des messages **MAP (Mobile Application Part)** pour des services tels que :

- **Requêtes HLR** : SRI (Send Routing Info), SRI-for-SM, Authentication Info
- **Mises à Jour de Localisations** : Update Location, Cancel Location
- **Gestion des Abonnés** : Provide Roaming Number (PRN), Insert Subscriber Data

Architecture Réseau

Activation du Mode Client MAP

Éditez config/runtime.exs et configurez les paramètres du client MAP. Pour une référence de configuration complète, voir [Paramètres de Connexion M3UA dans la Référence de Configuration](#).

Configuration de Base

```
config :omiss7,
  # Activer le mode Client MAP
  map_client_enabled: true,

  # Connexion M3UA pour le Client MAP (se connecte en tant qu'ASP à un STP/SGP distant)
  map_client_m3ua: %{
    mode: "ASP",
    callback: (MapClient, :handle_payload, []), # Callback pour les messages entrants
    process_name: :map_client_esp, # Nom du processus enregistré
    local_ip: {10, 0, 0, 100}, # Adresse IP locale
    local_port: 2905, # Port SCTP local
    remote_ip: {10, 0, 0, 1}, # IP STP/SGP distante
    remote_port: 2905, # Port STP/SGP distant
    routing_context: 1 # Contexte de routage M3UA
  }
```

Exemple de Configuration en Production

```
config :omiss7,
  # Activer le Client MAP pour la production
  map_client_enabled: true,

  # Connexion M3UA en production
  map_client_m3ua: %{
    mode: "ASP",
    callback: (MapClient, :handle_payload, []),
    process_name: :map_client_esp,
    local_ip: {10, 0, 0, 100},
    local_port: 2905,
    remote_ip: {10, 0, 0, 1}, # IP STP en production
    remote_port: 2905,
    routing_context: 1
  }

config :control_panel,
  web: %{
    listen_ip: "0.0.0.0",
    port: 443,
    hostname: "ss7-gateway.example.com",
    enable_tls: true,
    tls_cert: "/etc/ssl/certs/gateway.crt",
    tls_key: "/etc/ssl/private/gateway.key"
  }
```

Opérations MAP Disponibles

MAP Tester API 1.0.0 OAS 3.0

swagger.json

default ^

POST

/api/MT-forwardSM

MT-forwardSM MAP Request (For sending SMS for delivery by remote MSC/SMSC)

^

POST

/api/deliverPDU

Utility: Build SMS-DELIVER TPDU from originating address + GSM7

^

POST

/api/forwardSM

forwardSM MAP Request

^

POST

/api/prn

ProvideRoamingNumber (PRN) MAP Request

^

POST

/api/send-auth-info

SendAuthenticationInfo MAP Request

^

POST

/api/sendSM

Utility: Perform SRI-for-SM + MT-forwardSM from MSISDN and GSM7

^

POST

/api/sri

SendRoutingInfo MAP Request

^

POST

/api/sri-for-sm

SendRoutingInfoForSM MAP Request

^

POST

/api/updateLocation

UpdateLocation MAP Request

^

GET

/metrics

Prometheus metrics

^

GET

/swagger.json

OpenAPI spec

^

Schemas ^

AuthInfoRequest

>

ErrorResponse

>

ForwardSMRequest

>

PRNRequest

>

SMSDeliverPDURequest

>

SMSDeliverPDUResponse

>

SRIForSMRequest

>

SRIRequest

>

SRIResponse

>

SendSMRequest

>

UpdateLocationRequest

>

1. Envoyer des Informations de Routage pour SM (SRI-for-SM)

Interroge le HLR pour déterminer le MSC servant pour la livraison de SMS. Pour des informations détaillées sur la façon dont le HLR traite les requêtes SRI-for-SM, voir [SRI-for-SM dans le Guide HLR](#).

Point de terminaison API : POST /api/sri-for-sm

Requête :

```
{
  "msisdn": "447712345678",
  "serviceCenter": "447999123456"
}
```

Réponse :

```
{
  "result": {
    "imsi": "234509876543210",
    "locationInfoWithLMSI": {
      "networkNode-Number": "44799955111"
    }
  }
}
```

Exemple cURL :

```
curl -X POST http://localhost/api/sri-for-sm \
-H 'Content-Type: application/json' \
-d '{
  "msisdn": "447712345678",
  "serviceCenter": "447999123456"
}'
```

2. Envoyer des Informations de Routage (SRI)

Interroge le HLR pour des informations de routage d'appel vocal.

Point de terminaison API : POST /api/sri

Requête :

```
{
  "msisdn": "447712345678",
  "gmsc": "447999123456"
}
```

Réponse :

```
{
  "result": {
    "imsi": "234509876543210",
    "extendedRoutingInfo": {
      "routingInfo": {
        "roamingNumber": "44799955222"
      }
    }
  }
}
```

3. Fournir un Numéro de Roaming (PRN)

Demande un numéro de roaming temporaire (MSRN) au MSC servant.

Point de terminaison API : POST /api/prn

Requête :

```
{
  "msisdn": "447712345678",
  "gmsc": "447999123456",
  "msc_number": "447999555111",
  "imsi": "234509876543210"
}
```

4. Envoyer des Informations d'Authentification

Demande des vecteurs d'authentification au HLR pour l'authentification des abonnés.

Point de terminaison API : POST /api/send-auth-info

Requête :

```
{
  "imsi": "234509876543210",
  "vectors": 5
}
```

Réponse :

```
{
  "result": {
    "authenticationSetList": [
      {
        "rand": "0123456789ABCDEF0123456789ABCDEF",
        "xres": "ABCDEF0123456789",
        "ck": "0123456789ABCDEF0123456789ABCDEF",
        "ik": "FEDCBA9876543210FEDCBA9876543210",
        "autn": "0123456789ABCDEF0123456789ABCDEF"
      }
    ]
  }
}
```

5. Mettre à jour la Localisation

Enregistre la localisation actuelle d'un abonné auprès du HLR. Pour des informations détaillées sur le traitement de UpdateLocation et les séquences d'InsertSubscriberData, voir [Mises à Jour de Localisation dans le Guide HLR](#).

Point de terminaison API : POST /api/updateLocation

Requête :

```
{
  "imsi": "234509876543210",
  "vlr": "447999555111"
}
```

Résumé des Opérations MAP

Envoi de Requêtes via l'API

Utilisation de Swagger UI

L'interface Swagger UI fournit une interface interactive pour envoyer des requêtes SS7.

Accéder à Swagger UI :

- 1. Naviguez vers <http://your-server/swagger>
- 2. Parcourez les points de terminaison API disponibles
- 3. Cliquez sur n'importe quel point de terminaison pour développer ses détails

Envoyer une Requête :

- 1. Cliquez sur le point de terminaison que vous souhaitez utiliser (par exemple, /api/sri-for-sm)
- 2. Cliquez sur le bouton "Try it out"
- 3. Remplissez les paramètres requis dans le corps de la requête
- 4. Cliquez sur "Exécute"
- 5. Consultez la réponse ci-dessous

Codes de Réponse de l'API

- **200** - Succès, résultat retourné dans le corps de la réponse
- **400** - Mauvaise Requête, paramètres invalides
- **504** - Délai d'Attente de la Passerelle, pas de réponse du réseau SS7 dans les 10 secondes

Métriques du Client MAP

Métriques Disponibles

Métriques de Requête :

- `map_requests_total` - Nombre total de requêtes MAP envoyées
 - Étiquettes : operation (valeurs : sri, sri_for_sm, prn, authentication_info, etc.)
- `map_request_errors_total` - Nombre total d'erreurs de requêtes MAP
 - Étiquettes : operation
- `map_request_duration_milliseconds` - Histogramme des durées des requêtes MAP
 - Étiquettes : operation
- `map_pending_requests` - Nombre actuel de requêtes MAP en attente (gauge)

Exemples de Requêtes Prometheus

```
# Total des requêtes SRI-for-SM au cours de la dernière heure
increase(map_requests_total(operation="sri_for_sm")[1h])

# Temps de réponse moyen pour les requêtes SRI
rate(map_request_duration_milliseconds_sum(operation="sri")[5m]) /
rate(map_request_duration_milliseconds_count(operation="sri")[5m])

# Taux d'erreur pour toutes les opérations MAP
sum(rate(map_request_errors_total[5m])) by (operation)

# Requêtes en attente actuelles
map_pending_requests
```

Dépannage Client MAP

Problème : Délai d'Attente des Requêtes

Symptômes :

- L'API retourne 504 Gateway Timeout
- Pas de réponse du HLR/MS

Vérifications :

- 1. Vérifiez que la connexion M3UA est ACTIVE :

```
# Dans la console IEx
:sys.get_state(:map_client_asp)
```
- 2. Vérifiez la connectivité réseau vers le STP
- 3. Vérifiez le contexte de routage et l'adressage SCCP
- 4. Vérifiez les journaux pour des erreurs SCCP

Problème : Erreurs SCCP

Symptômes :

- L'API retourne des réponses d'erreur SCCP
- Les journaux montrent des messages "SCCP unitdata service"

Codes d'Erreur SCCP Courants :

- **Pas de Traduction** : Titre Global non trouvé dans la table de routage STP
- **Échec de Sous-système** : Sous-système de destination (HLR SSN 6) indisponible
- **Échec Réseau** : Congestion ou échec du réseau

Solutions :

- Contacter l'administrateur STP pour vérifier la configuration de routage
- Vérifiez que le Titre Global de destination est accessible
- Vérifiez si le sous-système de destination est opérationnel

Documentation Connexe

- [~ Retour à la Documentation Principale](#)
- [Guide des Fonctionnalités Communes](#) - Interface Web, API, Surveillance
- [Guide SIP](#) - Configuration de routage
- [Guide du Centre SMS](#) - Livraison de SMS
- [Référence Technique](#) - Spécifications du protocole

OmniSS7 par Omnitouch Network Services



Guide de Configuration du Centre SMS (SMSc)

[← Retour à la Documentation Principale](#)

Ce guide fournit une configuration détaillée pour utiliser OmniSS7 comme un **Centre SMS (SMSc)** en tant que frontend avec **OmniMessage** comme plateforme de stockage et de livraison des messages en backend.

Intégration d'OmniMessage

Le mode SMSc d'OmniSS7 fonctionne comme un frontend de signalisation SS7 qui s'interface avec **OmniMessage**, une plateforme SMS de niveau opérateur. Cette architecture sépare les préoccupations :

- **OmniSS7 (Frontend SMSc)** : Gère tous les signaux de protocole SS7/MAP, le routage SCCP et la communication réseau
- **OmniMessage (Backend SMS)** : Gère le stockage des messages, la mise en file d'attente, la logique de réessai, le suivi de livraison et les décisions de routage

Pourquoi OmniMessage ?

OmniMessage fournit des capacités de messagerie SMS de niveau opérateur avec des fonctionnalités incluant :

- **Gestion de la File d'Attente des Messages** : Stockage persistant avec une logique de réessai configurable et une mise en file d'attente par priorité
- **Suivi de Livraison** : Statut de livraison en temps réel, rapports de livraison (DLR) et suivi des raisons d'échec
- **Support Multi-SMSc** : Plusieurs instances de frontend peuvent se connecter à un seul backend OmniMessage pour l'équilibrage de charge et la redondance
- **Intelligence de Routage** : Règles de routage avancées basées sur la destination, l'expéditeur, le contenu du message et l'heure de la journée
- **Limitation de Taux** : Contrôles TPS (transactions par seconde) par route pour prévenir la congestion du réseau
- **Conception API-First** : API HTTP RESTful pour l'intégration avec les systèmes de facturation, les portails clients et les applications tierces
- **Analytique & Reporting** : Statistiques sur le volume des messages, taux de succès de livraison et métriques de performance

Toutes les données de message, l'état de livraison et les configurations de routage sont stockées et gérées dans OmniMessage. OmniSS7 interroge OmniMessage via des appels API HTTPS pour récupérer les messages en attente, mettre à jour l'état de livraison et s'enregistrer en tant que frontend actif.

Important : Le mode SMSc d'OmniSS7 est un **frontend de signalisation uniquement**. Toute la logique de routage des messages, la gestion des files d'attente, les algorithmes de réessai, le suivi de livraison et les règles métier sont gérés par OmniMessage. Ce guide couvre la configuration du protocole SS7/MAP dans OmniSS7. Pour des informations sur le routage des messages, la configuration des files d'attente, les rapports de livraison, la limitation de taux et l'analytique, **reportez-vous à la documentation d'OmniMessage**.

Table des Matières

1. [Intégration d'OmniMessage](#)
 2. [Qu'est-ce que le Mode Centre SMS ?](#)
 3. [Activation du Mode SMSc](#)
 4. [Configuration de l'API HTTP](#)
 5. [Flux de Messages SMS](#)
 6. [Prévention des Boucles](#)
 7. [Suivi des Abonnés SMSc](#)
 8. [Configuration de Flush Automatique](#)
 9. [Métriques et Surveillance](#)
 10. [Dépannage](#)
-

Qu'est-ce que le Mode Centre SMS ?

Remarque : Cette section couvre uniquement la configuration de signalisation SS7 d'OmniSS7. Pour les règles de routage des messages, la gestion des files d'attente, le suivi de livraison et la configuration de la logique métier, voir la **documentation produit d'OmniMessage**.

Le **Mode Centre SMS** permet à OmniSS7 de fonctionner comme un SMSc pour :

- **Livraison MT-SMS** : Livraison de SMS Terminés vers les abonnés
- **Gestion MO-SMS** : Réception et routage de SMS Origines Mobiles
- **Mise en File d'Attente des Messages** : File d'attente de messages soutenue par une base de données avec logique de réessai
- **Flush Automatique** : Livraison automatique de SMS depuis la file d'attente
- **Rapports de Livraison** : Suivi de l'état de livraison des messages

Architecture du Centre SMS

Activation du Mode SMSc

OmniSS7 peut fonctionner en différents modes. Pour l'utiliser comme un SMSc, vous devez activer le mode SMSc dans la configuration.

Changer vers le Mode SMSc

Le fichier config/runtime.exs d'OmniSS7 contient trois modes opérationnels préconfigurés. Pour activer le mode SMSc :

1. **Ouvrir** config/runtime.exs
2. **Trouver** les trois sections de configuration (lignes 53-204) :
 - Configuration 1 : Mode STP (lignes 53-95)
 - Configuration 2 : Mode HLR (lignes 97-142)
 - Configuration 3 : Mode SMSc (lignes 144-204)
3. **Commenter** toute autre configuration active (ajouter # à chaque ligne)
4. **Décommenter** la configuration SMSc (retirer # des lignes 144-204)
5. **Personnaliser** les paramètres de configuration selon les besoins
6. **Redémarrer** l'application : iex -S mix

Configuration du Mode SMSc

La configuration complète du SMSc ressemble à ceci :

```
config :omniSS7,  
  # Drapeaux de mode - Activer les fonctionnalités STP + SMSc  
  # Remarque : map_client_enabled est vrai car le SMSc a besoin de capacités de routage  
  map_client_enabled: true,  
  hlr_mode_enabled: false,  
  smsc_mode_enabled: true,  
  
  # Configuration de l'API Backend OmniMessage  
  smsc_api_base_url: "https://10.179.3.219:8443",  
  # Identification du SMSc pour l'enregistrement avec le backend  
  smsc_name: "ipsmgw",  
  # Adresse GT du Centre de Service pour les opérations SMS  
  smsc_service_center_gt_address: "5551234567",  
  
  # Configuration de Flush Automatique (traitement de la file d'attente SMS en arrière-plan)  
  auto_flush_enabled: true,  
  auto_flush_interval: 10_000,  
  auto_flush_dest_smsc: "ipsmgw",  
  auto_flush_tps: 10,  
  
  # Configuration de Connexion M3UA  
  # Se connecter en tant qu'ASP pour envoyer/recevoir des opérations MAP SMS  
  map_client_m3ua: %{
```

```

mode: "ASP",
callback: {MapClient, :handle_payload, []},
process_name: :stp_client_asp,
# Point de terminaison local (système SMSc)
local_ip: {10, 179, 4, 12},
local_port: 2905,
# Point de terminaison STP distant
remote_ip: {10, 179, 4, 10},
remote_port: 2905,
routing_context: 1
}

config :control_panel,
  use_additional_pages: [
    {SS7.Web.EventsLive, "/events", "Événements SS7"},
    {SS7.Web.TestClientLive, "/client", "Client SS7"},
    {SS7.Web.M3UAStatusLive, "/m3ua", "M3UA"},
    {SS7.Web.RoutingLive, "/routing", "Routage"},
    {SS7.Web.RoutingTestLive, "/routing_test", "Test de Routage"},
    {SS7.Web.SmscLinksLive, "/smsc_links", "Liens SMSc"}
  ],
  page_order: ["/events", "/client", "/m3ua", "/routing", "/routing_test", "/smsc_links",
"/application", "/configuration"]

```

Paramètres de Configuration à Personnaliser

Pour une référence complète de tous les paramètres de configuration, voir la [Référence de Configuration](#).

Paramètre	Type	Par Défaut	Description	Exemple
smsc_api_base_url	String	<i>Requis</i>	Point de terminaison de l'API backend OmniMessage Votre identifiant	"https://10.179.3.219:8443"
smsc_name	String	"{hostname}_SMSc"	SMSc pour l'enregistrement	"ipsmgw"
smsc_service_center_gt_address	String	<i>Requis</i>	Titre Global du Centre de Service	"5551234567"
auto_flush_enabled	Boolean	true	Activer le traitement automatique de la file d'attente	false
auto_flush_interval	Integer	10_000	Intervalle de traitement de la file d'attente en millisecondes	5_000
auto_flush_dest_smsc	String	<i>Requis</i>	Nom du SMSc de destination pour le flush automatique	"ipsmgw"
auto_flush_tps	Integer	10	Taux de traitement des messages (transactions/seconde)	20
local_ip	Tuple	<i>Requis</i>	Adresse IP de votre système SMSc	{10, 179, 4, 12}
local_port	Integer	2905	Port SCTP local	2905
remote_ip	Tuple	<i>Requis</i>	Adresse IP STP pour la connectivité SS7	{10, 179, 4, 10}
remote_port	Integer	2905	Port SCTP	2905

Paramètre	Type	Par Défaut	Description	Exemple
routing_context	Integer	1	distant ID de contexte de routage M3UA	1

Que Se Passe-t-il Lorsque le Mode SMSc est Activé

Lorsque `smsc_mode_enabled: true` et `map_client_enabled: true`, l'interface web affichera :

- **Événements SS7** - Journalisation des événements
- **Client SS7** - Test des opérations MAP
- **M3UA** - État de la connexion
- **Routage** - Gestion de la table de routage (STP activé)
- **Test de Routage** - Test de routage (STP activé)
- **Liens SMSc** - État de l'API SMSc + gestion de la file d'attente SMS ← *Spécifique au SMSc*
- **Ressources** - Surveillance du système
- **Configuration** - Visualiseur de configuration

L'onglet **Liens HLR** sera masqué.

Notes Importantes

- Le mode SMSc nécessite `map_client_enabled: true` pour les capacités de routage
- **Backend OmniMessage** : L'API OmniMessage doit être accessible à l'URL `smsc_api_base_url` configurée
- **Enregistrement du Frontend** : Le système s'enregistre automatiquement auprès d'OmniMessage toutes les **5 minutes** via le module `SMS.FrontendRegistry`
- **Délai d'Attente des Requêtes API** : Toutes les requêtes API OmniMessage ont un **délai d'attente codé en dur de 5 secondes**
- **Délai d'Attente des Requêtes MAP** : Toutes les requêtes MAP (SRI-for-SM, MT-ForwardSM, etc.) ont un **délai d'attente codé en dur de 10 secondes**
- Le flush automatique traite automatiquement la file d'attente SMS en arrière-plan
- La connexion M3UA au STP est requise pour envoyer/recevoir des opérations MAP SMS
- Après avoir changé de mode, vous devez redémarrer l'application pour que les changements prennent effet
- **Interface Web** : Voir le [Guide de l'Interface Web](#) pour des informations sur l'utilisation de l'interface web
- **Accès API** : Voir le [Guide API](#) pour la documentation de l'API REST et l'accès à l'interface Swagger

Configuration de l'API HTTP

Configuration du Backend OmniMessage

OmniSS7 communique avec OmniMessage via l'API REST HTTPS pour gérer la livraison des messages, suivre l'état des abonnés et s'enregistrer en tant que frontend actif :

```
config :omniss7,
  # URL de base de l'API OmniMessage
  smsc_api_base_url: "https://10.5.198.200:8443",
  # Identifiant du nom SMSc pour l'enregistrement (par défaut à hostname_SMSc si vide)
  smsc_name: "omni-smsc01",
  # Adresse GT du Centre de Service pour les opérations SMS
  smsc_service_center_gt_address: "5551234567"
```

Paramètres de Configuration :

Paramètre	Type Requis	Par Défaut	Description
smsc_api_base_url	StringOui	"https://localhost:8443"	URL de base pour l'API OmniMessage
smsc_name	StringNon	" (utilise "{hostname}_SMSc")	Identifiant SMSc pour l'enregistrement et la gestion de la file d'attente
smsc_service_center_gt_address	StringNon	"5551234567"	Adresse GT du Centre de Service renvoyée dans les réponses SRI-

Paramètre	Type Requis	Par Défaut	Description
			for-SM. Cela indique aux autres éléments du réseau où router les messages MT-ForwardSM. Voir le Guide SRI-for-SM pour plus de détails.

Enregistrement du Frontend

Le système s'enregistre automatiquement auprès d'OmniMessage au démarrage et **se réenregistre toutes les 5 minutes** via le module SMS.FrontendRegistry. Cela permet à OmniMessage de :

- Suivre les frontends actifs pour l'équilibrage de charge
- Surveiller le temps de fonctionnement et l'état de santé
- Collecter des informations de configuration
- Gérer le routage SMS distribué à travers plusieurs frontends

Détails de Mise en Œuvre :

- **Intervalle d'Enregistrement** : 5 minutes (codé en dur)
- **Processus** : Démarré automatiquement lorsque `smc_mode_enabled: true`

Charge Utile d'Enregistrement :

```
{
  "frontend_name": "omni-smc01",
  "configuration": "{...}",
  "frontend_type": "SS7",
  "hostname": "smc-server01",
  "uptime_seconds": 12345
}
```

Remarque : Le nom du frontend est pris du paramètre de configuration `smc_name`. S'il n'est pas défini, il par défaut à `"{hostname}_SMC"`.

Communication avec l'API OmniMessage

Lorsque OmniSS7 reçoit des opérations MAP du réseau SS7 ou traite la file d'attente de messages, il communique avec OmniMessage pour :

- **S'enregistrer en tant que frontend actif** et signaler l'état de santé
- **Soumettre des messages d'origine mobile (MO)** reçus des abonnés
- **Récupérer des messages terminés mobiles (MT)** de la file d'attente pour livraison
- **Mettre à jour l'état de livraison** avec des rapports de succès/échec
- **Interroger des informations de routage** pour le transfert de messages

Point de terminaison	Méthode	But	Corps de la Requête
/api/frontends	POST	Enregistrer une instance de frontend	{"frontend_name": "...", "frontend_type": "SMSc", "hostname": "...", "uptime_seconds": ...}
/api/messages_raw	POST	Insérer un nouveau message SMS	{"source_msisdn": "...", "source_smc": "...", "message_body": "..."} Obtenir la file d'attente de messages
/api/messages	GET	Marquer le message comme livré	En-tête : smc: <smc_name>
/api/messages/{id}	PATCH	Mettre à jour l'état du message	{"deliver_time": "...", "dest_smc": "..."} {"dest_smc": null}
/api/locations	POST	Insérer/mettre à jour la localisation de	{"msisdn": "...", "imsi": "...", "location": "...", "ims_capable": true, "csfb": false, "expires": "...", "user_agent": "...", "ran_location": "...", "imei": "...",

Point de terminaison	Méthode	But	Corps de la Requête
		l'abonné	"registered": "..."} Ajouter un
/api/events	POST	suivi d'événement	{"message_id": ..., "name": "...", "description": "..."} d'événement
/api/status	GET	Vérification de santé	-

Format de Réponse de l'API

Toutes les réponses de l'API utilisent le format JSON avec les conventions suivantes :

- **Réponses de succès** : HTTP 200-201 avec un corps JSON contenant les données de résultat
- **Réponses d'erreur** : HTTP 4xx/5xx avec des détails d'erreur dans le corps de la réponse
- **Horodatages** : Format ISO 8601 (par exemple, "2025-10-21T12:34:56Z")
- **IDs de Message** : Identifiants entiers ou chaînes

Modules Client API

Le système SMS se compose de trois modules principaux :

1. SMS.APIClient

Module principal du client API fournissant toute la communication HTTP API avec OmniMessage :

- `frontend_register/4` - Enregistrer le frontend auprès d'OmniMessage
- `insert_message/3` - Insérer un message SMS brut (version compatible Python à 3 paramètres)
- `insert_location/9` - Insérer/mettre à jour les données de localisation de l'abonné
- `get_message_queue/2` - Récupérer les messages en attente de la file d'attente
- `mark_dest_smsc/3` - Marquer le message comme livré ou échoué
- `add_event/3` - Ajouter un suivi d'événement pour les messages
- `flush_queue/2` - Traiter les messages en attente (SRI-for-SM + MT-forwardSM)
- `auto_flush/2` - Boucle de traitement continu de la file d'attente

2. SMS.FrontendRegistry

Gère l'enregistrement périodique du frontend auprès du backend :

- S'enregistre automatiquement au démarrage
- Se réenregistre toutes les 5 minutes
- Utilise `smc_name` de la config (retombe sur le nom d'hôte)
- Collecte des informations de configuration et de temps de fonctionnement du système

3. SMS.Util

Fonctions utilitaires pour les opérations SMS :

- `generate_tp_scts/0` - Générer un horodatage SMS au format TPDU

Flux de Messages SMS

Flux SMS Entrant (Mobile-Originé)

Flux SMS Sortant (Mobile-Terminé)

Étapes Clés Expliquées :

- **Demande SRI-for-SM** : Le SMSc interroge le HLR avec le MSISDN de destination pour déterminer où router le message SMS. Le HLR répond avec :
 - Un IMSI synthétique (calculé à partir du MSISDN pour la confidentialité) - voir [MSISDN ↔ IMSI Mapping](#)
 - L'adresse GT du SMSc (numéro de nœud réseau) où le MT-ForwardSM doit être envoyé

- Pour des détails complets sur le fonctionnement de cela, voir [SRI-for-SM dans le Guide HLR](#)
- **Demande MT-forwardSM** : Une fois les informations de routage obtenues, le SMSc envoie le message SMS réel au MSC/VLR servant l'abonné

Structure du SMS TPDU

Gestion du Centre de Service d'Alerte

Le SMSc peut recevoir des messages **alertServiceCenter** du HLR pour suivre l'état de disponibilité des abonnés.

Pour des informations sur la façon dont le HLR envoie des messages alertServiceCenter, voir [Intégration du Centre de Service d'Alerte dans le Guide HLR](#).

Qu'est-ce que alertServiceCenter ?

Lorsqu'un abonné effectue une UpdateLocation au HLR (c'est-à-dire, s'enregistre avec un nouveau VLR/MSC), le HLR peut notifier les systèmes SMSc que l'abonné est maintenant joignable en envoyant un message **alertServiceCenter** (opcode MAP 64).

Configuration

Le temps d'expiration de la localisation est configuré dans le HLR :

```
config :omniss7,  
  # Temps d'expiration de la localisation lorsque le SMSc reçoit alertServiceCenter (par défaut  
  : 48 heures)  
  hlr_alert_location_expiry_seconds: 172800
```

Comportement

Lorsque le SMSc reçoit un message alertServiceCenter :

1. **Décoder MSISDN** : Extraire le MSISDN de l'abonné du message (format TBCD)
2. **Supprimer le préfixe TON/NPI** : Enlever les préfixes courants comme "19", "11", "91" (par exemple, "19123123213" → "123123213")
3. **Calculer IMSI** : Générer un IMSI synthétique en utilisant le même mappage que SRI-for-SM
4. **POST à /api/location** : Mettre à jour la base de données de localisation avec :
 - msisdn: Numéro de téléphone de l'abonné (nettoyé)
 - imsi: IMSI synthétique
 - location: Nom du SMSc (par exemple, "ipsmgw")
 - expires: Heure actuelle + hlr_alert_location_expiry_seconds
 - csfb: true (abonné joignable via Circuit-Switched Fallback)
 - ims_capable: false (il s'agit d'un enregistrement CS 2G/3G, pas IMS/VoLTE)
 - user_agent: GT du HLR qui a envoyé l'alerte (pour le suivi)
 - ran_location: "SS7"
5. **Suivre dans le Suivi des Abonnés SMSc** : Enregistrer l'abonné avec GT HLR, status=actif, compteurs de messages à 0
6. **Envoyer ACK** : Répondre au HLR avec un accusé de réception alertServiceCenter

Gestion des Abonnés Absents

Lorsque le SMSc tente de livrer un message et reçoit une erreur "abonné absent" lors de SRI-for-SM (pour plus d'informations sur SRI-for-SM, voir [SRI-for-SM dans le Guide HLR](#)) :

1. **Détecter l'absence** : SRI-for-SM renvoie l'erreur absentSubscriberDiagnosticSM
2. **Expirer la localisation** : POST à /api/location avec expires=0 pour marquer l'abonné comme injoignable
3. **Agent utilisateur** : Défini sur "SS7_AbsentSubscriber" pour identifier la source
4. **Mettre à jour le tracker** : Marquer l'abonné comme failed dans le Suivi des Abonnés SMSc

Cela garantit que la base de données de localisation et le tracker reflètent avec précision l'état de disponibilité des abonnés.

Diagramme de Flux

Point de Terminaison API

POST /api/location

```
{
  "msisdn": "15551234567",
  "imsi": "001010123456789",
  "location": "ipsmgw",
  "ims_capable": false,
  "csfb": true,
  "expires": "2025-11-01T12:00:00Z",
  "user_agent": "15551111111",
  "ran_location": "SS7",
  "imei": "",
  "registered": "2025-10-30T12:00:00Z"
}
```

Remarque : Le champ `user_agent` contient le GT du HLR qui a envoyé l'alertServiceCenter, permettant au SMSc de suivre quel HLR fournit des mises à jour de localisation.

Pour les abonnés absents, `expires` est défini sur l'heure actuelle (expiration immédiate).

Prévention des Boucles

Le SMSc met en œuvre une **prévention automatique des boucles** pour éviter des boucles de routage de messages infinies lorsque les messages proviennent de réseaux SS7.

Pourquoi la Prévention des Boucles est Importante

Lorsque le SMSc reçoit des messages SMS d'origine mobile (MO) du réseau SS7, il les insère dans la file d'attente de messages avec un champ `source_smsc` identifiant leur origine (par exemple, "SS7_GT_15551234567"). Sans prévention des boucles, ces messages pourraient être :

1. Reçus du réseau SS7 → Mis en file d'attente avec `source_smsc` contenant "SS7"
2. Récupérés de la file d'attente → Traitement pour livraison
3. Renvois au réseau SS7 → Créant une boucle

Comment Cela Fonctionne

Le SMSc détecte et prévient automatiquement les boucles lors du traitement des messages :

Mise en Œuvre

Lors du traitement des messages de la file d'attente, le SMSc vérifie le champ `source_smsc` :

- **Si `source_smsc` contient "SS7" :**
 - Le message est ignoré
 - Événement ajouté : "Prévention des Boucles" avec une description expliquant la raison de l'ignorance
 - Message marqué comme échoué via une requête PUT
 - Journalisé avec un niveau d'avertissement
- **Sinon :**
 - Le message est traité normalement
 - Les opérations SRI-for-SM et MT-ForwardSM se poursuivent

Valeurs Source SMSC

Les messages peuvent avoir diverses valeurs `source_smsc` :

Source	Valeur Exemple	Action
Réseau SS7 (MO-FSM)	"SS7_GT_15551234567"	Ignoré - Prévention des boucles
API Externe/SMPP	"ipsmgw" ou "api_gateway"	Traité normalement
Autre SMSc	"sm-sc-node-01"	Traité normalement

Suivi des Événements

Lorsqu'un message est ignoré en raison de la prévention des boucles, un événement est enregistré :

```
{
  "message_id": 12345,
  "name": "Prévention des Boucles",
  "description": "Message ignoré - source_smsc 'SS7_GT_15551234567' contient 'SS7', empêchant la
boucle de message"
}
```

Cet événement est visible dans :

- **Interface Web** : Page des Événements SS7 (/events)
- **Base de Données** : Table events via l'API
- **Journaux** : Entrées de journal au niveau d'avertissement

Configuration

La prévention des boucles est **toujours activée** et ne peut pas être désactivée. C'est une fonctionnalité de sécurité critique pour prévenir les perturbations du réseau dues aux boucles de messages.

Scénario Exemple

Scénario : Un abonné mobile envoie un SMS via le réseau SS7

1. Téléphone mobile → MSC/VLR → SMSc (via MO-ForwardSM)
2. SMSc reçoit MO-FSM de GT 15551234567
3. SMSc insère dans la file d'attente : source_smsc = "SS7_GT_15551234567"
4. Le flush automatique récupère le message de la file d'attente
5. SMSc détecte "SS7" dans source_smsc → IGNORER
6. Événement enregistré : "Prévention des Boucles"
7. Message marqué comme échoué
8. Aucun SRI-for-SM ou MT-ForwardSM envoyé (boucle empêchée)

Sans prévention des boucles, l'étape 8 renverrait le message au réseau SS7, créant potentiellement une boucle infinie.

Suivi des Abonnés SMSc

Le SMSc comprend un GenServer **Suivi des Abonnés** qui maintient l'état en temps réel des abonnés basé sur les messages alertServiceCenter et les tentatives de livraison de messages.

Objectif

Le tracker fournit :

- **Surveillance de la Disponibilité** : Quels abonnés sont actuellement joignables
- **Suivi HLR** : Quel HLR a envoyé l>alertServiceCenter pour chaque abonné
- **Compteurs de Messages** : Nombre de messages envoyés/reçus par abonné
- **Suivi des Échecs** : Marquer les abonnés comme échoués lorsque les tentatives de livraison échouent
- **Visibilité de l'Interface Web** : Tableau de bord en temps réel montrant tous les abonnés suivis

Informations Suivies

Pour chaque abonné, le tracker stocke :

Champ	Description	Exemple
msisdn	Numéro de téléphone de l'abonné (clé)	"15551234567"

Champ	Description	Exemple
imsi	IMSI de l'abonné	"001010123456789"
hlr_gt	GT HLR qui a envoyé alertServiceCenter	"15551111111"
messages_sent	Compte des messages MT-FSM envoyés	5
messages_received	Compte des messages MO-FSM reçus	2
status	:active ou :failed	:active
updated_at	Horodatage Unix de la dernière mise à jour	1730246400

Transitions d'État

Comportement

Lorsque alertServiceCenter est reçu :

- Créer ou mettre à jour l'entrée de l'abonné
- Définir status = :active
- Enregistrer le GT HLR
- Réinitialiser ou préserver les compteurs de messages

Lorsque SRI-for-SM réussit :

- Incrémenter le compteur messages_sent
- Mettre à jour l'horodatage updated_at

Lorsque SRI-for-SM échoue :

- Définir status = :failed
- Garder dans le tracker pour surveillance

Lorsque l'abonné est supprimé :

- Supprimer de la table ETS
- N'apparaît plus dans l'interface Web

Interface Web - Page des Abonnés SMSc

Chemin : /smc_subscribers **Actualisation automatique :** Toutes les 2 secondes

Remarque : Cette page n'est disponible que lorsque vous exécutez en mode SMSc. Après avoir décommenté la configuration SMSc dans config/runtime.exs, vous devez redémarrer l'application pour que la route devienne disponible.

La page **Abonnés SMSc** fournit une surveillance en temps réel de tous les abonnés suivis :

Fonctionnalités

1. Tableau des Abonnés

- MSISDN, IMSI, HLR GT
- Compteurs de messages envoyés/reçus
- Badge de statut (Actif/Échoué) avec codage couleur
- Horodatage de la dernière mise à jour et durée
- Bouton de suppression pour les abonnés individuels

2. Statistiques Résumées

- Total des abonnés suivis
- Compte des abonnés actifs
- Compte des abonnés échoués
- Nombre de HLR uniques

3. Actions

- Tout Effacer : Supprimer tous les abonnés suivis
- Supprimer : Supprimer un abonné individuel

Exemple de Vue

Abonnés Suivis SMSc				Total : 3
MSISDN	IMSI	HLR GT	Msgs S/R	Statut
15551234567	001010123456789	15551111111	5/2	● Actif
15559876543	001010987654321	15551111111	0/0	● Actif
15551112222	001010111222233	15552222222	3/1	○ Échoué

Résumé : Total : 3 | Actifs : 2 | Échoués : 1 | HLR Uniques : 2

Fonctions API

Le tracker expose ces fonctions pour un accès programmatique :

```
# Appelé lorsque alertServiceCenter est reçu
SMSc.SubscriberTracker.alert_received(msisdn, imsi, hlr_gt)

# Incrémenter les compteurs de messages
SMSc.SubscriberTracker.message_sent(msisdn)
SMSc.SubscriberTracker.message_received(msisdn)

# Marquer comme échoué (échec SRI-for-SM)
SMSc.SubscriberTracker.mark_failed(msisdn)

# Supprimer du suivi
SMSc.SubscriberTracker.remove_subscriber(msisdn)

# Fonctions de requête
SMSc.SubscriberTracker.get_active_subscribers()
SMSc.SubscriberTracker.get_subscriber(msisdn)
SMSc.SubscriberTracker.count_subscribers()
SMSc.SubscriberTracker.clear_all()
```

Intégration

Le tracker est automatiquement intégré avec :

- **Gestionnaire alertServiceCenter** : Appelle alert_received/3 lors de la mise à jour de localisation réussie
- **Gestionnaire SRI-for-SM** : Incrémente messages_sent lors du routage réussi
- **Gestionnaire Abonné Absent** : Appelle mark_failed/1 lorsque l'abonné est absent
- **Erreurs d'abonnés inconnus** : Appelle mark_failed/1 lorsque SRI-for-SM échoue

Configuration de Flush Automatique de la File d'Attente SMS

Le service **Flush Automatique** traite automatiquement les messages SMS en attente.

Pour la référence des paramètres de configuration, voir [Configuration de Flush Automatique dans la Référence de Configuration](#).

Configuration

```
config :omniss7,
  auto_flush_enabled: true,          # Activer/désactiver le flush automatique
  auto_flush_interval: 10_000,      # Intervalle de sondage en millisecondes
  auto_flush_dest_smsc: nil,        # Filtre : nil = tous
  auto_flush_tps: 10                # Max transactions par seconde
```

Comment Cela Fonctionne

1. **Sondage** : Toutes les `auto_flush_interval` millisecondes, interroge l'API pour les messages en attente
2. **Filtrage** : Filtrer éventuellement par `auto_flush_dest_smsc`
3. **Limitation de Taux** : Traiter jusqu'à `auto_flush_tps` messages par cycle
4. **Livraison** : Pour chaque message :
 - Envoyer **SRI-for-SM** (Envoyer les Informations de Routage pour le Message Court) au HLR pour obtenir des informations de routage
 - Le HLR renvoie un IMSI synthétique calculé à partir du MSISDN
 - Le HLR renvoie l'adresse GT du SMSc où le MT-ForwardSM doit être envoyé
 - Voir [Détails SRI-for-SM dans le Guide HLR](#) pour la documentation complète
 - En cas de succès, envoyer **MT-forwardSM** au MSC/VLR
 - Mettre à jour l'état du message via l'API (livré/échoué)
 - Ajouter un suivi d'événement via l'API

❖ **Plongée Technique** : Pour une explication complète de la façon dont SRI-for-SM fonctionne, y compris le mappage MSISDN à IMSI, la configuration de l'adresse GT du centre de service et la génération d'IMSI synthétique préservant la confidentialité, voir la [section SRI-for-SM dans le Guide de Configuration HLR](#).

Métriques SMSc

Métriques Disponibles

Métriques de la File d'Attente SMS :

- `smc_queue_depth` - Nombre actuel de messages en attente
- `smc_messages_delivered_total` - Total des messages livrés avec succès
- `smc_messages_failed_total` - Total des messages ayant échoué à la livraison
- `smc_delivery_duration_milliseconds` - Histogramme des temps de livraison

Exemples de Requêtes :

```
# Profondeur de la file d'attente actuelle
smc_queue_depth

# Taux de succès de livraison (dernières 5 minutes)
rate(smc_messages_delivered_total[5m]) /
(rate(smc_messages_delivered_total[5m]) + rate(smc_messages_failed_total[5m]))

# Temps de livraison moyen
rate(smc_delivery_duration_milliseconds_sum[5m]) /
rate(smc_delivery_duration_milliseconds_count[5m])
```

Dépannage SMSc

Problème : Messages Non Livrés

Vérifications :

1. Vérifiez que le flush automatique est activé
2. Vérifiez la connexion à la base de données
3. Surveillez les journaux pour des erreurs
4. Vérifiez que la connexion M3UA est ACTIVE
5. Vérifiez les limites TPS

Problème : Haute Profondeur de File d'Attente

Causes Possibles :

- Limite TPS trop basse
- Problèmes de délai d'attente HLR
- Problèmes de connectivité réseau
- Numéros de destination invalides

Solutions :

- Augmenter auto_flush_tps
- Vérifier la disponibilité du HLR
- Examiner les journaux des messages échoués

API MT-forwardSM

Envoyer un SMS via l'API

Point de terminaison API : POST /api/MT-forwardSM

Requête :

```
{
  "imsi": "234509876543210",
  "destination_serviceCentre": "447999555111",
  "originating_serviceCenter": "447999123456",
  "smsPDU": "040B917477218345F600001570301857140C0BD4F29C0E9281C4E1F11A"
}
```

Réponse :

```
{
  "result": "success",
  "message_id": "12345"
}
```

Documentation Connexe

Documentation OmniSS7 :

- [← Retour à la Documentation Principale](#)
- [Guide de Configuration HLR](#) - Configuration et opérations en mode HLR
 - [Détails Techniques SRI-for-SM](#) - Documentation complète sur le mappage MSISDN à IMSI et la configuration du centre de service
- [Guide des Fonctionnalités Communes](#) - Interface Web, API, Surveillance
- [Guide Client MAP](#) - Opérations MAP
- [Référence Technique](#) - Spécifications de protocole

Documentation OmniMessage : Pour la configuration du routage des messages, la gestion des files d'attente, le suivi de livraison, la limitation de taux et l'analytique, reportez-vous à la **documentation produit d'OmniMessage**. OmniMessage contient toute la logique de routage des messages, les algorithmes de réessai de files d'attente, la gestion des rapports de livraison et le moteur de règles métier.

OmniSS7 par Omnitouch Network Services

[Retour à la Documentation Principale](#)

Table des Matières

1. [Qu'est-ce qu'un STP.2](#)
2. [Différence Réseau STP](#)

- ### Qu'est-ce qu'un Point de Transfert de Signalisation (STP) ?

The screenshot displays the OnosS97 Slack interface for the MSUA Routing Test. The sidebar on the left contains navigation links: S97 Events, S97 Client, MSUA, Routing, Routing Test, Resources, and Configuration. The main panel shows the MSUA Routing Test configuration, including a topology diagram and detailed node information.

MSUA Routing Test

Overview Routing Test

Down 121% ⚠ Use mouse wheel to zoom, click and drag to pan

Topology Diagram:

- SMSG** (Green box)
 - Routing Context: 1
 - Peer Config: 200 0.11.4
 - Routes to this peer: 1
 - Peer ID: 10.174.1.1
 - Peer ID: 10.174.1.1
- HLR** (Green box)
 - Routing Context: 2
 - Peer Config: 200 0.25.4
 - Routes to this peer: 1
 - Peer ID: 10.174.1.1
 - Peer ID: 10.174.1.1
- STP** (Blue circle)
 - Routing Context: 1
 - Peer Config: 200 0.11.4
 - Routes to this peer: 1
 - Peer ID: 10.174.1.1
 - Peer ID: 10.174.1.1
- Wotstation** (Green box)
 - Routing Context: 4
 - Peer Config: 200 0.10.4
 - Routes to this peer: 1
 - Peer ID: 10.174.1.1
 - Peer ID: 10.174.1.1

Node Details:

SMSG

Routing Context: 1

Peer Config: 200 0.11.4

Routes to this peer: 1

Peer ID: 10.174.1.1

Peer ID: 10.174.1.1

HLR

Routing Context: 2

Peer Config: 200 0.25.4

Routes to this peer: 1

Peer ID: 10.174.1.1

Peer ID: 10.174.1.1

STP

Routing Context: 1

Peer Config: 200 0.11.4

Routes to this peer: 1

Peer ID: 10.174.1.1

Peer ID: 10.174.1.1

Wotstation

Routing Context: 4

Peer Config: 200 0.10.4

Routes to this peer: 1

Peer ID: 10.174.1.1

Peer ID: 10.174.1.1

- **ROUTAGE DE MESSAGES :** Achève le trafic de signalisation SS7 en fonction du Code de Point de Destination (PC) ou du Titre Global (GT).
- **Traduction de Protocole :** Relie les réseaux SS7 traditionnels aux réseaux M3UA/CTCP basés sur IP.
- **Distribution de Charge :** Distribue le trafic entre plusieurs destinations en utilisant un routage basé sur la priorité.
- **Passerelle Réseau :** Connecte différents réseaux de signalisation et fournisseurs de services.
- **Masquage de Topologie :** Peut réécrire des adresses pour masquer la topologie interne du réseau.

ASP (Processus Serveur d'Application)

- **Rôle** : Client se connectant à un SGP/ST
- **Direction** : Connexion continue

- **Cas d'Utilisation :** Votre STP se connecte au STP d'un réseau partenaire

- **Rôle** : Serveur acceptant les connexions des ASP
- **Direction** : Connexion entrante

- **Cas d'Utilisation** : Les réseaux partenaires se connectent à votre STP

- **Définition** : Regroupement
- **But** : Fournir redondance et

- **Cas d'Utilisation :** Plusieurs ASP servant la même destination

OmniSS7 peut fonctionner en différents modes. Pour l'utiliser comme un STP, vous devez activer le mode STP dans la configuration.

Le fichier `config/runtime.exe` d'OmniSS7 contient trois modes opérationnels préconfigurés. Pour activer le mode STP :

1. Ouvrir `conf/runtime.exe`
2. Trouver les trois sections de configuration (lignes 53-174) :
 - Configuration 1 : Mode STP (lignes 53-85)
 - Configuration 2 : Mode HLR (lignes 87-123)
 - Configuration 3 : Mode SMSx (lignes 125-174)
3. Commenter la configuration actuellement active (ajouter # à chaque ligne)
4. Décommenter la configuration STP (retirer # des lignes 53-85)
5. Personnaliser les paramètres de configuration selon les besoins
6. Redémarrer l'application : `tex -S #ix`

OmniS7 Stack

SST Events

SST Client

MSUA

Routing

Routing Test

Configuration

MSUA Status

Last updated: 2025-10-28 22:58:12 UTC

Refresh

Name	PID	Status	ASIP State	Assoc/SCTP	Local	Remote	RC	24h Uptime	Actions
"SST-LABEL_Sslmmy"	sst_peer	DOWN	down	down	10.179.4.10:2005	10.179.4.11:0	?	<div><div></div></div>	<div></div>
"SST-ALB"	sst_peer	UP	active	established	10.179.4.10:2005	10.179.4.11:2005	?	<div><div></div></div>	<div></div>

MORE DETAILS

24-Hour Availability Timeline

Uptime: 2.7% Total Up: 47m Total Down: 13h 15m

Up Down

Basic Information

Name:	SST-ALB	PID:	sst_peer	Status:	UP	Mode:	server	ASIP State:	active	Association State:	established	
Routing Context:	?											

Network Configuration

Local IP:	10.179.4.10	Local Port:	2005	Remote IP:	10.179.4.11	Remote Port:	2005
-----------	-------------	-------------	------	------------	-------------	--------------	------

Additional Details

Peer ID:	?	Role:	server	Peer Code:	200
----------	---	-------	--------	------------	-----

Raw Data

(click to expand)

"SST-IMC1"	sst_peer	UP	active	established	10.179.4.10:2005	10.179.4.11:2005	?	<div><div></div></div>	<div></div>
"SST-Secretary"	sst_peer	UP	active	established	10.179.4.10:2005	10.5.190.200-2005	?	<div><div></div></div>	<div></div>

La configuration STP complète ressemble à ceci :

```
config :omiss7,
  # Drapeaux de mode - Activer uniquement les fonctionnalités STP
  map_client_enabled: true,
  hlr_mode_enabled: false,
  smsc_mode_enabled: false,
```

```
# Configuration de Connexion MSD
# Se connecter au test ou ASD (Processus Serveur d'Application) à un STP/SDM distant
mg_client_enable: true
node: "ASD"
colloc: (mg_client, charlie.payload, []).
process_name: stg_client_asd
# Point de terminaison LOCAL (ce système)
local_ip: (10, 179, 4, 10),
local_port: 2000,
# Point de terminaison STP/SDM distant
remote_ip: (10, 179, 4, 11),
remote_port: 2000,
routing_context: 1
}
```

Paramètres de Configuration à Personnaliser

Pour une référence complète de tous les paramètres de configuration, voir la [Bibliothèque de Configuration](#).

Paramètre	Type	Par Défaut	Description	Exemple
mg_client_enable	Boolean	true	Activer le client MAP et les capacités de routage	true
local_ip	Tuple	Adresse	Adresse IP de votre système	(10, 179, 4, 10)
local_port	Entier	2000	Port SCTP local	2000
remote_ip	Tuple	Adresse	Adresse IP STP/SDM distante	(10, 179, 4, 11)
remote_port	Entier	2000	Port SCTP distant	2000
routing_context	Entier	1	ID de contexte de routage MXUA	1
enable_gi_routing	Boolean	false	Activer le routage par Titre Global (en plus du routage par PC) True	True

Que Se Passe-t-il Lorsque le Mode STP est Actif

Lorsque mg_client_enable: true, l'interface web affichera :

- **Evénements SS7** - Journalisation des événements
- **Client SS7** - Tests de fonctionnement MAP
- **MXUA** - État de la connexion
- **Routage** - Contenu des tables de routage - Spécifique au STP
- **Test de Routage** - Test de routage - Spécifique au STP
- **Ressources** - Surveillance du système
- **Configuration** - Visualiseur de configuration

Les onglets **Liens HLR** et **Liens SMS** seront masqués.

Notes Importantes

- Le protocole SCTP (généralisé IP 132) doit être autorisé à travers les pare-feu
- Le port MXUA par défaut est 2005 (norme de l'industrie)
- Assurez-vous de disposer de ressources système suffisantes pour gérer le trafic de routage
- **Persistance de Routage** - Toutes les routes configurées via l'interface Web ou l'API sont stockées dans la **base de données Mnesia** et **survivent aux redémarrages**
- **Fonction de Configuration** - Les routes de routime.asx sont chargées au démarrage et synchronisées avec les routes Mnesia
- Après avoir changé de mode, vous devez redémarrer l'application pour que les modifications prennent effet
- **Interface Web** - Voir la [Guide API](#) pour gérer les routes via l'interface web
- **Accès API** - Voir la [Guide API](#) pour la documentation de l'API REST et l'accès à Swagger UI

Mode STP Autonome

En plus des capacités de routage STP disponibles lorsque mg_client_enable: true, vous pouvez exécuter un **serveur STP MXUA autonome** qui écoute les connexions entrantes.

Activation du STP Autonome

Ajoutez cette configuration à config/runtime.asx :

```
config:omniast7,
  mxua_stp: true
enddef: true
local_ip: (127, 0, 0, 1), # Adresse IP à écouter
local_port: 2000, # Port à écouter
point_code: 100 # Code de point propre à ce STP
}
```

Paramètres de Configuration STP

Paramètre	Type	Par Défaut	Description	Exemple
enable	Boolean	false	Activer le serveur STP autonome	true
local_ip	Tuple	(127, 0, 0, 1)	Adresse IP à écouter pour les connexions (R, 0, 0, 0)	
local_port	Entier	2005	Port à écouter	2005
point_code	Entier	100	Code de point SS7 propre à ce STP	100

Quand Utiliser le STP Autonome

- **Routage Par** - Lorsque vous avez uniquement besoin de routage MXUA sans fonctionnalité de client MAP
- **STP Central** - Pour créer un mode de supervision central pour plusieurs éléments de réseau
- **Architecture Hub** - Connecter plusieurs HLR, MSC et SMS

Remarque - Vous pouvez activer à la fois mg_client_mxua et mxua_stp simultanément si vous avez besoin à la fois de connexions sortantes et de fonctionnalités STP entrantes.

Persistance des Tables de Routage (Mnesia)

Toutes les tables de routage (pairs, routes de Code de Point et routes de Titre Global) sont stockées dans une **base de données Mnesia** pour la persistance.

Comment Fonctionne le Routage

1. **Routes runtime.asx** - Les routes définies dans config/runtime.asx sous mxua_peers, mxua_routes et mxua_gi_routes sont chargées au démarrage de l'application
2. **Routes Interface Web** - Les routes ajoutées via la [page de Routage de l'Interface Web](#) sont stockées dans Mnesia
3. **Fonction des Routes** - Au redémarrage, les routes runtime.asx sont synchronisées avec les routes Mnesia existantes (pas de doublons)
4. **Persistance** - Toutes les routes configurées via l'Interface Web **survivent aux redémarrages de l'application**

Type de Stockage Mnesia

Configurez comment les tables de routage sont stockées. Pour plus de détails sur la configuration de la base de données, voir [Description de Base de Données dans la Bibliothèque de Configuration](#).

```
config:omniast7,
  mnesia_storage_type: :disc_copies # ou :ram_copies pour les tests
}
```

Type de Stockage	Description	Persistance	Cas d'Utilisation
disc_copies	Stockage sur disque (par défaut)	Survive aux redémarrages	Environnement de production
ram_copies	Stockage en mémoire	Perte au redémarrage	Tests, développement

Par Défaut : disc_copies

Emplacement de la Base de Données Mnesia

Mnesia stocke les tables de routage dans le répertoire Mnesia de l'application :

- **Emplacement Mnesia** (node_name) (par exemple, mnesia.nonode@probat)
- **Tables** mxua_peer, mxua_route, mxua_gi_route

Gestion des Routes

Vous avez trois options pour gérer les routes :

1. **Runtime.asx** - Configuration statique chargée au démarrage
2. **Interface Web** - Gestion interactive des routes (voir [Guide de l'Interface Web](#))
3. **API REST** - Gestion programmatique des routes (voir [Guide API](#))

Meilleure Pratique : Utilisez runtime.asx pour la configuration de base et l'Interface Web pour les modifications dynamiques des routes pendant l'opération.

Configuration des Pairs M3UA

Les pairs représentent les points de terminaison de connexion MXUA (tous STP HLR, MSC, SMS). Ajoutez des pairs à config/runtime.asx.

OmniS7 Stack

S7 Events

MSUA Routing Management

Auto-refresh every 5 seconds

S7 Client

Peers (N) Point Code Routes (2) Global Title Routes (N)

MSUA

Routing

Add New Peer

Routing Test

Peer ID: Peer Name:

Ressources

Auto-generated if empty: e.g., STP_Vest

Configuration

Role: Point Code:

Client (ASP): Peer ID: 100

Local IP: Local Port: 0

Remote IP: Remote Port: 2000

Routing Context: Network Initiator: International

Test Peer

ID	Name	Role	Point Code	Remote	Status	Actions
1	HLR	server	100	10.179.4.11.0	active	<button>Set</button> <button>Delete</button>
4	Workstation	server	000	10.0.190.200.0	active	<button>Set</button> <button>Delete</button>
3	CAMEL_Gateway	server	100	10.179.4.10.0	down	<button>Set</button> <button>Delete</button>
7	SMS	server	100	10.179.4.10.0	active	<button>Set</button> <button>Delete</button>

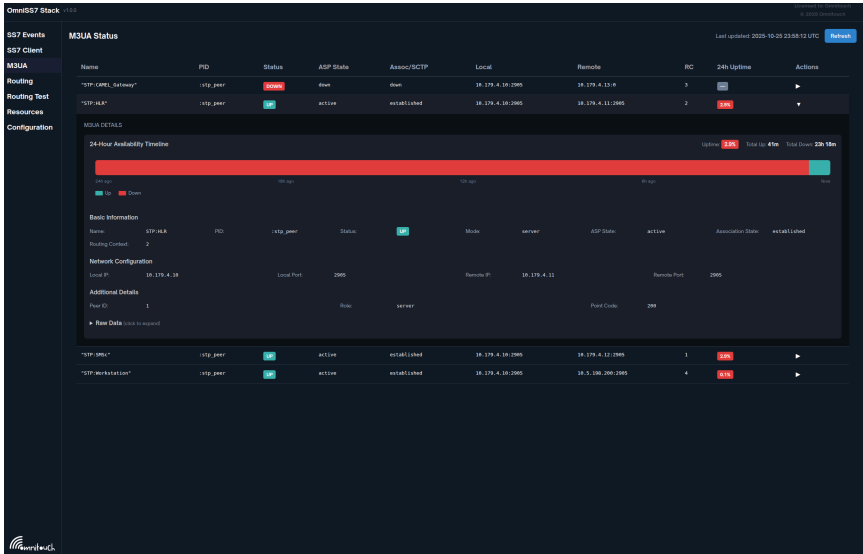
Example of Configuration of Pair

config:omniast7,
 mxua_peers: [
 # Connexion sortante au STP Partenaire (rôle : client)
 {
 peer_id: 1, # Identifiant unique
 name: "Partner_STP_Vest", # Nom descriptif
 role: "client", # client pour sortant, server pour entrant
 local_ip: (10, 0, 0, 1), # IP locale à l'client
 local_port: 0, # 0 = attribution dynamique de port
 remote_ip: (10, 0, 0, 10), # IP du pair distant
 remote_port: 2000, # Port du pair distant
 routing_context: 1, # Contexte de routage MXUA
 point_code: 100, # Code de point de ce pair
 network_indicator: "international", # international ou national
 },
 # Connexion au HLR Local (rôle : client)
 {
 peer_id: 2,
 name: "Local_HLR",
 role: "client",
 local_ip: (10, 0, 0, 1),
 local_port: 0,
 remote_ip: (10, 0, 0, 20),
 remote_port: 2000,
 routing_context: 2,
 point_code: 200,
 network_indicator: "international",
 },
 # Connexion entrante de MSC Distant (rôle : server)
 # Pour le rôle server, le STP attend une connexion entrante
 {
 peer_id: 3,
 name: "Remote_MSC",
 role: "server",
 remote_ip: (10, 0, 0, 30), # Accepter la connexion entrante
 remote_port: 2000, # IP source attendue (0 = accepter de n'importe quel port)
 routing_context: 3,
 },
],
}

```
point_code: 300;
network_indicator: international;
}

# Connexion entrante avec port source dynamique (pas de filtrage de port)

%
peer_id: 4;
name: "Dynamic_Client";
role: server;
remote_ip: (10, 0, 0, 40); # IP source attendue
remote_port: 4; # 0 = accepter les connexions de n'importe quel port source
routing_contact: 4;
point_code: 400;
network_indicator: international;
}
}
```



Paramètres de Configuration des Pairs

Paramètre	Type	Requis	Description
peer_id	Entier	Oui	Identifiant numérique unique pour le pair
name	Chaîne	Oui	Nom lisible par l'homme pour les journaux et la surveillance
role	Atome	Oui	<Client> (initiateur) ou <serveur> (répondant)
local_ip	Tuplet	Oui (client)/Adresse IP locale à l'ier	
local_port	Entier	Oui (client)/Port local (0 pour dynamique)	
remote_ip	Tuplet	Oui	Adresse IP du pair distant
remote_port	Entier	Oui	Port du pair distant (0 pour entrant = accepter de n'importe quel port source)
routing_contact	Entier	Oui	Identifiant de contact de routage MSUA
point_code	Entier	Oui	Code de point SST de ce pair
network_indicator	Atome	Non	: international ou :national

Filtrage de Port Source pour les Connexions Entrantes

Pour les connexions entrantes (rôle : <serveur>), le paramètre remote_port contrôle le filtrage de port source :

- **Port Spécifique** (par exemple, remote_port : 2005) : N'accepter que les connexions de ce port source exact
 - Permet une sécurité supplémentaire en validant le port source
 - Utiliser lorsque le pair distant utilise un port source fixe
- **N'importe quel Port** (remote_port : 0) : Accepter les connexions de n'importe quel port source
 - Utiliser lorsque le pair distant utilise des ports sources dynamiques/éphémères
 - Ne valide que l'adresse IP source
 - Plus flexible mais légèrement moins sécurisé

Exemple :

Accepter uniquement de 10.5.100.200-2005 (port spécifique)

```
%
peer_id: 1;
name: "Strict_Peer";
role: server;
remote_ip: (10, 5, 100, 200);
remote_port: 2005;
# ... autre config
}
```

Accepter de 10.5.100.200 avec n'importe quel port source

```
%
peer_id: 2;
name: "Flexible_Peer";
role: server;
remote_ip: (10, 5, 100, 200);
remote_port: 0; # Accepter de n'importe quel port source
# ... autre config
}
```

Support du Protocole M2PA

Omnis57 prend en charge à la fois les protocoles MSUA et M2PA pour le transport de signalisation SST.

Qu'est-ce que M2PA ?

M2PA (MTP User-to-Peer Adaptation Layer) est un protocole standardisé par l'ETSI (RFC 4165) pour transporter les messages MTP3 SST sur des réseaux IP en utilisant SCTP.

MSUA vs M2PA : Principales Différences

Functionalité	MSUA	M2PA
Architecture	Client/Serveur (ASPS/GSW)	Pair-à-Pair
Cas d'Utilisation	Passerelle entre SST et IP	Liens directs point à point
Gestion de l'État de Lien	Niveau application (ASPC/PASPC)	Style MTPO (Alignement, Vérification, Prêt)
Numéros de Séquence	Par de séquençage séquentiel	BIBNPTN de 24 bits pour l'événement end-to-end
Déploiement Typique	Passerelle SST vers IP SST	Liens de signalisation directs entre réseaux
BIC	RFC 4666	RFC 4165

Conseils de Sélection de Protocole

Recommandation : Utilisez MSUA par défaut. N'utilisez M2PA que lorsque cela est spécifiquement requis.

Quand Utiliser MSUA (Recommandé)

MSUA est le protocole recommandé pour la plupart des déploiements :

- **Déploiements SST** : Implémentations standard de point de transfert de signalisation
- **Fonctions de Passerelle** : Relier les réseaux SST avec la signalisation basée sur IP
- **Connecteurs d'Éléments de Réseau** : Connecter HLIR, MSC, SMSG et autres éléments de réseau à votre STP
- **Passerelles de Signalisation (GSW)** : Souvent utilisées pour accepter les connexions de plusieurs serveurs d'application
- **Implémenter l'Alignement** : Implémenter l'alignement avec contrôle continu
- **Réseaux Multi-Fournisseurs** : Normes de l'industrie largement supportées (RFC 4666)

Utilisez MSUA pour connecter les éléments de réseau (HLIR, MSC, SMSG, VLR, etc.) à votre STP.

Quand Utiliser M2PA (Cas Spéciaux Uniquement)

M2PA ne doit être utilisé que dans des scénarios spécifiques :

- **Liens STP à STP** : Connecter directement point à point entre Points de Transfert de Signalisation dans un réseau multi-STP
- **Remplacement d'UN Héritage** : Remplacer les liens TDM SST traditionnels lorsque le système distant expose spécifiquement M2PA
- **Compatibilité MTPO Requise** : Lors de la connexion à des systèmes hérités qui imposent une gestion de l'état de lien de style MTPO
- **Exigence Partenaire** : Lorsque un partenaire ou une interconnexion expose spécifiquement le protocole M2PA

Important : Ne pas utiliser M2PA pour connecter des éléments de réseau (HLIR, MSC, SMSG) à votre STP - utilisez MSUA à la place. M2PA est conçu pour les interconnexions STP à STP où les deux côtés fonctionnent comme des routeurs de routage.

Configuration des Pairs M2PA

Les pairs M2PA sont configurés de la même manière que les pairs MSUA, avec un paramètre protocol supplémentaire.

Configuration des Pairs M2PA

Ajustez des pairs M2PA à votre configuration x_hua_pairs dans config/runtime. xml (oui, ils partagent la même syntaxe de configuration malgré le fait qu'ils soient des protocoles différents) :

Paramètres Clés pour M2PA :

Paramètre	Valeur	Description
protocol	m2pa	Spécifie le protocole M2PA (par défaut : x_hua si omis)
role	<Client> ou <server>	Direction de la connexion
local_ip	Entier	Port SCTP local (le port standard M2PA est 3345)
remote_ip	Entier	Port SCTP distant (le port standard M2PA est 3345)
point_code	Entier	Valeur code de point
adj_point_code	Entier	Code de point du pair distant (spécifique à M2PA)

Remarque : M2PA utilise le port 3345 comme norme de l'industrie (différent du port 2005 de MSUA).

État de Lien M2PA

Les liens M2PA progressent à travers plusieurs états lors de l'initialisation :

1. **Down** - Aucun contact établi
2. **Alignement** - Échange de synchronisation initial (~1 seconde)
3. **Prêt** - Vérification de la qualité de lien (~2 secondes)
4. **Ready** - Lien actif et prêt pour le trafic

La progression de l'état de lien assure une signalisation fiable avant l'échange de trafic.

Gestion des Pairs M2PA via l'Interface Web

La page **Routage** dans l'Interface Web fournit un support complet pour la gestion des pairs M2PA :

1. **Naviguer** vers la page de filtrage
2. **Sélectionner l'onglet "Pairs"**
3. **Cliquez sur "Ajouter un Nouveau Pair"**
4. **Choisissez "M2PA (RFC 4165)"** dans le menu déroulant Protocole
5. **Renseignez la configuration du pair**
 - Nom du Pair (obligatoire descriptif)
 - Protocole : M2PA
 - Rôle : client ou serveur
 - Code du Pair (valeur PC)
 - Adresse IP Local/Client
 - Ports Local/Distant (typiquement 3345 pour M2PA)
 - Indicateur de Réseau (international ou national)
6. **Cliquez sur "Enregistrer le Pair"**

La table des pairs affiche le type de protocole avec un code couleur :

- **Bleu** - pairs MSUA
- **Vert** - pairs M2PA

Comportement de Routage M2PA

Les pairs M2PA s'intègrent parfaitement au système de routage d'Omnis57 :

- **Routes de Code de Point** : Fonctionnement identique pour M2PA et MSUA
- **Routes de Titre Global** : Entièrement supportées sur les liens M2PA

- **Priorité de Route** : Les pairs M2PA et M2UA peuvent être mélangés dans les mêmes tables de routage
- **Batons de Message** : Les messages peuvent arriver sur M2PA et être routés vers M2UA, et vice versa

Métriques M2PA

M2PA fournit des métriques Prometheus complètes pour surveiller la santé et le trafic des liens :

Métriques de Trafic :

- `m2pa_messages_sent_total` : Total des messages MTP3 envoyés par lien
- `m2pa_messages_received_total` : Total des messages MTP3 reçus par lien
- `m2pa_bytes_sent_total` : Total des octets envoyés sur M2PA
- `m2pa_bytes_received_total` : Total des octets reçus sur M2PA

Toutes les métriques de trafic sont échantillonnées par : `link_name, point_code, adjacent_pc`

Métriques d'État de Lien :

- `m2pa_link_state_changes_total` : Transitions d'état de lien (DOWN → ALIGNMENT → PROVISION → READY)
- Étiquettes : `link_name, from_state, to_state`

Métriques d'Erreur :

- `m2pa_errors_total` : Total des erreurs par type
 - `decode_error` : Échec de décodage de message M2PA
 - `encode_error` : Échec d'encodage de message M2PA
 - `sctp_send_error` : Échec de transmission SCTP
- Étiquettes : `link_name, error_type`

Accès aux Métriques :

- Point de terminaison Prometheus : `http://your-server:8888/metrics`
- Les métriques s'exportent automatiquement au démarrage de l'application

Mauvaises Pratiques M2PA

1. **Sélection de Port** : Utilisez le port 3565 pour M2PA (norme de l'industrie)
2. **Surveillance de Lien** : Surveillez les changements d'état de lien via les métriques
3. **Règles de Pare-feu** : Assurez-vous que SCTP (protocole IP/132) est autorisé
4. **Codes de Point** : Assurez-vous que les codes de point adjacents sont correctement configurés des deux côtés
5. **Indicateur de Réseau** : Inclut correspondance entre les pairs (international ou national)
6. **Tests** : Utilisez la page de Test de Routage pour vérifier la connectivité après configuration

Configuration du Routage par Code de Point

Le routage par Code de Point dirige les messages en fonction du **Code de Point de Destination (DPC)** dans l'entête MTP3.

Comprendre les Codes de Point dans la Pile de Protocole SS7

Les codes de point existent à différents niveaux de la pile de protocole SS7. Comprendre cette distinction est important :

Couches de la Pile de Protocole :

Couche d'Application (SCTP/TCAP/MAP)	
Couche MTP3 <ul style="list-style-type: none">- Étiquette de Routage (DPC, OPC, SLK)- État d'Information de Service (ISGI)	- Routage des Données Utilisateur
M2UA ou M2PA (Couche d'Adaptation) <ul style="list-style-type: none">- Données de Protocole (contenant MTP3)- Gestion de Réseau (DUNA/DANA)	- Protocole de Transport
M2P	- État du Réseau
SCTP (Transport)	

Deux Types de Codes de Point :

1. **Codes de Point de Couche MTP3** (Utilisés pour le Routage) :
 - Situés dans l'étiquette de routage MTP3 (DPC, OPC)
 - Présents dans le paramètre Données de Protocole M2UA (tag 528)
 - Présents dans les messages de Données Utilis M2PA
 - **Le STP utilise ces valeurs DPC pour les décisions de routage**
 - Elles déterminent où le message est finalement livré
2. **Codes de Point de Couche M2UA** (Utilisés pour la Gestion de Réseau) :
 - Présents dans les messages de gestion M2UA (DUNA, DANA, SCOM, DUPLO)
 - Indiquent les codes de point affectés pour l'état du réseau
 - Intervent les pairs des destinations disponibles/non disponibles
 - Non utilisés pour le routage des données utilisateur

Comment Fonctionne le Routage STP :

- **Pour les messages M2UA DATA** : Le STP envoie le message MTP3 du paramètre Données de Protocole (tag 528), qui contient l'étiquette de routage MTP3 (DPC, OPC, SLK). Le DPC de la couche MTP3 est utilisé pour rechercher des routes.
- **Pour les messages de Données Utilis M2PA** : Le STP envoie le message MTP3 du champ de données utilisateur M2PA, puis le DPC de l'étiquette de routage MTP3.
- **Messages de gestion M2UA** : Les messages de gestion du réseau (DUNA, DANA, SCOM) contiennent les codes de point affectés au réseau M2UA pour signaler l'état du réseau entre les pairs.

Routes de Code de Point de Base

Ajoutez des routes à `config/runtime.asx` :

```
config {
  runtime {
    routes {
      # Route tout le trafic pour le PC 100 vers le pair 1 (STP Porteminaire)
      % {
        dest_pc: 100,          # Code de point de destination
        peer_id: 1,           # Pair à travers lequel router
        priority: 1,          # Priorité (plus bas = plus haute priorité)
        network_indicator: international, # Optionnel : par défaut 14 (correspondance exacte)
        mask: 14
      }

      # Route tout le trafic pour le PC 200 vers le pair 2 (HLR Local)
      % {
        dest_pc: 200,
        peer_id: 2,
        priority: 1,
        network_indicator: international
      }

      # Exemple d'équilibrage de charge : PC 300 avec routes principale et de secours
      % {
        dest_pc: 300,
        peer_id: 3,          # Route principale
        priority: 1,
        network_indicator: international
      }

      % {
        dest_pc: 300,
        peer_id: 4,          # Route de secours (numéro de priorité plus élevé)
        priority: 2,
        network_indicator: international
      }
    }
  }
}
```

Remarque : Le champ `mask` est optionnel et par défaut à 14 (correspondance exacte). Ne spécifiez le `mask` que lorsque vous avez besoin d'un routage basé sur des plages (voir la section sur les Masques de Code de Point ci-dessous).

Logique de Routage

1. Le STP reçoit un message M2UA DATA ou un message de Données Utilis M2PA
2. Le STP extrait le **message MTP3** du champ Données de Protocole (M2UA) ou Données Utilis (M2PA)
3. Le STP lit le **Code de Point de Destination (DPC)** de l'étiquette de routage MTP3
4. Recherche dans la table de routage en fonction du DPC pour trouver la route correspondante (si aucun message de message)
5. Si plusieurs routes existent, sélectionnez la route avec le **message le plus spécifique** (valeur de `mask` la plus élevée), puis le **numéro de priorité le plus bas**
6. Envoyez le message MTP3 dans M2UA ou Données Utilis M2PA pour le pair de destination
7. Route le message vers le pair correspondant
8. Si le pair sélectionné est localement en panne, essayez la route de priorité la plus élevée suivante

Onmis57 Stack STP

SS7 Events

System Logs

SS7 Client

M2UA

Routing

Routing Test

Resources

Configuration

MSUA Routing Management

Peer ID: Point Code Routes (3) Global Title Routes (4)

Edit Global Title Route

OT Profile: Peer ID: 1

447 STP_East (D 2, PC 200)

Drop (DSCP route, local network, other route/route)

Source SSN (optional): Drop SSN (optional)

Leave empty for wildcard

Match on Color Party SSN (empty = any): Leave empty to preserve

Priority: Description

1 UK mobile numbers

Show Advanced Routing (TCP/IP/IPv6)

Update Route Cancel

OT Profile Source SSN TC/NP/PLI Peer ID Peer Dest SSN Priority Description Actions

51 any - 3 MSC_South (3) preserve 1 India numbers

124 any 1 STP_West (1) preserve 1 US numbers

447 any 2 STP_East (2) preserve 1 UK mobile numbers

44 any 2 STP_East (2) preserve 1 UK numbers

Common SSN Values

6: 14,9: Diverse Location Registered 7: VLR (Diverse Location Registered)

8: MSC (Mobile Switching Center) 9: EIR (Equipment Identity Registered)

10: AUC (Authentication Center) 14: 100000 14: 100000

14: gsmSCF (Service Control Function) 14: SCOM

Drop Routes - Preventing Routing Loops

Drop routes peer_id=2 identify discard traffic instead of forwarding it. This is useful for preventing routing loops in complex network topologies.

Common Use Case Profile Whitelisting

When you have a large OT profile range but only need to route specific numbers within that range.

Use a DROP route for the entire range with high priority number (e.g., priority 9)

Add specific routes for individual OTs you want to allow with low priority numbers (e.g., priority 1)

Since lower priority numbers are processed first, specific routes within the large OT range

Any OT not explicitly allowed will be caught by the DROP route and discarded

Example:

OT 1: 1000000, 100, any, Peer: 1, Priority: 9, Desc: "Drop entire OT range"

OT 1: 1000000, 100, any, Peer: 1, Priority: 1, Desc: "Allow specific number"

OT 1: 1000000, 100, any, Peer: 1, Priority: 1, Desc: "Allow another number"

Result: OT 1000000 and (1000000, 100, any, Peer: 1) allow OT range not dropped

Masques de Code de Point

Les codes de point ont des valeurs de 14 bits (plage 0-16383). Par défaut, les routes correspondent exactement à un seul code de point (masque /14). Cependant, vous pouvez utiliser des **masques de code de point** pour créer des routes qui correspondent à des **plages** de codes de point.

Comprendre les Masques

Le masque spécifie combien de bits les **plus significatifs** doivent correspondre entre le PC de destination de la route et le DPC du message entrant. Les bits restants peuvent avoir n'importe quelle valeur, créant une **plage** de codes de point correspondants.

Table de Référence des Masques :

Masque	Codes de Point Correspondants	Cas d'Utilisation
/14	1 PC (correspondance exacte)	Distributions uniques (par défaut)
/13	2 PCs	Petite plage
/12	4 PCs	Petite plage
/11	8 PCs	Petite plage
/10	16 PCs	Plage moyenne
/9	32 PCs	Plage moyenne
/8	64 PCs	Plage moyenne-grande
/7	128 PCs	Grande plage
/6	256 PCs	Grande plage
/5	512 PCs	Grande plage
/4	1,024 PCs	Très grande plage
/3	2,048 PCs	Très grande plage
/2	4,096 PCs	Plage extrêmement grande
/1	8,192 PCs	La moitié de tous les PCs
/0	16,384 PCs	Tous les PCs (route par défaut/correspondance)

Exemples de Masques de Code de Point

Remarque : Le champ `mask` est optionnel dans tous les exemples. S'il est omis, il par défaut à 14 (correspondance exacte).

Exemple 1 : Code de Point Unique (Comportement par Défaut)

Sans champ de masque (recommandé pour un PC unique)

```
%
dest_pc: 1000,
peer_id: 1,
priority: 1,
network_indicator: international
# Masque par défaut à 14 - Correspond à : Seulement PC 1000
# Masque explicite (même résultat)
%
dest_pc: 1000,
peer_id: 1,
priority: 1,
mask: 14,
network_indicator: international
# Correspondance exacte explicite
}
# Correspond à : Seulement PC 1000
```

Exemple 2 : Petite Plage

```
%
dest_pc: 1000,
peer_id: 2,
priority: 1,
mask: 15,
network_indicator: international
# Correspond à 4 PCs
}
# Correspond à : PC 1000, 1001, 1002, 1003
```

Exemple 3 : Plage Moyenne

```
%
dest_pc: 1000,
peer_id: 3,
priority: 1,
mask: 8,
network_indicator: international
# Correspond à 64 PCs
}
# Correspond à : PC 1000-1063 (64 codes de point consécutifs)
```

Exemple 4 : Route par Défaut/De Secours

```
%
dest_pc: 0,
peer_id: 4,
priority: 10,
mask: 0,
network_indicator: international
# Route priorité (numéro élevé)
# Correspond à tous les PCs
}
# Correspond à : Tous les codes de point (0-26383)
# Utiliser comme une route de secours/rachet-ail avec une faible priorité
```

Combinaison de Routes Spécifiques et Masques

Vous pouvez combiner des routes spécifiques avec des masques masqués pour un routage flexible :

```
config omis17,
kha_routes: [
# Route spécifique pour le PC 1000 (prend la priorité)
%
dest_pc: 1000,
peer_id: 1,
priority: 1,
network_indicator: international
# masque par défaut à 14 (correspondance exacte)
},
# Route de plage pour les PCs 1000-1063
%
dest_pc: 1000,
peer_id: 2,
priority: 1,
mask: 8,
network_indicator: international
# Correspond à 64 PCs
},
# Route par défaut/de secours pour tous les autres PCs
%
dest_pc: 0,
peer_id: 3,
priority: 10,
mask: 0,
network_indicator: international
# Base priorité
# correspond à tous les PCs
},
]
```

Décision de Routage pour DPC 1000 :

1. Correspond à la route masque /14 (PC 1000 exactement) - **Sélectionnée** (la plus spécifique)
2. Correspond également à la route masque /8 (plage PC 1000-1063) - Ignorée (moins spécifique)
3. Correspond également à la route masque /0 (tous les PCs) - Ignorée (la moins spécifique)

Décision de Routage pour DPC 1013 :

1. Ne correspond pas à la route masque /14 (PC 1000 uniquement)
2. Correspond à la route masque /8 (plage PC 1000-1063) - **Sélectionnée** (correspondance la plus spécifique)
3. Correspond également à la route masque /0 (tous les PCs) - Ignorée (la moins spécifique)

Décision de Routage pour DPC 1000 :

1. Ne correspond pas à la route masque /14
2. Ne correspond pas à la route masque /8
3. Correspond à la route masque /0 (tous les PCs) - **Sélectionnée** (seule correspondance, route de secours)

Meilleures Pratiques

1. **Omettre mask pour les Destinations Uniques** : Pour des correspondances exactes de code de point, omettez complètement le champ mask (par défaut à /14)
2. **Utiliser /14 Explicitement Seulement Lorsque Nécessaire** : Ne spécifiez mask /14 que lorsque vous devez le clarifier dans la documentation ou lorsque vous mélangez avec des routes de plage
3. **Utiliser des Masques de Plage pour des Blocs Réseaux** : Routage de segments de réseau entiers vers des pairs spécifiques avec des masques /8 à /13
4. **Utiliser 0 comme Route de Secours** : Créer une route par défaut avec une faible priorité pour attraper le trafic non supporté
5. **La Plus Spécifique Capture** : Le moteur de routage sélectionnera toujours la correspondance de route la plus spécifique (valeur de masque la plus élevée) en premier
6. **Priorité comme Critère de Sélection** : Si plusieurs routes ont le même masque, le nombre de priorité le plus bas l'emporte

Configuration du Routage par Titre Global (GT)

Le routage par Titre Global permet un **routage basé sur le contenu** en utilisant des numéros de téléphone ou des valeurs DNS au lieu de codes de point. Pour un routage associé par Titre Global basé sur l'appelant/l'appelé, voir le [Guide NGT de Titre Global](#).

Omni57 Stack

SST Events

SST Client

M3UA

Routing

Routing Test

Resources

Configuration

M3UA Routing Management

Peer ID *
Select a peer...

GT Profile *
Leave empty for fallback route

Peer ID *
Select a peer...

Empty / Fallback Route Used when no other route matches

Source SSN (optional)
Leave empty for wildcard

Dest SSN (optional)
Leave empty for preserve

Match on outgoing SSN (optional) - yes

Match SSN when incoming empty - keep original

Priority
1

Description
e.g. US numbers

Add Route

GT Profile	Source SSN	Peer ID	Peer	Dest SSN	Priority	Description	Actions
91	any	1	CAMEL_Gateway [2]	preserve	1	India numbers	Go Delete
1224	any	1	HLR [1]	preserve	1	US numbers	Go Delete
447	any	2	SMSC [2]	preserve	1	UK mobile numbers	Go Delete
44	any	2	SMSC [2]	preserve	1	UK numbers	Go Delete
Common SSN Values							
6 - HLIR (Home Location Register)				7 - VM (Visitor Location Register)			
8 - MSC (Mobile Switching Center)				9 - EN (Equipment Identity Register)			
10 - AUC (Authentication Center)				101 - RANAP			
101 - GPRS (GPRS Service Control Function)				101 - GSM			

Prérequis

- Activer le routage GT: enable_gt_routing: true dans config/runtime.xml

Configuration des Routes GT

```
config omis17,
# Activer le routage GT
enable_gt_routing: true,
kha_gt_routes: [
# Route tous les numéros UK (préfixe 44) vers le pair 1
%
gt_prefix: "44",
peer_id: 1,
priority: 1,
description: "Numéros UK"
},
# Route les numéros US (préfixe 1) vers le pair 2
%
gt_prefix: "1",
peer_id: 2,
priority: 1,
description: "Numéros US"
},
# Route plus spécifique : numéros mobiles UK commençant par 447
%
gt_prefix: "447",
peer_id: 3,
priority: 1,
description: "Numéros mobiles UK"
},
# Routage spécifique à SSN (optionnel)
%
gt_prefix: "555",
source_ssn: 8,
peer_id: 4,
dest_ssn: 8,
priority: 1,
description: "Trafic SMS pour préfixe 61"
},
]
```

Logique de Routage GT

L'algorithme de routage GT suit ce processus décisionnel :

Étapes de Routage :

1. **Correspondance de Préfixe le Plus Long** : Le SST trouve toutes les routes GT où le préfixe correspond au début du Titre Global.
 - Exemple : GT "44712345678" correspond à "44" et "447", mais "447" gagne (correspondance la plus longue)
2. **Correspondance SSN (Optionnel)** :
 - Si source_ssn est spécifié, la route ne correspond que lorsque le SSN de la Partie Appelée SCCP est égal à cette valeur
 - Si source_ssn est nil, la route correspond à n'importe quel SSN (wildcard)

3. **Correspondance TUNPUNAI (Optionnel) :**
- Si source TT, source NAI ou source NAI sont spécifiés, les routes doivent correspondre à ces indicateurs
 - Les valeurs n1 agissent comme des wildcards (correspondent à n'importe quelle valeur)
4. **Sélection Basée sur la Spécificité :**
- Les routes avec des critères de correspondance plus spécifiques passent sur les wildcards
 - Ordre de priorité : Longueur de Préfixe GT > SSN > TT > NP > NAI > Numéro de Priorité
5. **Réécriture des Indicateurs (Optionnel) :**
- Si dest_4to, dest_1to, dest_npi ou dest_nai sont spécifiés, le STP réécrit ces indicateurs
 - Utile pour la normalisation des protocoles et l'interconnexion des réseaux
6. **Retour au Code de Point :**
- Si aucune route GT ne correspond, le STP revient au routage par Code de Point en utilisant le DPC

Routage Avancé GT : Type de Traduction, NPI et NAI

En plus de la correspondance de préfixe GT et de SSN, le STP prend en charge le routage et la transformation basés sur les indicateurs de Titre Global SSCP :

- **Type de Traduction (TT)** : Identifie le plan de numérotation et le type d'adresse
- **Indicateur de Plan de Numérotation (NPI)** : Indique le plan de numérotation (par exemple, ISDN, Domain, Telex)
- **Indicateur de Nature d'Adresse (NAI)** : Spécifie le format d'adresse (par exemple, International, National, Abonné)

OmniSST Stack STP 10.5

SS7 Events

System Logs

SS7 Client

MSUA

Routing

Routing Test

Resources

Configuration

MSUA Routing Management

Peers (2)

Point Code Routes (0)

Global Title Routes (4)

Edit Global Title Route

GT Prefix

91

Peer ID *

DRCP - Discard traffic (neverto hop)

Dest SSN (optional)

Select DRCP to identify discard traffic to this Global Title route for processing routing input

Dest SSN (optional)

Leave empty to preserve

Route's SSN when forwarding (empty = keep original)

Description

India numbers

Hide Advanced Routing (TT/NPI/NAI)

Configure routing based on SSCP Global Title indicators. Leave empty for wildcard matching

Source TT (Match)

0-255 or empty

Dest TT (Rewrite)

0-255 or empty

Source SSN (Match)

0-255 or empty

Dest SSN (Rewrite)

Source NPI (Match)

0-16 or empty

Dest NPI (Rewrite)

Source NAI (Match)

0-16 or empty

Dest NAI (Rewrite)

Common Values Reference

TT: 0-Incoming, 1-4-6, 2-National

NPI: 0-Incoming, 1-4-6, 2-National

NAI: 0-Incoming, 2-National, 4-6-8

Update Route

Cancel

GT Prefix	Source SSN	TT/NPI/NAI	Peer ID	Peer	Dest SSN	Priority	Description	Actions
91	any	-	3	MSG_South (8)	preserve	1	India numbers	Refresh Edit Delete
1234	any	-	1	STP_Wired (1)	preserve	1	US numbers	Refresh Edit Delete
447	any	-	2	STP_Wired (2)	preserve	1	UK mobile numbers	Refresh Edit Delete
44	any	-	2	STP_Wired (2)	preserve	1	UK numbers	Refresh Edit Delete

Common SSN Values

0 - HLR Home Location Register

1 - HLR Mobile Location Register

2 - HLR Mobile Switching Center

3 - HLR Equipment Identity Register

4 - HLR Authentication Center

5 - HLR Authentication Center

6 - HLR Authentication Center

7 - HLR Authentication Center

8 - HLR Authentication Center

9 - HLR Authentication Center

10 - HLR Authentication Center

11 - HLR Authentication Center

12 - HLR Authentication Center

13 - HLR Authentication Center

14 - HLR Authentication Center

15 - HLR Authentication Center

16 - HLR Authentication Center

17 - HLR Authentication Center

18 - HLR Authentication Center

19 - HLR Authentication Center

20 - HLR Authentication Center

21 - HLR Authentication Center

22 - HLR Authentication Center

23 - HLR Authentication Center

24 - HLR Authentication Center

25 - HLR Authentication Center

26 - HLR Authentication Center

27 - HLR Authentication Center

28 - HLR Authentication Center

29 - HLR Authentication Center

30 - HLR Authentication Center

31 - HLR Authentication Center

32 - HLR Authentication Center

33 - HLR Authentication Center

34 - HLR Authentication Center

35 - HLR Authentication Center

36 - HLR Authentication Center

37 - HLR Authentication Center

38 - HLR Authentication Center

39 - HLR Authentication Center

40 - HLR Authentication Center

41 - HLR Authentication Center

42 - HLR Authentication Center

43 - HLR Authentication Center

44 - HLR Authentication Center

45 - HLR Authentication Center

46 - HLR Authentication Center

47 - HLR Authentication Center

48 - HLR Authentication Center

49 - HLR Authentication Center

50 - HLR Authentication Center

51 - HLR Authentication Center

52 - HLR Authentication Center

53 - HLR Authentication Center

54 - HLR Authentication Center

55 - HLR Authentication Center

56 - HLR Authentication Center

57 - HLR Authentication Center

58 - HLR Authentication Center

59 - HLR Authentication Center

60 - HLR Authentication Center

61 - HLR Authentication Center

62 - HLR Authentication Center

63 - HLR Authentication Center

64 - HLR Authentication Center

65 - HLR Authentication Center

66 - HLR Authentication Center

67 - HLR Authentication Center

68 - HLR Authentication Center

69 - HLR Authentication Center

70 - HLR Authentication Center

71 - HLR Authentication Center

72 - HLR Authentication Center

73 - HLR Authentication Center

74 - HLR Authentication Center

75 - HLR Authentication Center

76 - HLR Authentication Center

77 - HLR Authentication Center

78 - HLR Authentication Center

79 - HLR Authentication Center

80 - HLR Authentication Center

81 - HLR Authentication Center

82 - HLR Authentication Center

83 - HLR Authentication Center

84 - HLR Authentication Center

85 - HLR Authentication Center

86 - HLR Authentication Center

87 - HLR Authentication Center

88 - HLR Authentication Center

89 - HLR Authentication Center

90 - HLR Authentication Center

91 - HLR Authentication Center

92 - HLR Authentication Center

93 - HLR Authentication Center

94 - HLR Authentication Center

95 - HLR Authentication Center

96 - HLR Authentication Center

97 - HLR Authentication Center

98 - HLR Authentication Center

99 - HLR Authentication Center

100 - HLR Authentication Center

101 - HLR Authentication Center

102 - HLR Authentication Center

103 - HLR Authentication Center

104 - HLR Authentication Center

105 - HLR Authentication Center

106 - HLR Authentication Center

107 - HLR Authentication Center

108 - HLR Authentication Center

109 - HLR Authentication Center

110 - HLR Authentication Center

111 - HLR Authentication Center

112 - HLR Authentication Center

113 - HLR Authentication Center

114 - HLR Authentication Center

115 - HLR Authentication Center

116 - HLR Authentication Center

117 - HLR Authentication Center

118 - HLR Authentication Center

119 - HLR Authentication Center

120 - HLR Authentication Center

121 - HLR Authentication Center

122 - HLR Authentication Center

123 - HLR Authentication Center

124 - HLR Authentication Center

125 - HLR Authentication Center

126 - HLR Authentication Center

127 - HLR Authentication Center

128 - HLR Authentication Center

129 - HLR Authentication Center

130 - HLR Authentication Center

131 - HLR Authentication Center

132 - HLR Authentication Center

133 - HLR Authentication Center

134 - HLR Authentication Center

135 - HLR Authentication Center

136 - HLR Authentication Center

137 - HLR Authentication Center

138 - HLR Authentication Center

139 - HLR Authentication Center

140 - HLR Authentication Center

141 - HLR Authentication Center

142 - HLR Authentication Center

143 - HLR Authentication Center

144 - HLR Authentication Center

145 - HLR Authentication Center

146 - HLR Authentication Center

147 - HLR Authentication Center

148 - HLR Authentication Center

149 - HLR Authentication Center

150 - HLR Authentication Center

151 - HLR Authentication Center

152 - HLR Authentication Center

153 - HLR Authentication Center

154 - HLR Authentication Center

155 - HLR Authentication Center

156 - HLR Authentication Center

157 - HLR Authentication Center

158 - HLR Authentication Center

159 - HLR Authentication Center

160 - HLR Authentication Center

161 - HLR Authentication Center

162 - HLR Authentication Center

163 - HLR Authentication Center

164 - HLR Authentication Center

165 - HLR Authentication Center

166 - HLR Authentication Center

167 - HLR Authentication Center

168 - HLR Authentication Center

169 - HLR Authentication Center

170 - HLR Authentication Center

171 - HLR Authentication Center

172 - HLR Authentication Center

173 - HLR Authentication Center

174 - HLR Authentication Center

175 - HLR Authentication Center

176 - HLR Authentication Center

177 - HLR Authentication Center

178 - HLR Authentication Center

179 - HLR Authentication Center

180 - HLR Authentication Center

181 - HLR Authentication Center

182 - HLR Authentication Center

183 - HLR Authentication Center

184 - HLR Authentication Center

185 - HLR Authentication Center

186 - HLR Authentication Center

187 - HLR Authentication Center

188 - HLR Authentication Center

189 - HLR Authentication Center

190 - HLR Authentication Center

191 - HLR Authentication Center

192 - HLR Authentication Center

193 - HLR Authentication Center

194 - HLR Authentication Center

195 - HLR Authentication Center

196 - HLR Authentication Center

197 - HLR Authentication Center

198 - HLR Authentication Center

199 - HLR Authentication Center

200 - HLR Authentication Center

201 - HLR Authentication Center

202 - HLR Authentication Center

203 - HLR Authentication Center

204 - HLR Authentication Center

205 - HLR Authentication Center

206 - HLR Authentication Center

207 - HLR Authentication Center

208 - HLR Authentication Center

209 - HLR Authentication Center

210 - HLR Authentication Center

211 - HLR Authentication Center

212 - HLR Authentication Center

213 - HLR Authentication Center

214 - HLR Authentication Center

215 - HLR Authentication Center

216 - HLR Authentication Center

217 - HLR Authentication Center

218 - HLR Authentication Center

219 - HLR Authentication Center

220 - HLR Authentication Center

221 - HLR Authentication Center

222 - HLR Authentication Center

223 - HLR Authentication Center

224 - HLR Authentication Center

225 - HLR Authentication Center

226 - HLR Authentication Center

227 - HLR Authentication Center

228 - HLR Authentication Center

229 - HLR Authentication Center

230 - HLR Authentication Center

231 - HLR Authentication Center

232 - HLR Authentication Center

233 - HLR Authentication Center

234 - HLR Authentication Center

235 - HLR Authentication Center

236 - HLR Authentication Center

237 - HLR Authentication Center

238 - HLR Authentication Center

239 - HLR Authentication Center

240 - HLR Authentication Center

241 - HLR Authentication Center

242 - HLR Authentication Center

243 - HLR Authentication Center

244 - HLR Authentication Center

245 - HLR Authentication Center

246 - HLR Authentication Center

247 - HLR Authentication Center

248 - HLR Authentication Center

249 - HLR Authentication Center

250 - HLR Authentication Center

251 - HLR Authentication Center

252 - HLR Authentication Center

253 - HLR Authentication Center

254 - HLR Authentication Center

255 - HLR Authentication Center

Correspondance (Indicateurs Sources)

Les routes peuvent correspondre sur les indicateurs des messages entrants :

- source TT : Correspondre aux messages avec un Type de Traduction spécifique
- source NAI : Correspondre aux messages avec un Indicateur de Plan de Numérotation spécifique
- source NPI : Correspondre aux messages avec un Indicateur de Nature d'Adresse spécifique
- Valeur n1 = wildcard (correspond à n'importe quelle valeur)

Transformation (Indicateurs de Destination)

Les routes peuvent réécrire les indicateurs lors du transfert :

- dest TT : Transformer le Type de Traduction en nouvelle valeur
- dest NAI : Transformer l'Indicateur de Plan de Numérotation en nouvelle valeur
- dest NPI : Transformer l'Indicateur de Nature d'Adresse en nouvelle valeur
- Valeur n1 = préserver la valeur d'origine (pas de transformation)

Sélection Basée sur la Spécificité

Lorsque plusieurs routes correspondent, la route la plus spécifique est sélectionnée en utilisant cet ordre de priorité :

1. Correspondance de préfixe GT le plus long
2. SSN source spécifique sur SSN wildcard
3. TT source spécifique sur TT wildcard
4. NPI source spécifique sur NPI wildcard
5. NAI source spécifique sur NAI wildcard
6. Numéro de priorité le plus bas

Exemples de Configuration

```
config (msmt)
  enable_gt_routing true;

  # Exemple 1 : Correspondre et transformer le Type de Traduction
  #
  # gt_prefix: "44";
  # peer_id: 1;
  # source_tt: 4;      # Correspondre TT=4 (Inconnu)
  # dest_tt: 3;        # Transformer en TT=3 (National)
  # priority: 1;
  # description: "Numéros UK : transformation TT 4-3"
  }

  # Exemple 2 : Correspondre NPI spécifique et transformer NAI
  #
  # gt_prefix: "1";
  # peer_id: 2;
  # source_npi: 1;     # Correspondre NPI=1 (ISDN/Telex)
  # source_nai: 4;     # Correspondre NAI=4 (International)
  # dest_nai: 3;        # Transformer en NAI=3 (National)
  # priority: 1;
  # description: "Numéros US : International-to-National NAI"
  }

  # Exemple 3 : Routage combiné SSN et indicateurs
  #
  # gt_prefix: "10";
  # source_ssn: 8;     # Correspondre au trafic SMC
  # source_tt: 6;      # Correspondre TT=6
  # dest_ssn: 6;       # Réécrire SSN à MSA
  # dest_tt: 2;        # Transformer en TT=2
  # dest_npi: 1;       # Définir NPI=1 (ISDN)
  # dest_nai: 4;       # Définir NAI=4 (International)
  # peer_id: 3;
  # priority: 1;
  # description: "SMS français : Normalisation complète"
  }

  # Exemple 4 : Wildcard TT, NPI spécifique
  #
  # gt_prefix: "40";
  # source_tt: n1;     # Correspondre à n'importe quel TT (wildcard)
  # source_npi: 1;     # Correspondre NPI=1 (ISDN)
  # dest_npi: 6;       # Transformer en NPI=6 (ISDN)
  # peer_id: 4;
  # priority: 1;
  # description: "Normalisation du réseau de données allemand"
  }
}
```

Valeurs Courantes de TUNPUNAI

Type de Traduction (TT) :

- 0 = Inconnu
- 1 = International
- 2 = National
- 3 = Spécifique au Réseau

Indicateur de Plan de Numérotation (NPI) :

- 0 = Inconnu
- 1 = ISDN/Glaphone (E.164)
- 2 = Données (E.121)
- 4 = Telex (E.16)
- 6 = Mobile Terrestre (E.212)

Indicateur de Nature d'Adresse (NAI) :

- 0 = Inconnu
- 1 = Numéro d'Abonné
- 2 = Réserve pour Utilisateur Nationale
- 3 = Numéro Supplément National
- 4 = Numéro International

Exemple de Décision de Routage

Pour un message entrant avec :

- GT : "44712345678"
- SSN : 8
- TT : 0
- NPI : 1
- NAI : 4

Avec ces routes configurées :

```
# Route A : Wildcard TT
%gt_prefix: "447", peer_id: 1, priority: 1;

# Route B : TT spécifique
%gt_prefix: "447", source_tt: 8, peer_id: 2, priority: 1;

# Route C : TT spécifique + NPI
%gt_prefix: "447", source_tt: 8, source_npi: 1, peer_id: 3, priority: 1;
```

Résultat : La Route C est sélectionnée (la plus spécifique : correspond à GT + TT + NPI)

Le message est transféré avec des indicateurs transformés selon les valeurs dest_tt, dest_npi, dest_nai de la Route C.

Exemples de Routage GT

GT Appelé	SSN Source	TUNPUNAI	Route Correspondante	Ratons
44712345678	-	-	"44" = pair 3	Correspondance de préfixe le plus longue
441234567890	-	-	"44" = pair 1	Correspondance de préfixe, aucune route plus spécifique
1212551234	6	-	"1" = pair 4	Correspondance de préfixe pour numéros US
558812345678	-	-	"55" (SSN 8) = pair 4	Correspondance GT + SSN, réécrit SSN à 6
558812345678	-	-	"55" (SSN 8) = pair 4	Correspondance GT + SSN, réécrit SSN à 6
441234567890	0	1	"44" (TT=0) = pair 1	Correspondance GT + TT, transforme TT en 3
1212551234	6	0	"1" (TT=0, NPI=1, NAI=4)	Plus spécifique : correspondance GT+TT+NPI+NAI

Cas d'Utilisation Courants pour le Routage TUNPUNAI

1. Normalisation de l'Interconnexion Réseaux

- Différents réseaux peuvent utiliser des conventions d'indicateur différentes
- Transformer les indicateurs au point d'interconnexion pour assurer la compatibilité
- Exemple : Le réseau primaire utilise TT=0 pour international, votre réseau utilise TT=1

2. Conversion de Protocole

↳ Convertir entre des plans de numérotation lors du routage entre différents types de réseau

↳ Exemple : Route d'un réseau mobile (NPN=0) vers le PSTN (NPN=1)
3. Standardisation du Format d'Adresse

↳ Normaliser tout le trafic entrant pour utiliser des valeurs NAI cohérentes

↳ Exemple : Convertir tous les formats internationaux (NAI=4) en format national (NAI=3) pour le routage domestique
4. Routage Spécifique au Fournisseur

↳ Router en fonction du type de traduction vers différents fournisseurs de services

↳ Exemple : 37=0 route vers le Fournisseur A, 37=2 route vers le Fournisseur B
5. Intégration de Systèmes Hérités

↳ Les systèmes modernes peuvent utiliser des valeurs d'indicateurs différentes du celles des systèmes hérités

↳ Transformer en STP pour maintenir la compatibilité avec les anciens systèmes

Fonctionnalités de Gestion des Routes

Désactivation des Routes

Les routes peuvent être temporairement désactivées sans être supprimées. Cela est utile pour les tests, la maintenance ou la gestion du trafic.

Drapeau Actif

Les routes par Code de Point et par Titre Global prennent en charge un drapeau `enabled` optionnel :

```
config omis17,
alias routes: [
  # Route active
  {
    dest_pc: 100,
    peer_id: 1,
    priority: 1,
    network_indicator: international,
    enabled: true # Route active (par défaut si omis)
  },
  # Route désactivée (not évaluée lors du routage)
  {
    dest_pc: 200,
    peer_id: 2,
    priority: 1,
    network_indicator: international,
    enabled: false # Route désactivée
  },
],
alias gt_routes: [
  # Route GT désactivée
  {
    gt_prefix: "44",
    peer_id: 1,
    priority: 1,
    description: "Numéros UK - temporairement désactivée",
    enabled: false
  }
]
```

Comportement par Défaut :

- Si `enabled` n'est pas spécifié, les routes sont par défaut `enabled: true`
- Les routes désactivées sont complètement ignorées lors de la recherche de routes
- Utilisez l'interface Web pour activer/désactiver les routes sans modifier la configuration

Cas d'Utilisation :

- Tester les modifications de flux de trafic
- Problème de maintenance temporaire
- Tests AB de différents chemins de routage
- Déploiement progressif de nouvelles routes

Routes DROP - Prévention des Bouches de Routage

Les routes DROP (avec `peer_id: 0`) rejettent silencieusement le trafic au lieu de le transférer. Cela empêche les bouches de routage et permet un filtrage avancé du trafic.

Configuration des Routes DROP

```
config omis17,
alias routes: [
  # Route DROP pour un code de point spécifique
  {
    dest_pc: 999,
    peer_id: 0, # peer_id=0 signifie DROP
    priority: 1,
    network_indicator: international
  },
],
alias gt_routes: [
  # Route DROP pour préfixe GT
  {
    gt_prefix: "999",
    peer_id: 0, # peer_id=0 signifie DROP
    priority: 99, # peer_id=99, " # peer_id=0 signifie DROP
    description: "Bloquer la plage de test"
  }
]
```

Comment Fonctionnent les Routes DROP

Lorsqu'un message correspond à une route DROP :

1. Le message de routage détermine `peer_id: 0`
2. Le message est **silencieusement rejeté** (non transféré)
3. Un **journal INFO** est généré "Route DROP correspondante pour DPC 999" ou "Route DROP correspondante pour GT 999"
4. La recherche de routage retourne [erreur, "dropped"]

Important : Le trafic rejeté est enregistré au niveau INFO pour la surveillance et le débogage.

Cas d'Utilisation Courant : Liste Blanche de Préfixes

L'une des utilisations les plus puissantes des routes DROP est la **liste blanche de préfixes** : permettant uniquement des numéros spécifiques au sein d'une grande plage tout en bloquant tous les autres.

Le Modèle :

1. Créer une route DROP pour l'ensemble de préfixes avec un **numéro de priorité élevé** (par exemple, 99)
2. Créer des routes d'autorisation spécifiques pour des numéros individuels avec des **numéros de priorité bas** (par exemple, 1)
3. Étant donné que les numéros de priorité plus bas sont évalués en premier, les routes autorisées correspondront avant la route DROP
4. Tout message non explicitement autorisé est écarté par la route DROP

Scénario Exemple :

Vous avez un préfixe GT 1234 qui représente une plage de 10 000 numéros (1234000000 - 1234999999), mais vous ne souhaitez router que 3 numéros spécifiques : 1234567890, 1234555080, et 1234112222.

```
config omis17,
alias gt_routes: [
  # Route DROP avec PRIORITE ELEVEE (évaluée en dernier)
  {
    gt_prefix: "1234",
    peer_id: 0, # DROP
    priority: 99, # Numéro élevé = faible priorité - évalué en dernier
    description: "Bloquer tout les 1234" sauf "les numéros sur liste blanche"
  },
  # Routes d'autorisation spécifiques avec NUMEROS DE PRIORITE FAIBLES (évaluées en premier)
  {
    gt_prefix: "1234567890",
    peer_id: 1, # Route vers le pair 1
    priority: 1, # Numéro bas = haute priorité - évalué en premier
    description: "Numéro autorisé 1"
  },
  {
    gt_prefix: "1234555080",
    peer_id: 1,
    priority: 1,
    description: "Numéro autorisé 2"
  },
  {
    gt_prefix: "1234112222",
    peer_id: 1,
    priority: 1,
    description: "Numéro autorisé 3"
  }
]
```

Comportement de Routage :

CT Entrant	Routes Correspondantes	Route Sélectionnée	Action
1234567890	0 "1234" DROP (priorité 99)	0 "1234" DROP (priorité 99)	Rejeté vers le pair 1
123455080	0 "1234" DROP (priorité 99)	0 "123455080" (priorité 1)	Rejeté vers le pair 1
1234112222	0 "1234" DROP (priorité 99)	0 "1234112222" (priorité 1)	Rejeté vers le pair 1
1234999999	0 "1234" DROP (priorité 99)	0 "1234" DROP (sans correspondance)	Rejeté + enregistré
1234000000	0 "1234" DROP (priorité 99)	0 "1234" DROP (sans correspondance)	Rejeté + enregistré

Résultat :

- 0 Seuls 3 numéros spécifiques sont routés vers le pair 1
- 0 Tous les autres numéros 1234* sont silencieusement rejetés
- 0 Tout le trafic rejeté est enregistré pour la surveillance

Journaux Générés :

```
[INFO] Route DROP correspondante pour GT 1234000000
[INFO] Route DROP correspondante pour GT 1234000000
```

Routes DROP pour les Codes de Point

Le même modèle de liste blanche fonctionne pour le routage par Code de Point :

```
config omis17,
alias routes: [
  # DROP toute la plage /8 (64 codes de point : 1000-1063)
  {
    dest_pc: 1000,
    peer_id: 0,
    priority: 99,
    network_indicator: international
  },
  # Autoriser des PC spécifiques
  {
    dest_pc: 1010, peer_id: 1, priority: 1, network_indicator: international,
    dest_pc: 1020, peer_id: 1, priority: 1, network_indicator: international,
    dest_pc: 1030, peer_id: 1, priority: 1, network_indicator: international
  }
]
```

Résultat : Seules les PCs 1010, 1020 et 1030 sont routées. Tous les autres PCs dans la plage 1000-1063 sont rejetés.

Surveillance des Routes DROP

Vérifiez les Journaux :

```
# Surveillez le trafic rejeté
tail -f logs/app-log | grep "Route DROP correspondante"
```

```
# Sortir les erreurs
[INFO] Route DROP correspondante pour GT 1234000000
[INFO] Route DROP correspondante pour DPC 1000
```

Via l'interface Web :

- Naviguez vers l'onglet **Journal des Systèmes**
- Filtrer par niveau INFO
- Rechercher "Route DROP correspondante"

Meilleures Pratiques :

1. A Surveillez régulièrement les journaux pour vous assurer que les routes DROP ne bloquent pas le trafic légitime
2. A Utilisez des champs de description des routes pour documenter pourquoi les routes sont rejetées
3. A Utilisez des numéros de priorité élevés (99) pour les routes DROP afin de garantir qu'elles soient des routes catch-all
4. A Testez le comportement des routes DROP avant de déployer en production
5. A Configurez des alertes pour des augmentations anormales du trafic rejeté

Routage Avancé : Routage Basé sur SSN et Réécriture

Numéros de Sous-Système (SSN)

Les Numéros de Sous-Système identifient la couche d'application :

- **SSN 0** : HLR (Registre de Localisation de l'Abonné)
- **SSN 7** : VLR (Registre de Localisation Visiteur)
- **SSN 8** : SMSC (Centre de Communication Mobile) / SMS-C (Centre de SMS)
- **SSN 9** : CMSC (Centre de Localisation Mobile Passee/Reçu)

Exemple de Routage Basé sur SSN

Routage du trafic SMS vers différents HLR en fonction du préfixe de numéro :

```
alias gt_routes: [
  # Route SMS pour les numéros UK vers HLR UK, réécrit SSN de 8 (SMSC) à 6 (HLR)
  {
    gt_prefix: "44",
    peer_id: 0, # Correspondre au SSN entrant 8 (SMSC)
    peer_id: 1, # Réécrire à SSN 6 (HLR)
    dest_ssn: 6,
    priority: 1,
    description: "SMS UK vers HLR"
  }
]
```

```
},
# Route du trafic vocal pour les numéros UK (SSN 6) sans réécriture
{
  "set_prefix": "44",
  "source_ssn": 6,
  "peer_id": 1,
  "dest_ssn": 411,
  "priority": 1,
  "description": "Trafic vocal UK"
}
}
```

Tester la Configuration de Routage STP

Après avoir configuré les pairs et les routes, vérifiez votre configuration :

1. Vérifier l'État des Pairs

Via l'interface Web :

- Naviguez vers [l'interface Web](#)
- Vérifiez la page d'état MSUA.
- Assurez-vous que les pairs affichent l'état : **ACTIF**

Via la Console CLI :

```
# Obtenir tous les états des pairs
MSUA_STP.get_peers_status()

# Sortie attendue :
# [
#   { "peer_id": 1, "name": "Partner_STP_Moët", "status": "active", "point_code": 100, ... },
#   { "peer_id": 2, "name": "Local_HLR", "status": "active", "point_code": 200, ... }
# ]
```

2. Tester le Routage par Code de Point

```
# Envoyer un message MSUA de test au DPC 100
test_payload = << 2, 3, >> # Charge utile fictive
MSUA_STP.route_by_pc(100, test_payload, 0)

# Vérifier les journaux pour la décision de routage
# Journal attendu : "Routage du message : DPC->...-> DPC-100 via pair 1"
```

OnMS57 Stack

SS7 Events

SS7 Client

MSUA

Routing

Routing Test

Resources

Configuration

MSUA Routing Test

Overview

Routing Test

Message Parameters

Common SSN Values

Source Point Code (DPC)

Destination Point Code (DPC)

Calling Global Title

Called Global Title

Calling SSN (optional)

Called SSN (optional)

Test Routing

Common SSN Values

Common SSN Values

3. Tester le Routage par Titre Global

```
# Rechercher manuellement la route GT
MSUA_Routing.lookup_peer_by_gti("44772245678")

# Sortie attendue :
# [{"pk": [{"msua_peer": 3, "IM_Mobile_Peer", ...}], 411}]

# Rechercher la route GT avec SSN
MSUA_Routing.lookup_peer_by_gti("5555551234567", 0)

# Sortie attendue avec réécriture SSN :
# [{"pk": [{"msua_peer": 4, "SSN_Mob_Peer", ...}], 4}]
```

4. Surveiller les Métriques de Routage

Accédez aux métriques Prometheus à /metrics

```
Métriques clés :

# Messages reçus par pair
#msua_stp_messages_received_total{peer_name="Partner_STP_Moët",point_code="100"} 1523

# Messages envoyés par pair
#msua_stp_messages_sent_total{peer_name="Local_HLR",point_code="200"} 1408

# Échecs de routage
#msua_stp_routing_failures_total{reason="no_route"} 5
#msua_stp_routing_failures_total{reason="no_peer"} 2
```

Métriques et Surveillance STP

Métriques Disponibles

Métriques de Trafic par Pair :

- msua_stp_messages_received_total : Total des messages reçus de chaque pair
 - Filtrages : peer_name, point_code
- msua_stp_messages_sent_total : Total des messages transférés à chaque pair
 - Filtrages : peer_name, point_code

***Métriques d'Échec:



Guide de l'interface utilisateur Web

[← Retour à la documentation principale](#)

Ce guide fournit une documentation complète pour l'utilisation de l'OmniSS7 **Web UI** (interface Phoenix LiveView).

Table des matières

1. [Aperçu](#)
 2. [Accéder à l'interface Web](#)
 3. [Page de gestion du routage](#)
 4. [Page des abonnés actifs](#)
 5. [Opérations courantes](#)
 6. [Comportement d'auto-rafraîchissement](#)
-

Aperçu

L'interface Web OmniSS7 est une application **Phoenix LiveView** qui fournit des capacités de surveillance et de gestion en temps réel. Les pages disponibles dépendent du mode opérationnel actif (STP, HLR ou SMSc).

Architecture de l'interface Web

Configuration du serveur

- **Protocole:** HTTPS
- **Port:** 443 (configuré dans config/runtime.exs)
- **IP par défaut:** 0.0.0.0 (écoute sur toutes les interfaces)
- **Certificats:** Situés dans priv/cert/

URL d'accès: https://[server-ip]:443

Accéder à l'interface Web

Prérequis

1. **Certificats SSL:** Assurez-vous que des certificats SSL valides sont présents dans priv/cert/:

- omnitouch.crt - Fichier de certificat
- omnitouch.pem - Fichier de clé privée

2. **Application en cours d'exécution:** Démarrez l'application avec `iex -S mix`

3. **Pare-feu:** Assurez-vous que le port 443 est ouvert pour le trafic HTTPS

Pages disponibles par mode

Page	Mode STP	Mode HLR	Mode SMSc	Description
Événements SS7	?	?	?	Journalisation des événements et capture des messages SCCP
Client SS7	?	?	?	Tests manuels des opérations MAP
M3UA	?	?	?	État de la connexion M3UA
Routage	?	?	?	Gestion de la table de routage M3UA
Test de routage	?	?	?	Tests et validation de routes
Liens HLR	?	?	?	État de l'API HLR et gestion des abonnés
Abonnés actifs	?	?	?	Suivi de la localisation des abonnés en temps réel (HLR)
Liens SMSc	?	?	?	État de l'API SMSc et gestion des files d'attente
Abonnés SMSc	?	?	?	Suivi des abonnés en temps réel (SMSc)
Application	?	?	?	Ressources système et surveillance
Configuration	?	?	?	Visualiseur de configuration

Gestion du routage

Page: /routing

Modes: STP, SMSc

Auto-rafraîchissement: Toutes les 5 secondes

La page de gestion du routage fournit une interface à onglets pour gérer les tables de routage M3UA.

Mise en page de la page

Onglet Pairs

Gérez les connexions de pairs M3UA (autres STP, HLR, MSC, SMSC).

Colonnes du tableau des pairs

Colonne	Description	Exemple
ID	Identifiant unique du pair	1
Nom	Nom du pair lisible par l'homme	"STP_West"
Rôle	Rôle de la connexion	client, server, stp
Code de point	Code de point SS7 du pair	100
Distant	IP:Port distant	10.0.0.10:2905
Statut	Statut de la connexion	active, aspup, down
Actions	Boutons Modifier/Supprimer	-

Ajouter un pair

1. **Cliquez** sur l'onglet Pairs
2. **Remplissez** les champs du formulaire :
 - **ID du pair**: Généré automatiquement s'il est laissé vide
 - **Nom du pair**: Nom descriptif (obligatoire)
 - **Rôle**: Sélectionnez client, server ou stp
 - **Code de point**: Code de point SS7 (obligatoire)
 - **IP locale**: Adresse IP de votre système
 - **Port local**: 0 pour une attribution de port dynamique
 - **IP distante**: Adresse IP du pair
 - **Port distant**: Port du pair (généralement 2905)
 - **Contexte de routage**: ID de contexte de routage M3UA
 - **Indicateur de réseau**: international ou national
3. **Cliquez** sur "Ajouter un pair"

Persistence: Le pair est immédiatement enregistré dans Mnesia et survit au redémarrage.

Modifier un pair

1. **Cliquez** sur le bouton "Modifier" de la ligne du pair
2. **Modifiez** les champs du formulaire si nécessaire
3. **Cliquez** sur "Mettre à jour le pair"

Remarque: Si vous changez l'ID du pair, l'ancien pair est supprimé et un nouveau est créé.

Supprimer un pair

1. **Cliquez** sur le bouton "Supprimer" de la ligne du pair
2. **Confirmez** la suppression (toutes les routes utilisant ce pair seront également supprimées)

Indicateurs de statut des pairs

Statut	Couleur	Description
active	◇ Vert	Le pair est connecté et routant des messages
aspup	◇ Jaune	L'ASP est en ligne mais pas encore actif
down	◇ Rouge	Le pair est déconnecté

Onglet Routes de Code de Point

Configurez des règles de routage basées sur les codes de point de destination.

Colonnes du tableau des routes

Colonne	Description	Exemple
PC de destination	Code de point cible (format zone.area.id)	1.2.3 (100)
Masque	Masque de sous-réseau pour la correspondance de PC	/14 (exact), /8 (plage)
ID du pair	Pair cible pour cette route	1
Nom du pair	Nom du pair cible	"STP_West"
Priorité	Priorité de la route (1 = la plus élevée)	1
Réseau	Indicateur de réseau	international
Actions	Boutons Modifier/Supprimer	-

Ajouter une route de code de point

1. **Cliquez** sur l'onglet "Routes de Code de Point"
2. **Remplissez** les champs du formulaire :
 - **Code de point de destination:** Entrez au format zone.area.id (par exemple, 1.2.3) ou entier (0-16383)
 - **Masque:** Sélectionnez le masque /14 pour une correspondance exacte, des valeurs inférieures pour des plages
 - **ID du pair:** Sélectionnez le pair cible dans le menu déroulant
 - **Priorité:** Entrez la priorité (1 = la plus élevée, par défaut)
 - **Indicateur de réseau:** Sélectionnez international ou national
3. **Cliquez** sur "Ajouter une route"

Format de code de point: Vous pouvez entrer des codes de point dans deux formats :

- **Format 3-8-3:** zone.area.id (par exemple, 1.2.3)
- **Format entier:** 0-16383 (par exemple, 1100)

Le système convertit automatiquement entre les formats.

Comprendre les masques

Les codes de point sont des valeurs de 14 bits (0-16383). Le masque spécifie combien de bits les plus significatifs doivent correspondre :

Masque	PC correspondants	Cas d'utilisation
/14	1 (correspondance exacte)	Route vers une destination spécifique
/13	2 PC	Petite plage
/8	64 PC	Plage moyenne
/0	Tous les 16 384 PC	Route par défaut/de secours

Exemples :

- PC 1000 /14 → Correspond uniquement au PC 1000
- PC 1000 /8 → Correspond aux PC 1000-1063 (64 PC consécutifs)
- PC 0 /0 → Correspond à tous les codes de point (route par défaut)

Carte de référence du masque de code de point

La page Web comprend une référence interactive montrant toutes les valeurs de masque et leurs plages.

Onglet Routes de Titre Global

Configurez des règles de routage basées sur les adresses de Titre Global SCCP.

Exigence: Le routage par Titre Global doit être activé dans la configuration :

```
config :omniss7,  
    enable_gt_routing: true
```

Colonnes du tableau des routes

Colonne	Description	Exemple
Préfixe GT	Préfixe GT du parti appelé (vide = secours)	"1234", ""
SSN source	Correspondre au SSN du parti appelé (optionnel)	6 (HLR), any
ID du pair	Pair cible	1
Pair	Nom du pair	"HLR_West (1)"
SSN de destination	Réécrire le SSN lors du transfert (optionnel)	6, preserve
Priorité	Priorité de la route	1
Description	Description de la route	"US numbers"
Actions	Boutons Modifier/Supprimer	-

Ajouter une route de titre global

1. **Cliquez** sur l'onglet "Routes de Titre Global"
2. **Remplissez** les champs du formulaire :
 - **Préfixe GT**: Laissez vide pour la route de secours, ou entrez des chiffres (par exemple, "1234")
 - **SSN source**: Optionnel - filtrer par SSN du parti appelé
 - **ID du pair**: Sélectionnez le pair cible
 - **SSN de destination**: Optionnel - réécrire le SSN lors du transfert
 - **Priorité**: Priorité de la route (1 = la plus élevée)
 - **Description**: Description lisible par l'homme
3. **Cliquez** sur "Ajouter une route"

Routes de secours: Si le préfixe GT est vide, la route agit comme un attrape-tout pour les GT qui ne correspondent à aucune autre route.

Valeurs SSN courantes

La page comprend une carte de référence avec des valeurs SSN courantes :

SSN	Élément de réseau
6	HLR (Home Location Register)
7	VLR (Visitor Location Register)
8	MSC (Mobile Switching Center)
9	EIR (Equipment Identity Register)
10	AUC (Authentication Center)
142	RANAP
145	gsmSCF (Service Control Function)
146	SGSN

Réécriture de SSN

- **SSN source**: Correspondre au SSN du parti appelé dans les messages entrants
- **SSN de destination**: Si défini, réécrit le SSN du parti appelé lors du transfert
 - Vide = préserver le SSN original
 - Valeur = remplacer par ce SSN

Cas d'utilisation: Router des messages avec SSN=6 (HLR) vers un pair, et réécrire vers SSN=7 (VLR) du côté sortant.

Persistance de la table de routage

Toutes les routes sont stockées dans Mnesia et survivent aux

redémarrages de l'application.

Comment les routes persistent

1. **Modifications de l'interface Web:** Toutes les opérations d'ajout/modification/suppression sont immédiatement enregistrées dans Mnesia
2. **Redémarrage de l'application:** Les routes sont chargées depuis Mnesia au démarrage
3. **Fusion de runtime.exs:** Les routes statiques de config/runtime.exs sont fusionnées avec les routes Mnesia (pas de doublons)

Priorité de la route

Lorsque plusieurs routes correspondent à une destination :

1. **Plus spécifique d'abord:** Les valeurs de masque plus élevées (plus spécifiques) prennent la priorité
2. **Champ de priorité:** Les numéros de priorité inférieurs routent en premier (1 = priorité la plus élevée)
3. **Statut du pair:** Seules les routes vers des pairs actifs sont utilisées

Abonnés actifs

Page: /subscribers

Mode: HLR uniquement

Auto-rafraîchissement: Toutes les 2 secondes

Affiche le suivi en temps réel des abonnés qui ont envoyé des demandes UpdateLocation.

Fonctionnalités de la page

Colonnes du tableau des abonnés

Colonne	Description	Exemple
IMSI	IMSI de l'abonné	"50557123456789"
Numéro VLR	Adresse GT VLR actuelle	"555123155"
Numéro MSC	Adresse GT MSC actuelle	"555123155"
Mis à jour à	Dernière horodatage UpdateLocation	"2025-10-25 14:23:45 UTC"
Durée	Temps depuis l'enregistrement	"2h 15m 34s"

Résumé des statistiques

Lorsque des abonnés sont présents, une carte de résumé affiche :

- **Total Actif:** Nombre total d'abonnés enregistrés
- **VLRs Uniques:** Nombre d'adresses VLR distinctes
- **MSCs Uniques:** Nombre d'adresses MSC distinctes

Effacer les abonnés

Bouton Effacer Tout: Supprime tous les abonnés actifs du tracker.

Confirmation: Nécessite une confirmation avant de vider (ne peut pas être annulé).

Cas d'utilisation: Effacer les enregistrements d'abonnés obsolètes après une maintenance ou un test du réseau.

Auto-rafraîchissement

La page se rafraîchit automatiquement toutes les **2 secondes** pour afficher les mises à jour des abonnés en temps réel.

Abonnés SMSc

Page: /smsc_subscribers

Mode: SMSc uniquement

Auto-rafraîchissement: Toutes les 2 secondes

Affiche le suivi en temps réel des abonnés basé sur les messages alertServiceCenter reçus des HLR, l'état de livraison des messages et le suivi des échecs.

Fonctionnalités de la page

Colonnes du tableau des abonnés

Colonne	Description	Exemple
MSISDN	Numéro de téléphone de l'abonné	"15551234567"
IMSI	IMSI de l'abonné	"001010123456789"
HLR GT	HLR GT qui a envoyé alertServiceCenter	"15551111111"
Msgs Envoyés	Nombre de messages MT-FSM envoyés	5
Msgs Reçus	Nombre de messages MO-FSM	2

Colonne	Description	Exemple
Statut	reçus Actif ou Échoué (codé par couleur) ● Actif	
Dernière mise à jour	Dernière horodatage de mise à jour	"2025-10-30 14:23:45 UTC"
Durée	Temps depuis la dernière mise à jour	"15m 34s"

Indicateurs de statut

- **Actif** (Vert): L'abonné est joignable, dernier alertServiceCenter reçu avec succès
- **Échoué** (Rouge): Dernière tentative de livraison échouée (SRI-for-SM ou erreur d'abonné absent)

Résumé des statistiques

Lorsque des abonnés sont présents, une carte de résumé affiche :

- **Total Suivi**: Nombre total d'abonnés suivis
- **Actifs**: Nombre d'abonnés avec un statut actif
- **Échoués**: Nombre d'abonnés avec un statut échoué
- **HLRs Uniques**: Nombre de HLR distincts envoyant des alertes

Gestion des abonnés

Bouton Supprimer: Supprime un abonné individuel du suivi.

Bouton Effacer Tout: Supprime tous les abonnés suivis.

Confirmation: Effacer Tout nécessite une confirmation avant de vider (ne peut pas être annulé).

Cas d'utilisation :

- Supprimer les entrées obsolètes après des problèmes de réseau
- Effacer les données de test après le développement
- Surveiller quels HLR envoient des alertes

Compteurs de messages

Le tracker incrémente automatiquement les compteurs :

- **Messages Envoyés**: Incrémenté lorsque SRI-for-SM réussit et MT-FSM est envoyé
- **Messages Reçus**: Incrémenté lorsque MO-FSM est reçu de l'abonné

Auto-rafraîchissement

La page se rafraîchit automatiquement toutes les **2 secondes** pour afficher les mises à jour en temps réel des abonnés et des statuts.

Opérations courantes

Recherche et filtrage

Actuellement, l'interface Web ne comprend pas de fonctionnalité de recherche/filtrage intégrée. Pour trouver des routes spécifiques :

1. Utilisez la fonction de recherche de votre navigateur (Ctrl+F / Cmd+F)
2. Recherchez des noms de pairs, des codes de point ou des préfixes GT

Opérations en masse

Pour effectuer des modifications de routes en masse :

1. **Option 1:** Utilisez l'[API REST](#) pour un accès programmatique
2. **Option 2:** Modifiez `config/runtime.exs` et redémarrez l'application
3. **Option 3:** Utilisez l'interface Web pour des modifications de routes individuelles

Exportation/Importation

Remarque: L'interface Web ne prend actuellement pas en charge l'exportation ou l'importation de tables de routage. Les routes sont :

- Stockées dans des fichiers de base de données Mnesia
- Configurées dans `config/runtime.exs`

Pour sauvegarder les routes :

1. **Mnesia:** Sauvegardez le répertoire `Mnesia.{node_name}/`
 2. **Configuration:** Contrôle de version de `config/runtime.exs`
-

Comportement d'auto-rafraîchissement

Différentes pages ont différents intervalles de rafraîchissement :

Page	Intervalle de rafraîchissement	Raison
Gestion du	5 secondes	Les changements de route sont peu

Page	Intervalle de rafraîchissement	Raison
routage		fréquents
Abonnés actifs	2 secondes	L'état des abonnés change fréquemment
État M3UA	Varie selon la page	Surveillance de l'état de connexion

Connexion WebSocket: Toutes les pages utilisent les connexions WebSocket de Phoenix LiveView pour des mises à jour en temps réel.

Interruption réseau: Si la connexion WebSocket est perdue, la page tentera de se reconnecter automatiquement.

Dépannage

Page ne se charge pas

1. **Vérifiez le certificat HTTPS:** Assurez-vous que `priv/cert/omnitouch.crt` et `.pem` sont présents
2. **Vérifiez le port 443:** Vérifiez que les règles de pare-feu autorisent le trafic HTTPS
3. **Application en cours d'exécution:** Confirmez que l'application est en cours d'exécution avec `iex -S mix`
4. **Console du navigateur:** Vérifiez les erreurs de certificat SSL (avertissements de certificat auto-signé)

Routes ne persistant pas

1. **Vérifiez le stockage Mnesia:** Vérifiez `mnesia_storage_type`: `:disc_copies` dans la configuration
2. **Répertoire Mnesia:** Assurez-vous que le répertoire Mnesia est accessible en écriture
3. **Vérifiez les journaux:** Recherchez des erreurs Mnesia dans les journaux de l'application

Auto-rafraîchissement ne fonctionnant pas

1. **Connexion WebSocket:** Vérifiez la console du navigateur pour des erreurs WebSocket
2. **Réseau:** Vérifiez la connexion réseau stable
3. **Rafraîchissement de la page:** Essayez de rafraîchir la page (F5)

Documentation connexe

- [Guide STP](#) - Configuration détaillée du routage
 - [Guide HLR](#) - Gestion des abonnés
 - [Guide API](#) - API REST pour un accès programmatique
 - [Référence de configuration](#) - Tous les paramètres de configuration
-

Résumé

L'interface Web OmniSS7 fournit une gestion intuitive et en temps réel des tables de routage et du suivi des abonnés :

- ◇ **Mises à jour en temps réel** - L'auto-rafraîchissement maintient les données à jour
- ◇ **Stockage persistant** - Mnesia garantit que les routes survivent aux redémarrages
- ◇ **UI basée sur les rôles** - Les pages s'adaptent au mode opérationnel (STP/HLR/SMSc)
- ◇ **Gestion interactive** - Ajouter, modifier, supprimer des routes sans redémarrage
- ◇ **Surveillance de l'état** - État de connexion et statut des pairs en direct

Pour des opérations avancées ou de l'automatisation, consultez le [Guide API](#).