

OmniMME Configuration Reference

OmniMME is configured via `/etc/omnimme/runtime.exs`. This file is evaluated at startup and overrides compile-time defaults. Changes require a service restart to take effect.

Configuration Structure

Configuration is grouped by OTP application. The `:mme` application holds the core MME behaviour and the parameters for every interface the MME originates; the transport-level libraries (`:diameter_ex`, `:gtpc`) and the management surfaces (`:control_panel`, `:api_ex`) are configured under their own keys.

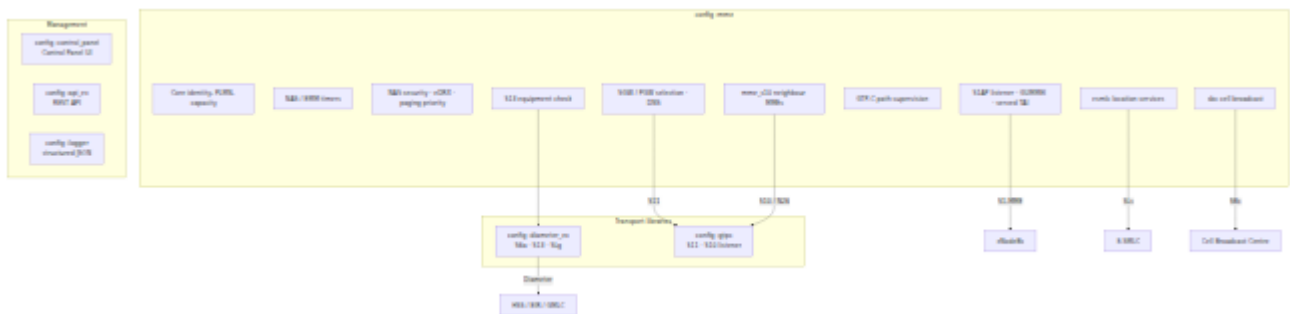


Table of Contents

- MME Core Parameters
- EMM / NAS Timers
- NAS Security
- Extended Idle-mode DRX (eDRX)
- Paging Priority

- [Reject Cause Mapping](#)
 - [Equipment Identity Check \(S13\)](#)
 - [S1AP Interface](#)
 - [Served GUMMEI](#)
 - [Served TAI](#)
 - [Serving Gateway \(SGW\)](#)
 - [Packet Data Network Gateway \(PGW\)](#)
 - [Neighbour MME \(S10\)](#)
 - [GTP-C Path Supervision](#)
 - [Diameter \(S6a / S13 / SLg\)](#)
 - [GTPv2-C \(S11\)](#)
 - [Cell Broadcast \(SBc\)](#)
 - [Location Services \(E-SMLC / SLs\)](#)
 - [NIDD / Control-Plane CIoT \(T6a\)](#)
 - [Control Panel](#)
 - [REST API](#)
 - [Logging](#)
 - [Configuration Example](#)
-

MME Core Parameters

```
config :mme,  
  mme_name: "omnimme",  
  operator_name: "Omnitouch",  
  country: "Australia",  
  network_name_short: "omnitouch",  
  network_name_long: "omnitouch",  
  timezone: "Australia/Sydney",  
  default_apn: "internet",  
  apn_oi_domain: :gprs,  
  mme_capacity: 255,  
  home_plmn: %{mcc: "001", mnc: "01"},  
  emergency_support_enabled: true
```

Parameter	Type	Required	Default	Description
<code>mme_name</code>	String	Yes	-	Human-readable name for the MME node. Included in logs.
<code>operator_name</code>	String	No	-	Operator label associated with the home PLMN, displayed alongside the PLMN in the Console and used when describing the network.
<code>country</code>	String	No	-	Country label associated with the home PLMN, displayed alongside the PLMN and <code>operator_name</code> .
<code>network_name_short</code>	String	Yes	-	Short network name sent to UE in EMM Information Attach Accept. Typically the brand abbreviation.
<code>network_name_long</code>	String	Yes	-	Full network name sent to UE in EMM Information Attach Accept.
<code>timezone</code>	String	Yes	-	IANA time zone used for time formatting.

Parameter	Type	Required	Default	Description
				Control Panel "Australia" "Etc/UTC" not affect signalling.
default_apn	String	Yes	-	APN used for default PDN connection. UE does not need a specific APN.
apn_oi_domain	Atom	No	:gprs	Controls the Operator Identifier (APN-OI) domain suffix appended to the request form the APN. See APN OI Identifier .
mme_capacity	Integer	Yes	-	Relative MME capacity available to eNodeB Setup (0-2 by eNodeB balance in connection available MME be overridden eNB at runtime the Control without re:
home_plmn	Map	Yes	-	Home PLMN Must match

Parameter	Type	Required	Default	Description
				PLMN conf the HSS ar SIM provis PLMN Para
<code>emergency_support_enabled</code>	Boolean	No	<code>false</code>	When <code>true</code> accepts unauthenticated emergency requests a in 3GPP TS §5.3.4.1 .

PLMN Parameters

Parameter	Type	Description
<code>mcc</code>	String	Mobile Country Code — three-digit string (e.g. <code>"001"</code>).
<code>mnc</code>	String	Mobile Network Code — two or three-digit string (e.g. <code>"01"</code>).

APN Operator Identifier

The APN sent by the UE (the APN Network Identifier, e.g. `internet`) is combined with an **APN Operator Identifier (APN-OI)** domain suffix to form the fully-qualified APN-FQDN used for P-GW selection and stored on the session ([TS 23.003 §9.1.2 / §19.4.2.2](#)). The same suffix is stripped again when matching the bare APN names provisioned in the subscription, so a subscriber provisioned with `internet` matches a request that the MME has expanded to `internet.mnc001.mcc001.gprs`.

`apn_oi_domain` selects which suffix form is used. The `<MNC>/<MCC>` are taken from the subscriber's matched PLMN.

Value	Resulting APN-FQDN	Notes
<code>:gprs</code> (default)	<code><apn>.mnc<MNC>.mcc<MCC>.gprs</code>	Legacy APN-OI form.
<code>:epc</code>	<code><apn>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org</code>	EPC APN-OI form used for S-NAP / DNS-based P-C selection.
<code>:none</code>	<code><apn></code>	No suffix; the bare APN is used end-to-end. Use when the P-GW and subscriber both expect un-suffixed APNs.

How it works: for a subscriber on PLMN MCC 001 / MNC 01 requesting `internet`, `:gprs` produces `internet.mnc001.mcc001.gprs`, `:epc` produces `internet.apn.epc.mnc001.mcc001.3gppnetwork.org`, and `:none` produces `internet`. The suffix is applied consistently to home and visited subscribers and is removed before the APN is matched against the provisioned APN list, so changing this value does not require re-provisioning bare APN names in the HSS.

Use case: set `:epc` when P-GW selection relies on the 3GPP EPC APN-FQDN/S-NAPTR convention; set `:none` for cores that provision and route on bare APN strings.

Deprecated: `persistent_emm_deregistered_cleanup_interval` and `persistent_ecm_idle_cleanup_interval` were context-eviction intervals in earlier releases. They are **no longer read by OmniMME** — leaving them in `runtime.exs` has no effect. UE-context lifecycle is now governed by the standards-based Mobile Reachable and Implicit Detach timers (see [EMM / NAS Timers](#)); a UE that fails to perform a periodic TAU is implicitly detached and its context removed.

EMM / NAS Timers

OmniMME exposes the 3GPP NAS timers from [TS 24.301 §10.2 / Annex B](#) and the mobility-management timers from [TS 23.401 §5.3.5](#). All values are integers; the unit is noted per timer. Every timer has a spec-default and may be omitted.

```
config :mme,
  t3412: 3240, # periodic TAU interval, seconds (54 min)
  t3485: 8,    # seconds (spec default T3485 = 8 s)
  t3413: 5,
  paging_max_attempts: 3,
  t3346: 600,
  t3396: 600,
  t3450: 6,
  t3460: 6,
  t3470: 6,
  t3486: 8,
  t3489: 4,
  t3492: 6,
  nas_max_retransmissions: 4,
  m_tmsi_freeze_interval: 60
```

Parameter	Type	Unit	Default	Description
t3412	Integer	seconds	- (required)	Periodic TAU timer to UEs in Attach Accept. UEs start periodic TAU timer expires registered. E-UTRAN NAS GPRS Timer 24.008 §10.5.1 in 2-second units in 1-minute otherwise in (decihour) units. t3412 is sent in minutes (9 decihour). Used as the default when HSS subscription no SubscribeRAU-TAU-Time provided value is honoured instead.
t3485	Integer	seconds	- (required)	Retransmission Activate/Modify (Dedicated) ESM Context Request expiry timer. If the ESM is abandoned, the SGW is told to abort the procedure failure. Used as the default for retransmission timer in the ESM Information Request.

Parameter	Type	Unit	Default	Description
t3413	Integer	seconds	5	Paging-response timer. Expiry of this timer causes the MME to retransmit the paging message. 23.401 §5.3.4
paging_max_attempts	Integer	count	3	Total page attempts before the MME sends a Paging Data Notification Indication to the UE.
t3346	Integer	seconds	600	EMM (mobility management) back-off. Send a GPRS-Timer congestion EMM if it does not receive a response immediately (§4.5).
t3396	Integer	seconds	600	ESM (session management) back-off. Send congestion ESM if it does not receive a response immediately (§4.5).
t3450	Integer	seconds	6	Retransmission timer for Attach Accept / GUTI Accept Command (not initiated, awaiting matching Command).
t3460	Integer	seconds	6	Retransmission timer for Authentication Command.

Parameter	Type	Unit	Default	Description
				and Security Command.
t3470	Integer	seconds	6	Retransmission Identity Request
t3486	Integer	seconds	8	Retransmission Activate Default Bearer Context
t3489	Integer	seconds	4	Supervises the Information element 24.301 §6.6.1 when the MM ESM Information if the UE does the ESM Information Response with the attach is (Attach Reject Request itself retransmitted
t3492	Integer	seconds	6	Retransmission the (network detach / PDN path.
nas_max_retransmissions	Integer	count	4	Maximum retransmissions of a network-attach procedure is 24.301 Annex 1 retransmission initial transmission

Parameter	Type	Unit	Default	Descr
m_tmsi_freeze_interval	Integer	seconds	60	Guard period an M-TMSI fro Purge-UE-Ans Flags Freeze- 29.272 §7.3) from realloca

Mobile Reachable & Implicit Detach

```

config :mme,
  mobile_reachable_timer: 2640,    # seconds; default = (t3412 in
seconds) + 240
  implicit_detach_timer: 2640      # seconds; default = (t3412 in
seconds) + 240

```

Parameter	Type	Unit	Default	Description
mobile_reachable_timer	Integer	seconds	t3412 + 240	Started when a UE enters ECM-IDLE (TS 23.401 §5.3.5). Must be longer than the periodic TAU timer.
implicit_detach_timer	Integer	seconds	t3412 + 240	Started when the Mobile Reachable timer expires. On its expiry the UE is implicitly detached and its context removed.

NAS Security

NAS ciphering and integrity algorithm policy (TS 33.401 §5). For each UE the MME selects the highest-priority configured algorithm the UE supports, signalled in the Security Mode Command. List algorithms strongest-first.

NAS **integrity is always applied** (EIA2 by default): every NAS message after the Security Mode Command is integrity-protected, and the UE is authenticated against the HSS. NAS **ciphering is OFF (EEA0/null) by default** — NAS payloads are already integrity-protected and the radio bearer carrying them is ciphered at the AS (PDCP) layer over the air, so null NAS ciphering maximises interoperability without weakening confidentiality on the air interface.

```

config :mme,
  nas_security: %{
    # Ciphering off by default (omit the key for the same effect):
    ciphering: [:eea0],
    integrity: [:eia2, :eia1, :eia3]
  }

```

Parameter	Type	Default	Description
<code>ciphering</code>	List	<code>[:eea0]</code>	Ordered NAS ciphering algorithm preference. Valid values: <code>:eea0</code> (null / off), <code>:eea2</code> (128-EEA2, AES-CTR). Default is ciphering off. See Implemented ciphers for why <code>:eea1</code> / <code>:eea3</code> are not selectable.
<code>integrity</code>	List	<code>[:eia2, :eia1, :eia3]</code>	Ordered NAS integrity algorithm preference. Valid values: <code>:eia1</code> , <code>:eia2</code> , <code>:eia3</code> . The null integrity algorithm <code>:eia0</code> is deliberately not selectable for an authenticated UE and must not be added here.

If `nas_security` is omitted, the defaults above apply (ciphering off, integrity EIA2).

Implemented ciphers

The MME has implemented only two NAS ciphering algorithms — **EEA0** (null) and **128-EEA2** (AES-CTR, [TS 33.401 §5.1.3.2](#)). 128-EEA1 (SNOW 3G) and 128-EEA3 (ZUC) are **not implemented**.

To protect against a misconfiguration that would select a cipher the MME cannot perform — which would leave the downlink NAS unreadable to the UE and stall the attach — the configured `ciphering` list is filtered to the implemented set before selection. Any `:eea1`/`:eea3` entry is dropped and logged with a warning (`ignoring unimplemented NAS ciphering algorithms`);

if filtering leaves the list empty, the MME falls back to the implemented set. Configured priority order is preserved among the surviving entries.

Enabling EEA2

To turn NAS ciphering on, list `:eea2` ahead of `:eea0`:

```
config :mme,  
  nas_security: %{  
    ciphering: [:eea2, :eea0],  
    integrity: [:eia2, :eia1, :eia3]  
  }
```

How it works: the MME offers 128-EEA2 in the Security Mode Command. A UE advertising EEA2 support in its UE Network Capability gets AES-CTR NAS ciphering; a UE that does not support EEA2 falls back to `:eea0` (null), so the attach still completes.

Use case: deployments that require NAS-layer confidentiality in addition to the always-present AS-layer (PDCP) ciphering — for example to protect NAS signalling across a backhaul segment that is not otherwise encrypted.

NAS ciphering algorithm reference

Value	Algorithm	Implemented	Reference
<code>:eea0</code>	Null (no ciphering)	Yes	TS 33.401 §5.1.3.2
<code>:eea1</code>	128-EEA1 (SNOW 3G)	No — dropped with a warning	TS 33.401 Annex B
<code>:eea2</code>	128-EEA2 (AES-128-CTR)	Yes	TS 33.401 Annex B
<code>:eea3</code>	128-EEA3 (ZUC)	No — dropped with a warning	TS 33.401 Annex B

Extended Idle-mode DRX (eDRX)

```
config :mme,  
    edrx_enabled: true
```

Parameter	Type	Default	Description
<code>edrx_enabled</code>	Boolean	<code>false</code>	When <code>true</code> , the MME grants the UE-requested Extended DRX Parameters in the Attach/TAU Accept and aligns paging to the eDRX window (TS 23.401 §4.3.5.9 / TS 24.301 §9.9.3). When <code>false</code> , eDRX is inert and UEs page on their normal DRX cycle.

Dual Connectivity with NR (EN-DC / NR-NSA)

```
config :mme, :dcnr,  
  enabled: true
```

EN-DC (E-UTRAN New Radio – Dual Connectivity, "NSA") lets a UE use a gNB as a secondary node while the eNB remains the master. NSA is RAN-driven, so the MME's role is to decide whether a UE may use NR as a secondary RAT and signal that decision consistently to the UE (the `RestrictDCNR` flag in the EPS Network Feature Support IE, [TS 24.301 §9.9.3.12A](#)) and to the eNB (the `NRrestrictioninEPSasSecondaryRAT` extension in the S1AP Handover Restriction List, [TS 36.413](#)).

Parameter	Type	Default	Description
<code>enabled</code>	Boolean	<code>true</code>	When <code>true</code> , DCNR is allowed network-wide and gated per-subscriber: a subscriber whose HSS Access-Restriction-Data has the "NR as Secondary RAT Not Allowed" bit set (TS 29.272 §7.3.31) is restricted, everyone else is allowed. When <code>false</code> , DCNR is restricted for every UE regardless of subscription — set this if the network has no NR deployment. Defaults to <code>true</code> , preserving the prior behaviour of advertising DCNR as allowed.

When DCNR is restricted (by config or subscription) the MME both sets `RestrictDCNR` in the Attach/TAU Accept and sends a Handover Restriction List carrying `NRrestrictioninEPSasSecondaryRAT` to the eNB. NR secondary-RAT usage reported by the eNB is forwarded to the SGW/PGW for charging on an eNB-initiated S1 release ([TS 23.401 §5.7A](#)).

Paging Priority

```
config :mme,  
  paging_priority_arp_threshold: 8
```

Parameter	Type	Default	Description
<code>paging_priority_arp_threshold</code>	Integer	<code>nil</code>	ARP priority-level threshold for the S1AP Paging Priority IE (TS 23.401 §4.3.7.4 / TS 36.413). When set to an integer N (1-15), a page for a UE whose most-important active-bearer ARP priority level is $\leq$ N carries the Paging Priority IE (ARP level mapped to <code>priolevel1-priolevel8</code> , 1 = highest), so MPS / priority-service subscribers are paged preferentially. When <code>nil</code> , no Paging Priority IE is sent.

Reject Cause Mapping

Both maps override the built-in default mapping tables; absent keys keep their defaults. They are keyed by the stable symbolic names defined in

`Mme.Control.Emm.CauseMapping` / `Mme.Control.Esm.CauseMapping`. Use them to force a *permanent* reject so an unprovisioned UE stops retrying (issue #26).

```
config :mme,  
  emm_cause_mapping: %{  
    rat_not_allowed: :plmn_not_allowed,  
    default: :no_suitable_cells_in_tracking_area  
  },  
  esm_cause_mapping: %{  
    apn_access_denied_no_subscription:  
:operator_determined_barring,  
    default: :missing_or_unknown_apn  
  }
```

Parameter	Type	Default	Description
<code>emm_cause_mapping</code>	Map	<code>%{}</code>	Diameter-result → EMM-cause override When an S6a Update-Location-Answer fails, the MME rejects the UE's Attach/TAU with an EMM cause derived from the Diameter Result-Code / Experimental-Result-Code. Symbolic keys include <code>:user_unknown</code>, <code>:unknown_eps_subscription</code>, <code>:rat_not_allowed</code>, <code>:roaming_not_allowed</code>, <code>:authorization_rejected</code>, <code>:realm_not_served</code>, <code>:default</code> (full list in <code>Mme.Control.Emm.CauseMapping</code>)
<code>esm_cause_mapping</code>	Map	<code>%{}</code>	GTP-C-failure → ESM-cause override When the SGW/PGW rejects a Create Session Request, the MME rejects PDN connectivity with an ESM cause derived from the failure. Symbolic keys include <code>:no_resources_available</code>, <code>:all_dynamic_addresses_are_occupied</code>, <code>:service_denied</code>, <code>:apn_access_denied_no_subscription</code>, <code>:default</code> (full list in <code>Mme.Control.Esm.CauseMapping</code>).

Equipment Identity Check (S13)

```
config :mme,  
  s13: %{  
    enabled: true,  
    allowed_equipment_status: [:whitelist, :greylist]  
  }
```

Parameter	Type	Required	Default	Description
<code>enabled</code>	Boolean	No	<code>false</code>	When Omni sends Identity Check Request (ECR) EIR via during attack S13, Diamond applic must declare (see Diamond)
<code>allowed_equipment_status</code>	List	No	<code>[:whitelist]</code>	Equipment status value returned the EIR are permitted attack. Accepted value <code>:whitelist</code> , <code>:blacklist</code> , <code>:greylist</code> . Additionally <code>:blacklist</code> would black

Parameter	Type	Required	Default	Description
				device configuration with c Defined in TS 29 §7.3.7

S1AP Interface

```
config :mme,  
  slap: %{  
    listen_ip: "192.0.2.10",  
    listen_port: 36412,  
    secondary_bind_ips: ["192.0.2.11"]  
  }
```

Parameter	Type	Required	Default	Description
<code>listen_ip</code>	String	Yes	-	Primary IP address on which the MME listens for inbound S1AP SCTP associations from eNodeBs. Must be a specific interface IP — do not use <code>0.0.0.0</code> .
<code>listen_port</code>	Integer	No	<code>36412</code>	SCTP port for S1AP connections. Standard port is 36412 per TS 36.412 .
<code>secondary_bind_ips</code>	List	No	<code>[]</code>	Additional local IPv4 addresses bound alongside <code>listen_ip</code> for SCTP multihoming / path redundancy (TS 36.412 / RFC 4960 §5). These addresses are advertised to peers as alternate paths and are also applied to the SBc and SLs SCTP listeners .

Parameter	Type	Required	Default	Description
				Defaults to single-homed.

Served GUMMEI

The Globally Unique MME Identifier list declares which PLMN, MME Group, and MME Code combinations this MME serves. This is advertised to eNodeBs during S1 Setup and used for S-TMSI-based paging and handover.

```
config :mme,  
  served_gummei: [  
    %{  
      plmn_list: [  
        %{mcc: "001", mnc: "01"}  
      ],  
      group_id: 1,  
      code: 2  
    }  
  ]  
]
```

GUMMEI Parameters:

Parameter	Type	Required	Description
<code>plmn_list</code>	List	Yes	One or more PLMNs served under this GUMMEI entry. Each entry uses <code>mcc</code> and <code>mnc</code> keys as described in PLMN Parameters .
<code>group_id</code>	Integer	Yes	MME Group ID (0-65535). Groups MMEs that share UE context for handover within the same pool.
<code>code</code>	Integer	Yes	MME Code (0-255). Uniquely identifies this MME within its group. Together with the group ID and PLMN, forms the GUMMEI. Defined in TS 23.003 §2.8.4 .

The GUMMEI also determines which GUTIs are recognised as **local** versus **foreign**. A UE presenting a foreign GUTI on TAU triggers an S10 Context Request to the previous MME — see [Neighbour MME \(S10\)](#).

Served TAI

The Tracking Area Identity list declares which TAIs this MME accepts UEs from. eNodeBs whose TAIs are not in this list will have those TAIs rejected during S1 Setup.

```
config :mme,
  served_tai: [
    %{
      plmn: %{mcc: "001", mnc: "01"},
      tac_list: [1, 2, 3, 4, 5, 6, 7, 100, 2899, 10000]
    }
  ]
```

TAI Entry Parameters:

Parameter	Type	Required	Description
<code>plmn</code>	Map	Yes	PLMN for this TAI group. Uses <code>mcc</code> and <code>mnc</code> keys.
<code>tac_list</code>	List	Yes	List of Tracking Area Codes (integers, 0-65535) served under this PLMN. Add a TAC to allow UEs camping in that area to attach.

Multiple entries support multi-PLMN deployments or MOCN configurations.

Serving Gateway (SGW)

OmniMME supports two SGW selection methods: static peer list or DNS-based topology lookup. The method may be chosen globally or **per subscriber type** (home vs. roaming).

```

config :mme,
  sgw: %{
    # An atom (applied to both types) or a per-type map, e.g.
    #   %{home: :random_peer, roaming: :dns_lookup}
    selection_method: :random_peer,
    dns: [
      %{
        server: "192.0.2.53",
        domain: "3gppnetwork.org",
        type: :home
      }
    ],
    peers: [
      %{
        ip: "192.0.2.20",
        host: "sgw01.mnc001.mcc001.3gppnetwork.org",
        port: 2123,
        type: :home
      }
    ]
  }
}

```

Top-level SGW Parameters:

Parameter	Type	Required	Default	Description
<code>selection_method</code>	Atom Map	Yes	-	How OmniMME selects an SGW. <code>:random_peer</code> — randomly select from <code>peers</code> ; <code>:dns_lookup</code> — resolve a topology DNS query per TS 29.303 . May instead be a per-type map <code>% {home: ..., roaming: ...}</code> to use, e.g., static peers for home subscribers and DNS for inbound roamers.
<code>dns</code>	List	No	<code>[]</code>	DNS resolver configuration, used when the effective method is <code>:dns_lookup</code> . See DNS Parameters .
<code>peers</code>	List	No	<code>[]</code>	Static SGW peer list, used when the effective method is <code>:random_peer</code> . See SGW/PGW Peer Parameters .

DNS Parameters

Parameter	Type	Required	Description
<code>server</code>	String	Yes	IP address of the DNS server to query for topology-based node selection.
<code>domain</code>	String	Yes	Base domain for EPC DNS queries. OmniMME prepends <code>epc.mncYYY.mccZZZ.</code> when constructing lookup names per TS 23.003 §19.4 .
<code>type</code>	Atom	Yes	Topology type: <code>:home</code> , <code>:roaming</code> , or <code>:home_and_roaming</code> .

EPC DNS is queried over TCP. OmniMME sends all node-selection queries (NAPTR / SRV / A / AAAA) to the configured `server` over **TCP on port 53** — it does not use UDP. EPC S-NAPTR answers routinely exceed the 512-byte UDP limit (an APN-FQDN can return many candidate nodes), and large-UDP/EDNS0 responses are frequently dropped on GRX/IPX paths, so TCP is used exclusively to avoid silent truncation. The configured DNS server **must accept TCP connections on port 53**. Each resolution is bounded by a short overall timeout and retries transient failures a small number of times; if it still fails, node selection falls back per the configured `selection_method`.

A global `dns_ip_version` setting controls which address family is preferred when an S-NAPTR-resolved node returns both A (IPv4) and AAAA (IPv6) records:

```
config :mme,  
  dns_ip_version: :ipv4
```

Parameter	Type	Default	Description
dns_ip_version	Atom	:ipv4	Preferred IP version (:ipv4 :ipv6) for S-NAPTR-resolved nodes. The non-preferred family is still used as a fallback so IPv6-only nodes are never dropped (TS 29.303 Annex C.1).

SGW/PGW Peer Parameters

Parameter	Type	Required	Default	Description
<code>ip</code>	String	Yes	-	IP address of the SGW or PGW interface.
<code>host</code>	String	Yes	-	Hostname in EPC FQDN form <code>sgw01.mnc001.mcc001.3gppn</code>
<code>port</code>	Integer	No	<code>2123</code>	GTPv2-C UDP port. Standard per TS 29.274 .
<code>type</code>	Atom	Yes	-	Subscriber type for which this is used: <code>:home</code> , <code>:roaming</code> , or <code>:home_and_roaming</code> .
<code>priority</code>	Integer	No	<code>1</code>	Priority tier for <code>:random_peer</code> . Peers in the numerically low present are used; higher tier standby, selected only when remains in a lower tier.
<code>weight</code>	Integer	No	<code>100</code>	Relative share of traffic within tier, weighted-random per RFC 8462 . Two peers in the same tier with <code>weight: 100</code> and <code>weight: 50</code> split traffic 2:1. All-zero weights in a tier fall to uniform split.

`priority` and `weight` are optional; omitting them reproduces the previous uniform-random behaviour. They apply only to `:random_peer` selection (DNS-based selection honours the SRV priority/weight in the DNS records instead). Both can also be changed at runtime — without an MME restart — via the REST API (see below); runtime changes are **not persisted** and revert to this configuration on restart.

Runtime peer management (REST API). The `/sgw_peers` and `/pgw_peers` endpoints expose the effective peer pool (including per-peer `type`, `weight` and `priority`) and let an operator adjust it live:

Method / Path	Effect
<code>GET /sgw_peers</code> , <code>GET /pgw_peers</code>	List the effective peers with their selection weighting and (SGW only) recovery/liveness/session state.
<code>GET /sgw_peers/{ip}</code> , <code>GET /pgw_peers/{ip}</code>	A single peer by IP.
<code>POST /sgw_peers</code> , <code>POST /pgw_peers</code>	Add a peer at runtime (<code>ip</code> required; <code>host/port/type/weight/priority</code> optional).
<code>PUT /sgw_peers/{ip}</code> , <code>PUT /pgw_peers/{ip}</code>	Update a peer's <code>weight</code> and/or <code>priority</code> .
<code>DELETE /sgw_peers/{ip}</code> , <code>DELETE /pgw_peers/{ip}</code>	Remove a peer from the pool.

All write operations are **non-persistent**: they mutate the running node only and are lost on restart, when the peer pool is re-seeded from this configuration.

Packet Data Network Gateway (PGW)

PGW selection uses the same structure as SGW. Configure under `pgw:` with identical parameters, including the per-type `selection_method` map.

```
config :mme,  
  pgw: %{  
    selection_method: :random_peer,  
    dns: [ ... ],  
    peers: [  
      %{  
        ip: "192.0.2.21",  
        host: "pgw01.mnc001.mcc001.3gppnetwork.org",  
        port: 2123,  
        type: :home_and_roaming  
      }  
    ]  
  }  
}
```

See [SGW/PGW Peer Parameters](#) for field descriptions. `type:`
`:home_and_roaming` is common for PGWs that handle both home and roaming PDN sessions.

Neighbour MME (S10)

The S10 interface (GTPv2-C between MMEs) carries inter-MME mobility: idle-mode context transfer for foreign-GUTI TAU and connected-mode Forward Relocation handover. `mme_s10` configures how a target MME is discovered.

```
config :mme,  
  mme_s10: %{  
    # :dns_lookup resolves the target TAI via S-NAPTR (x-3gpp-  
mme:x-s10);  
    # :random_peer uses the static peers list below.  
    selection_method: :dns_lookup,  
    dns: [  
      %{  
        server: "192.0.2.53",  
        domain: "3gppnetwork.org"  
      }  
    ],  
    peers: [  
      %{  
        ip: "192.0.2.30",  
        host:  
"mme01.mmegi8001.mme.epc.mnc001.mcc001.3gppnetwork.org",  
        port: 2123  
      }  
    ],  
    # Negative-cache window for a foreign GUTI that resolves to no  
reachable peer.  
    unresolvable_guti_backoff_seconds: 30,  
    # How long to wait for a Forward Relocation Response when  
preparing a handover.  
    handover_request_timeout_ms: 1500  
  }
```

Parameter	Type	Required	Description
<code>selection_method</code>	Atom	Yes	<code>:dns_lookup</code> the target TAI neighbour MM NAPTR (<code>x-3gpp</code> <code>mme:x-s10</code> , TS \$5.4); <code>:random</code> uses the static list.
<code>dns</code>	List	No	DNS resolver(when <code>selection_method</code> <code>:dns_lookup</code> . <code>server</code> and <code>c</code> as in DNS Par
<code>peers</code>	List	No	Static neighbour list, used when <code>selection_method</code> <code>:random_peer</code> fallback). Each <code>ip</code> , <code>host</code> (MM FQDN), <code>port</code> GTP-C port, type 2123).
<code>unresolvable_guti_backoff_seconds</code>	Integer	No (default <code>30</code>)	How long a for GUTI that resolvable no reachable neighbour MM source SGSN is negatively cached. While cached, that keeps re- a Tracking Area

Parameter	Type	Required	Description
			Update with the unresolvable declined immediate (TAU Reject) value re-running procedure discovery, prevent a retrying UE triggering connection request signal every attempt
handover_request_timeout_ms	Integer	No (default 1500)	How long to wait for Forward Relocation Response when preparing an outbound S1-MME handover. Deliberately set longer than the generic GTPv2-C T3 timer: timer source eNB at Handover Preparation when its <code>tS1-MME-relocprep</code> expires (2 s in typical RAN, TS 36.413 §8.4.1 relocation that is going to fail not inside that window the MME's Handover Preparation Failure reach the eNB. This is the whole budget — the message is sent once, i

Parameter	Type	Required	Description
			retransmitted because the target MME builds a context and a SGW session copy it receives it must also leave room for a <i>subsequent</i> relocation, where the target only arrives after its own Context Session and the eNB's HandoverRequest. Raise it if the <code>tS1relocprep</code> is longer than 2 seconds; otherwise, it is shorter. Applies to the handover path for the idle-mode Request and session management the longer T3

Target-MME selection never returns this MME's own S10 address, over either method: a Forward Relocation Request to self can never complete, and a Tracking Area served by an MME pool otherwise resolves to a candidate list that includes this node. Identifying "self" relies on the GTPv2-C `listen_ip` being this node's real address rather than a wildcard bind — which inter-MME handover requires in any case, since the same value is sent as the source MME F-TEID.

The S10 service shares the GTPv2-C listener configured under **GTPv2-C (S11)**. For EPS↔5GS interworking, target-AMF discovery over N26 uses `x-3gpp-amf:x-n26` and the same DNS resolvers.

GTP-C Path Supervision

Active GTP-C path management ([TS 29.274 §7.2.1](#)): the MME periodically Echoes each SGW it has S11 sessions with and, after enough consecutive misses, declares the path down and releases the stale sessions anchored there.

```
config :mme,  
  gtpc_path_supervision: %{  
    enabled: true,  
    interval_ms: 60_000,  
    failure_threshold: 3  
  }
```

Parameter	Type	Default	Description
<code>enabled</code>	Boolean	<code>false</code>	When <code>true</code> , the MME actively Echoes peers and releases sessions on path failure. Opt-in: a too-aggressive interval/threshold could drop live sessions on a transient blip. The MME always <i>answers</i> inbound Echo Requests regardless of this setting.
<code>interval_ms</code>	Integer	<code>60000</code>	Interval between Echo Requests to each peer, in milliseconds.
<code>failure_threshold</code>	Integer	<code>3</code>	Consecutive missed Echo responses before the path is declared down.

Diameter (S6a / S13 / SLg)

OmniMME connects to the HSS (S6a), EIR (S13) and GMLC (SLg, for Location Services) via Diameter, typically through a Diameter Routing Agent (DRA).

```
config :diameter_ex,  
  diameter: %{  
    service_name: :omnitouch_mme,  
    listen_ip: "192.0.2.10",  
    listen_port: 3868,  
    host: "mme01.epc.mnc001.mcc001.3gppnetwork.org",  
    realm: "epc.mnc001.mcc001.3gppnetwork.org",  
    product_name: "OmniMME",  
    request_timeout: 5000,  
    peer_selection_algorithm: :random,  
    allow_undefined_peers_to_connect: true,  
    log_unauthorized_peer_connection_attempts: true,  
    control_module: Mme.Control.Diameter,  
    processor_module: DiameterEx.Processor,  
    auth_application_ids: [],  
    acct_application_ids: [],  
    vendor_id: 10415,  
    supported_vendor_ids: [5535, 10415],  
    applications: [ ... ],  
    peers: [ ... ]  
  }
```

Diameter Core Parameters:

Parameter	Type	Required	Default
service_name	Atom	Yes	-
listen_ip	String	Yes	-
listen_port	Integer	No	386
host	String	Yes	-
realm	String	Yes	-
product_name	String	No	-
request_timeout	Integer	No	500

Parameter	Type	Required	Default
peer_selection_algorithm	Atom	No	random
allow_undefined_peers_to_connect	Boolean	No	false
log_unauthorized_peer_connection_attempts	Boolean	No	true
control_module	Module	Yes	-
processor_module	Module	Yes	-
auth_application_ids	List	No	[]
acct_application_ids	List	No	[]

Parameter	Type	Required	Default
<code>vendor_id</code>	Integer	Yes	-
<code>supported_vendor_ids</code>	List	No	<code>[]</code>
<code>applications</code>	List	Yes	-
<code>peers</code>	List	No	<code>[]</code>

Application Parameters

Parameter	Type	Required	Description
<code>application_name</code>	Atom	Yes	Internal name for application (e.g. <code>:s13</code> , <code>:slg</code>).
<code>application_dictionary</code>	Atom	Yes	Erlang Diameter core module (e.g. <code>:diameter_gen_30</code>).
<code>vendor_specific_application_ids</code>	List	Yes	Vendor-specific application declarations. Each <code>vendor_id</code> , <code>auth_application</code> , <code>acct_application</code>

Supported Diameter Applications:

Application Name	Auth App ID	Interface	Reference
:s6a	16777251	S6a — MME ↔ HSS authentication and subscription	TS 29.272
:s13	16777252	S13 — MME ↔ EIR equipment identity check	TS 29.272
:slg	16777255	SLg — MME ↔ GMLC Location Services (PLR/LRR)	TS 29.172
:t6a	16777346	T6a — MME ↔ SCEF CIoT Non-IP Data Delivery (dictionary :diameter_gen_3gpp_t6a)	TS 29.128

Declare only the applications you use. :slg is required for the Location Services feature; :s13 is required when S13 equipment check is enabled; :t6a is required for NIDD / Control-Plane CIoT.

Diameter Peer Parameters

Parameter	Type	Required	Default	Description
host	String	Yes	-	Diameter Identity of peer (Original Host). Must match the configured identity for validation.
realm	String	Yes	-	Diameter realm of the peer.
ip	String	Yes	-	IP address to connect to or accept from.
port	Integer	No	3868	Diameter port of the peer.
tls	Boolean	No	false	Enable TLS for this peer connection.
transport	Atom	No	:diameter_tcp	:diameter_tls or :diameter_sctp. SCTP is preferred for Diameter over RFC 6733 .
initiate_connection	Boolean	No	false	When true, OmniMME initiates the connection.

Parameter	Type	Required	Default	Description
				connection this peer; <code>false</code> , it v for the pe connect inbound. Typically t for DRA pe

GTPv2-C (S11)

The S11 interface connects OmniMME to the Serving Gateway for session and bearer lifecycle management. This same GTPv2-C service also carries the **S10** inter-MME interface.

```
config :gtpc,  
  service: %{\br/>    name: :s11,  
    listen_ip: "192.0.2.10",  
    listen_port: 2123,  
    control_module: Mme.Control.Gtpc,  
    t3: 5000,  
    n3: 3  
  }
```

Parameter	Type	Required	Default	Description
<code>name</code>	Atom	Yes	-	Interface name identifier. Must be <code>:s11</code> .
<code>listen_ip</code>	String	Yes	-	IP address to bind for GTPv2-C. Must be a specific interface IP — not <code>0.0.0.0</code> . The SGW and neighbour MMEs send responses here.
<code>listen_port</code>	Integer	No	<code>2123</code>	UDP port for GTPv2-C. Standard port is 2123 per TS 29.274 .
<code>control_module</code>	Module	Yes	-	Module that handles decoded GTP-C messages. For OmniMME this is <code>Mme.Control.Gtpc</code> .
<code>t3</code>	Integer	No	<code>5000</code>	T3-RESPONSE timer in milliseconds. Time to wait for a GTPv2 response before retransmitting.
<code>n3</code>	Integer	No	<code>3</code>	N3 retransmission count before a transaction is considered failed.

Cell Broadcast (SBc)

The SBc interface (SBc-AP over SCTP) connects OmniMME to a Cell Broadcast Centre (CBC) for Public Warning System messages — ETWS and CMAS / Write-Replace Warning (TS 29.168). When enabled, the MME accepts Write-Replace Warning / Stop Warning from the CBC and forwards them to the eNBs serving the targeted warning area.

```
config :mme, :sbc,  
    enabled: true,  
    port: 29168,  
    indication_timeout: 10_000
```

Parameter	Type	Default	Description
<code>enabled</code>	Boolean	<code>false</code>	When <code>true</code> , OmniMME opens the SBc-AP SCTP listener and processes warning messages.
<code>port</code>	Integer	<code>29168</code>	SCTP port for the SBc-AP listener.
<code>indication_timeout</code>	Integer	<code>10000</code>	Milliseconds to wait for eNB confirmations before sending the Write-Replace Warning Indication back to the CBC.

The SBc listener binds the primary `slap.listen_ip` and any `secondary_bind_ips`.

Location Services (E-SMLC / SLs)

The SLs interface (LCS-AP over SCTP) connects OmniMME to an E-SMLC for control-plane positioning (TS 29.171), used together with the SLg Diameter

application to answer GMLC location requests. When enabled, the MME relays LPPa/LPP positioning between the E-SMLC, eNBs and UEs, and exposes the [Location Services Control Panel page](#).

```
config :mme, :esmlc,  
  enabled: true,  
  sls_port: 9082
```

Parameter	Type	Default	Description
<code>enabled</code>	Boolean	<code>false</code>	When <code>true</code> , OmniMME opens the SLs (LCS-AP) SCTP listener and processes positioning requests. Requires the <code>:slg</code> Diameter application to be declared for GMLC-initiated requests.
<code>sls_port</code>	Integer	<code>9082</code>	SCTP port for the SLs (LCS-AP) listener.

The SLs listener binds the primary `slap.listen_ip` and any [secondary_bind_ips](#).

NIDD / Control-Plane CloT (T6a)

Non-IP Data Delivery (NIDD) lets Cellular-IoT / NB-IoT devices exchange small Non-IP data over the Control-Plane CloT EPS optimisation, relayed to an SCEF over the T6a Diameter interface ([TS 29.128](#) / [TS 23.682](#)). The same optimisation also carries NB-IoT **IP** data with the MME terminating the user plane on S11-U. See the [NIDD & T6a Interface](#) guide for the full feature description. Disabled by default — with no `:nidd` configuration the MME does not advertise Control-Plane CloT support and behaves exactly as a non-CIoT MME.

```
config :mme, :nidd,  
  enabled: true,  
  s11u_ip: "10.7.25.185"
```

Parameter	Type	Default	Description
<code>enabled</code>	Boolean	<code>false</code>	When <code>true</code> , OmniMME advertises Control-Plane CloT support in EPS Network Feature Support and serves Non-IP PDN connections (and NB-IoT IP-over-S11-U) for CloT devices.
<code>s11u_ip</code>	String	S11 GTP-C <code>listen_ip</code>	IP address for the MME's S11-U GTP-U endpoint (UDP 2152) used for NB-IoT IP data. Defaults to the GTPv2-C (S11) <code>listen_ip</code> .

Enabling NIDD also requires:

- The `:t6a` Diameter application declared in the `applications` list, and the SCEF reachable as a Diameter **peer** (directly or via the DRA). See [Supported Diameter Applications](#).
- The Non-IP APN provisioned in the **HSS** subscription: an APN-Configuration with `PDN-Type = Non-IP (4)` and an `SCEF-ID`.

Control Panel

The Control Panel is a real-time web UI for operators to inspect and manage UEs, eNodeBs, Diameter peers, location services and inter-MME handover.

```
config :control_panel,  
  page_order: ["/ues", "/enodebs", "/diameter", "/application",  
  "/configuration"]  
  
config :control_panel, ControlPanelWeb.Endpoint,  
  url: [host: "0.0.0.0", path: "/"],  
  https: [  
    port: 10443,  
    keyfile: "priv/cert/omnitouch.pem",  
    certfile: "priv/cert/omnitouch.crt"  
  ]
```

General Parameters:

Parameter	Type	Required	Description
<code>page_order</code>	List	No	Ordered list of sidebar navigation entries. Determines the left-nav order in the Control Panel.

Endpoint Parameters:

Parameter	Type	Required	Default	Description
<code>url.host</code>	String	No	<code>"0.0.0.0"</code>	Bind address for the HTTPS listener.
<code>url.path</code>	String	No	<code>"/"</code>	URL path prefix for the Control Panel.
<code>https.port</code>	Integer	Yes	-	HTTPS port for the Control Panel.
<code>https.keyfile</code>	String	Yes	-	Path to the TLS private key file (PEM format).
<code>https.certfile</code>	String	Yes	-	Path to the TLS certificate file (PEM format).

REST API

The REST API provides programmatic access to UE, eNodeB, Diameter, SGW-peer and S10 context, plus UE/eNB/GUTI/offload actions. Interactive OpenAPI documentation is available at `/api/swagger`. See the [Operations Guide](#) for the endpoint catalogue.

```
config :api_ex,  
  api: %{  
    port: 8443,  
    listen_ip: "0.0.0.0",  
    product_name: "OmniMME",  
    title: "API - OmniMME",  
    hostname: "localhost",  
    enable_tls: true,  
    tls_cert_path: "priv/cert/omnitouch.crt",  
    tls_key_path: "priv/cert/omnitouch.pem"  
  }
```

Parameter	Type	Required	Default	Description
<code>port</code>	Integer	Yes	-	HTTPS port for the REST API.
<code>listen_ip</code>	String	No	<code>"0.0.0.0"</code>	IP address to bind the API listener.
<code>product_name</code>	String	No	-	Product name string in OpenAPI metadata.
<code>title</code>	String	No	-	Title shown in the OpenAPI / Swagger UI.
<code>hostname</code>	String	Yes	-	Hostname used to construct API base URLs in the OpenAPI specification.
<code>enable_tls</code>	Boolean	No	<code>true</code>	Enable HTTPS for the API. When <code>false</code> , the API serves plain HTTP (not recommended in production).
<code>tls_cert_path</code>	String	When TLS	-	Path to the TLS certificate file (PEM format).
<code>tls_key_path</code>	String	When TLS	-	Path to the TLS private key file (PEM format).

Logging

OmniMME emits structured JSON logs via `OmniLogger`. Configure the default formatter (and, optionally, a rotating file handler) under `:logger`.

```
config :logger, :default_formatter,  
  format: {OmniLogger.JsonFormatter, :format},  
  metadata: :all
```

Parameter	Type	Description
<code>format</code>	Tuple	Formatter MFA. Use <code>{OmniLogger.JsonFormatter, :format}</code> for structured JSON logs (one object per line).
<code>metadata</code>	Atom List	Which metadata keys to include; <code>:all</code> emits every key.

A rotating file handler can be added with `config :logger, :default_handler, ... (file, max_no_bytes, max_no_files, compress_on_rotate)`. In production, log destination is managed under `/etc/omnimme/`.

Complete Configuration Example

The following is a complete, annotated `runtime.exs` suitable as a starting point. Replace all placeholder values with your network's actual addressing and identifiers.

```

import Config

config :mme,
  # Node identity
  mme_name: "omnimme",
  operator_name: "MyNet",
  country: "Australia",
  network_name_short: "MyNet",
  network_name_long: "My Network",
  timezone: "Australia/Sydney",
  default_apn: "internet",
  apn_oi_domain: :gprs,  # APN-OI suffix form (:gprs / :epc /
: none)

  # Capacity and identity
  mme_capacity: 128,
  home_plmn: %{mcc: "505", mnc: "01"},
  emergency_support_enabled: false,

  # NAS timers
  t3412: 3240,  # periodic TAU interval, seconds (54 min)
  t3485: 8,     # bearer-context retransmission, seconds
  t3346: 600,   # EMM congestion back-off, seconds
  t3396: 600,   # ESM congestion back-off, seconds

  # NAS security policy (strongest first). Ciphering is off (EEA0)
  by default;
  # only EEA0 and EEA2 are implemented. List [:eea2, :eea0] to
  enable EEA2.
  nas_security: %{
    ciphering: [:eea0],
    integrity: [:eia2, :eia1, :eia3]
  },

  # Extended idle-mode DRX
  edrx_enabled: false,

  # Paging Priority for MPS subscribers (omit to disable)
  # paging_priority_arp_threshold: 8,

  # Reject-cause overrides (issue #26)
  emm_cause_mapping: %{},
  esm_cause_mapping: %{}

```

```

# Equipment identity check
s13: %{
    enabled: true,
    allowed_equipment_status: [:whitelist, :greylist]
},

# SLAP listener (optionally multi-homed)
slap: %{
    listen_ip: "192.0.2.10",
    listen_port: 36412
    # secondary_bind_ips: ["192.0.2.11"]
},

# GUMMEI – adjust group_id and code to match your MME pool plan
served_gummei: [
    %{
        plmn_list: [%{mcc: "505", mnc: "01"}],
        group_id: 1,
        code: 1
    }
],

# Tracking areas this MME serves
served_tai: [
    %{
        plmn: %{mcc: "505", mnc: "01"},
        tac_list: [1, 2, 3]
    }
],

# Gateway selection
dns_ip_version: :ipv4,
sgw: %{
    selection_method: :random_peer,
    peers: [
        %{ip: "192.0.2.20", host:
"sgw01.mnc001.mcc505.3gppnetwork.org", port: 2123, type: :home}
    ]
},
pgw: %{
    selection_method: :random_peer,
    peers: [
        %{ip: "192.0.2.30", host:

```

```

"pgw01.mnc001.mcc505.3gppnetwork.org", port: 2123, type:
:home_and_roaming}
    ],
},

    # Neighbour MME (S10) discovery for inter-MME handover /
foreign-GUTI TAU
    mme_s10: %{
        selection_method: :dns_lookup,
        dns: [%{server: "192.0.2.53", domain: "3gppnetwork.org"}],
        peers: [
            %{ip: "192.0.2.50", host:
"mmec01.mmegi8001.mme.epc.mnc001.mcc505.3gppnetwork.org", port:
2123}
        ]
    },

    # Active GTP-C path supervision (opt-in)
    gtpc_path_supervision: %{enabled: false, interval_ms: 60_000,
failure_threshold: 3}

# Public Warning System (ETWS / CMAS) over SBc
config :mme, :sbc,
    enabled: true,
    port: 29168

# Control-plane positioning (LCS) over SLs to the E-SMLC
config :mme, :esmlc,
    enabled: false,
    sls_port: 9082

config :diameter_ex,
    diameter: %{
        service_name: :omnitouch_mme,
        listen_ip: "192.0.2.10",
        listen_port: 3868,
        host: "mme01.epc.mnc001.mcc505.3gppnetwork.org",
        realm: "epc.mnc001.mcc505.3gppnetwork.org",
        product_name: "OmniMME",
        request_timeout: 5000,
        peer_selection_algorithm: :random,
        allow_undefined_peers_to_connect: true,
        log_unauthorized_peer_connection_attempts: true,
        control_module: Mme.Control.Diameter,

```

```
processor_module: DiameterEx.Processor,
auth_application_ids: [],
acct_application_ids: [],
vendor_id: 10415,
supported_vendor_ids: [5535, 10415],
applications: [
  %{
    application_name: :s6a,
    application_dictionary: :diameter_gen_3gpp_s6a,
    vendor_specific_application_ids: [
      %{vendor_id: 10415, auth_application_id: 16_777_251,
acct_application_id: nil}
    ]
  },
  %{
    application_name: :s13,
    application_dictionary: :diameter_gen_3gpp_s13,
    vendor_specific_application_ids: [
      %{vendor_id: 10415, auth_application_id: 16_777_252,
acct_application_id: nil}
    ]
  },
  %{
    application_name: :slg,
    application_dictionary: :diameter_gen_3gpp_slg,
    vendor_specific_application_ids: [
      %{vendor_id: 10415, auth_application_id: 16_777_255,
acct_application_id: nil}
    ]
  }
],
peers: [
  %{
    host: "dra01.epc.mnc001.mcc505.3gppnetwork.org",
    realm: "epc.mnc001.mcc505.3gppnetwork.org",
    ip: "192.0.2.40",
    port: 3868,
    tls: false,
    transport: :diameter_sctp,
    initiate_connection: true
  }
]
}
```

```
config :gtpc,
  service: %{
    name: :s11,
    listen_ip: "192.0.2.10",
    listen_port: 2123,
    control_module: Mme.Control.Gtpc,
    t3: 5000,
    n3: 3
  }

config :control_panel,
  page_order: ["/ues", "/enodebs", "/diameter", "/application",
"/configuration"]

config :control_panel, ControlPanelWeb.Endpoint,
  url: [host: "0.0.0.0", path: "/"],
  https: [
    port: 10443,
    keyfile: "/etc/omnimme/certs/server.pem",
    certfile: "/etc/omnimme/certs/server.crt"
  ]

config :api_ex,
  api: %{
    port: 8443,
    listen_ip: "0.0.0.0",
    product_name: "OmniMME",
    title: "API - OmniMME",
    hostname: "mme01.example.com",
    enable_tls: true,
    tls_cert_path: "/etc/omnimme/certs/server.crt",
    tls_key_path: "/etc/omnimme/certs/server.pem"
  }

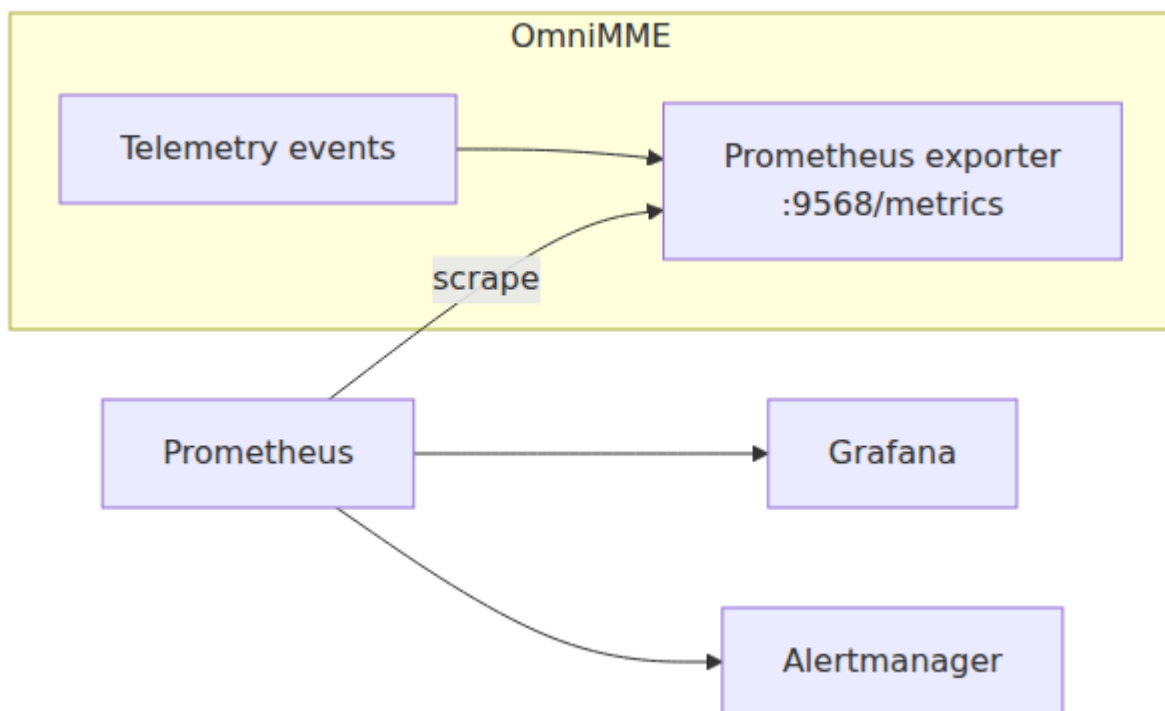
config :logger, :default_formatter,
  format: {OmniLogger.JsonFormatter, :format},
  metadata: :all
```

OmniMME Metrics Reference

OmniMME exposes Prometheus metrics for MME control-plane activity and BEAM VM health.

Scraping

Property	Value
Endpoint	<code>http://<mme-host>:9568/metrics</code>
Exporter	<code>TelemetryMetricsPrometheus</code> (started in <code>Mme.Web.Supervisor</code>)
Format	Prometheus text exposition



Naming: metrics are defined internally with dot-separated names (e.g. `mme.attach.count`); the Prometheus exporter renders these with underscores

(e.g. `mme_attach_count`). This document uses the Prometheus (underscore) names throughout.

Label defaults: every counter/distribution label defaults to `none` at any emit site that does not set it. So a metric like `mme_attach_count` always carries its full label set; a dimension that wasn't applicable to a particular event shows `none` rather than being absent.

MME Gauges

Point-in-time values, recomputed periodically from live MME state.

Metric	Labels	Description
<code>mme_ue_count</code>	—	Total UE contexts with a valid IMSI (connected + idle + retained).
<code>mme_ue_connected_count</code>	—	UE contexts in ECM-CONNECTED.
<code>mme_ue_idle_count</code>	—	UE contexts in ECM-IDLE (reachable via paging).
<code>mme_bearer_count</code>	<code>bearer_type</code>	Active EPS bearers, by <code>default</code> / <code>dedicated</code> .
<code>mme_session_count</code>	<code>apn</code>	Active PDN sessions, by APN.
<code>mme_session_emergency_count</code>	—	Active emergency PDN sessions.
<code>mme_session_unauthenticated_count</code>	—	Limited-service (no IMSI) UE contexts that hold a PDN session.

Metric	Labels	Description
<code>mme_esm_procedure_pending_count</code>	<code>procedure_type</code>	In-flight ESM procedures, by type (leak detector).
<code>mme_timer_active_count</code>	—	MME timers scheduled but not yet fired (leak detector).
<code>mme_sgw_session_count</code>	<code>sgw</code>	Sessions currently homed on each S-GW (live load distribution).
<code>mme_pgw_session_count</code>	<code>pgw</code>	Sessions currently homed on each P-GW (live load distribution).
<code>mme_enb_connected_count</code>	—	eNBs with a connected S1 association.
<code>mme_sctp_association_count</code>	<code>state</code>	SCTP associations grouped by eNB S1 status.
<code>mme_slap_enb_status</code>	<code>ip</code> , <code>enb_id</code>	Per-eNB S1 status: <code>1</code> connected, <code>0</code> disconnected.

Example queries:

```
# Connected / total ratio  
mme_ue_connected_count / mme_ue_count
```

```
# Any disconnected eNB  
mme_slap_enb_status == 0
```

```
# Possible ESM-procedure leak: pending procedures climbing  
rate(mme_esm_procedure_pending_count[15m]) > 0
```

EMM Procedure Counters

Metric	Labels	Description
mme_attach_count	result, via, cause	EPS attach outcomes. result = attempt/success/rejected; via : identity type; cause on reject.
mme_tau_count	result, via, type, cause	Tracking Area Update outcomes by result, identity type and TAU type (periodic/mobility/combined).
mme_service_request_count	result, cause	Service Request / Extended Service Request outcomes.
mme_detach_count	initiator, type, cause	Detach events, by initiator (ue/mme/hss/sgw_pgw) and type.
mme_auth_count	result, cause	Authentication outcomes; cause = mac_failure/synch_failure/timeout on failure.
mme_security_mode_count	result, cause	NAS Security Mode Command outcomes (complete/reject).
mme_identity_count	result	Identity procedure outcomes.

```
# Attach success rate over 5m
sum(rate(mme_attach_count{result="success"}[5m]))
  / sum(rate(mme_attach_count{result="attempt"}[5m]))

# Authentication failures by cause
sum by (cause) (rate(mme_auth_count{result="failure"}[5m]))
```

ESM Procedure Counters

Metric	Labels	Description
<code>mme_pdn_connectivity_count</code>	<code>result</code> , <code>apn</code> , <code>cause</code>	PDN Connectivity outcomes; <code>cause</code> captures PDN-type override/reject.
<code>mme_pdn_disconnect_count</code>	<code>initiator</code> , <code>apn</code>	PDN disconnect events, by initiator and APN.
<code>mme_bearer_activation_count</code>	<code>bearer_type</code> , <code>initiator</code> , <code>result</code> , <code>cause</code>	EPS bearer activations.
<code>mme_bearer_deactivation_count</code>	<code>bearer_type</code> , <code>initiator</code> , <code>result</code> , <code>cause</code>	EPS bearer deactivations.
<code>mme_bearer_modification_count</code>	<code>result</code> , <code>cause</code>	Bearer modification (Update Bearer / Modify EPS Bearer Context) outcomes.
<code>mme_esm_procedure_timeout_count</code>	<code>procedure_type</code>	ESM T3485 timeouts, by procedure type.

Node Selection Counters

Metric	Labels	Description
<code>mme_sgw_selection_count</code>	<code>sgw</code> , <code>result</code>	S-GW selections per session, by chosen S-GW and result.
<code>mme_pgw_selection_count</code>	<code>pgw</code> , <code>apn</code> , <code>result</code>	P-GW selections per session, by chosen P-GW, APN and result.
<code>mme_mme_peer_selection_count</code>	<code>result</code>	Target-MME (S10) discovery results (<code>x-3gpp-mme:x-s10</code>).
<code>mme_amf_selection_count</code>	<code>result</code>	Target-AMF (N26) discovery results (<code>x-3gpp-amf:x-n26</code>).

DNS Metrics

S-NAPTR / DNS resolution used for SGW/PGW/MME/AMF selection ([TS 29.303](#)).

Metric	Type	Labels	
mme_dns_query_count	Counter	query_type, result, purpose	
mme_dns_query_duration_milliseconds	Histogram	query_type, result, purpose	
mme_dns_answer_records	Histogram	query_type, purpose	
mme_dns_resolution_count	Counter	purpose, result	
mme_dns_resolution_duration_milliseconds	Histogram	purpose	

GTP-C (S11) Metrics

Metric	Type	Labels	
mme_gtpc_message_count	Counter	direction, message_type	(c
mme_gtpc_request_duration_milliseconds	Histogram	message_type	F t r
mme_gtpc_timeout_count	Counter	message_type	(t r
mme_gtpc_handler_crash_count	Counter	message_type	l c r
mme_gtpc_echo_count	Counter	direction	E k l
mme_gtpc_modify_bearer_response_count	Counter	result, procedure, cause	M c a (1 t (
mme_gtpc_peer_restart_count	Counter	—	s c c (

Metric	Type	Labels	
mme_gtpc_path_failure_count	Counter	—	S C s §

Diameter S6a Metrics

Metric	Type	Labels	
mme_s6a_request_count	Counter	command, result_code	MM rec (Al cor Dia coc
mme_s6a_request_duration_milliseconds	Histogram	command	S6a trip HS
mme_s6a_server_initiated_count	Counter	command, result	HS me (Cl by res

```
# S6a (HSS) latency p95 over 5m
histogram_quantile(0.95,
  sum by (le, command)
    (rate(mme_s6a_request_duration_milliseconds_bucket[5m])))
```

S1AP Metrics

Metric	Labels	Description
mme_slap_message_count	direction, message_type, enb_id	S1AP messages by direction, type and enb
mme_slap_degraded_ie_count	message_type, ie, criticality, reason, enb_id	S1AP IEs the codec could not shape. reason=unknown_ie is an IE this MME does not know (TS 36.413 §10.3.2); reason=shaping_failure is a codec limitation leaving a raw ASN.1 value.
mme_slap_encode_failure_count	message_type, enb_id	S1AP encode failures.
mme_slap_error_indication_count	cause, enb_id	S1AP Error Indications from eNBs.
mme_slap_setup_count	result, enb_id	S1 Setup outcomes (eNB onboarding).
mme_slap_reset_count	direction, enb_id	S1AP Reset / Reset Acknowledge.
mme_erab_setup_count	result, cause, enb_id	E-RAB setup outcome

Metric	Labels	Description
<code>mme_erab_release_count</code>	<code>result</code> , <code>cause</code> , <code>enb_id</code>	E-RAB release outcomes.
<code>mme_initial_context_setup_count</code>	<code>result</code> , <code>enb_id</code>	Initial Context Setup outcomes.

Mobility & Paging Metrics

Metric	Labels	Description
<code>mme_paging_count</code>	<code>result</code> , <code>stage</code>	Paging events; <code>result</code> = attempt/success, <code>stage</code> = paging procedure stage (S-TMSI / IMSI).
<code>mme_handover_count</code>	<code>kind</code> , <code>direction</code> , <code>result</code>	Handovers by <code>kind</code> (x2/s1/s10/n26/offload), direction and result.

Inter-MME / inter-system discovery counters are listed under [Node Selection](#) (`mme_mme_peer_selection_count`, `mme_amf_selection_count`).

Histogram Buckets

All `*_duration_milliseconds` histograms share these latency buckets (ms):

1, 5, 10, 25, 50, 100, 250, 500, 1000, 2500, 5000, 10000

`mme_dns_answer_records` uses count buckets `0, 1, 2, 3, 5, 8, 13, 21, 50`.

BEAM VM Metrics

OmniMME exports BEAM runtime metrics for capacity planning and diagnosing memory or process leaks. All memory metrics are in bytes.

Metric	Description
<code>beam_memory_total</code>	Total memory allocated by the BEAM VM (all categories).
<code>beam_memory_processes</code>	Memory allocated to Erlang processes (heap, stack, mailboxes).
<code>beam_memory_processes_used</code>	Memory actively used within process heaps.
<code>beam_memory_system</code>	Memory used by the BEAM system (code, ETS, atoms, etc.).
<code>beam_memory_atom</code>	Memory allocated for the atom table (used + reserved).
<code>beam_memory_atom_used</code>	Memory actively used by atoms.
<code>beam_memory_binary</code>	Off-heap (reference-counted) binary memory. A sustained climb may indicate a binary leak.
<code>beam_memory_code</code>	Memory used by loaded BEAM module code. Generally stable after startup.
<code>beam_memory_ets</code>	Memory used by ETS tables. OmniMME stores UE/eNB contexts in ETS, so this grows with subscriber count.
<code>beam_processes_count</code>	Number of running Erlang processes. A sustained climb may indicate a process leak.
<code>beam_ports_count</code>	Number of open Erlang ports (sockets, file descriptors). Roughly tracks active SCTP/TCP connections.

Metric	Description
<code>beam_atom_count</code>	Total atoms in the atom table. Atoms are never GC'd — a growing count indicates dynamic atom creation (a leak).
<code>beam_vm_uptime</code>	Seconds since the BEAM VM started.

```
# ETS memory as a percentage of total  
beam_memory_ets / beam_memory_total * 100
```

```
# Unexpected restart (uptime resets near zero)  
beam_vm_uptime < 300
```

Recommended Alerts

Alert	Expression	Severity
eNB offline	<code>mme_slap_enb_status == 0</code>	Warning
Zero connected UEs during business hours	<code>mme_ue_connected_count == 0</code>	Critical
Attach success rate degraded	<code>sum(rate(mme_attach_count{result="success"}[5m])) / sum(rate(mme_attach_count{result="attempt"}[5m])) < 0.9</code>	Warning
HSS (S6a) errors rising	<code>sum(rate(mme_s6a_request_count{result_code!~"2.*"}[5m])) > 0</code>	Warning
GTP-C path failure	<code>increase(mme_gtpc_path_failure_count[5m]) > 0</code>	Warning
GTP-C handler crashes	<code>increase(mme_gtpc_handler_crash_count[5m]) > 0</code>	Warning
ESM procedure leak	<code>mme_esm_procedure_pending_count > 100</code>	Warning
High memory	<code>beam_memory_total > 3221225472</code>	Warning

Alert	Expression	Severity
usage		
Process count spike	<code>beam_processes_count > 50000</code>	Warning
BEAM restart detected	<code>beam_vm_uptime < 120</code>	Critical
Atom table growth	<code>deriv(beam_atom_count[10m]) > 100</code>	Warning

NIDD & the T6a/T6b Interface — Non-IP Data Delivery for CIoT

Non-IP Data Delivery (NIDD) lets a Cellular-IoT (CIoT / NB-IoT) device exchange small **Non-IP** data with an application server **without ever being allocated an IP address**. The data rides the NAS signalling plane (the **Control-Plane CIoT EPS optimisation**) between the UE and the MME, and the MME relays it to a **Service Capability Exposure Function (SCEF)** over the **T6a** Diameter interface.

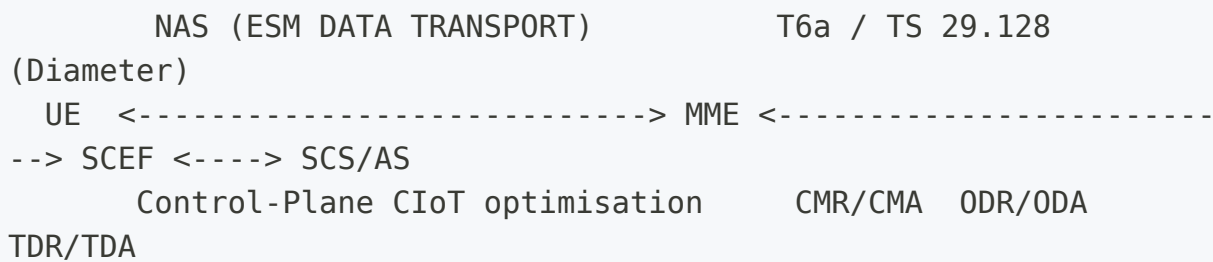
The interface is defined in [3GPP TS 29.128](#) (T6a/T6b Diameter application, application-id **16777346**) and the procedures in [3GPP TS 23.682](#) §5.13. The NAS data transport uses the ESM DATA TRANSPORT message of [3GPP TS 24.301](#).

Optional and disabled by default. With no `:nidd` configuration the MME does not advertise Control-Plane CIoT support, and Non-IP PDN connections are not served over T6a. A non-CIoT MME behaves exactly as before.

Table of Contents

- [Architecture](#)
- [Connection establishment](#)
- [Mobile-Originated data](#)
- [Mobile-Terminated data](#)
- [Configuration](#)
- [Supported scope and limitations](#)

Architecture



A Non-IP PDN connection has **no PGW, no SGW, and no GTP-U tunnel**. Instead the MME holds a tunnel-less Non-IP PDN session bound to the SCEF by the **SCEF-ID** and the Diameter **Session-Id** the MME allocated for the T6a connection.

The MME is a Diameter peer of the SCEF (directly, or via a DRA). The same Diameter service that carries S6a/S13 also carries T6a — application `:t6a` is registered alongside `:s6a`.

Connection establishment

(TS 23.682 §5.13.1) When a UE attaches with **PDN type "Non-IP"** and the subscription's APN-Configuration for that APN carries a **PDN-Type = Non-IP (4)** plus an **SCEF-ID** (the stage-3 encoding of the "Invoke SCEF Selection" indicator), the MME — instead of a GTP-C Create Session towards a PGW — sends a **Connection-Management-Request (CMR)** to the SCEF:

AVP	Value
Connection-Action	CONNECTION_ESTABLISHMENT (0)
Service-Selection	the APN (e.g. non-ip)
User-Identifier	{ User-Name = IMSI }
Bearer-Identifier	the allocated EPS Bearer Identity
Destination-Host / -Realm	derived from the subscription's SCEF-ID

On a successful **Connection-Management-Answer (CMA, Result-Code 2001)** the MME records the Non-IP PDN session and advertises **Control-Plane CIoT EPS optimisation** to the UE in the EPS Network Feature Support of the Attach Accept. The connection is released with a CMR carrying `CONNECTION_RELEASE (1)` when the PDN connection is torn down, and an SCEF-initiated CMR release is honoured too.

Mobile-Originated data

(TS 23.682 §5.13.4) The UE sends Non-IP data in a NAS **ESM DATA TRANSPORT** (message type `0xEB`) User-data container. The MME forwards it to the SCEF as a T6a **MO-Data-Request (ODR)** whose `Non-IP-Data` AVP is the verbatim payload.

```
UE --ESM DATA TRANSPORT(user data)--> MME --ODR(Non-IP-Data)-->
SCEF
```

Mobile-Terminated data

(TS 23.682 §5.13.3) The SCEF sends downlink Non-IP data in a T6a **MT-Data-Request (TDR)**. The MME maps the `Non-IP-Data` AVP into a downlink NAS

ESM DATA TRANSPORT to the UE and answers the SCEF with an **MT-Data-Answer (TDA)**.

```
SCEF --TDR(Non-IP-Data)--> MME --ESM DATA TRANSPORT(user data)-->
UE
MME --TDA(Result-Code)--> SCEF
```

A TDR is matched to the UE by **User-Name (IMSI) + Bearer-Identifier (EBI)**. If the UE or its SCEF session cannot be found the MME answers the SCEF with `UNABLE_TO_COMPLY (5012)` so the SCEF can apply its own buffering / retransmission policy.

Configuration

Two pieces are required:

1. **Enable NIDD** so the MME advertises Control-Plane Clot support:

```
config :mme, :nidd, enabled: true
```

2. **Register the SCEF as a Diameter peer** in the `:diameter_ex :peers` list (or reach it via the existing DRA). The `:t6a` application (dictionary `:diameter_gen_3gpp_t6a`, application-id `16_777_346`) is registered automatically in the `applications:` list.

The Non-IP APN itself is provisioned in the **HSS** subscription: an APN-Configuration with `PDN-Type = Non-IP (4)` and an `SCEF-ID`.

See the [Configuration Reference](#) for the full parameter table, including the `s11u_ip` endpoint for NB-IoT IP data.

NB-IoT IP data over Control-Plane CIoT (S11-U)

Beyond Non-IP NIDD, the same Control-Plane CIoT optimisation carries **IP** data for NB-IoT (TS 23.401 §5.3.4B). Here the PDN is a normal IP PDN towards a PGW, but the data rides NAS:

```
UE <--ESM DATA TRANSPORT (IP packet)--> MME <--GTP-U on S11-
U--> SGW <---> PGW
      Control-Plane CIoT optimisation           (MME terminates
the user plane)
```

The MME terminates the user plane on the **S11-U** interface instead of the eNB on S1-U:

- The Create Session Request carries the MME's **S11-U GTP-U F-TEID** (interface type 38) in the bearer context; the SGW returns its **S11-U GTP-U F-TEID** (type 39). No S1-U E-RAB is set up.
- **Uplink**: an IP packet in an ESM DATA TRANSPORT is GTP-U-encapsulated (G-PDU, TEID = the SGW S11-U TEID) and sent to the SGW.
- **Downlink**: a G-PDU arriving on the MME's S11-U TEID is decapsulated and delivered to the UE as a downlink ESM DATA TRANSPORT (reusing the idle-UE buffering/paging).

This path is selected when CP-CIoT is enabled (`config :mme, :nidd, enabled: true`), the UE signalled Control-Plane CIoT support, and the PDN type is IP. The MME's S11-U GTP-U endpoint listens on UDP **2152** (`config :mme, :nidd, s11u_ip:` — defaults to the S11 GTP-C IP). NB-IoT **Control Plane Service Request** (`0x4D`) re-establishes the connection for an idle UE.

Attach without a user-plane bearer

A Non-IP / CP-CIoT PDN connection carries no user plane, so the Attach Accept (with the Activate Default EPS Bearer Context Request, PDN type Non-IP) is delivered over NAS in a **Downlink NAS Transport** — there is no Initial Context Setup Request and no S1-U E-RAB. Data then rides ESM DATA TRANSPORT on

the same S1 signalling connection. This is selected automatically when the default bearer's PDN type is Non-IP.

Idle-UE Mobile-Terminated delivery

When MT data arrives for an **idle** UE, the MME buffers it on the UE context and **pages** the UE (TS 23.682 §5.13.3 steps 2–4). The SCEF is told

`DIAMETER_SUCCESS` — the MME has taken responsibility for delivery. The buffer is flushed as soon as the UE answers paging with any uplink NAS message. (Buffering is in volatile context state, so it does not survive an MME restart.)

Supported scope and limitations

- **Non-roaming only.** NIDD is served for home subscribers over T6a. Roaming NIDD — T6b to an IWK-SCEF in the visited network — is not supported.
- **Maximum Non-IP message size.** Each Non-IP message, uplink or downlink, carries up to **255 bytes** of user data; larger application payloads must be segmented by the application.
- **Connections are identified by IMSI.** Each SCEF connection is keyed on the subscriber's IMSI (per TS 23.682 §5.13.1.2); MSISDN-based identification is not used.
- **Not supported:** the Mobile-Originated exception-data indication and the Reliable Data Service.

OmniMME Operations Guide

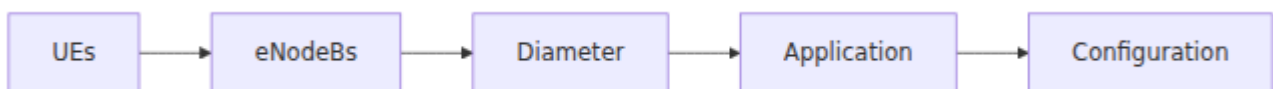
This guide covers day-to-day operation of OmniMME using the Control Panel web interface and REST API.

Table of Contents

- [Control Panel Overview](#)
 - [Managing User Equipment](#)
 - [Managing eNodeBs](#)
 - [Diameter Peer Status](#)
 - [Location Services](#)
 - [S10 Inter-MME Handover](#)
 - [REST API](#)
 - [UE States Reference](#)
 - [Troubleshooting](#)
-

Control Panel Overview

The Control Panel is accessible at `https://<mme-host>:10443`. It provides real-time views of UE contexts, eNodeB connections, and Diameter peer status, refreshing automatically every second.



The sidebar navigation order is configurable via `page_order` in `runtime.exs`. See [Configuration Reference](#). The [Location](#) and [S10](#) pages are available in addition to the pages above when their interfaces are enabled; add their paths to `page_order` to surface them in the sidebar.

Managing User Equipment

The **UEs** page shows all UE contexts currently held by the MME — connected, idle, and recently detached.

UE Status Summary

At the top of the UEs page, a live count shows:

Status	Meaning
Connected	UE is EMM-Registered and ECM-Connected (active S1AP association, data plane active)
Idle	UE is EMM-Registered and ECM-Idle (S1AP released, context retained — reachable via paging)
Disconnected	UE is EMM-Deregistered (detached; context retained briefly for context-based re-attachment)

Searching and Filtering

The search box matches against IMSI, MSISDN, IMEISV, MME UE S1AP ID, eNB UE S1AP ID, and eNodeB name. Results update as you type with a 300ms debounce.

The **Filters** button provides status-based filtering:

- **All Status** — Show all contexts
- **Connected** — ECM-Connected only
- **Idle** — ECM-Idle only
- **Disconnected** — EMM-Deregistered only

Results are paginated at 10 per page. Use the pagination controls to navigate large subscriber populations.

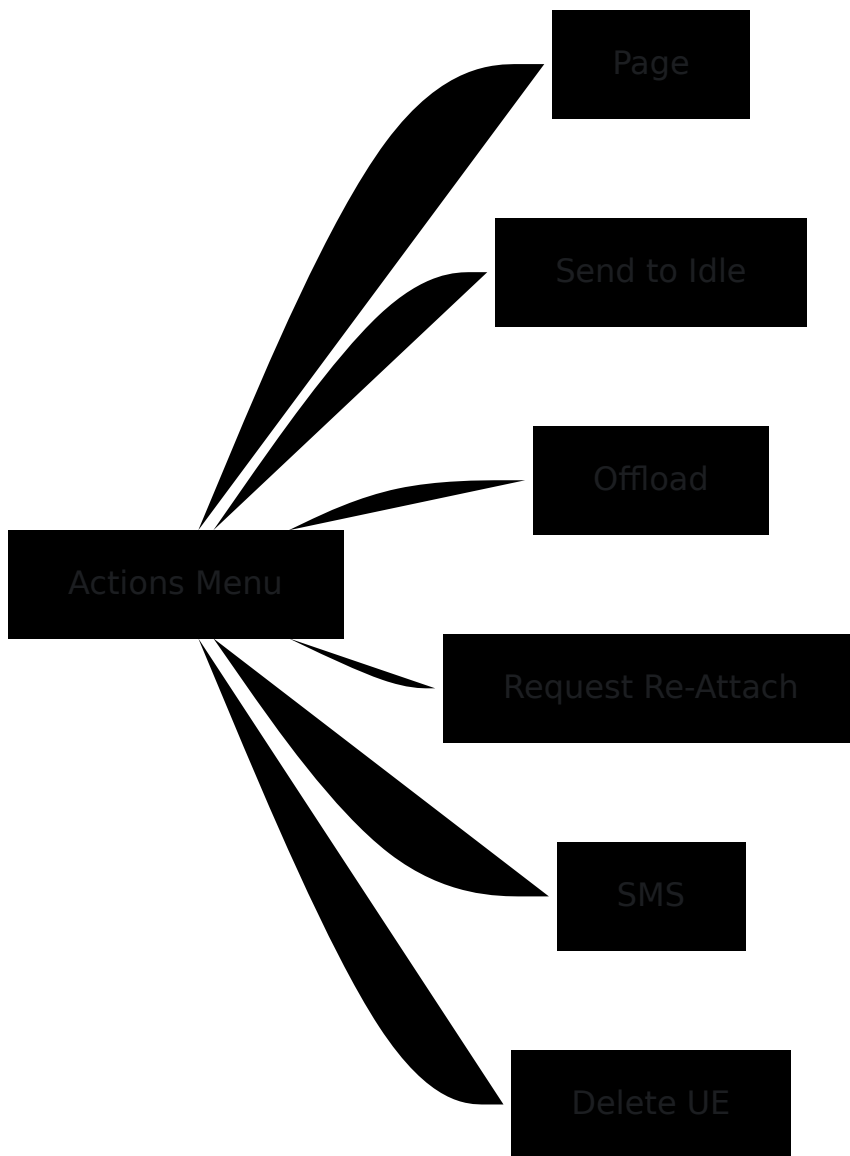
UE Detail View

Click any UE row to expand its detail view. Sections shown depend on available context:

Section	Contents
Basic Information	IMSI, MSISDN, IMEISV, device type, GUTI, current TAI, current ECGI, UE AMBR, S11 tunnel endpoints, context timestamps
Radio Capability	Supported LTE bands, MIMO capability, release level, UE category
UE Network Capability	EPS encryption and integrity algorithms, codec support
Security Context	NAS security algorithm and key set identifier
PDN Sessions	Active PDN connections with APN, AMBR, and bearer details
Allowed APNs	APN configuration profile from the HSS subscription
Recent ESM Procedures	In-progress or recently completed bearer setup/teardown transactions

UE Actions

Each UE has an actions menu (: button). Actions are disabled for EMM-Deregistered UEs where they would have no effect.



Page

Sends a paging message to retrieve the UE from ECM-Idle. Two paging methods are available:

Method	Behaviour	When to use
S-TMSI	Pages using the UE's S-Temporary Mobile Subscriber Identity. Standard paging mechanism.	Default — use this in normal operation.
IMSI	Pages using the UE's full IMSI.	Use only when S-TMSI paging fails. Warning: IMSI paging may cause the UE to detach and reattach.

The page action is only available for registered UEs (Connected or Idle).

Send to Idle

Sends a UE Context Release Command to the eNodeB, transitioning the UE from ECM-Connected to ECM-Idle. The UE's context is retained in the MME and the UE remains registered. Use this to free radio resources for an idle subscriber.

Offload

Moves a UE to a different MME or forces a re-selection by sending a UE Context Release Command with the cause `load-balancing-tau-required`. If the UE is currently idle, it is paged first to ensure the release is delivered.

This briefly interrupts the UE's data connection. The UE will perform a TAU and typically reattach to a less loaded MME.

Request Re-Attach

Detaches the UE and triggers an immediate re-attach by sending a Detach Request with re-attach required. If the UE is currently idle, it is paged first.

Use this to force re-authentication or to apply a subscription change that requires a fresh attach.

SMS

Sends an SMS message to the UE over the NAS interface (SMS-over-NAS). If the UE is currently idle, it is paged first before the message is delivered.

Fill in:

- **Sender MSISDN** — The number that will appear as the message sender (digits only)
- **Message** — The SMS text body

Delete UE

Removes all stored context for this UE immediately. The UE will need to perform a full attach procedure to reconnect. This does not send any signalling to the UE or eNodeB — it is a local state deletion only.

Use this to clear a stale or stuck context that is preventing normal attach.

Managing eNodeBs

The **eNodeBs** page shows all eNodeBs that have previously connected to the MME, with live S1 connection status.

eNB Status Summary

Status	Meaning
Connected	Active SCTP association; S1 Setup completed
Disconnected	SCTP association lost or S1 Setup not yet completed

eNB Detail View

Click any eNB row to expand its detail view:

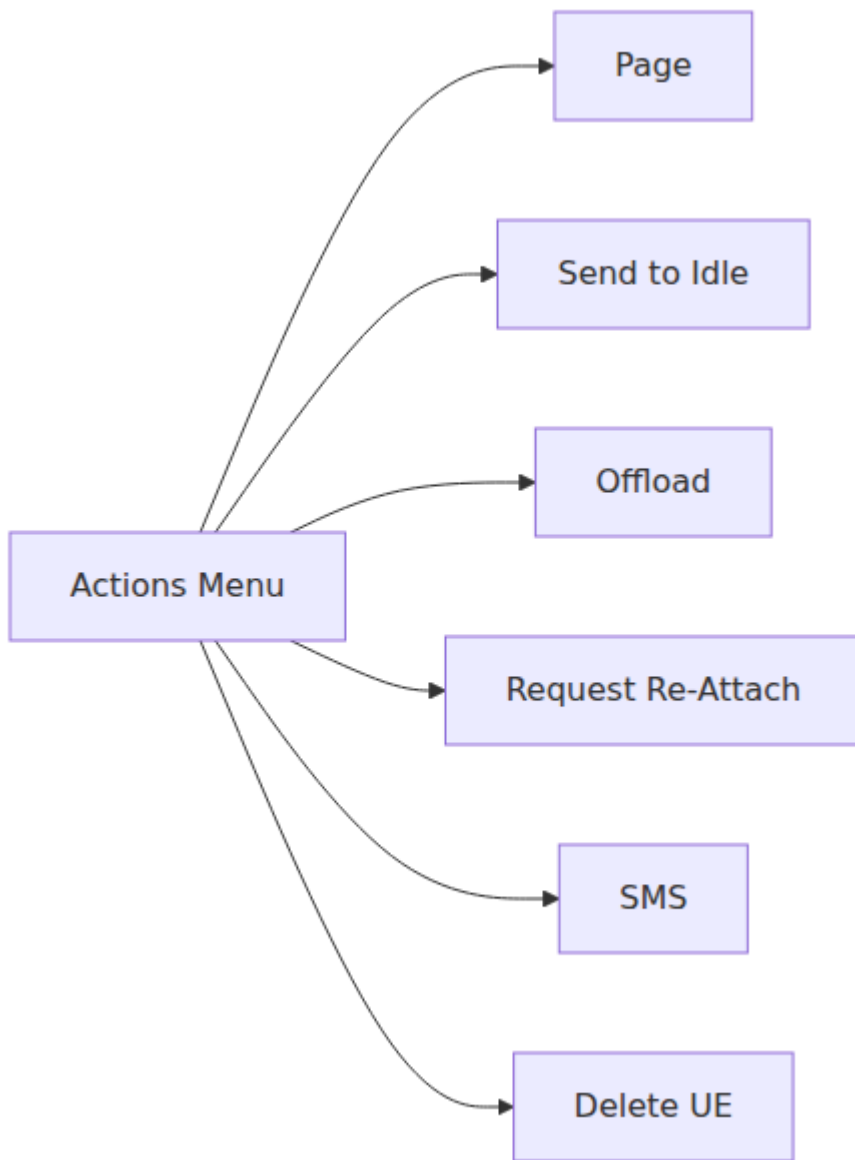
Section	Contents
Basic Information	PLMN, Default Paging DRX, NB-IoT Paging DRX, advertised MME capacity
Connection Details	SCTP association ID, local and remote address/port, stream counts, SCTP state and history
TAI Configuration	TAIs advertised by the eNB and the subset accepted by the MME
Connected en-gNBs	5G NR secondary nodes (en-gNBs) connected to this eNB for NR-NSA operation

Updating Advertised MME Capacity

OmniMME can instruct an eNodeB to use a different **relative MME capacity** value without requiring a restart. This is useful for graceful load-balancing or maintenance drains.

1. Open the actions menu (:) next to the eNB — only available when the eNB is **Connected**.
2. Select **Update Capacity**.
3. Enter a value between 0 and 255.
4. Click **Send to eNB**.

OmniMME sends an MME Configuration Update message to the eNB with the new relative capacity. The change takes effect immediately on the eNB side but reverts to the value in `runtime.exs` upon MME restart.



Diameter Peer Status

The **Diameter** page shows all configured Diameter peers and their current connection state.

For each peer, the following is displayed:

Field	Description
Host	Diameter Identity (Origin-Host) of the peer
Status	Current connection state: Connected, Disconnected, or Connecting
IP / Port	Network address of the peer
Transport	TCP or SCTP
Connection Initiation	Whether OmniMME initiates (<code>outbound</code>) or accepts (<code>inbound</code>) the connection
Realm	Diameter Realm reported by the peer in CEA
Product Name	Vendor product string reported by the peer in CEA
Application IDs	Diameter application IDs negotiated in CEA

Expand a peer row to see full connection detail.

A healthy deployment requires all configured S6a peers to show as **Connected**. Loss of all S6a peers will prevent new UE attach procedures from completing authentication.

Location Services

The **Location** page provides control-plane positioning (LCS) for registered UEs. It is available only when the SLs interface to the E-SMLC is enabled (`esmlc.enabled`, see [Configuration Reference](#)); positioning results come from the E-SMLC over SLs (LCS-AP), with measurements gathered from the eNB (LPPa) and/or the UE (LPP).

At the top of the page, live counts show **Total**, **Connected**, **Idle**, and **Located** UEs. Search matches IMSI, MSISDN, or MME UE S1AP ID.

Positioning Methods

Select the method before requesting a fix:

Method	Source	Typical accuracy	Notes
Cell ID	Serving cell (ECGI) and tracking area (TAI)	Cell-level	Fastest; no UE/eNB measurement campaign required.
E-CID (Enhanced Cell ID)	eNB measurements via LPPa (TS 36.455)	Tens-hundreds of m	Selectable quantities: Cell ID, TA Type 1, TA Type 2, Angle of Arrival, RSRP, RSRQ.
GNSS (GPS)	UE GPS via LPP (TS 36.355)	10-50 m	Most precise; requires UE LPP support and GPS visibility.
OTDOA	eNB PRS + UE timing differences via LPP	Tens of m	Requires multiple cells with PRS enabled.

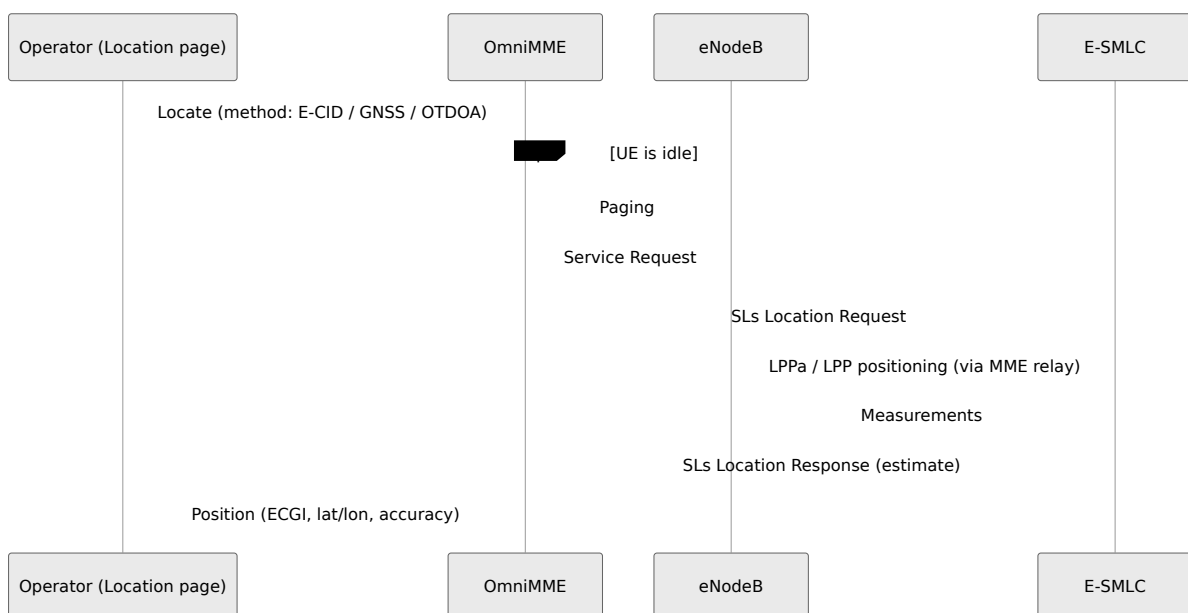
For E-CID, use the measurement-quantity toggles to control which quantities the E-SMLC requests.

Requesting a Location

Action	Behaviour
Locate	Runs a live positioning request using the selected method. If the UE is idle it is paged first. The result is fetched asynchronously and the row updates when it arrives.
Cached	Returns the UE's last known location (serving ECGI + TAI) without contacting the E-SMLC or paging the UE.

The result panel shows ECGI, TAI, latitude/longitude/altitude, uncertainty and confidence; E-CID measurement detail (cell, TAC, TA types, AoA, RSRP, RSRQ); and OTDOA cell info (PCI, EARFCN, PRS bandwidth/config). When GNSS coordinates are present, an embedded map pin is shown.

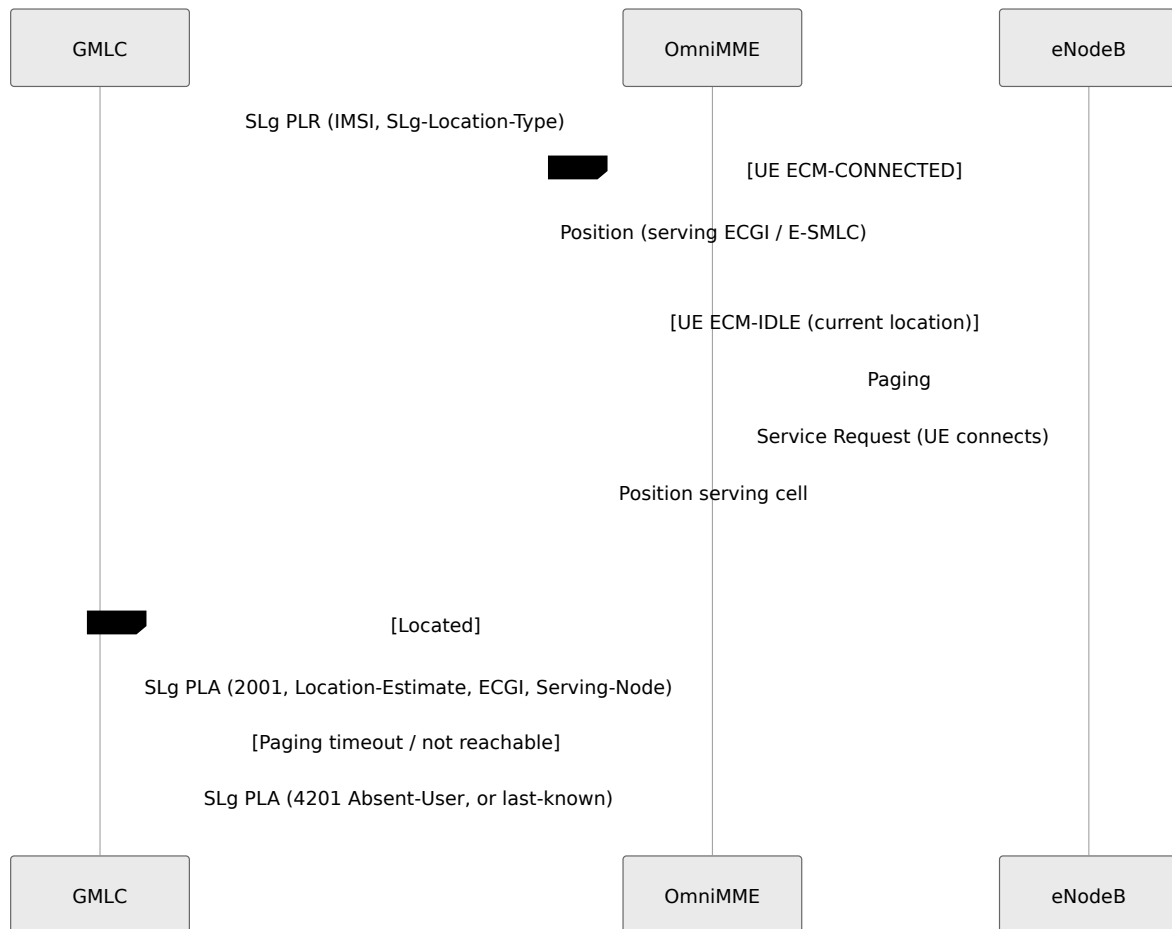
A **Locate** request follows the control-plane LCS flow: the MME drives the E-SMLC over SLs, which in turn gathers measurements from the eNB (LPPa) and/or the UE (LPP).



SLg Location Request (from a GMLC)

When a GMLC sends a **Provide-Location-Request (PLR)** over SLg ([TS 29.172](#)), the MME resolves the subscriber's location and replies with a **Provide-**

Location-Answer (PLA). For a *current-location* request of an idle UE, the MME pages the UE first (network-triggered), then positions it:



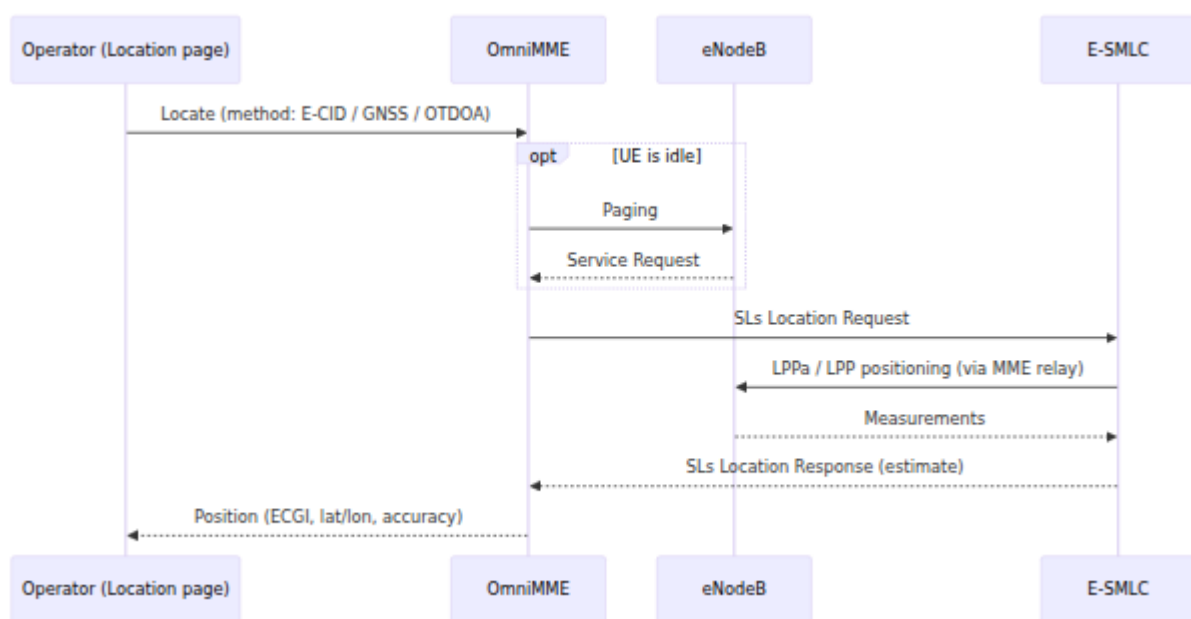
- **Current / Initial / Notification-verification** location types page an idle UE (bounded by T3413), then return the serving cell. On paging timeout they fall back to last-known for *current-or-last-known*, or `DIAMETER_ERROR_ABSENT_USER` (4201) for strict current.
- **Current-or-last-known** returns the cached serving ECGI/TAI without paging when no live fix is available.
- Result codes: `2001` success, `5001` user unknown, `4201` absent/unreachable, `4260` position-method-failure.

When `esmlc.enabled` is set, the PLR is satisfied through the SLs/E-SMLC positioning path above; otherwise the MME answers from its own serving-cell / last-known state.

S10 Inter-MME Handover

The **S10** page is a read-only monitor for inter-MME mobility — idle-mode context transfer (foreign-GUTI TAU) and connected-mode Forward Relocation — over the S10 GTP-C interface, plus N26 interworking to 5GS. See [Neighbour MME \(S10\)](#) for configuration.

When a UE arrives on a TAU presenting a GUTI that belongs to another MME (a *foreign* GUTI), OmniMME pulls the UE's context from the previous MME over S10 rather than rejecting it:



Neighbour Discovery

Shows the configured `selection_method` (DNS-based S-NAPTR or static peers) and, for static configuration, the neighbour-MME peer list: **Host**, **IP**, and **Port**.

Active Handovers

Lists in-progress S10/N26 relocations with a live count, each row showing:

Field	Description
IMSI	Subscriber being relocated.
MME UE S1AP ID	Local S1AP identifier for the UE context.
Phase	Relocation stage — e.g. acquiring-context, preparing-relocation, relocation-complete.

There are no operator actions on this page; force-offload to a peer MME is driven through the [REST API](#).

REST API

The REST API (`https://<mme-host>:8443`) provides programmatic access for OSS/BSS integration and automation. Interactive documentation is available at `/api/swagger`.

UE Endpoints

List UEs

```
GET /api/ues
```

Query parameters:

Parameter	Type	Description
<code>search</code>	String	Filter by IMSI, MSISDN, IMEISV, MME UE S1AP ID, eNB UE S1AP ID, or eNB name
<code>status</code>	String	Filter by status: <code>connected</code> , <code>idle</code> , or <code>disconnected</code>
<code>page</code>	Integer	Page number (default: 1)
<code>per_page</code>	Integer	Results per page (default: 50)

Response:

```
{
  "data": [ ... ],
  "page": 1,
  "per_page": 50,
  "total": 142,
  "total_pages": 3
}
```

Each UE object in `data` includes: `context_id`, `imsi`, `imeisv`, `msisdn`, `mme_ue_slap_id`, `enb_ue_slap_id`, `global_enb_id`, `enb_name`, `emm_state`, `ecm_state`, `current_tai`, `current_ecgi`, `guti`, `s_tmsi`, `ue_ambr`, `timestamps`, `session_contexts`, `esm_procedures`, and `apn_configuration_profile`.

Get UE by Context ID

```
GET /api/ues/:context_id
```

Returns a single UE context object. Returns `404` with `{"error": "not_found"}` if the context ID does not exist.

UE Actions

```
POST /api/ues/:ue_id/actions
```

Performs an operator action on a UE — the API equivalent of the UEs-page actions menu.

Body parameters:

Parameter	Type	Description
<code>action</code>	String	One of <code>page</code> , <code>send_to_idle</code> , <code>offload</code> , <code>delete</code> , <code>request_reattach</code> , <code>send_sms</code> .
<code>paging_type</code>	String	For <code>page</code> : <code>s_tmsi</code> (default) or <code>imsi</code> .
<code>sender_msisdn</code>	String	For <code>send_sms</code> : the sender number shown to the UE (digits only).
<code>text</code>	String	For <code>send_sms</code> : the message body.

Idle UEs are paged first where the action requires a NAS path. See [UE Actions](#) for the behaviour of each action.

eNodeB Endpoints

List eNodeBs

```
GET /api/enodebs
```

Query parameters: `status` — `connected` or `disconnected`.

Get eNodeB

```
GET /api/enodebs/:id
```

Returns a single eNodeB context by global eNB ID.

eNodeB Actions

```
POST /api/enodebs/:enodeb_id/actions
```

Body parameters:

Parameter	Type	Description
<code>action</code>	String	Currently <code>update_mme_capacity</code> .
<code>relative_mme_capacity</code>	Integer	New relative MME capacity (0-255). Sends an MME Configuration Update to the eNB (see Updating Advertised MME Capacity).

Diameter Endpoints

```
GET /api/diameter
GET /api/diameter/:id
```

List Diameter peers (optionally filtered by `status`), or fetch one by host. Mirrors the [Diameter page](#).

SGW Peer Endpoints

```
GET /api/sgw_peers
GET /api/sgw_peers/:id
```

List the S-GW peers that currently anchor S11 sessions, or fetch one by IP. Useful for confirming session distribution and peer recovery state.

S10 / Inter-MME Handover

```
GET /api/s10
POST /api/s10/offload
```

GET /api/s10 returns S10/N26 neighbour discovery state and the list of active handovers (mirrors the [S10 page](#)).

POST /api/s10/offload force-offloads a subscriber to a peer MME. Body: `imsi` (required). For a connected UE this performs a connected-mode relocation and waits for completion; an idle UE is flagged so it is released with `load-balancing-TAU-required` on its next Service Request or TAU (it is **not** paged to offload, per [TS 23.401 §4.3.7.3](#)). Offload of a UE with a dedicated/GBR bearer is refused (it would drop the call) — use a connected-mode S1 handover instead.

GUTI Reallocation

```
POST /api/guti/reallocate
```

Triggers the GUTI Reallocation procedure ([TS 24.301](#)) for a UE. Body: `imsi` (required). The UE must be **connected** — there is no NAS path to an idle UE, so a request for an idle/unknown UE is rejected.

DNS / Route Testing

```
POST /api/dns-test/pgw
POST /api/dns-test/sgw
POST /api/dns-test/mme
```

Dry-runs the P-GW / S-GW / target-MME selection pipeline for a given subscriber — builds the FQDN, resolves it via DNS (S-NAPTR, over TCP), and applies the configured selection method — and returns **what would be selected, without attaching a subscriber, sending any GTP-C, or changing state**. Use it to validate DNS and routing configuration (new gateway pools, APN-OI replacement, home vs roaming, PLMN-specific routes)

as a safe, repeatable pre-change check, instead of attaching a live UE and reading the choice out of the logs.

The dry-run uses the **same selection code as the live attach path**, so its result matches what a real subscriber would get.

Request body (JSON) — supply the PLMN either explicitly (`mcc/mnc`) or as an `imsi` to derive it:

Field	PGW	SGW	MME	Description
apn	required	-	-	APN Network Identifier (e.g. <code>ims</code>) or a full APN-FQDN
tac	-	required	required	Tracking Area Code of the target TAI
imsi	optional	optional	optional	Derives <code>mcc</code> / <code>mnc</code> and the home/roaming classification (as attach does)
<code>mcc</code> , <code>mnc</code>	optional	optional	optional	Serving/target PLMN, when no <code>imsi</code> is given
subscriber_type	optional	optional	-	<code>home</code> or <code>roaming</code> ; overrides the derived classification
apn_oi_replacement	optional	-	-	Exercises the home-PGW APN-OI Replacement path

Example:

```
curl -sk -X POST https://<mme>:8443/api/dns-test/pgw \
-H 'content-type: application/json' \
-d '{"apn":"ims","imsi":"001010000004157"}'
```

Response exposes each stage so it is diagnosable, not just the final IP:

```
{
  "node": "PGW",
  "subscriber_type": "home",
  "selection_method": "dns_lookup",
  "fqdn": "ims.apn.epc.mnc001.mcc001.3gppnetwork.org",
  "attempts": [{"dns_server": "10.103.1.53", "fqdn": "...",
"candidate_count": 2}],
  "candidates": [{"host": "pgw01...", "ips": ["10.103.1.21"],
"port": 2123, "service": "x-3gpp-pgw:x-s5-gtp"}],
  "selected": {"host": "pgw01...", "ip": "10.103.1.21", "port":
2123},
  "notes": []
}
```

`candidates` is the resolved list in selection order; `selected` is the peer that would be chosen (for weight/priority pools this is one weighted pick — the full ranked `candidates` list is the deterministic view). `notes` flags fallbacks such as no candidates resolved. For a `random_peer` (static) pool, `candidates` is the configured pool and `fqdn` is `null`.

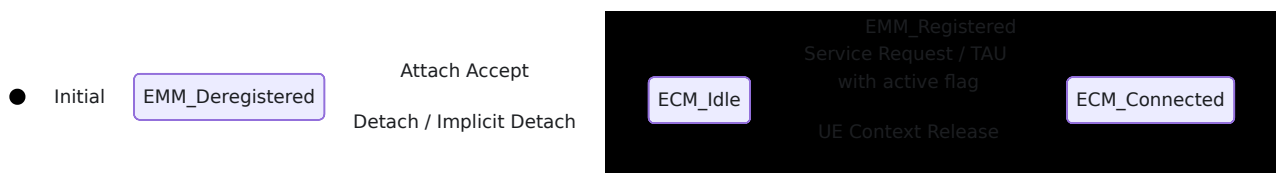
System

GET /api/status

Health check; returns `{"result": "ok"}` when the API is serving.

UE States Reference

OmniMME tracks two independent state machines per UE:



EMM States (EPS Mobility Management):

State	Meaning
<code>emm_registered</code>	UE has successfully attached. Authentication and subscription retrieval complete.
<code>emm_deregistered</code>	UE has detached or been implicitly detached. Context may still be retained for a short period.

ECM States (EPS Connection Management):

State	Meaning
<code>ecm_connected</code>	Active S1AP association between MME and eNodeB for this UE. Data plane active.
<code>ecm_idle</code>	S1AP association released. UE context retained in MME. UE reachable via paging.

The ECM state is only meaningful when `emm_state` is `emm_registered`. An `emm_deregistered` UE has no meaningful ECM state.

Troubleshooting

UEs Unable to Attach

Symptoms: New attach requests fail; UEs show authentication or rejection errors.

Possible causes:

- Diameter S6a peer disconnected — HSS unreachable for authentication
- Home PLMN misconfigured — UE's IMSI PLMN does not match `home_plmn` in configuration

- S13 equipment check blocking — device IMEISV classified as blacklisted
- Served TAI not including the eNB's TAC — eNB TAI not accepted during S1 Setup

Resolution:

1. Check the Diameter page in the Control Panel — all S6a peers should show Connected.
 2. Verify `home_plmn` matches the MCC/MNC encoded in subscriber SIMs.
 3. If `s13.enabled` is `true`, confirm `allowed_equipment_status` includes the expected classification.
 4. Check eNB detail view → TAI Configuration section to confirm the attaching UE's TAC appears in the accepted TAI list.
-

eNodeB Disconnecting Frequently

Symptoms: eNB status flaps between Connected and Disconnected; UEs experience dropped sessions.

Possible causes:

- Network path instability between MME and eNB
- MTU mismatch causing SCTP fragmentation issues
- MME overloaded — SCTP heartbeats delayed

Resolution:

1. Check network path quality between `slap.listen_ip` and the eNB IP shown in the Connection Details.
 2. Verify that SCTP traffic (IP protocol 132) is not being blocked or NAT'd on the path.
 3. Review BEAM metrics (`beam_processes_count`, `beam_memory_total`) for signs of resource exhaustion.
-

SMS Delivery Failing

Symptoms: SMS action returns "UE paged, but no response."

Possible causes:

- UE is genuinely unreachable (powered off, out of coverage)
- UE does not support SMS over NAS
- Paging area misconfigured — TAI list does not cover the UE's last known TAI

Resolution:

1. Verify the UE's last known TAI and confirm that TAC is in `served_tai`.
 2. Check that the eNB serving that TAC is currently Connected.
 3. Confirm the UE's subscription supports SMS over NAS.
-

Stale UE Contexts Accumulating

Symptoms: `mme_ue_count` grows over time but connected/idle counts remain stable; many contexts in Disconnected state.

Possible causes:

- Idle UEs are not being implicitly detached — e.g. the Mobile Reachable / Implicit Detach timers are set far longer than the periodic TAU interval, or UEs are leaving coverage without detaching.

Resolution:

1. UE-context lifecycle is governed by the Mobile Reachable and Implicit Detach timers (see [Configuration Reference](#)). A UE that misses its periodic TAU (`t3412`) is implicitly detached and its context removed once these timers expire.
2. For high-churn networks, review `t3412` and the derived `mobile_reachable_timer` / `implicit_detach_timer` so stale contexts are evicted on a timescale that fits your subscriber base.

3. Individual stale contexts can be removed immediately via the **Delete UE** action in the Control Panel, or `POST /api/ues/:ue_id/actions` with `action: "delete"`.

The legacy `persistent_emm_deregistered_cleanup_interval` / `persistent_ecm_idle_cleanup_interval` settings no longer have any effect — see the note under [MME Core Parameters](#).

Roaming

This guide covers how OmniMME handles **inbound roaming** subscribers — UEs whose IMSI belongs to another PLMN — and how it keeps roaming traffic on dedicated, edge-facing gateways.

For every Attach and Tracking Area Update the MME makes one decision that drives everything else on this page: is this subscriber **home** or **roaming**? That class then selects which Serving Gateway (SGW) and Packet Data Network Gateway (PGW) the session is anchored on, which DNS pool is queried, and which inter-operator border the traffic crosses.

Table of Contents

- [Home and Roaming Classification](#)
- [Unknown PLMN Off-Net Fallback](#)
- [SGW and PGW Selection](#)
- [EPC DNS Resolution](#)
- [Dedicated Roaming SGWs](#)
- [Operator PLMN Override File](#)
- [IMSI Operator Lookup API](#)
- [Troubleshooting](#)

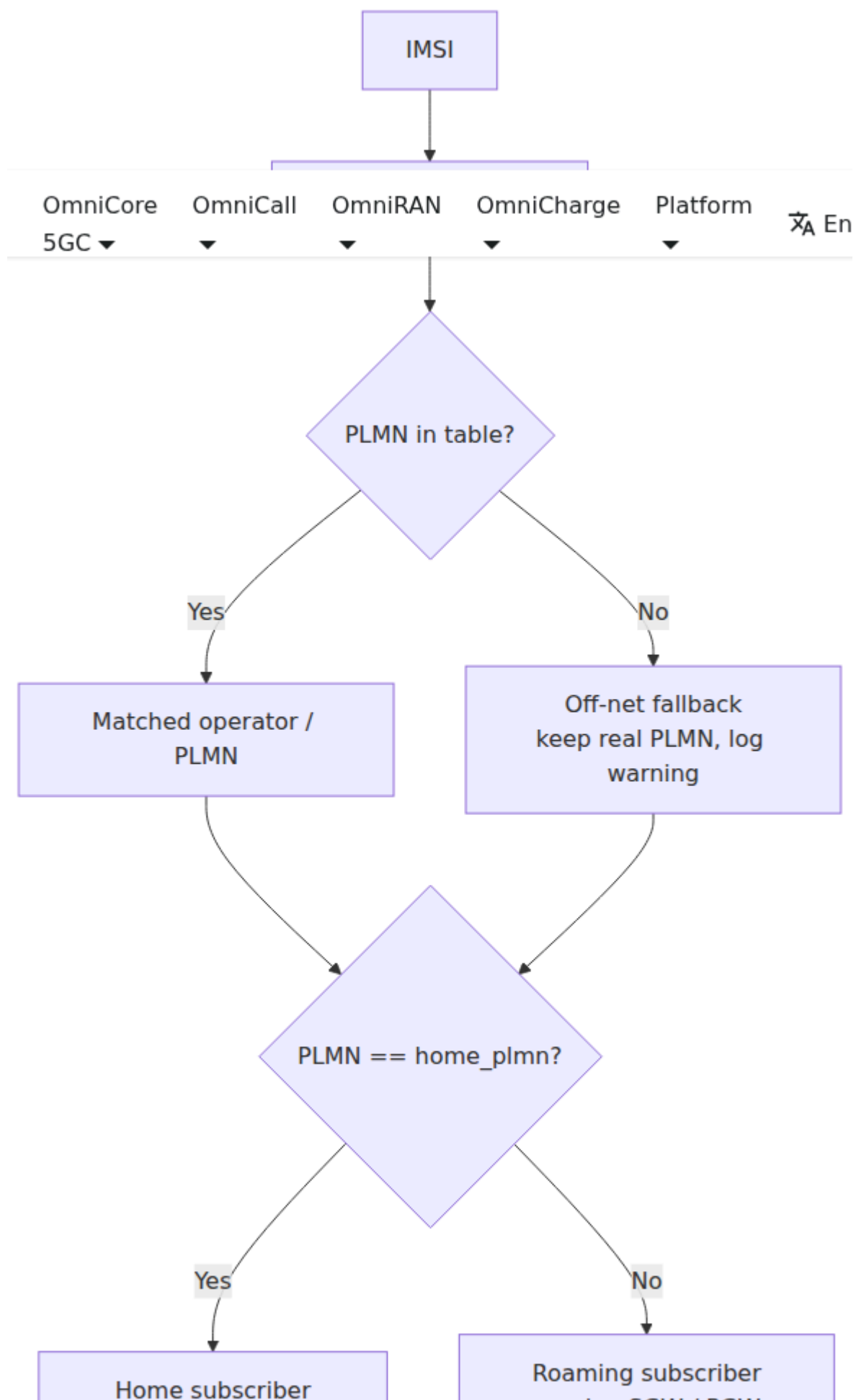
Home and Roaming Classification

The leading digits of the IMSI are the subscriber's PLMN: a three-digit Mobile Country Code (MCC) followed by a two- or three-digit Mobile Network Code (MNC), per [TS 23.003 §2.2](#). OmniMME resolves this against its PLMN reference table — the shipped global operator database plus any [operator override](#) — to recover the operator name, country, and MNC length:

1. The first **six** digits are looked up as a three-digit-MNC PLMN.
2. If that misses, the first **five** digits are looked up as a two-digit-MNC PLMN.

3. If both miss, the **off-net fallback** applies.

The matched PLMN is compared against the configured `home_plmn`. If the MCC **and** MNC both match, the subscriber is **home**; otherwise it is **roaming**. This single classification feeds SGW selection, PGW selection, the DNS / peer pool chosen by subscriber `type`, and the APN-OI suffix.



home SGW / PGW pool

roaming SGW / PGW
pool

The examples on this page assume `home_plmn` is set to MCC `001` / MNC `01` (Example Home Network), with Example Roaming Partner (MCC `999` / MNC `970`) as an inbound roamer.

Unknown PLMN Off-Net Fallback

When a subscriber's PLMN is **not** present in the table — a roaming partner or private network that has not been added — OmniMME does **not** assume the subscriber is home. It keeps the subscriber's real MCC/MNC taken directly from the IMSI, so the subscriber correctly classifies as **roaming** and is routed to the roaming gateway pool rather than a local home gateway.

Because an IMSI alone does not state whether its MNC is two or three digits, the MNC length is inferred from other rows sharing the same MCC (the MNC length is consistent within an MCC region per [TS 23.003](#)), defaulting to three digits when the MCC is entirely unknown.

Each off-net fallback is recorded at `warning` so operators can see exactly which PLMN is missing and should be added to the [override file](#):

```
level=warning msg="IMSI PLMN not in PLMN table; classifying
subscriber as off-net (roaming)"
  protocol=slap imsi=9999700000000001 mcc=999 mnc=970 mnc_length=3
inferred=true
```

A roaming operator that **is** in the table (matched, but not the home PLMN) does not produce this warning — it is expected roaming. The warning specifically flags PLMNs the MME has no record of, which is the most common cause of a roamer being mis-routed.

SGW and PGW Selection

Once classified, the session is anchored on gateways chosen for that subscriber type:

Class	SGW pool	PGW interface	PGW DNS service
Home	Home SGWs	S5	x-3gpp-pgw:x-s5-gtp
Roaming	Roaming SGWs	S8	x-3gpp-pgw:x-s8-gtp

Roaming PDN connectivity is **home-routed** (TS 23.401 §4.3): the visited-network SGW connects over **S8** to the roamer's **home** PGW, so the roamer's traffic breaks out in their home network. Home subscribers use **S5** to a local PGW.

Each gateway is selected by one of two methods, configurable globally or **per subscriber type** (%{home: ..., roaming: ...}):

Method	Behaviour
:random_peer	Pick at random from the statically configured peers whose <code>type</code> matches the subscriber class (<code>:home</code> , <code>:roaming</code> , or <code>:home_and_roaming</code>).
:dns_lookup	Resolve a topology DNS query against the DNS servers whose <code>type</code> matches the subscriber class. See EPC DNS Resolution .

A common deployment uses static peers for home subscribers and DNS for inbound roamers, so roaming partners can publish their own topology via DNS. The `selection_method`, `peers`, and `dns` parameters are documented in the [Serving Gateway](#) and [PGW](#) sections of the Configuration Reference.

EPC DNS Resolution

DNS-based selection follows the Straightforward-NAPTR (S-NAPTR) procedure of [TS 29.303](#), resolving a service name to a concrete node address through a NAPTR → SRV → A/AAAA chain.

SGW (S11). The MME builds a **TAI-FQDN** from the UE's tracking area and PLMN:

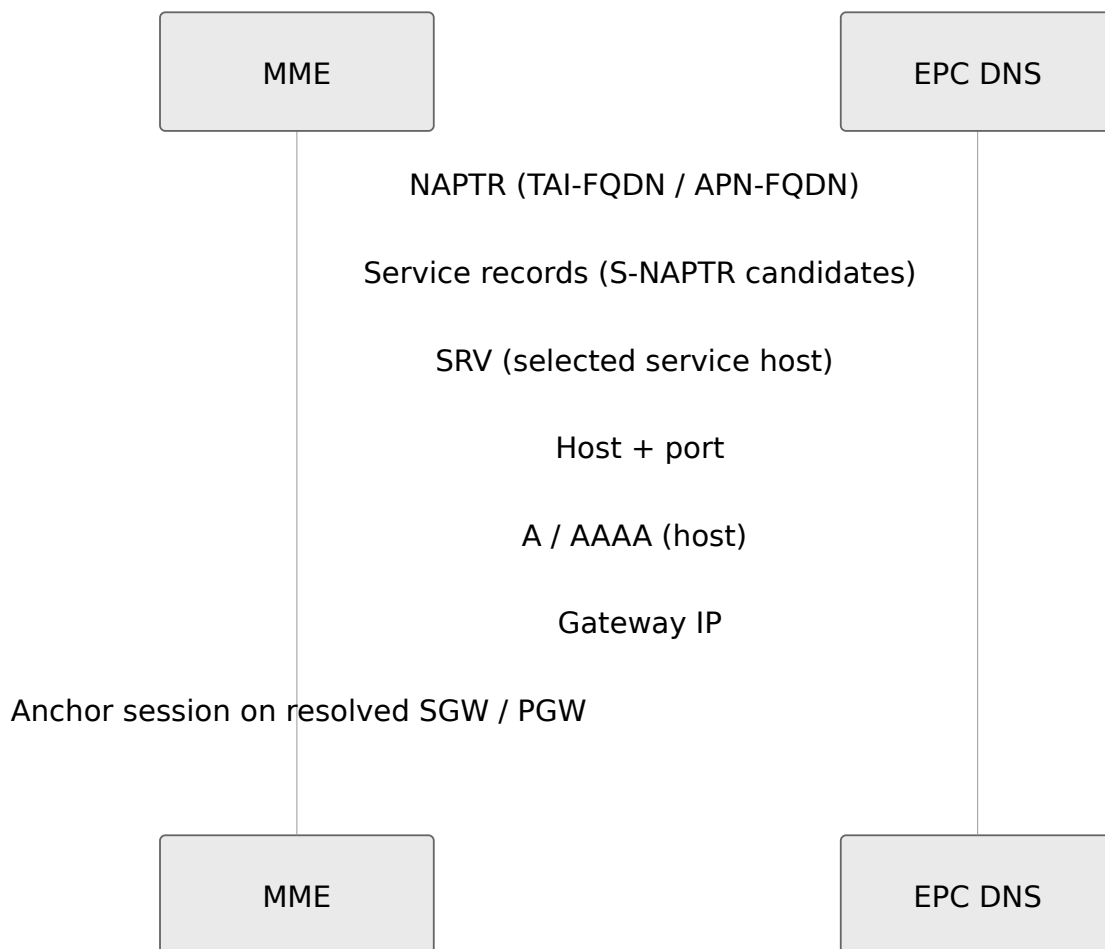
```
tac-lb<low-byte>.tac-hb<high-  
byte>.tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

and runs S-NAPTR for the `x-3gpp-sgw:x-s11` service. If the SGW publishes only its S5/S8 records at that name, the MME takes the SGW's canonical node name (stripping the leading `topon/topoff` topology labels per [TS 29.303 §4.3.2](#)) and runs a second S-NAPTR for `x-s11` against it.

PGW (S5/S8). The MME builds an **APN-FQDN** from the requested APN and PLMN:

```
<apn>.apn.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

and runs S-NAPTR for `x-3gpp-pgw:x-s5-gtp` (home) or `x-3gpp-pgw:x-s8-gtp` (roaming).



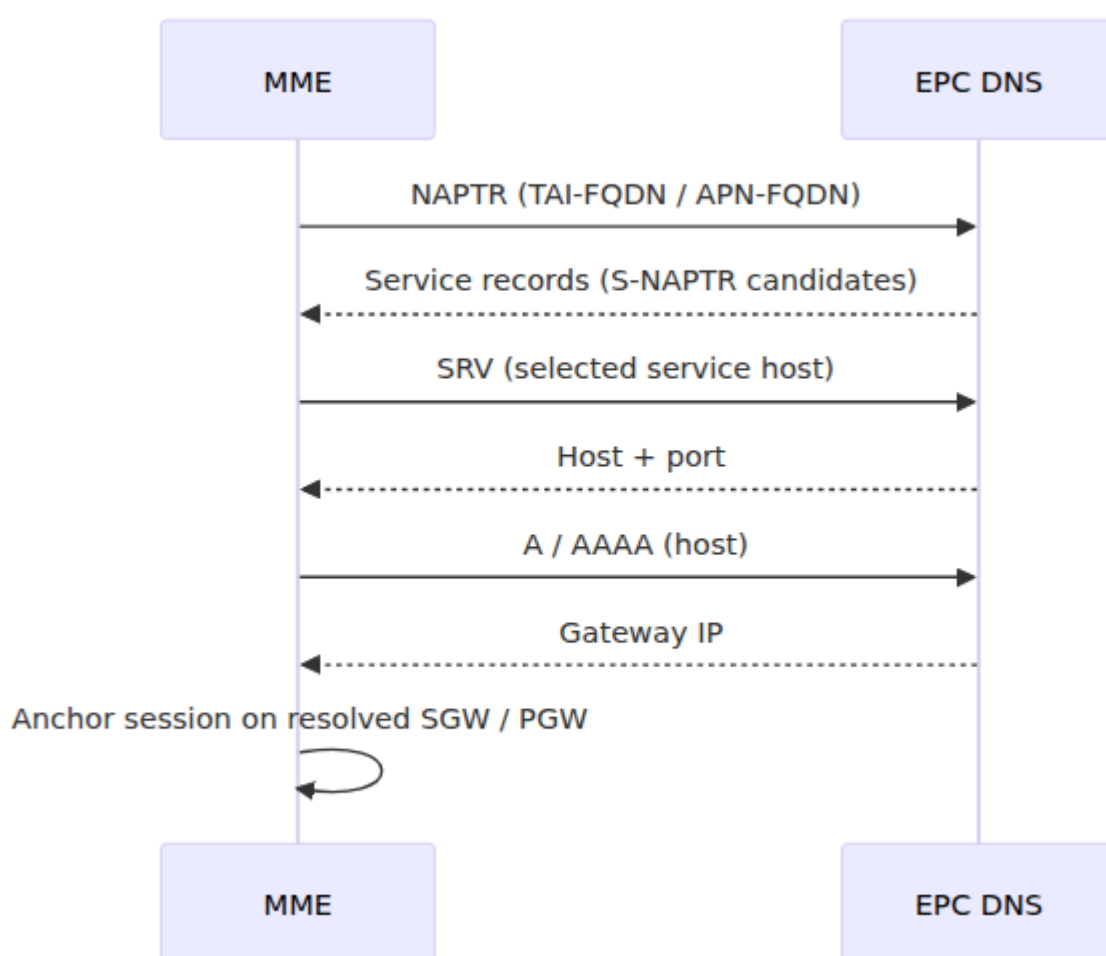
The PLMN labels (`mnc<MNC>.mcc<MCC>`) always carry the subscriber's **real** PLMN, so a roamer's query resolves against their home or partner topology — never the visited network's. When an S-NAPTR node returns both IPv4 and IPv6 addresses, the `dns_ip_version` preference decides which family is used, with the other kept as a fallback. DNS server pools are themselves tagged `:home` / `:roaming` / `:home_and_roaming`, so home and roaming lookups can be sent to entirely separate resolvers. See [DNS Parameters](#) for configuration.

Dedicated Roaming SGWs

Roaming SGWs are deliberately kept **separate** from home SGWs and are the only gateways exposed at the network edge to roaming partners.

In home-routed roaming the visited SGW must reach the roamer's **home** PGW across the inter-operator boundary (the IPX/GRX network, per [GSMA IR.88](#)). That is an external, partner-facing connection. By dedicating a pool of SGWs to roaming and steering only roamers to them, the operator:

- **Limits exposure** — only the roaming SGWs are reachable from the inter-PLMN border; home SGWs (and the rest of the core) stay internal and unreachable from partner networks.
- **Hides topology** — partners and the IPX see a small, fixed set of edge nodes, not the operator's internal gateway layout.
- **Simplifies the border** — inter-PLMN firewalling, IPsec, and rate-limiting are applied to a known, contained edge pool rather than the whole SGW estate.
- **Contains blast radius** — a compromised or abused roaming connection is confined to the edge SGWs.



The MME's home/roaming classification is the control point that makes this work: it is what steers an inbound roamer onto the edge-exposed roaming SGW pool and keeps home subscribers on the internal home pool. A misclassified roamer (for example, one mistaken for a home subscriber because its PLMN is missing from the table) would be anchored on an internal home SGW — defeating the separation — which is exactly why the **off-net fallback** classifies unknown PLMNs as roaming and warns.

Operator PLMN Override File

OmniMME ships a global PLMN database covering known operators. Operators add their **own** entries — home PLMN corrections, roaming partners, private networks — through an optional override file, without rebuilding or redeploying the release.

```
config :mme,  
  plmn_override_path: "/etc/omnimme/plmn.exs"
```

Parameter	Type	Required	Default	Description
plmn_override_path	String	No	/etc/omnimme/plmn.exs	Files path of the override file. If the file is not found, the default path is used.

The override file is a map keyed by the "<MCC><MNC>" PLMN string, in the same shape as the shipped table:

```
%{
  # Add a roaming partner the global database does not contain
  "999970" => %{
    country: :example_country,
    operator: "Example Roaming Partner",
    mcc: "999",
    mnc: "970",
    mnc_length: 3
  },
  # Correct an existing entry by reusing its PLMN key
  "00101" => %{
    country: :example_country,
    operator: "Example Home Network",
    mcc: "001",
    mnc: "01",
    mnc_length: 2
  }
}
```

Field	Type	Description
<code>mcc</code>	String	Mobile Country Code — three digits. Must equal the first three digits of the PLMN key.
<code>mnc</code>	String	Mobile Network Code — two or three digits. Must equal the remaining digits of the PLMN key.
<code>mnc_length</code>	Integer	Number of MNC digits (2 or 3). Determines whether the IMSI prefix is matched as five or six digits.
<code>operator</code>	String	Operator name, used for display and in the lookup API .
<code>country</code>	Atom String	Country label for the operator.

Override semantics:

- **Merge, not replace.** The override is merged *over* the shipped defaults. A PLMN key present in the override replaces that single shipped row; every other shipped row is left intact. Operators only maintain their own deltas — there is no need to copy the global database.
- **Validated.** Each override row is checked at load: the MCC must be exactly three digits and the MNC two or three digits (TS 23.003 §2.x).
- **Fail-safe.** If the override file cannot be read, has a syntax error, or contains an invalid row, it is ignored in full and the MME continues on the shipped defaults, logging a `warning`. A malformed override can never take down PLMN resolution or prevent boot.

```
level=warning msg="invalid PLMN override file; using shipped
defaults only"
  path=/etc/omnimme/plmn.exs error=<reason>
```

The override is read at startup and re-read on configuration reload, so adding a roaming partner does not require a process restart.

IMSI Operator Lookup API

A read-only endpoint resolves any IMSI to its operator/PLMN and the home-vs-roaming classification the MME would apply — useful for confirming an override took effect or diagnosing why a subscriber routed to a particular gateway pool.

```
GET https://<mme-host>:8443/imsi/{imsi}
```

Field	Type	Description
<code>imsi</code>	String	The IMSI that was queried.
<code>mcc</code>	String	Matched (or IMSI-derived) Mobile Country Code.
<code>mnc</code>	String	Matched (or IMSI-derived) Mobile Network Code.
<code>operator</code>	String null	Operator name, or <code>null</code> when the PLMN is not in the table.
<code>country</code>	String null	Operator country, or <code>null</code> when the PLMN is not in the table.
<code>mnc_length</code>	Integer	Number of MNC digits (2 or 3).
<code>matched</code>	Boolean	<code>true</code> if the PLMN was found in the table; <code>false</code> if it was inferred from the IMSI via the off-net fallback.
<code>classification</code>	String	<code>home</code> or <code>roaming</code> — the gateway-selection class the MME applies to this subscriber.

Example — a home subscriber:

```
{
  "imsi": "001010000000001",
  "mcc": "001",
  "mnc": "01",
  "operator": "Example Home Network",
  "country": "example_country",
  "mnc_length": 2,
  "matched": true,
  "classification": "home"
}
```

Example — a PLMN absent from the table (off-net):

```
{
  "imsi": "999970000000001",
  "mcc": "999",
  "mnc": "970",
  "operator": null,
  "country": null,
  "mnc_length": 3,
  "matched": false,
  "classification": "roaming"
}
```

A `matched: false` result classified as `roaming` confirms the fallback in action: the subscriber keeps its real PLMN and routes as a roamer. Adding that PLMN to the override file changes `matched` to `true` and populates `operator/country`. An IMSI that is not 5–15 digits returns `400 Bad Request`.

Troubleshooting

A roamer is anchored on a home / local SGW

Symptoms: An inbound roaming subscriber's session is set up on an internal home SGW or PGW instead of the roaming pool.

Possible causes:

- The roamer's PLMN is missing from the PLMN table, so it was correctly classified as off-net — but no roaming peers/DNS of `type: :roaming` are configured, so selection fell back to whatever pool exists.
- The roamer's PLMN was mistakenly added to the override with the **home** MCC/MNC.

Resolution:

1. Search the logs for `IMSI PLMN not in PLMN table` to confirm the PLMN and that it classified as off-net.

2. Query `GET /imsi/{imsi}` and confirm `classification` is `roaming`.
3. Ensure roaming SGW/PGW peers (or DNS servers) with `type: :roaming` are configured. See [SGW/PGW Peer Parameters](#).

The lookup API shows `operator: null` / `matched: false`

Symptoms: A known roaming partner resolves with a null operator and `matched: false`.

Resolution: The partner's PLMN is not in the table. Add it to the [override file](#) and reload. Re-query the API to confirm `matched` is now `true`.

DNS selection returns no gateway

Symptoms: Session setup fails with no SGW/PGW resolved when `selection_method` is `:dns_lookup`.

Possible causes:

- No DNS server of the matching `type` (`:home` / `:roaming`) is configured for that subscriber class.
- The partner has not published the expected `x-s11` / `x-s8-gtp` S-NAPTR records.

Resolution:

1. Confirm a DNS server with the correct `type` is configured (see [DNS Parameters](#)).
2. Verify the partner publishes the expected service records for the TAI-FQDN / APN-FQDN.

SGs Interface — CS Fallback & SMS-over-SGs

The **SGs interface** connects the MME to a 2G/3G **Mobile Switching Centre / Visitor Location Register (MSC/VLR)** so that LTE subscribers can use circuit-switched (CS) services that the EPS packet core does not provide natively:

- **CS Fallback (CSFB) voice** — when an LTE subscriber makes or receives a voice call, the MME redirects the UE to 2G/3G for the call.
- **SMS-over-SGs** — short messages are relayed between the UE and the MSC over the SGs interface, with no packet-switched SMS path required.

The interface is defined in [3GPP TS 29.118](#) (SGsAP protocol) and the procedures in [3GPP TS 23.272](#) (CS Fallback).

Optional and disabled by default. The SGs interface is inert unless explicitly configured. With no `:sgs` configuration the MME never connects to an MSC, never advertises CS availability to UEs, and behaves exactly as a packet-only MME. CS Fallback *voice* has its own separate switch (`csfb_enabled`) that is also off by default, so SMS-over-SGs can be run without enabling voice fallback.

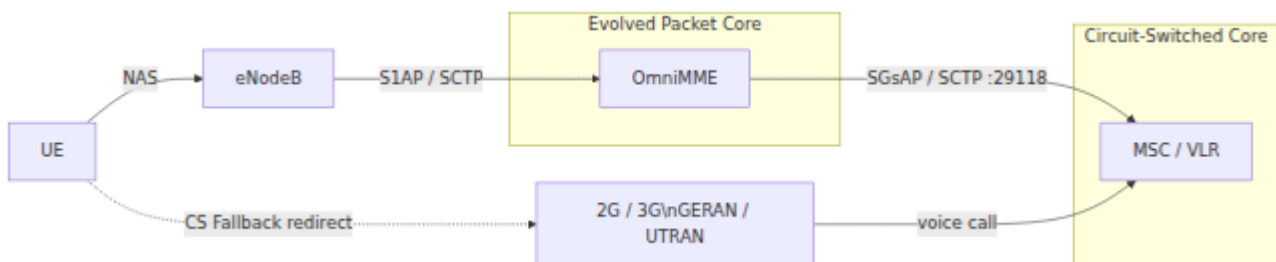
Table of Contents

- [Architecture](#)
- [Association Management](#)
- [Combined Attach and TAU](#)
- [SMS over SGs](#)
- [Mobile-Terminated CS Call \(Paging\)](#)
- [CS Fallback Voice Redirect](#)
- [Configuration](#)

- Metrics
- Troubleshooting

Architecture

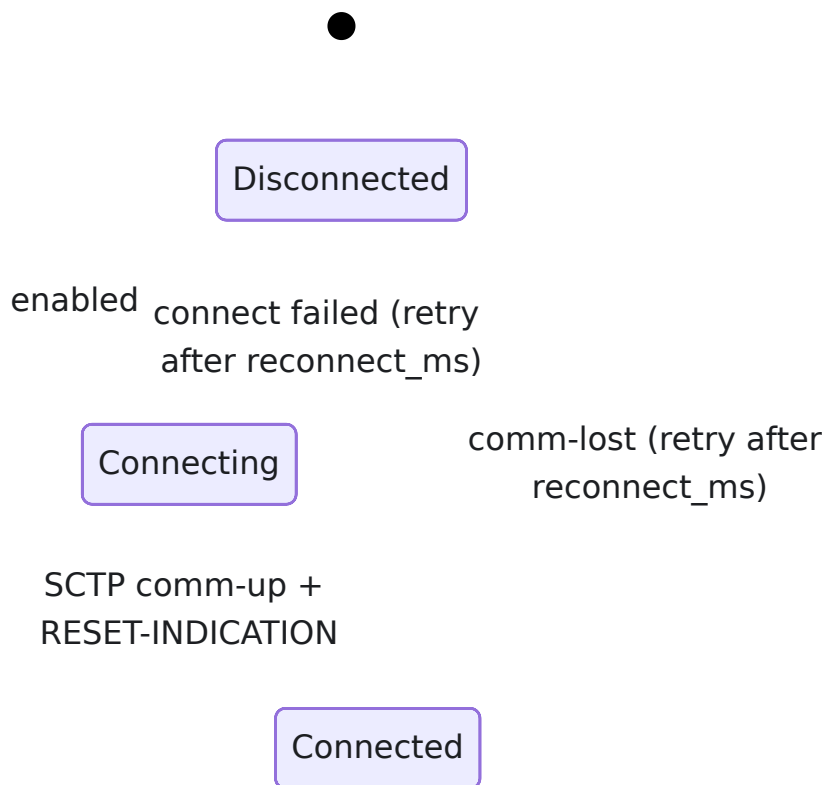
The MME is the **SCTP client** on the SGs interface: it connects *out* to the MSC/VLR (default port **29118**) and maintains a single SCTP association, re-connecting automatically if the association drops.



Element	Role
MME	SCTP client; sends location updates, paging responses, SMS and CSFB indications to the MSC; relays SMS to the UE
MSC / VLR	SCTP server; holds the UE's CS registration; pages for MT calls; sends MT SMS
eNodeB	Carries NAS between UE and MME; performs the radio redirect to 2G/3G on a CS Fallback request

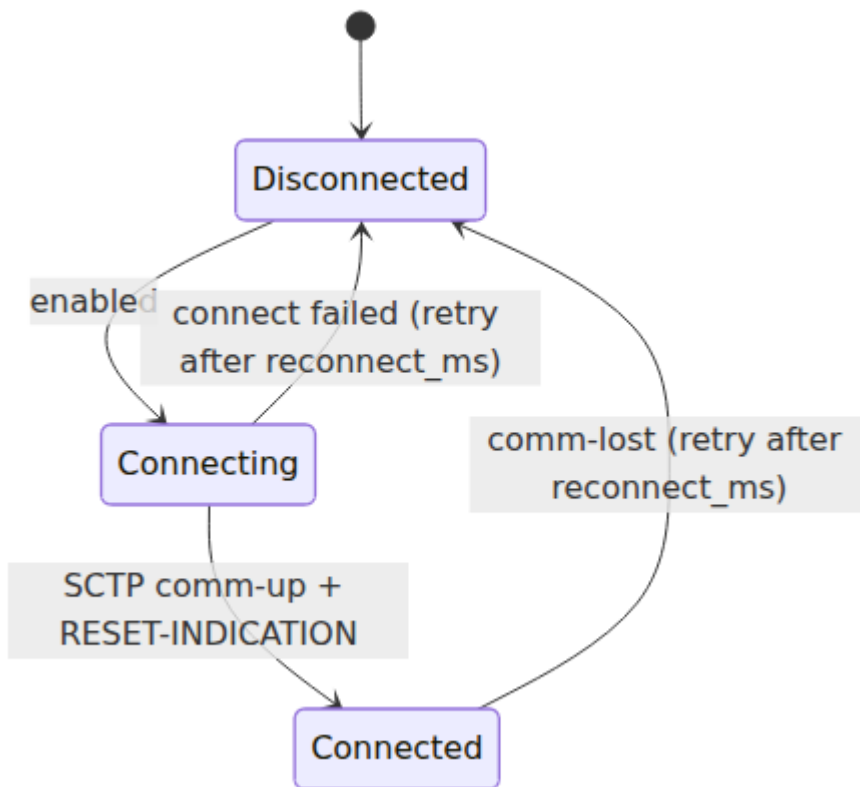
Association Management

On startup (when enabled) the MME connects to the configured MSC and, once the SCTP association comes up, sends an SGsAP **RESET-INDICATION** so the MSC clears any stale state from a previous MME incarnation ([TS 29.118 §8.20](#)). If the association drops, the MME retries on the `reconnect_ms` interval.



Combined Attach and TAU

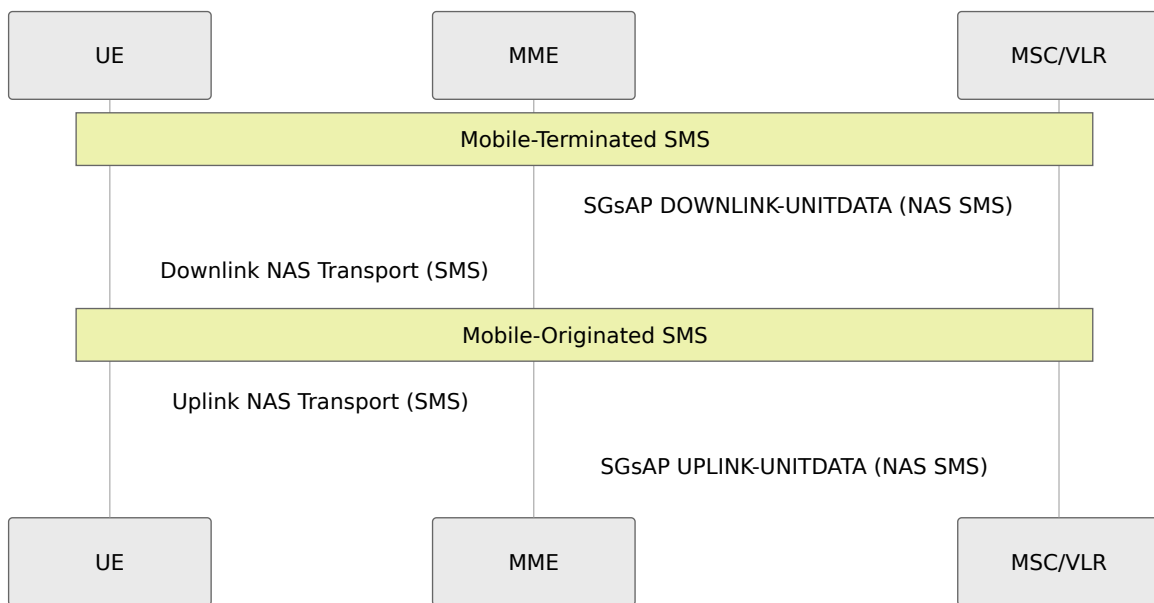
When a UE performs a **combined EPS/IMSI attach** (or combined TAU), it is requesting both packet (EPS) and circuit-switched registration. With SGs enabled, the MME registers the subscriber with the MSC via a **LOCATION-UPDATE-REQUEST** and only grants the combined result once the MSC accepts:



If the MSC **rejects** the location update, or does not respond within `lu_timeout_ms`, the MME falls back to an **EPS-only** Attach Accept — the packet attach is never delayed or blocked by a slow or unavailable MSC. The combined result is honest: the UE is told CS is available only when it genuinely is.

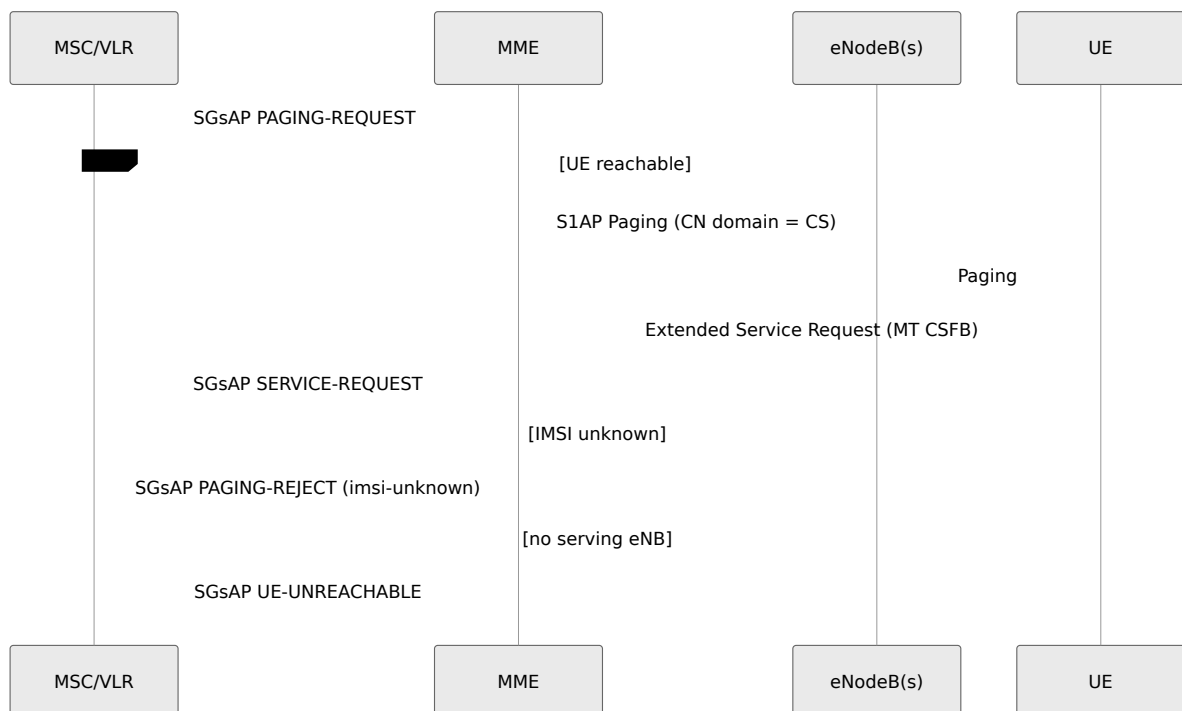
SMS over SGs

Short messages are carried transparently between the UE and the MSC inside SGsAP unitdata messages; the MME relays the NAS payload in each direction.



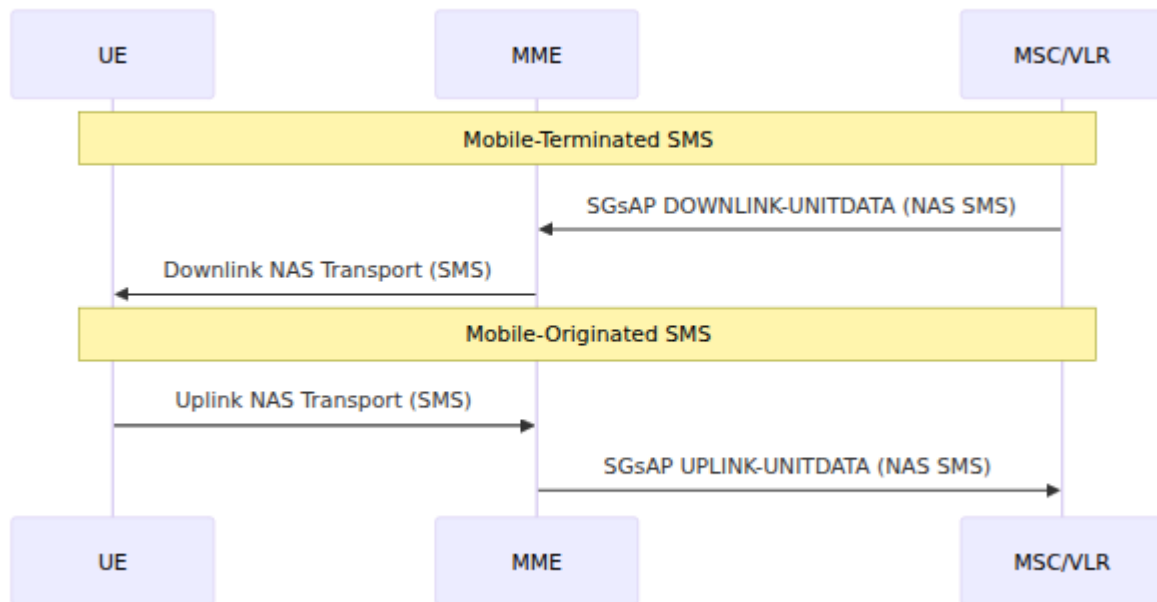
Mobile-Terminated CS Call (Paging)

When the MSC needs to deliver a CS call (or SMS) to an idle UE, it pages over SGs. The MME pages the UE for the **CS domain** across the eNodeBs serving the UE's registered Tracking Area list. If the UE cannot be reached, the MME tells the MSC.



CS Fallback Voice Redirect

CS Fallback voice is gated by the **separate** `csfb_enabled` switch (default off). When enabled, an **Extended Service Request** from a registered UE causes the MME to notify the MSC over SGs and instruct the eNodeB — via an S1AP **UE Context Modification** carrying the **CS Fallback Indicator** — to redirect the UE to 2G/3G for the call.



When `csfb_enabled` is off, or the UE is not SGs-associated, the MME answers the Extended Service Request with a **Service Reject** — the same behaviour as a packet-only MME.

Configuration

The SGs interface is configured under the `:sgs` key in `runtime.exs`. The entire block is optional; omit it to disable the interface.

```
config :mme, :sgs,  
  # Master switch for the SGs interface  
  enabled: true,  
  
  # CS Fallback voice – separate switch, off by default  
  csfb_enabled: false,  
  
  # MSC / VLR connection (the MME connects out to this)  
  vlr_ip: "10.0.0.10",  
  vlr_port: 29118,  
  
  # MME identity advertised to the MSC  
  mme_name: "mmec01.mmegi8001.mme.mnc001.mcc001.3gppnetwork.org",  
  
  # Timers  
  reconnect_ms: 5_000,  
  lu_timeout_ms: 4_000
```

Parameters

Parameter	Type	Required	Default	Description
<code>enabled</code>	Boolean	No	<code>false</code>	Master switch for the SGs interface. When <code>false</code> (or the <code>:sgs</code> block is absent) the MME never connects to an MSC and behaves as a packet-only MME.
<code>csfb_enabled</code>	Boolean	No	<code>false</code>	Enables CS Fallback voice redirect on an Extended Service Request. Independent of SMS-over-SGs: leave <code>false</code> to run SMS-over-SGs without CS voice fallback. Has no effect unless <code>enabled</code> is <code>true</code> .
<code>vlr_ip</code>	String	Yes (when enabled)	-	IPv4 address of the MSC/VLR the MME connects out to.
<code>vlr_port</code>	Integer	No	<code>29118</code>	SCTP port of the MSC/VLR. The standard SGsAP port is 29118 per TS 29.118 §5.2 .
<code>mme_name</code>	String	No	derived from the	The MME node FQDN advertised in the

Parameter	Type	Required	Default	Description
			node FQDN	SGsAP MME Name IE (TS 29.118 §9.4.13). Must be ≤ 55 octets. When omitted, it is derived from the configured MME name / GUMMEI.
local_ip	String	No	the S1AP listen IP	Local IPv4 address the MME binds for the outbound SGs association. Defaults to the S1AP listen IP.
reconnect_ms	Integer	No	5000	Interval, in milliseconds, between SCTP re-connection attempts after a failed or dropped association.
lu_timeout_ms	Integer	No	4000	Maximum time, in milliseconds, a combined attach waits for the MSC's LOCATION-UPDATE-ACCEPT before falling back to an EPS-only Attach Accept. Prevents a slow or absent MSC from stalling the EPS attach.

Examples

Example 1: SMS-over-SGs only (no CS voice)

```
config :mme, :sgs,  
  enabled: true,  
  csfb_enabled: false,  
  vlr_ip: "10.0.0.10",  
  mme_name: "mmec01.mmegi8001.mme.mnc001.mcc001.3gppnetwork.org"
```

How it works: The MME registers combined-attach UEs with the MSC and relays SMS in both directions, but answers any voice CS Fallback request with a Service Reject.

Use case: Networks that want SMS for LTE subscribers via a legacy MSC but provide voice through VoLTE (or not at all).

Example 2: Full CS Fallback (voice + SMS)

```
config :mme, :sgs,  
  enabled: true,  
  csfb_enabled: true,  
  vlr_ip: "10.0.0.10",  
  vlr_port: 29118,  
  mme_name: "mmec01.mmegi8001.mme.mnc001.mcc001.3gppnetwork.org",  
  reconnect_ms: 5_000,  
  lu_timeout_ms: 4_000
```

How it works: In addition to SMS, an Extended Service Request triggers a redirect of the UE to 2G/3G for the circuit-switched call, with the MSC notified over SGs.

Use case: LTE networks without VoLTE that rely on 2G/3G for voice.

Metrics

All SGs metrics are exported on the standard Prometheus scrape endpoint.

Metric: `mme_sgs_message_count` **Type:** Counter **Description:** SGsAP messages exchanged with the MSC/VLR. **Labels:**

- `direction` — `inbound` (from MSC) or `outbound` (to MSC)
- `message_type` — the SGsAP message, e.g. `location_update_accept`, `paging_request`, `downlink_unitdata`

Metric: `mme_sgs_procedure_count` **Type:** Counter **Description:** Outcomes of MME-side SGs procedures. **Labels:**

- `procedure` — e.g. `location_update_accept`, `paging_request`, `downlink_unitdata`, `reset_indication`
- `result` — e.g. `associated`, `rejected`, `paged`, `ue_unreachable`, `relayed`, `acked`

Metric: `mme_sgs_association_event_count` **Type:** Counter **Description:** SGs SCTP association lifecycle events. **Labels:**

- `event` — `connect_attempt`, `comm_up`, `comm_lost`, `connect_failed`

Metric: `mme_sgs_association_up` **Type:** Gauge **Description:** Whether the SGs association to the MSC/VLR is currently up (1) or down (0).

Example queries

```
# Is the SGs association up?
mme_sgs_association_up

# Inbound vs outbound SGsAP message rate by type
sum by (direction, message_type) (rate(mme_sgs_message_count[5m]))

# Combined-attach registration success vs reject rate
sum by (result)
(rate(mme_sgs_procedure_count{procedure="location_update_accept"}
[5m]))

# CS pages that found no reachable UE
rate(mme_sgs_procedure_count{result="ue_unreachable"}[15m])

# Association flaps in the last hour
increase(mme_sgs_association_event_count{event="comm_lost"}[1h])
```

Troubleshooting

SGs association never comes up

Symptoms: `mme_sgs_association_up` stays `0`; repeated `connect_failed` events.

Possible causes:

- `vlr_ip` / `vlr_port` incorrect or the MSC is not listening on the SGsAP port
- A firewall is blocking SCTP between the MME and the MSC
- The local bind address is not reachable from the MSC

Resolution:

1. Confirm the MSC is listening for SGsAP (default port 29118) and reachable from the MME.
2. Verify firewall rules permit SCTP between the MME and MSC.
3. Check `vlr_ip`, `vlr_port`, and the local bind address.

Combined attach is granted as EPS-only

Symptoms: UEs requesting combined attach are accepted but told CS is not available.

Possible causes:

- The SGs association is down, so the MME cannot register the UE with the MSC
- The MSC is rejecting the LOCATION-UPDATE-REQUEST (e.g. subscriber not provisioned in the VLR)
- The MSC responds slower than `lu_timeout_ms`

Resolution:

1. Confirm `mme_sgs_association_up` is `1`.
2. Inspect `mme_sgs_procedure_count{procedure="location_update_accept"}` for `rejected` results and check the subscriber's CS provisioning on the MSC.
3. If the MSC is healthy but slow, raise `lu_timeout_ms`.

Voice calls are rejected with "CS service temporarily not available"

Symptoms: Extended Service Requests for voice are answered with a Service Reject.

Possible causes:

- `csfb_enabled` is `false` (the default)
- The UE is not SGs-associated (its combined attach was granted EPS-only)

Resolution:

1. Set `csfb_enabled: true` to enable CS Fallback voice.
2. Confirm the UE completed a combined attach (see the previous section).

