← Overview

OmniAMF Configuration Reference

OmniAMF reads operator configuration from the Elixir application environment under the `:omniamf` key, populated at boot from `config/runtime.exs`. Every runtime key is driven by an environment variable with a built-in default, so a deployment can be tuned entirely through environment variables.

Table of Contents

Example Configuration

```
config :omniamf,
  # SBI HTTP server (produced Namf services)
  sbi_scheme: "http",
  sbi_addr: "127.0.0.5",
  sbi_port: 7777,

  # NRF (registration, heartbeat, discovery)
  nrf_uri: "http://127.0.0.1:7777",

  # Consumed peer NF base URIs (static fallbacks; NRF discovery
preferred)
  ausf_uri: "http://127.0.0.12:7777",
  udm_uri: "http://127.0.0.12:7777",
  smf_uri: "http://127.0.0.4:7777",
  nssf_uri: "http://127.0.0.14:7777",

  # Serving PLMN
  mcc: "999",
  mnc: "70",

  # AMF identity (GUAMI)
  amf_name: "OmniAMF",
  amf_id: %{region_id: 2, set_id: 1, pointer: 0},

  # Observability
  prometheus_metrics_port: 9569,

  # N2 / NGAP (SCTP listener for gNBs)
  ngap_addr: "0.0.0.0",
  ngap_port: 38412,

  # NRF heartbeat cadence
  heartbeat_interval: 10_000,

  # N26 EPS↔5GS interworking with a 4G MME
  n26_enabled: true,
  n26_addr: "0.0.0.0",
  n26_mme_peer: %{ip: "127.0.0.11", port: 2123}
```

SBI Server Parameters

Parameter	Type	Required	Default	Env Var	Descrip
`sbi_scheme`	String	No	`"http"`	`SBI_SCHEME`	URI sche advertis for the S HTTP se
`sbi_addr`	String	No	`"127.0.0.5"`	`SBI_ADDR`	IP addre the SBI H server b to and advertis `Locatio` headers to the NI
`sbi_port`	Integer	No	`7777`	`SBI_PORT`	TCP port SBI HTTP server listens o

NRF and Peer NF Parameters

Peer NF URIs are **static fallbacks**. When `nrf_uri` is configured, OmniAMF prefers NRF service discovery (cached, 60 s TTL) and only falls back to the static URI when discovery is unavailable. Setting a static URI does not disable discovery per NF unless discovery itself is unreachable.

Parameter	Type	Required	Default
`nrf_uri`	String	No	`"http://127.0.0.1:7777"`
`ausf_uri`	String	No	`"http://127.0.0.12:7777"`
`udm_uri`	String	No	`"http://127.0.0.12:7777"`
`smf_uri`	String	No	`"http://127.0.0.4:7777"`
`nssf_uri`	String	No	`"http://127.0.0.14:7777"`
`pcf_uri`	String	No	`"http://127.0.0.7:7777"`

Parameter	Type	Required	Default	
`heartbeat_interval`	Integer (ms)	No	`10000`	

PLMN and AMF Identity Parameters

The **GUAMI** (Globally Unique AMF Identifier) is formed from the serving PLMN (`mcc`/`mnc`) plus the AMF Identifier, which is itself composed of `region_id`, `set_id`, and `pointer`. The GUAMI is advertised in NG Setup and used to allocate the 5G-GUTI to UEs.

Parameter	Type	Required	Default	Env Var	
`mcc`	String	No	`"999"`	`MCC`	
`mnc`	String	No	`"70"`	`MNC`	
`amf_name`	String	No	`"OmniAMF"`	`AMF_NAME`	
`amf_id.region_id`	Integer (8-bit)	No	`2`	`AMF_REGION_ID`	
`amf_id.set_id`	Integer (10-bit)	No	`1`	`AMF_SET_ID`	
`amf_id.pointer`	Integer (6-bit)	No	`0`	`AMF_POINTER`	

Parameter	Type	Required	Default	Env Var	

N2 / NGAP Parameters

Parameter	Type	Required	Default	Env Var	Description
`ngap_addr`	String	No	`"0.0.0.0"`	`NGAP_ADDR`	IP address the SCTP/NGAP listener binds to. Use a specific interface address to restrict which gNBs can connect
`ngap_port`	Integer	No	`38412`	`NGAP_PORT`	SCTP port for NGAP. The well-known port is 38412 per TS 38.412.

N26 Interworking Parameters

The N26 interface enables inter-system mobility between 5GS and EPS by speaking GTPv2-C to a 4G MME (it reuses the S10-style Forward Relocation message set). It is started as a separate GTPv2-C endpoint only when `n26_enabled` is true.

Parameter	Type	Required	Default	Env Var
`n26_enabled`	Boolean	No	`true` (`runtime.exs`)	`N26_ENABLED`
`n26_addr`	String	No	value of `ngap_addr`	`N26_ADDR`
`n26_mme_peer.ip`	String	No	`"127.0.0.11"`	`N26_MME_IP`

Parameter	Type	Required	Default	Env Var
`n26_mme_peer.port`	Integer	No	`2123`	`N26_MME_POR`

The GTPv2-C listener bound by the shared `gtpc` library uses the following, also environment-driven:

Parameter	Type	Required	Default	Env Var	Descriptio
listen IP	String	No	value of `n26_addr` (then `ngap_addr`)	`N26_ADDR` / `NGAP_ADDR`	Local bind address for the N26 GTPv2-C socket.
listen port	Integer	No	`2123`	`N26_PORT`	Local UDP port for the N26 GTPv2-C socket (standard GTP-C port)

Observability Parameters

Parameter	Type	Required	Default	Env Var
`prometheus_metrics_port`	Integer	No	`9569`	`PROMETHEUS_P`

See the Metrics & Monitoring guide for the metrics exposed on this endpoint.

Advanced Parameters (application config)

These keys have sensible defaults and are not wired to environment variables in `runtime.exs`. Set them in application config only when overriding behaviour is required.

Parameter	Type	Default	Des
`relative_amf_capacity`	Integer (0–255)	`255`	Relative A advertise Response at runtim managem Influence balancing
`served_guami_list`	List of maps	`[{plmn_id, amf_id}]` derived from `mcc`/`mnc`/`amf_id`	GUAMI lis serves; vi settable v managem NG Setup advertise GUAMI in (mapped entry's `plmn_id`/ multi-GUA configurat honoured gNB.
`served_nssai`	List of maps	`[{sst:1}, {sst:1,sd:000001}, {sst:2,sd:000002}, {sst:3,sd:000003}]`	S-NSSAIs supports. drive the `SliceSup` advertise Setup Res support it 38.413 §8
`supported_ta_list`	List of maps	`[{tac:1, plmn_list: [{mcc,mnc}]}]`	Tracking a serves. A Setup

Parameter	Type	Default	Des
			`Supporte` is validate list; a gNE matching **rejected** Setup Fail `unknown-` `SNPN`).
`force_null_ciphering`	Boolean	`false`	Default (`f` the AMF's NAS ciphe algorithm also supp preferring falling bac (null) whe not offer N Integrity i the same preferring back to N to force N regardless capabilitie debuggin
`dns_port`	Integer	`53`	UDP/TCP p the N26 S queries de under `n26_dns_` Rarely cha primarily override.

Parameter	Type	Default	Des
`maintenance_mode`	Boolean	`false`	Persisted mode flag the AMF d from the N rejects ne registratio restart). N toggled at the mana rather tha
`n26_selection_method`	Atom	`:dns_lookup`	Target-MM for 5G→4G `:dns_loo` an S-NAPT (service `x` `s10`) on th TAI FQDN 29.303 §5 back to `n` if DNS yie `:static` (other than `:dns_loo` DNS and u `n26_mme_` See Targe discovery.
`n26_dns_servers`	List of maps	`[%{server: "127.0.0.53", domain: "3gppnetwork.org"}]`	DNS resol (in order) NAPTR MN when `n26_sele` is `:dns_l`

Parameter	Type	Default	Des
			entry has (resolver over TCP) (the base network d appended TAI FQDN, `3gppnetw`
`n26_smf_uri`	String	`"http://127.0.0.4:8443"`	SMF inter interwork URL, quer 5G→4G ha the UE's r connectio EBI, PGW-

Structured Config Sub-Fields

Several advanced keys are lists of maps. Their sub-fields and semantics are:

`served_guami_list` - the GUAMIs this AMF serves. Each entry:

Sub-field	Type	Description
`plmn_id.mcc` / `plmn_id.mnc`	String	Serving PLMN of the GUAMI (defaults to top-level `mcc`/`mnc`).
`amf_id.region_id`	Integer (8-bit)	AMF Region ID.
`amf_id.set_id`	Integer (10-bit)	AMF Set ID.
`amf_id.pointer`	Integer (6-bit)	AMF Pointer within the set.

`served_nssai` - the S-NSSAIs this AMF supports. Each entry is a map with **string keys**:

Sub-field	Type	Description
`"sst"`	Integer (0–255)	Slice/Service Type. Standardised values: `1` eMBB, `2` URLLC, `3` MIoT.
`"sd"`	String (6 hex digits)	Optional Slice Differentiator. Omit for an SST-only slice (e.g. `%{"sst" => 1}`).

`supported_ta_list` - the Tracking Areas this AMF serves. Each entry:

Sub-field	Type	Description
`tac`	Integer	Tracking Area Code.
`plmn_list`	List of maps	PLMNs served in this TA; each is `%{mcc: ..., mnc: ...}`.

A gNB's SupportedTAList is matched against this list (a TA matches when both `tac` and one PLMN match). A gNB advertising no matching TA is **rejected** at NG Setup with an NG Setup Failure - see gNB NG Setup rejected.

`n26_dns_servers` - resolvers for N26 S-NAPTR MME discovery. Each entry:

Sub-field	Type	Description
`server`	String	Resolver IP, queried over TCP.
`domain`	String	Base home-network domain appended to the EPS TAI FQDN (e.g. `3gppnetwork.org`).

Management API and Control Panel

OmniAMF exposes an operator management REST API and a web Control Panel over HTTPS. These are configured in application (compiled) config rather than `runtime.exs`; the runtime-relevant knobs are the listen address, ports, and TLS material.

Parameter	Type	Default	Description
management API `port`	Integer	`8443`	HTTPS port for the operator management/statu API (status, UE/gNE inventory, OAM actions).
management API `listen_ip`	String	`"0.0.0.0"`	Bind address for the management API.
management API `enable_tls`	Boolean	`true`	Serve the management API over TLS.
management API `tls_cert_path` / `tls_key_path`	String	`priv/cert/omnitouch.crt` / `.pem`	TLS certificate and private key for the management API.
Control Panel HTTPS `port`	Integer	`7443`	HTTPS port for the web Control Panel UI.

The management API surfaces read-only status (NRF/NF/license status, gNB and UE inventory, per-UE PDU sessions, statistics) and OAM actions (runtime config view/update, cache clear, log level change, maintenance mode, NRF re-registration, diagnostics, and forced UE/PDU/gNB teardown). The full endpoint list, per-action semantics, and preconditions are documented in the Management API guide.

← Overview

OmniAMF Management API

The management (OAM) API is an operator-facing REST interface, separate from the 5G SBI. It exposes read-only status/inventory, statistics, runtime configuration, and OAM control actions (per-UE, per-gNB, NRF, maintenance, and diagnostics). It is served over HTTPS on its own port and is independent of the NGAP and SBI listeners.

Back to the Operations Guide and the Configuration Reference.

Access

Property	Value
Scheme	HTTPS (TLS)
Port	`8443`
Bind address	`0.0.0.0`
Path prefix	`/api`

All responses are JSON wrapped in a standard envelope with a `success` / `error` status. The bind address, port, and TLS material are set in application config (see Management API and Control Panel). A separate web Control Panel UI is served over HTTPS on port `7443`.

Status and Inventory (read-only)

Method	Path	Description
`GET`	`/api/status/api`	Liveness probe.
`GET`	`/api/status/nrf`	NRF registration status: `nrf_status`, `nf_instance_id`, `nrf_uri`.
`GET`	`/api/status/nf`	NF service status: advertised `namf-comm`/`namf-evts` services, `sbi_addr`/`sbi_port`, GUAMI.
`GET`	`/api/status/license`	License status.
`GET`	`/api/gnb`	List connected gNBs (SCTP associations): `gnb_id`, `gnb_name`, `ip`/`port`, `assoc_id`, `sctp_assoc_state`, `connected_since`, `supported_ta_list`, and connected-UE count.
`GET`	`/api/gnb/{id}`	Detail for one gNB by SCTP `assoc_id`. Returns 404 if unknown.

Method	Path	Description
`GET`	`/api/ue`	List UE contexts. Optional query filters: `gnb_id`, `imsi` (substring), `state` (`registered` | `idle` | `connected`). Each entry carries `supi`, `cm_state`, `rm_state`, and `pdu_sessions_count`.
`GET`	`/api/ue/{supi}`	Detail for one UE by SUPI, including security context summary, auth state, and per-session PDU session list. Returns 404 if not found.
`GET`	`/api/ue_pdu_sessions/{supi}`	PDU sessions for one UE by SUPI.
`GET`	`/api/ue_context`	List all active UE contexts. Each entry carries `suci`, `guti`, `tmsi_5g`, `gmm_state`, `allowed_nssai`, a security-context present flag, and creation/last-activity timestamps.
`GET`	`/api/statistics`	Aggregate counts: registered UEs, CM-CONNECTED / CM-IDLE, gNB count, total PDU sessions.

Runtime Configuration

Method	Path	Description
`GET`	`/api/oam/config`	Read current mutable runtime config: `relative_amf_capacity`, `nf_capacity`, `nf_priority`, `amf_name`, `supported_ta_list`, `served_guami_list`, `log_level`.
`PATCH`	`/api/oam/config/{id}`	Update one or more of the above keys. Unknown keys are rejected with 400; invalid values (e.g. an out-of-range capacity or an unknown log level) are rejected before any update is applied.
`POST`	`/api/oam/log_level`	Change the runtime log level. Body: `{"level": "..."}` where `level` is one of `emergency`, `alert`, `critical`, `error`, `warning`, `warn`, `notice`, `info`, `debug`.

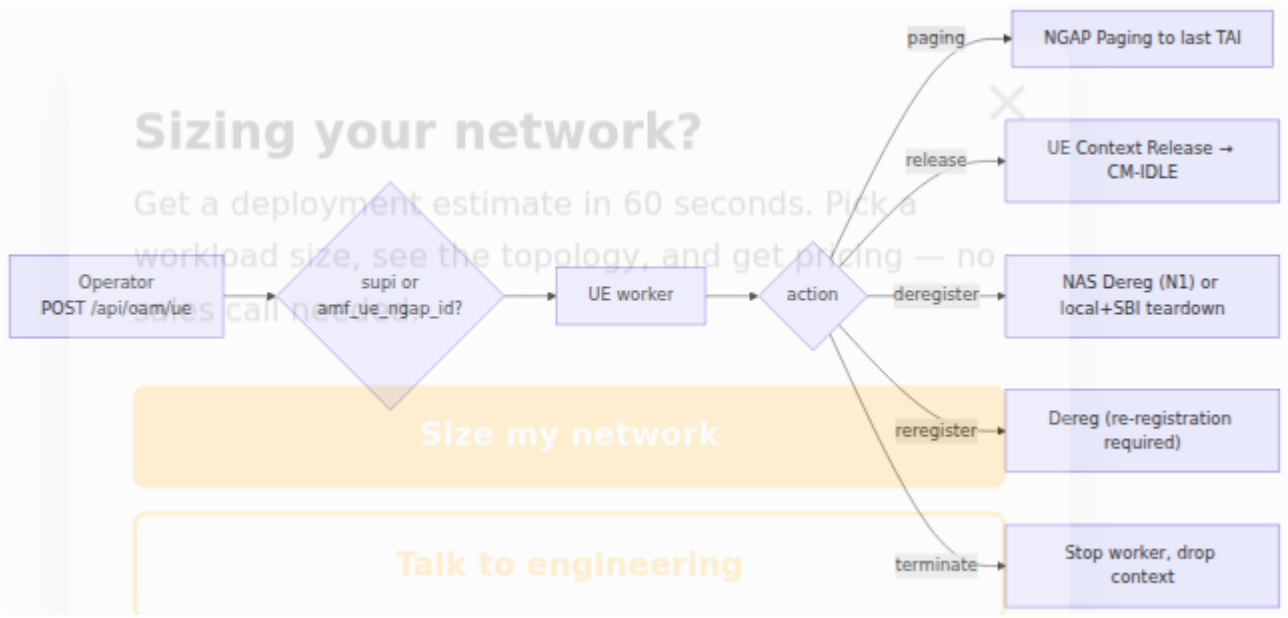
Changing `relative_amf_capacity` affects the value advertised to gNBs and the NRF, influencing how gNBs load-balance across AMFs. See Advanced Parameters.

UE Control Actions

`POST /api/oam/ue` with a JSON body. The target UE is selected by `supi` (a registered UE) **or** `amf_ue_ngap_id` (any live context, including an unauthenticated UE that has no SUPI yet). The `action` field selects the operation:

`action`	Effect	Preconditions
`paging`	Send a real NGAP Paging to the UE's last TAI.	UE must be RM-REGISTERED and CM-IDLE (requires a SUPI).
`release`	AN release: send UE Context Release Command and move the UE to CM-IDLE.	CM-CONNECTED.
`deregister`	Network-initiated deregistration. Sends a NAS Deregistration Request over N1 if CM-CONNECTED, otherwise performs a local + SBI teardown.	none
`reregister`	Force re-attach: deregistration with "re-registration required", so the UE immediately re-registers.	none
`terminate`	Hard purge: stop the UE worker and drop its context (no NAS signalling).	none

A request that violates a precondition (e.g. `paging` a CM-CONNECTED UE) returns `409` with the offending `cm_state`/`rm_state`. An unknown target returns `404`.



The `deregister` / `reregister` semantics (T3522, explicit vs implicit, security-context retention) are described in the operations guide under Deregistration.

UE Resource (REST verbs)

In addition to the action-oriented `POST /api/oam/ue`, the UE and UE-context resources expose direct REST verbs.

Method	Path	Description
`DELETE`	`/api/ue/{supi}`	Deregister a single UE and release its context. This is the REST verb on the UE resource; it performs the same teardown as the `deregister` OAM action (NAS Deregistration Request over N1 if CM-CONNECTED, otherwise local + SBI teardown). Returns 404 if the SUPI is unknown.
`DELETE`	`/api/ue_context`	**Destructive.** Clears **all** UE contexts at once. Every live UE must re-register.

The bulk `DELETE /api/ue_context` overlaps with the UE-context teardown performed by `POST /api/oam/cache/clear`; the difference is that the cache-

clear endpoint also invalidates the NF discovery cache, whereas `DELETE /api/ue_context` only drops UE contexts. Use either with care in production.

gNB Control Actions

`DELETE /api/oam/gnb/{id}` where `{id}` is the SCTP `assoc_id` from `GET /api/gnb`. The `action` query/body parameter selects the operation:

`action`	Effect
(none) / `disconnect`	SCTP ABORT the association: a hard disconnect.
`ng_reset`	Send an NGReset (reset-all) to the gNB.
`deregister_subscribers`	Terminate every UE context currently served by that gNB.

Unknown `assoc_id` returns `404`.

PDU Session Control

Method	Path	Description
`DELETE`	`/api/oam/pdu_session/{id}`	Force-release a single PDU session. `{id}` is `supi:psi`, e.g. `imsi-999700000000001:1`. A malformed id or unknown PSI returns 400; an unknown UE returns 404.

Maintenance Mode

Maintenance mode deregisters the AMF from the NRF and rejects new UE registrations, allowing it to be drained before a restart.

Method	Path	Description
`GET`	`/api/oam/maintenance`	Report current maintenance state.
`POST`	`/api/oam/maintenance`	Enter maintenance mode: deregister from NRF, reject new registrations.
`DELETE`	`/api/oam/maintenance/{id}`	Exit maintenance mode: re-register with the NRF.

NRF and Cache Control

Method	Path	Description
`POST`	`/api/oam/nrf/reregister`	Force an immediate NRF re-registration; returns the resulting `nrf_status` and `nf_instance_id`.
`GET`	`/api/oam/nrf_discovery`	List the current NF discovery cache entries with `nf_type`, resolved `uri`, and `ttl_remaining_seconds`, plus whether discovery is enabled.
`POST`	`/api/oam/cache/clear`	Clear all internal caches: invalidate the NF discovery cache and drop all UE contexts. Returns the number of contexts cleared.
`GET`	`/api/oam/peers`	View resolved peer NF URIs (AUSF/UDM/SMF/PCF/NSSF/NRF) alongside the current SCTP association list.

Clearing the NF discovery cache forces the next SBI call to re-resolve peers via the NRF. Clearing UE contexts is destructive: live UEs must re-register. See NF discovery.

Diagnostics

Method	Path	Description
`GET`	`/api/oam/resources`	BEAM resource snapshot: process/port counts and limits, scheduler count, uptime, OTP/BEAM versions.
`GET`	`/api/oam/diagnostics`	Node diagnostics: uptime, connected nodes, process count, run-queue length, cumulative I/O bytes, and GC statistics.

These complement the Prometheus metrics endpoint for point-in-time inspection during an incident.

← Overview

OmniAMF Metrics

Metrics are exposed on the `/metrics` endpoint at `prometheus_metrics_port` (default `9569`). Only the metrics below are registered with the Prometheus exporter.

Table of Contents

Registration and Authentication

Metric: `omni_amf_registration_requests_count` **Type**: Counter **Description**: Registration requests received, by registration type. **Labels**: `type`: registration type (e.g. initial, mobility, periodic).

```
sum by (type) (rate(omni_amf_registration_requests_count[5m]))
```

Metric: `omni_amf_registrations_total` **Type**: Counter **Description**: Registration procedure outcomes. **Labels**: `result`: e.g. `success`, `failure`.

```
sum(rate(omni_amf_registrations_total{result="failure"}[5m]))
  / sum(rate(omni_amf_registrations_total[5m]))
```

Metric: `omni_amf_auth_requests_count` **Type**: Counter **Description**: Authentication requests initiated. **Labels**: none.

```
sum(rate(omni_amf_auth_requests_count[15m]))
```

Metric: `omni_amf_authentications_total` **Type**: Counter **Description**: Authentication procedure outcomes. **Labels**: `result`.

```
sum by (result) (rate(omni_amf_authentications_total[5m]))
```

Service Requests and PDU Sessions

Metric: `omni_amf_service_requests_total` **Type**: Counter **Description**: Service Request procedure outcomes. **Labels**: `result`.

```
sum by (result) (rate(omni_amf_service_requests_total[5m]))
```

Metric: `omni_amf_pdu_session_requests_count` **Type**: Counter **Description**: PDU session requests relayed, by session identifier. **Labels**: `pdu_session_id`: PDU session identifier (bounded, `0`-`15`).

```
sum by (pdu_session_id)
(rate(omni_amf_pdu_session_requests_count[5m]))
```

Metric: `omni_amf_pdu_session_requests_total` **Type**: Counter **Description**: PDU session establishment request outcomes. **Labels**: `result`.

```
sum by (result) (rate(omni_amf_pdu_session_requests_total[5m]))
```

NGAP and SCTP

Metric: `omni_amf_ngap_messages_total` **Type**: Counter **Description**: NGAP messages handled, by procedure. **Labels**: `procedure`: e.g. `ng_setup_request`, `initial_ue_message`.

```
topk(10, sum by (procedure)
(rate(omni_amf_ngap_messages_total[5m])))
```

Metric: `omni_amf_sctp_associations_count` **Type**: Gauge **Description**: Active SCTP (N2) associations from gNBs. Emitted whenever a gNB association comes up or is torn down, and re-sampled periodically. **Labels**: none.

```
omni_amf_sctp_associations_count
```

UE State

Metric: `omni_amf_connected_ues_count` **Type**: Gauge **Description**: Number of connected UEs. Emitted on UE context setup and release, and re-sampled periodically. **Labels**: none.

Metric: `omni_amf_cm_connected_ues_count` **Type**: Gauge **Description**: Number of UEs in CM-CONNECTED state. Emitted on UE context setup and release, and re-sampled periodically. **Labels**: none.

```
omni_amf_cm_connected_ues_count
```

NRF Registration

Metric: `omni_amf_nrf_registration_status` **Type**: Gauge **Description**: NRF registration status (`1` = registered, `0` = not registered). **Labels**: `nf_type`.

```
min(omni_amf_nrf_registration_status)
```

BEAM VM

The runtime also exports BEAM VM gauges for capacity monitoring: `beam_memory_total`, `beam_memory_processes`, `beam_memory_processes_used`, `beam_memory_system`, `beam_memory_atom`, `beam_memory_atom_used`, `beam_memory_binary`, `beam_memory_code`, `beam_memory_ets`, `beam_processes_count`, `beam_ports_count`, `beam_atom_count`, and `beam_vm_uptime` (seconds).

```
beam_memory_total
rate(beam_vm_uptime[5m])  # 0 indicates a restart within the
window
```

← Overview

OmniAMF Operations Guide

OmniAMF is the mobility and connection anchor for every UE in the 5G Core. It accepts SCTP/NGAP associations from gNBs on the N2 interface, terminates NAS (N1) signalling relayed inside NGAP, and coordinates with peer NFs over the SBI to authenticate the UE, retrieve subscription data, select slices, and manage PDU sessions.

Table of Contents

- NGAP Procedures Summary
- 5GMM Timer Reference

Concurrency Model

Each UE is handled by a dedicated `UeWorker` process supervised under a UE supervisor. NGAP messages are demultiplexed by NGAP UE identifiers to the owning worker, so UE state machines run in isolation. A separate ETS-backed **GUTI Context Store** persists each UE's native 5G NAS security context (SUPI, K_AMF, NAS counts, security capabilities) keyed by 5G-TMSI, independent of worker lifetime. This survives worker churn and lets a UE returning from idle mode resume without re-authentication.

The overall component architecture is shown in the Architecture Overview on the landing page.

3GPP Role and Specification

References

Aspect	Reference
AMF functional definition	TS 23.501 §6.2.1
System procedures (registration, service request, handover, interworking)	TS 23.502
Registration procedure (NAS)	TS 24.501 §5.5.1
Deregistration procedure	TS 24.501 §5.5.2
Service Request procedure	TS 24.501 §5.6.1
Security Mode Control (NAS SMC)	TS 24.501 §5.4.2
NAS message coding	TS 24.501 §8
NAS/IEI encoding rules (Type-1/3/4 IEs)	TS 24.007
Authentication (5G-AKA)	TS 33.501 §6.1.3
Key derivation (K_AMF, K_NASint/enc, K_gNB, NH)	TS 33.501 Annex A
NGAP (N2) application protocol	TS 38.413
NGAP transport (SCTP, PPID 60, port 38412)	TS 38.412
Namf_Communication / Namf_EventExposure	TS 29.518
N26 (EPS↔5GS interworking, GTPv2-C)	TS 23.502 §4.11, TS 29.518
AUSF service (Nausf)	TS 29.509
UDM services (Nudm)	TS 29.503

Aspect	Reference
NSSF service (Nnssf)	TS 29.531
SMF service (Nsmf)	TS 29.502
PCF AM policy (Npcf_AMPolicyControl)	TS 29.507
NRF discovery/registration (Nnrf)	TS 29.510
S-NAPTR MME discovery (N26)	TS 29.303

Interfaces

Interface	Peer	Transport	Purpose
N1	UE (relayed via gNB)	NAS-in-NGAP	UE mobility management and session management NAS signalling (TS 24.501)
N2	gNB	SCTP / NGAP	NG Setup, UE context management, NAS transport, paging, handover (TS 38.413)
N8	UDM	SBI (HTTP/2)	Subscriber data (Nudm_SDM) and UE context registration (Nudm_UECM)
N11	SMF	SBI	PDU session create/update/release; N1N2 message transfer from SMF
N12	AUSF	SBI	UE authentication (5G-AKA), Nausf_UEAuthentication
N15	PCF	SBI	Access & Mobility policy association (Npcf_AMPolicyControl)
N22	NSSF	SBI	Network slice selection (Nnssf_NSSelection)
N26	4G MME	GTPv2-C (UDP 2123)	EPS↔5GS interworking / inter-system handover (optional)
Nnrf	NRF	SBI	NF registration, heartbeat, service discovery

SBI Endpoints

OmniAMF **produces** the `namf-comm/v1` and `namf-evts/v1` services and **consumes** `nausf-auth/v1`, `nudm-sdm/v2`, `nudm-uecm/v1`, `nnssf-nsselection/v2`, `nsmf-pdusession/v1`, and `npcf-am-policy-control/v1`. It also advertises `namf-callback/v1` notification URIs (SDM data-change notify, AM policy notify, SM context status notify) to peer NFs when creating those subscriptions. Produced endpoints are served on the SBI HTTP server (`sbi_addr:sbi_port`). Requests and responses use `application/json`; N1/N2 binary content is carried as `multipart/related` per TS 29.518 §6.

Namf_Communication (TS 29.518)

Method	Path	Description	Su
POST	`/namf-comm/v1/ue-contexts/{ueContextId}/n1-n2-messages`	N1N2 message transfer from SMF	200 (deli / 20 Acce (pag `Loca` set)
POST	`/namf-comm/v1/ue-contexts/{ueContextId}/transfer`	UE context transfer (inter-AMF); may return multipart N2 info	200
POST	`/namf-comm/v1/ue-contexts/{ueContextId}/transfer-update`	Registration status update (post context transfer)	200
POST	`/namf-comm/v1/ue-contexts/{ueContextId}/assign-ebi`	EPS Bearer ID assignment	200
POST	`/namf-comm/v1/ue-contexts/{ueContextId}/release`	UE context release	204 Cont
POST	`/namf-comm/v1/non-ue-n2-messages/transfer`	Non-UE N2 message transfer (e.g. PWS)	200
POST	`/namf-comm/v1/subscriptions`	AMF status change	201 Crea

Method	Path	Description	Su
		subscribe	(Loc set)
PUT	`/namf-comm/v1/subscriptions/{subscriptionId}`	AMF status change subscription modify	200
DELETE	`/namf-comm/v1/subscriptions/{subscriptionId}`	AMF status change unsubscribe	204 Cont

Namf_EventExposure (TS 29.518)

Method	Path	Description	Su
POST	`/namf-evts/v1/subscriptions`	Subscribe to AMF events	201 Crea (Loc set)
PATCH	`/namf-evts/v1/subscriptions/{subscriptionId}`	Modify subscription (RFC 6902 JSON Patch)	200
DELETE	`/namf-evts/v1/subscriptions/{subscriptionId}`	Unsubscribe	204 Cont

Unmatched paths return a `404` RFC 7807 problem document.

N2 / NGAP (non-SBI)

Transport	Address	Description
SCTP	`{ngap_addr}:{ngap_port}` (default `0.0.0.0:38412`)	NGAP messages from gNBs, PPID 60 per TS 38.412

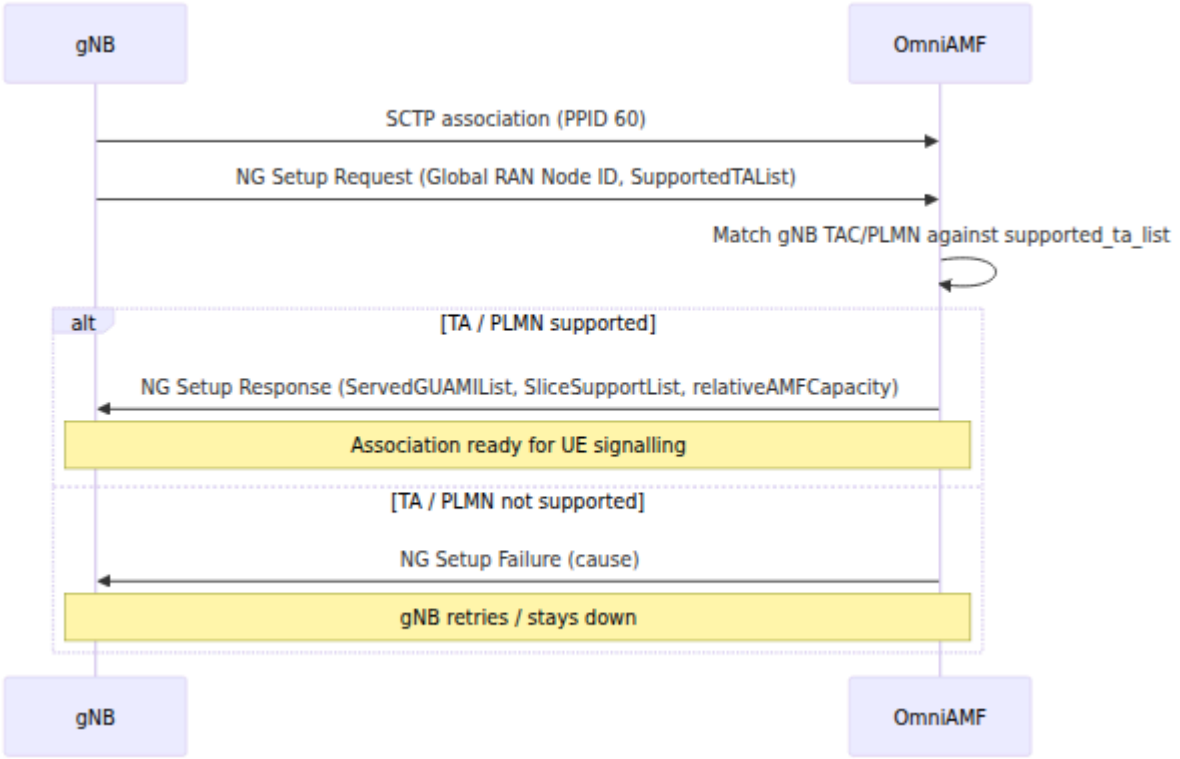
Key Procedures

NG Setup (gNB Association Bring-Up)

NG Setup is the first NGAP exchange over a newly established SCTP association. The gNB presents its `Global RAN Node ID`, `RAN Node Name`, and `SupportedTAList` (TAC plus the broadcast PLMN and slice list per TA). The AMF validates the gNB's TA and PLMN against its configured `supported_ta_list`. On a match it returns an **NG Setup Response** advertising itself to the gNB; on a mismatch it returns an **NG Setup Failure** and the association never carries UE traffic (TS 38.413 §8.7.1).

The NG Setup Response carries:

Element	Source	Meaning
`ServedGUAMIList`	`served_guami_list`	The full set of GUAMIs this AMF serves (PLMN + AMF Region/Set/Pointer).
PLMN Support Item `SliceSupportList`	derived from `served_nssai`	The S-NSSAIs (SST, optional SD) the AMF supports for each served PLMN.
`relativeAMFCapacity`	`relative_amf_capacity`	Weighting the gNB uses to load-balance UEs across AMFs in the set.



If a gNB persistently receives NG Setup Failure, align `supported_ta_list` with the gNB's TAC/PLMN. See gNB NG Setup rejected (TA / PLMN mismatch).

Initial UE Registration (with 5G-AKA)

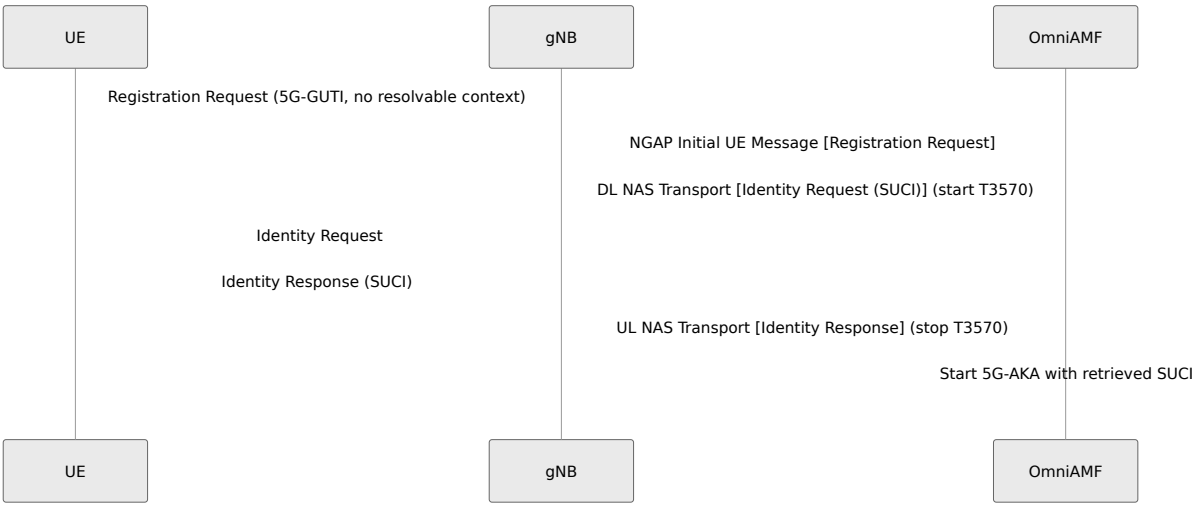
Parse error on line 19: ...AND ‖ RES*)[0..127];
compare to AUSF ----------
----------^ Expecting 'SPACE', 'NEWLINE', 'create', 'box', 'end', 'autonumber',
'activate', 'deactivate', 'title', 'legacy_title', 'acc_title', 'acc_descr',
'acc_descr_multiline_value', 'loop', 'rect', 'opt', 'alt', 'par', 'par_over', 'critical',
'break', 'option', 'and', 'else', 'participant', 'participant_actor', 'destroy', 'note',
'links', 'link', 'properties', 'details', 'ACTOR', got 'INVALID'

Try again

On the Authentication Response the AMF first performs a local **HRES*** check: it computes `HRES* = SHA-256(RAND ‖ RES*)` truncated to the leftmost 128 bits and compares it to the `hxresStar` returned by the AUSF (TS 33.501 §6.1.3.2). Only on a match does it forward the RES* in the 5G-AKA confirmation; a mismatch is treated as an authentication failure. If the UE instead returns a NAS **Authentication Failure** with cause `#21` (Synch failure), the AMF runs the SQN Resynchronization procedure rather than rejecting. On any other authentication failure or rejection, the AMF sends a NAS **Registration Reject** with the appropriate 5GMM cause to the UE.

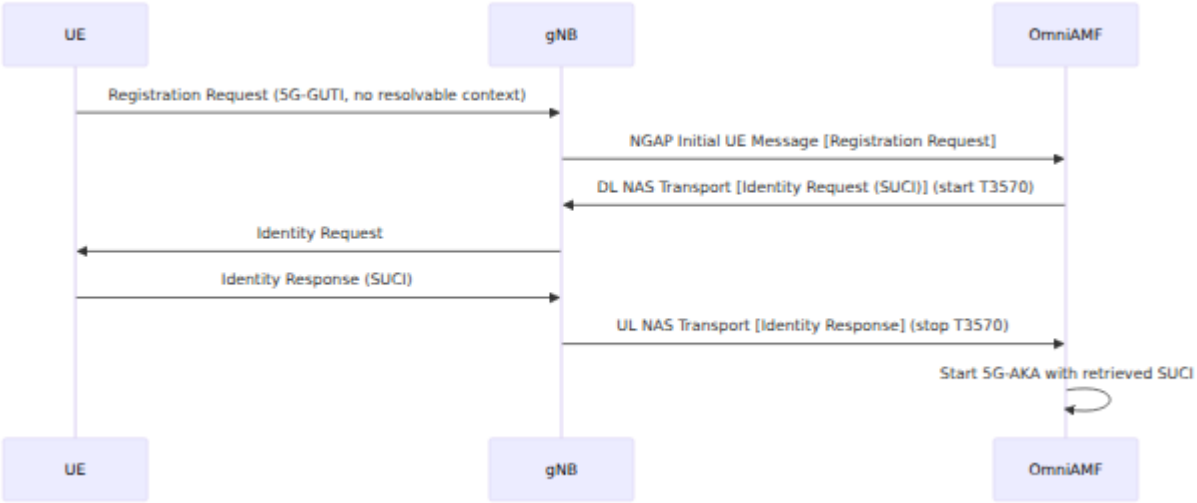
Identity Request / Response (SUCI Retrieval)

When a UE presents a 5G-GUTI the AMF cannot resolve to a stored context (for example after an AMF restart), the AMF must obtain the UE's concealed permanent identity before it can authenticate. It sends a NAS **Identity Request** with identity type `SUCI`; the UE answers with an **Identity Response** carrying the SUCI, which the AMF then uses to start 5G-AKA. The request is guarded by timer T3570 and retransmitted on expiry up to the retry limit (TS 24.501 §5.4.3).



SQN Resynchronization (AUTS)

If the UE detects that the AUTN sequence number is out of range it rejects the challenge with a NAS **Authentication Failure**, 5GMM cause `#21` (Synch failure), carrying a 14-byte **AUTS** parameter. Rather than failing the registration, the AMF parses the AUTS and re-requests authentication vectors from the AUSF, adding a `resynchronizationInfo` object (the original `RAND` plus the `AUTS`) to the `Nausf_UEAuthentication` request. The home network (AUSF/UDM/ARPF) uses the AUTS to recover the UE's SQN and returns a fresh vector, and the AMF re-issues the Authentication Request (TS 33.501 §6.1.3.4).



If resynchronization still does not yield a UE-accepted challenge, the AMF falls back to sending a Registration Reject.

Allowed NSSAI Computation

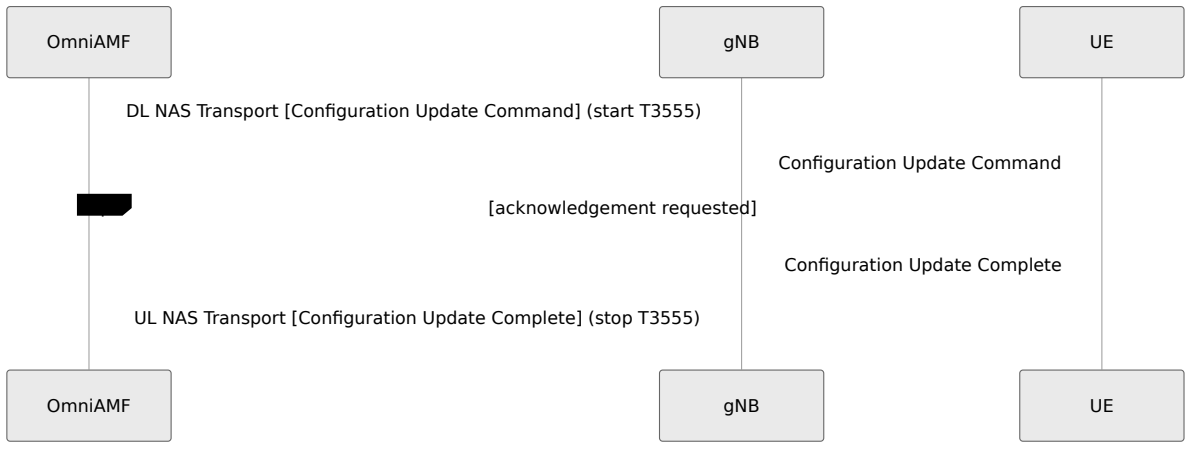
The **Allowed NSSAI** returned in the Registration Accept is not simply echoed back from the UE. The AMF computes it as the intersection of three sets:

1. the **Requested NSSAI** the UE included in the Registration Request,
2. the **Subscribed S-NSSAIs** retrieved from the UDM (`nudm-sdm/v2/{supi}/nssai`), and
3. the AMF's own configured **`served_nssai`**.

The resulting slices (with default-slice handling) are encoded per TS 24.501 §9.11.3.37. If the intersection is empty (the UE requests only slices that are neither subscribed nor served), the AMF rejects the registration with the appropriate 5GMM cause rather than accepting with no usable slice. Slice-selection consultation with the NSSF (Nnssf_NSSelection) may further refine the result where configured.

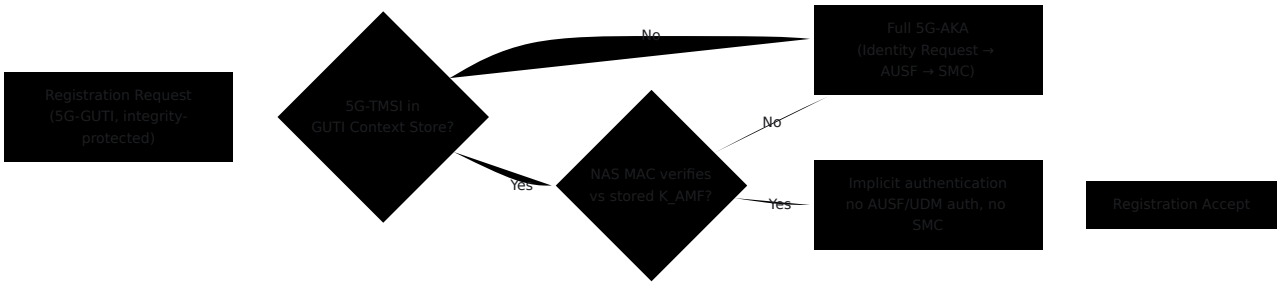
Configuration Update Command

The AMF can push updated UE configuration (new 5G-GUTI, updated Allowed/Configured NSSAI, TAI list, network name/time, or a request to re-register) at any time while the UE is CM-CONNECTED, using a NAS **Configuration Update Command**. When the command sets the acknowledgement-requested flag the UE replies with a **Configuration Update Complete**; the command is guarded by timer T3555 and retransmitted on expiry up to the retry limit (TS 24.501 §5.4.4). This is the mechanism behind a network-triggered GUTI reallocation and behind the `reregister` OAM action's "re-registration required" path.



GUTI Resume (Idle-Mode Fast-Path)

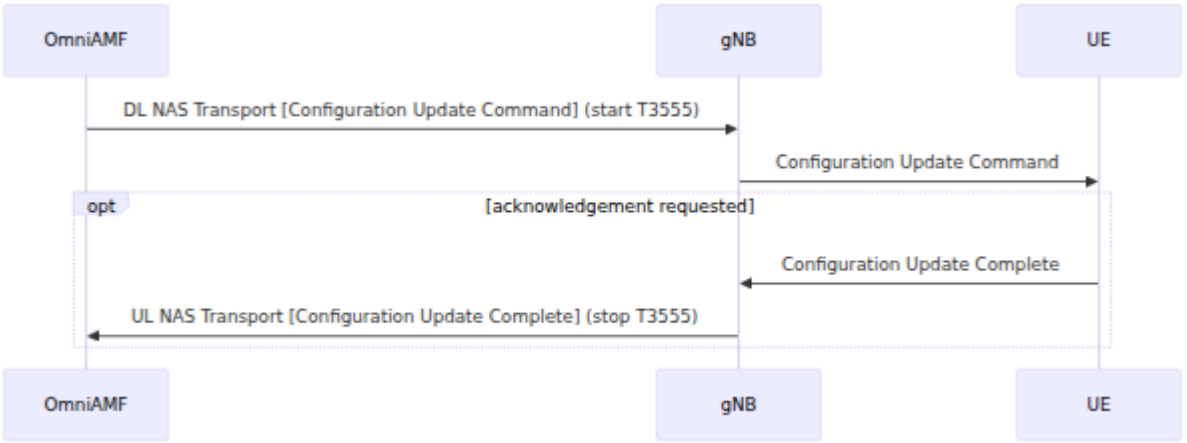
When a registered UE goes CM-IDLE and later returns, it identifies with its 5G-GUTI rather than a SUCI. OmniAMF looks up the stored native security context by 5G-TMSI and verifies the integrity (MAC) of the mobility Registration Request against the re-derived NAS keys.



This avoids a full re-authentication round trip (per TS 24.501 §5.5.1.3 / TS 33.501 §6.4.3) and prevents idle-mode flap on flaky radio, where the longer procedure frequently drops mid-flight.

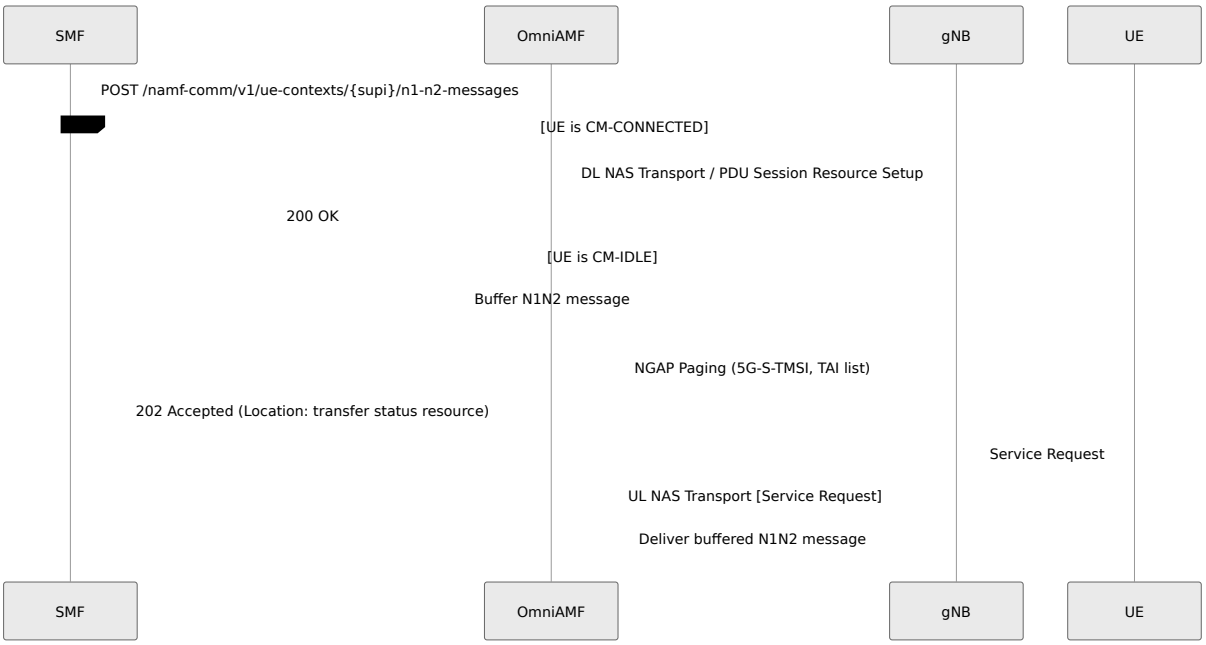
PDU Session Establishment Relay (N11)

The AMF relays 5GSM NAS between the UE and the SMF and drives the corresponding N2 resource setup toward the gNB.



The AMF's Uplink NAS Transport parser is IEI-aware per TS 24.007: the **PDU Session ID** and **Request Type** IEs are Type-3 (TV, no length octet). Correct tokenization keeps concurrent PDU sessions distinct, which matters for a UE bringing up both `internet` and `ims` (VoNR), where mis-parsing the PDU Session ID as a TLV would collapse all sessions onto one PSI.

N1N2 Message Transfer and Paging



Per TS 29.518 §5.2.2.3.2, the CM-IDLE case returns **202 Accepted** with a `Location` header pointing at the created N1N2 transfer status resource, and paging is sent as NGAP Paging to every gNB serving the UE's TAI list. Paging is retransmitted on the T3513 timer up to the retry limit, after which a paging-failure event is raised.

Service Request (User-Plane Reactivation)

When a CM-IDLE registered UE has uplink data or responds to paging, it sends a Service Request. The AMF re-establishes AS security (re-derives K_gNB / NH from the stored K_AMF), delivers any buffered N1N2 messages, and asks the SMF to reactivate the user plane for each active PDU session so the DRB/N3 tunnel is rebuilt (TS 23.502 §4.2.3.2).

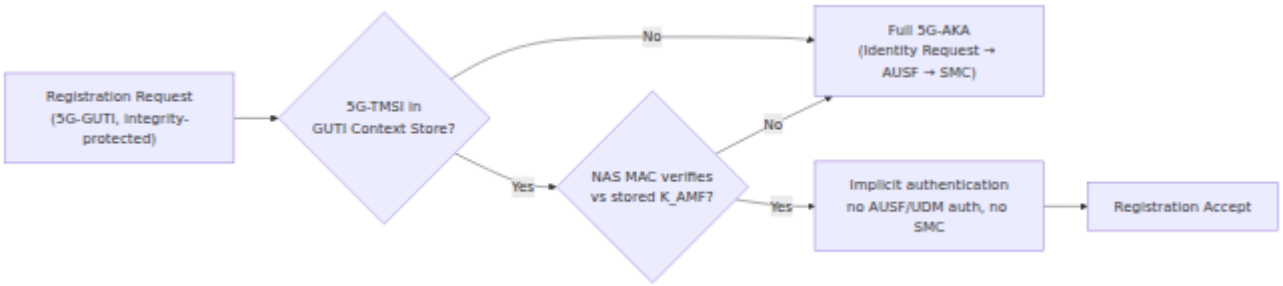
Parse error on line 9: ...ext; re-derive K_gNB, NH AMF->>gNB: ---------- --^ Expecting 'SOLID_OPEN_ARROW', 'DOTTED_OPEN_ARROW', 'SOLID_ARROW', 'BIDIRECTIONAL_SOLID_ARROW', 'DOTTED_ARROW', 'BIDIRECTIONAL_DOTTED_ARROW', 'SOLID_CROSS', 'DOTTED_CROSS', 'SOLID_POINT', 'DOTTED_POINT', got ','

Try again

If the UE is not RM-REGISTERED, the AMF returns a **Service Reject** (5GMM cause `#9` UE identity cannot be derived) to force re-registration with a SUCI.

Deregistration

Deregistration can be UE-initiated or network-initiated (via the management/OAM API). Network-initiated deregistration is `:explicit` (or `:reregistration_required`) when the UE is CM-CONNECTED (a NAS Deregistration Request is sent under T3522); otherwise it falls back to an implicit local + SBI teardown.

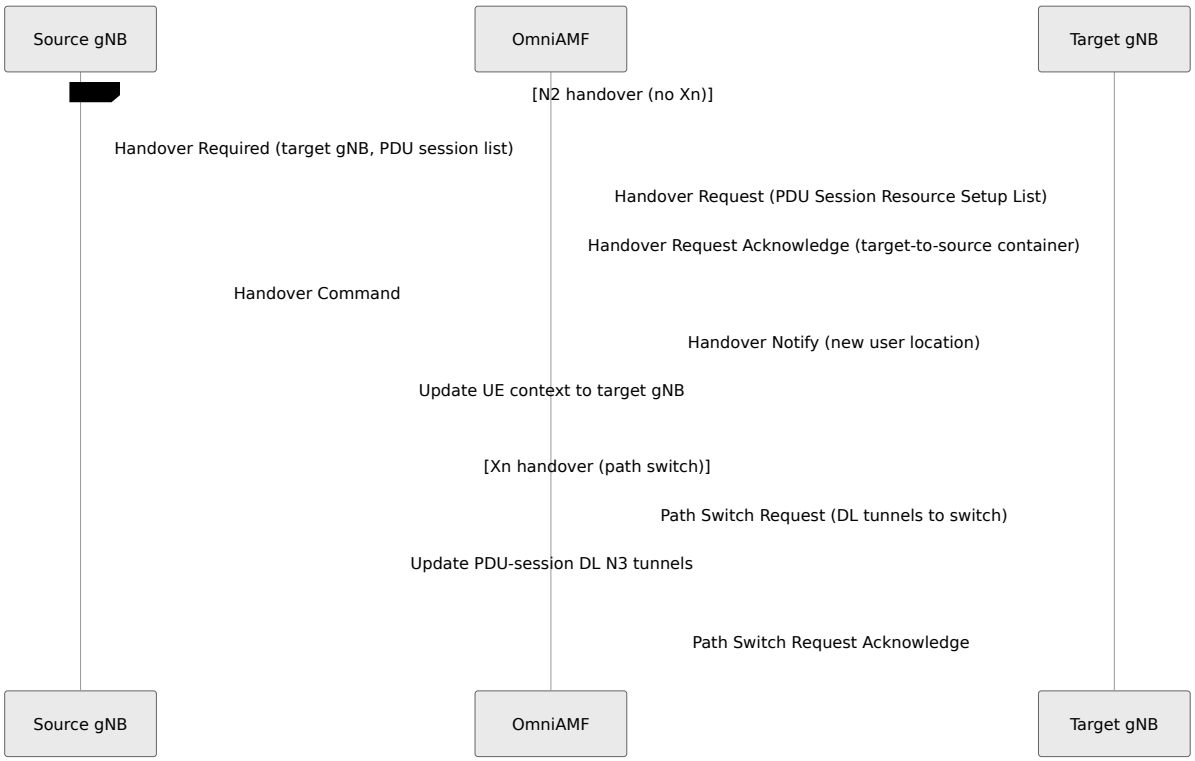


On **explicit** deregistration the stored native security context is dropped (the UE discards its context too); on **implicit** deregistration (e.g. Mobile Reachable / Implicit Deregistration timer expiry) the context is retained so a returning UE can still GUTI-resume.

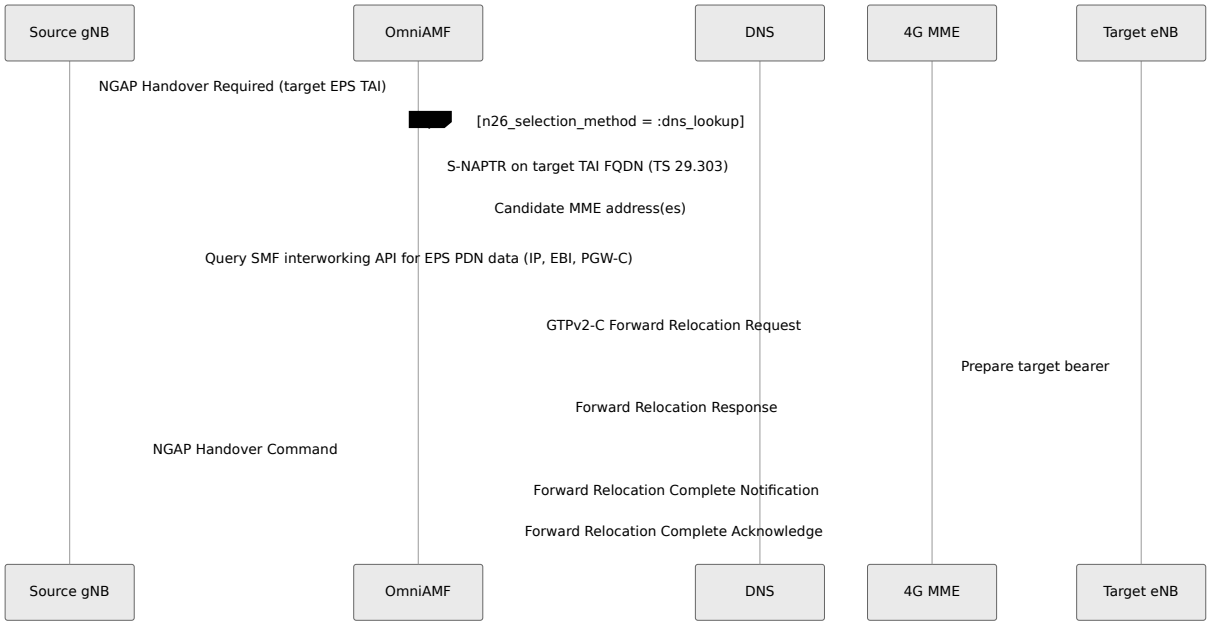
N2 / Xn Handover (Intra-5GS Mobility)

OmniAMF supports both AMF-anchored handover paths between gNBs within the 5G System:

- **N2 handover** (HandoverPreparation): the source gNB sends **Handover Required**; the AMF drives **Handover Request** toward the target gNB, relays **Handover Command** back to the source, and finalises on **Handover Notify**. HandoverFailure and HandoverCancel are handled.
- **Xn handover** (PathSwitchRequest): the target gNB sends **Path Switch Request** after the UE has already moved over Xn; the AMF updates the PDU-session downlink tunnels and returns **Path Switch Request Acknowledge**.



N26 Handover (5G → 4G)

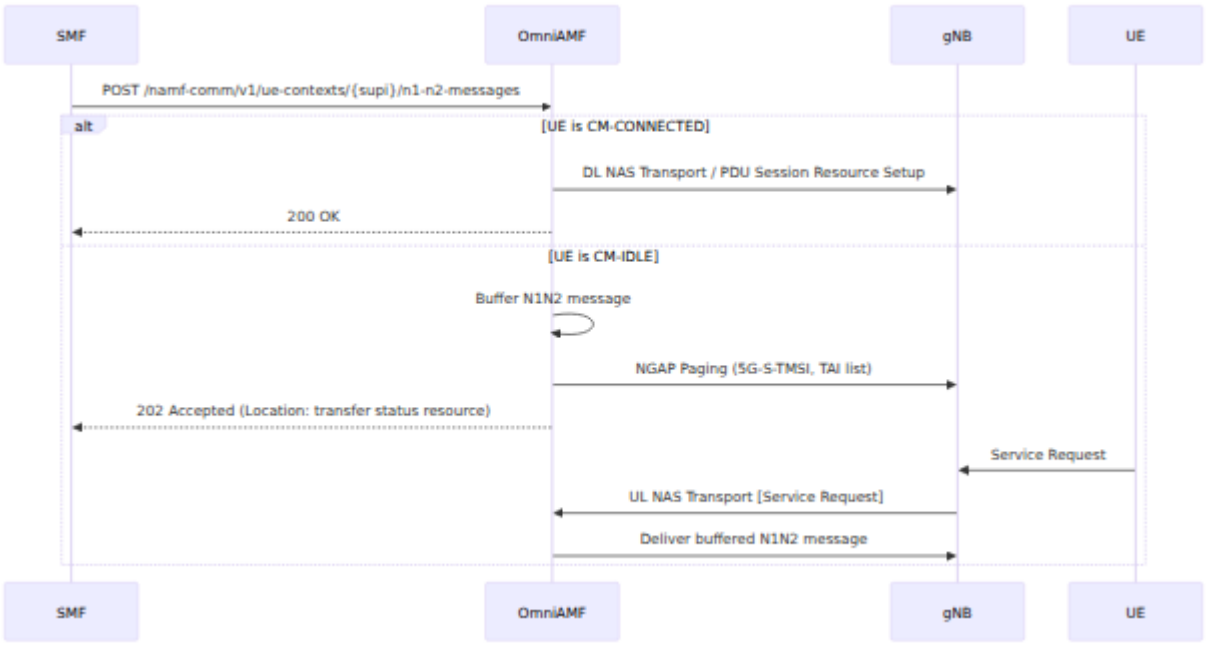


For 4G→5G, the MME sends a Forward Relocation Request to the AMF's N26 endpoint; the AMF maps the EPS context into 5GS and drives the target gNB.

Error Handling N2 Procedures

Beyond the mainline procedures above, the AMF handles two N2 procedures that keep gNB and AMF state consistent when something goes wrong:

- **NGAP Error Indication** (TS 38.413 §8.7.5). Sent by either peer to report a received NGAP message it could not process (unknown UE NGAP IDs, syntax/abstract-syntax errors, unexpected procedure). The AMF logs the reported `Cause` and, where the message carried UE NGAP IDs, reconciles or releases the affected UE association rather than leaving a half-open context. The AMF also emits its own Error Indication toward a gNB when it receives an NGAP PDU it cannot associate with a known UE.
- **gNB-initiated UE Context Release Request** (TS 38.413 §8.3.2). The gNB asks the AMF to release the UE's logical N2 context (for example on radio link failure or user inactivity), supplying a `Cause`. The AMF responds by driving a **UE Context Release Command / Complete** exchange, releasing the associated PDU-session N3 tunnels toward the SMF, and moving the UE to CM-IDLE. This differs from the AMF/OAM-initiated `release` action, which the AMF starts itself.



NGAP Procedures Summary

The AMF acts on the following NGAP (N2) elementary procedures (TS 38.413). Interface-management and error-handling procedures apply to the whole association; the remainder are per-UE.

Category	Procedures
Interface management	NG Setup, NG Reset, AMF Configuration Update, RAN Configuration Update, Error Indication
NAS transport	Initial UE Message, Uplink/Downlink NAS Transport
UE context management	Initial Context Setup, UE Context Modification, UE Context Release (AMF-initiated), UE Context Release Request (gNB-initiated)
PDU session management	PDU Session Resource Setup / Modify / Release
Mobility	Handover Preparation (N2), Path Switch (Xn), Handover Cancel, Handover Notify
Paging	Paging

Target MME discovery

For a 5G→4G handover the AMF must locate the GTPv2-C peer (the target MME) that serves the target eNB's EPS Tracking Area. How it does so is governed by `n26_selection_method`:

- **`:dns_lookup` (default): S-NAPTR discovery (TS 29.303 §5.4).** The AMF extracts the target EPS TAI (PLMN + 16-bit TAC) from the NGAP `targeteNB-ID`, builds the EPS TAI FQDN

  ```
  tac-lb<lo>.tac-hb<hi>.tac.epc.mnc<MNC>.mcc<MCC>.<domain>
  ```

(MCC zero-padded to 3 digits, MNC to 2–3 digits, `<domain>` from `n26_dns_servers`, default `3gppnetwork.org`), and issues an S-NAPTR query for the **`x-3gpp-mme:x-s10`** application service against each configured DNS server in turn. Queries use TCP (EPC NAPTR responses routinely exceed the 512-byte UDP limit). The first candidate yielding a usable IPv4 address is used as the target MME. This is the mirror of the S10 MME-to-MME discovery a legacy MME would perform, so the same EPC DNS records serve both.

- **Fallback to static.** If every configured DNS server fails or returns no usable candidate (or the target EPS TAI cannot be parsed from the NGAP `targeteNB-ID`), the AMF falls back to the static `n26_mme_peer` (default `127.0.0.11:2123`) and logs the fallback.

- **`:static`: no DNS.** Set `n26_selection_method` to `:static` (any value other than `:dns_lookup`) to skip discovery entirely and always use `n26_mme_peer`. Use this when you do not run EPC DNS.

See N26 Interworking Parameters and the advanced parameters (`n26_selection_method`, `n26_dns_servers`) for configuration.

5GMM Timer Reference

These timers run per UE context within the 5GMM state machine (TS 24.501 §10.2).

Timer	Duration	Trigger	Action on Expiry
T3512	54 min (sent to UE)	Registration Accept	UE initiates periodic registration update
T3550	6 s	Registration Accept sent	Retransmit Registration Accept (max retries)
T3560	6 s	Auth Request / SMC sent	Retransmit Auth Request or SMC (max retries)
T3570	6 s	Identity Request sent	Retransmit Identity Request (max retries)
T3513	6 s	Paging initiated	Retransmit paging, then signal paging failure
T3522	6 s	Network Deregistration Request sent	Retransmit Deregistration Request (max retries)
T3555	6 s	Config Update Command sent	Retransmit Config Update Command (max retries)
Mobile Reachable	T3512 + 4 min	UE enters CM-IDLE	Start Implicit Deregistration timer
Implicit Deregistration	~58 min	Mobile Reachable expires	Implicitly deregister UE, release sessions

← Overview

OmniAMF Troubleshooting

Table of Contents

---

gNB cannot connect (SCTP connection refused)

Symptoms: gNB reports no N2 connection; no NG Setup logged.

Possible causes:

- `ngap_addr` bound to an interface the gNB cannot reach.
- Host firewall blocking SCTP on `ngap_port` (38412).
- SCTP kernel support missing, or the port already held by another process.

Resolution:

1. Confirm `ngap_addr`/`ngap_port` and that the bound address is reachable from the gNB.

2. Permit SCTP on the NGAP port in the host firewall.
3. Verify SCTP is available in the kernel and the port is free.

gNB NG Setup rejected (TA / PLMN mismatch)

Symptoms: The SCTP association comes up but the gNB never becomes operational: it receives an **NG Setup Failure** in response to NG Setup Request and no UE signalling is ever carried. gNB logs show the setup being rejected.

Possible causes:

- The gNB's `SupportedTAList` (its TAC and broadcast PLMN) is not present in the AMF's configured `supported_ta_list`, so the AMF cannot serve that Tracking Area and rejects the setup (TS 38.413 §8.7.1).
- The gNB's PLMN does not match any PLMN in `supported_ta_list`.

Resolution:

1. Compare the gNB's configured TAC and PLMN against the AMF's `supported_ta_list`.
2. Align the two: either add the gNB's TAC/PLMN to `supported_ta_list`, or reconfigure the gNB to broadcast a TAC/PLMN the AMF already serves.
3. Confirm the successful NG Setup: the gNB should now receive an NG Setup Response (see NG Setup).

UE registration fails at authentication

Symptoms: Registration never completes; authentication step errors.

Possible causes:

- AUSF unreachable at the resolved URI.
- Subscriber not provisioned in UDM/UDR (AUSF returns 404).

Resolution:

1. Verify AUSF reachability (via NRF discovery or the static `ausf_uri`).
2. Confirm the subscriber's SUPI/IMSI is provisioned in the UDM/UDR backend.

Registration stalls after Security Mode Complete

Symptoms: Authentication succeeds but Registration Accept is never sent.

Possible causes:

- UDM unreachable or timing out on AM-data / NSSAI / SMF-selection fetch.
- PCF unreachable during AM policy create.

Resolution:

1. Confirm UDM reachability and check UDM logs for the SUPI.
2. Confirm PCF reachability at the resolved `pcf_uri`.

Idle UE re-attaches with full re-authentication (no GUTI resume)

Symptoms: A returning UE always runs a full 5G-AKA instead of resuming.

Possible causes:

- GUTI Context Store not running (AMF restarted; ETS table lost).
- NAS integrity check against the stored context failed (stale/rotated keys).

Resolution:

1. Confirm the AMF has not restarted between the UE going idle and returning (the store is in-memory).
2. A MAC mismatch legitimately falls back to full 5G-AKA; verify UE and AMF NAS counts are consistent.

N1N2 message from SMF not delivered

Symptoms: SMF-originated N1N2 transfer does not reach the UE.

Possible causes:

- UE is CM-IDLE and not responding to paging (out of coverage / wrong TAI list).
- For CM-CONNECTED UEs, missing NGAP identifiers in the UE context.

Resolution:

1. For CM-IDLE, confirm paging reaches the correct gNBs (TAI list) and the UE is in coverage.
2. For CM-CONNECTED, confirm the UE context carries the gNB association and NGAP UE IDs (set during Initial UE Message).

N26 handover to 4G fails

Symptoms: 5G→4G handover never reaches the MME.

Possible causes:

- `n26_addr` left as `0.0.0.0`, so F-TEIDs advertise an unroutable address.
- DNS S-NAPTR discovery returns nothing and no usable static `n26_mme_peer`.
- SMF interworking API (`n26_smf_uri`) unreachable, so EPS PDN data is unavailable.

Resolution:

1. Set `n26_addr` to the AMF's routable address.
2. Verify `n26_dns_servers` resolve the target TAI FQDN, or set `n26_selection_method: :static` with a valid `n26_mme_peer`.
3. Confirm `n26_smf_uri` is reachable.

UE context not found for SBI request

Symptoms: SBI requests return `404 CONTEXT_NOT_FOUND`.

Possible causes:

- `ueContextId` does not match the stored SUPI.
- UE has not completed registration (context still keyed by SUCI, later promoted to SUPI).

Resolution:

1. Ensure the `ueContextId` path parameter exactly matches the SUPI (e.g. `imsi-999700000000001`).
2. Confirm the UE has completed registration.