

Advanced Call Control Features

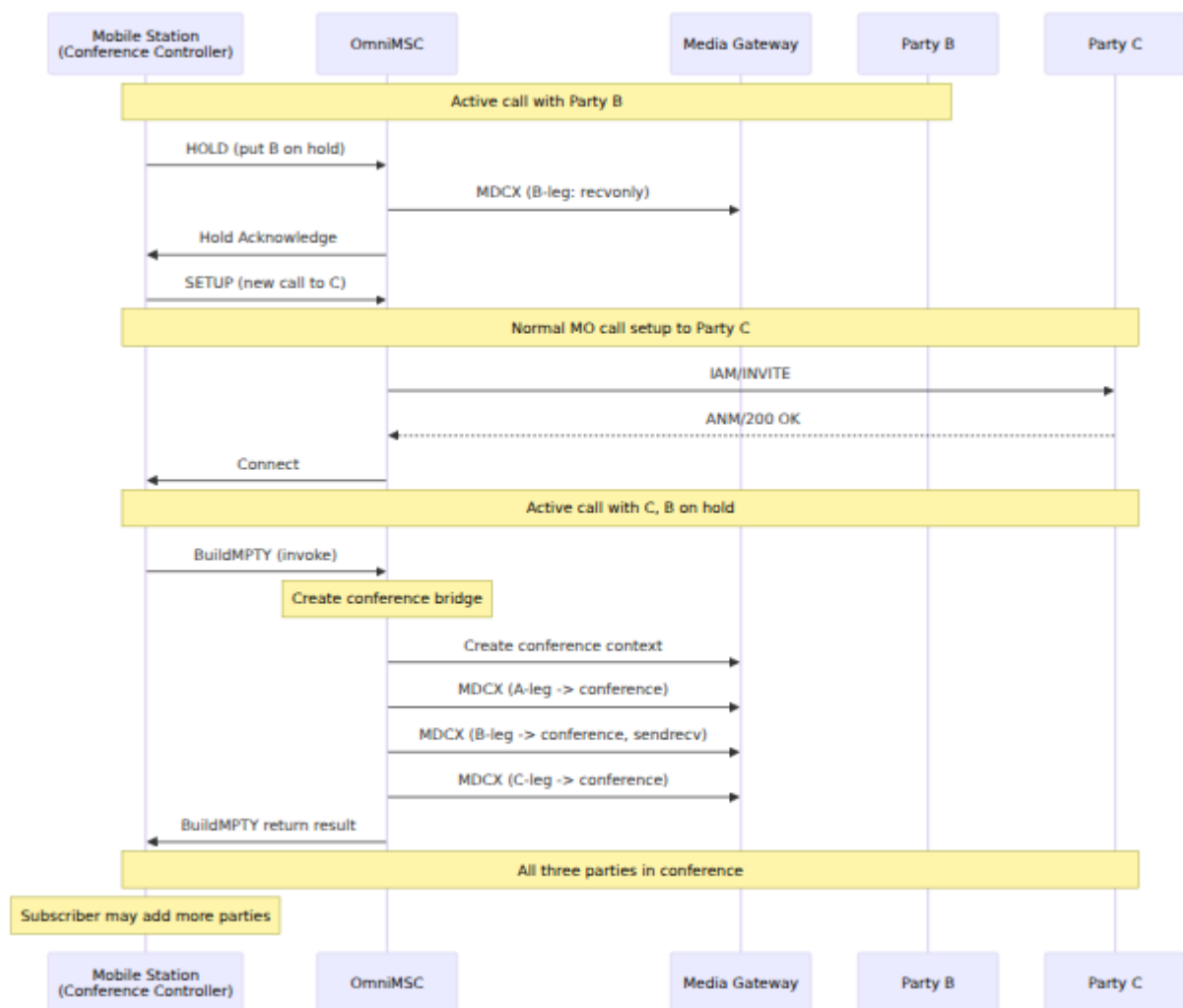
This document describes the advanced circuit-switched call control features implemented in OmniMSC, including multi-party calling, call transfer, call completion, call deflection, multicall, priority services, and charging.

For basic supplementary services (call forwarding, barring, CLIP/CLIR, USSD), see [Supplementary Services](#). For call flow diagrams, see [Call Flow Diagrams](#). For configuration parameters, see [Configuration Reference](#). For general operations, see [Operations Guide](#).

MPTY (Multi-Party / Conference Calling)

MPTY allows a subscriber to establish a conference call with multiple remote parties per 3GPP TS 24.084. The subscriber acts as the conference controller, bridging held and active calls into a single multi-party conversation.

MPTY Sequence



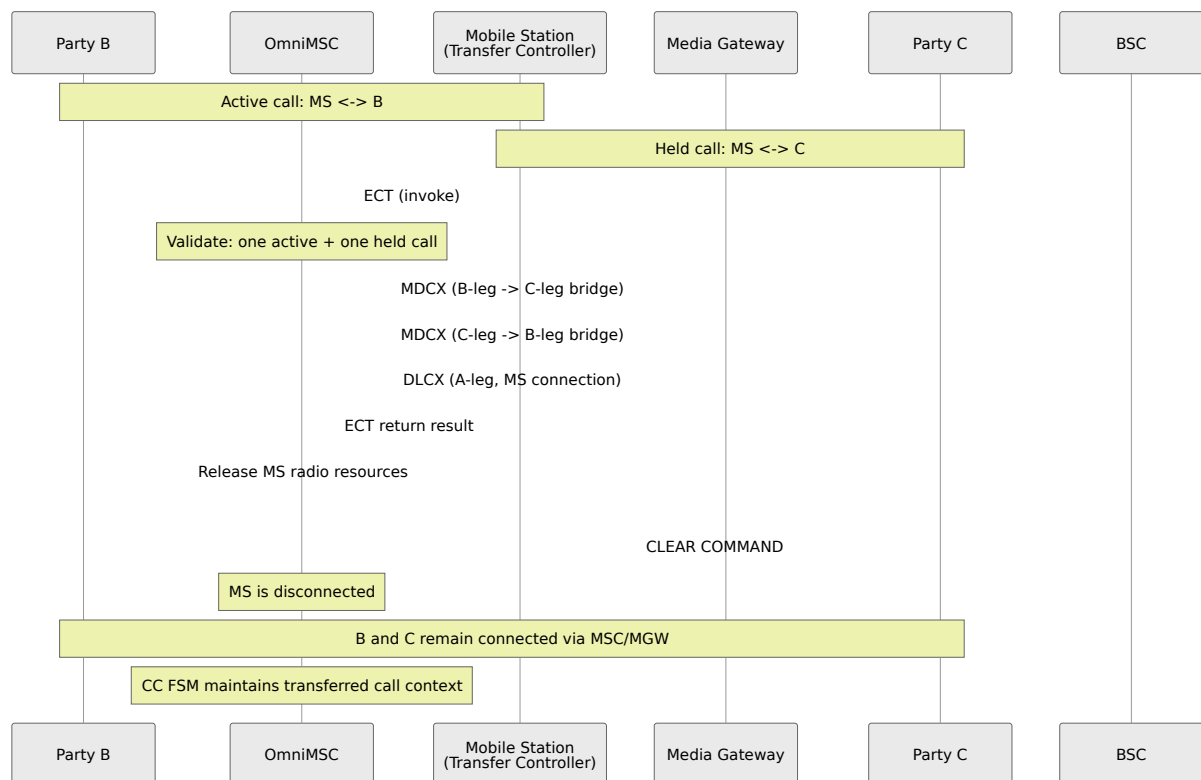
MPTY Configuration

MPTY has no static configuration; it enforces no party maximum in code, and all parameters are derived per call from the MPTY supplementary service operations.

ECT (Explicit Call Transfer)

ECT allows a subscriber to connect two calls together and then drop out of the connection per 3GPP TS 24.091. The subscriber must have one active call and one held call. After ECT, the two remote parties are connected directly through the MSC.

ECT Sequence



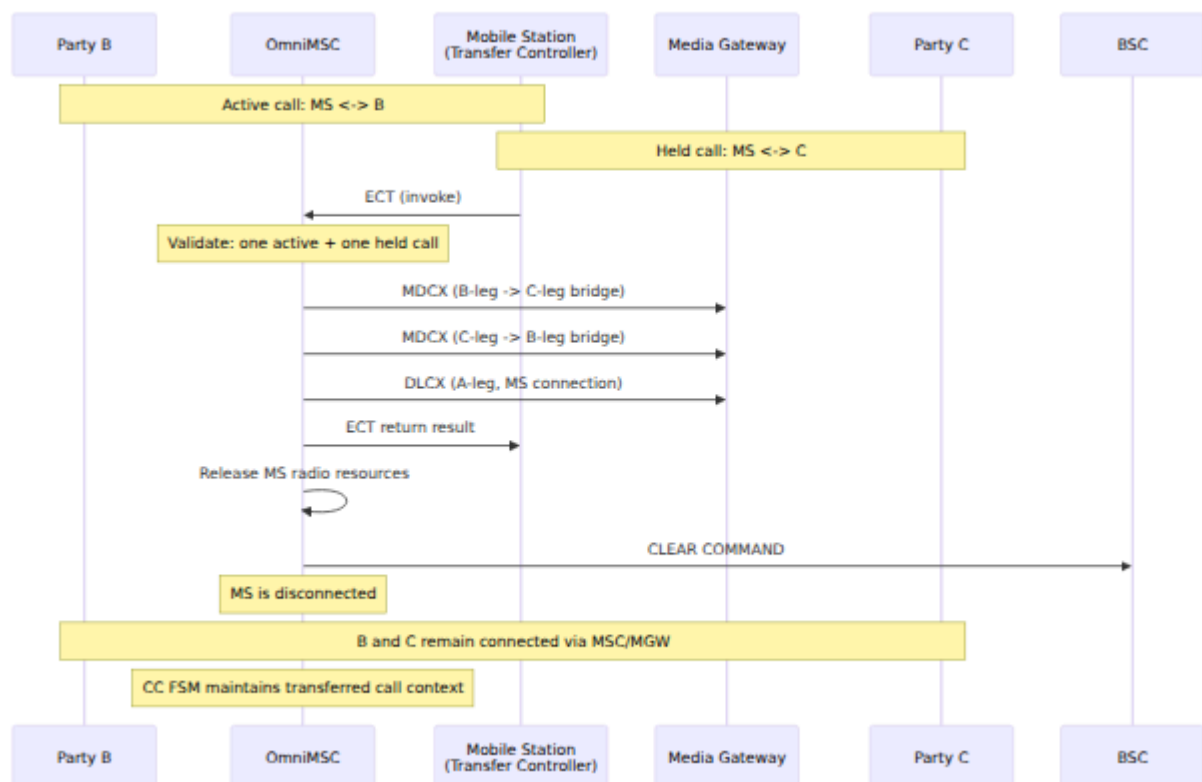
ECT Configuration

ECT has no static configuration; its behaviour is driven per call by the ECT supplementary service invocation.

CCBS (Call Completion to Busy Subscriber)

CCBS allows a caller to request automatic callback when a busy called subscriber becomes free, per 3GPP TS 24.093 and 3GPP TS 23.135. The MSC monitors the called subscriber's state and initiates a callback when they become idle.

CCBS Flow



CCBS Configuration

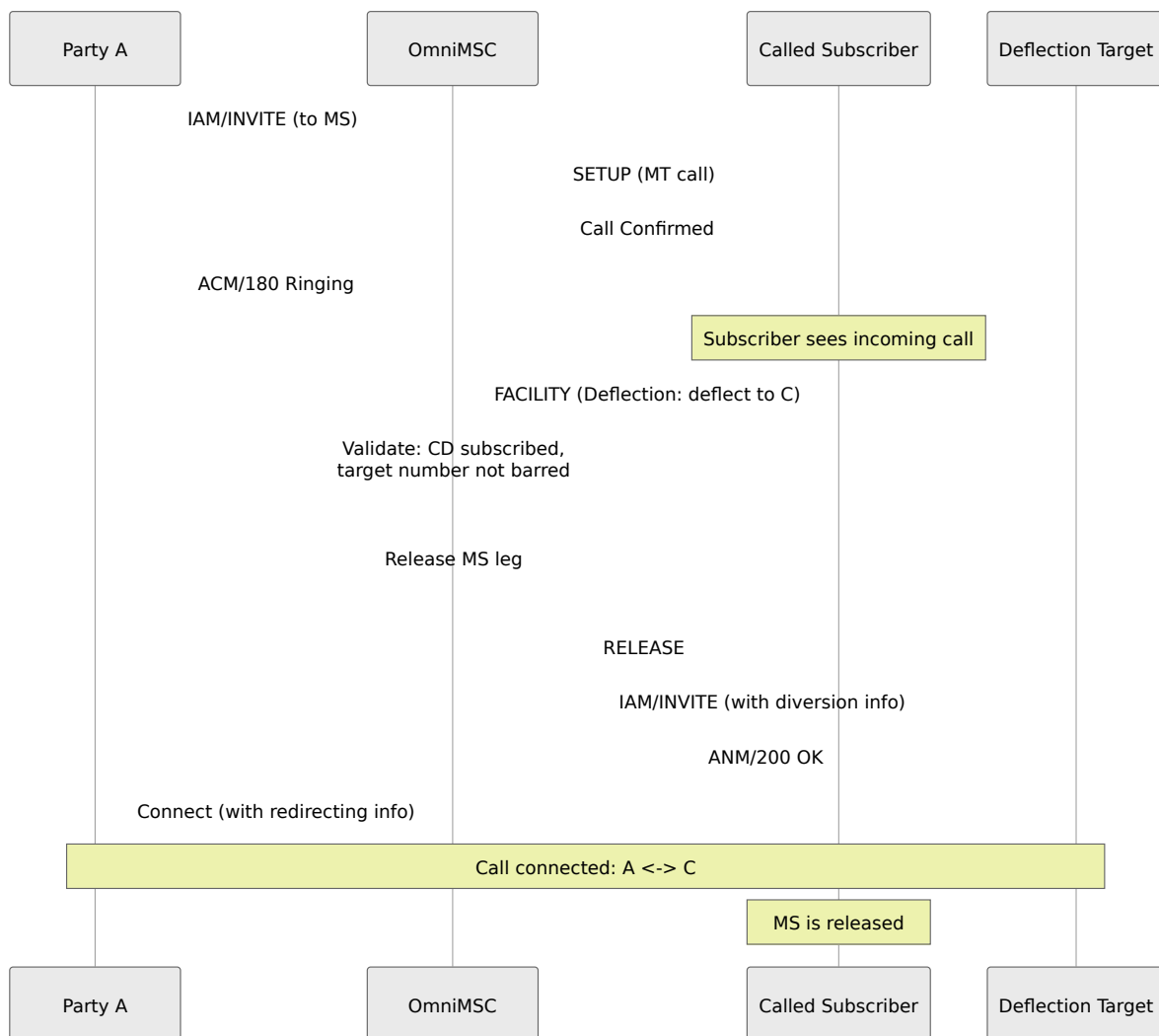
CCBS is configured under `config :omnimsc, :ccbs:`

Parameter	Type	Default	Description
<code>:max_queue_size</code>	integer	5	Maximum number of pending CCBS requests per subscriber. Additional requests are rejected. Per 3GPP TS 23.135 Sec 4.2.
<code>:request_lifetime_ms</code>	integer	180_000	Lifetime in milliseconds of a queued CCBS request. If the called subscriber does not become free within this period, the request expires.
<code>:recall_timeout_ms</code>	integer	30_000	Time in milliseconds to wait for the originating subscriber to answer the CCBS recall.

Call Deflection

Call Deflection (CD) allows a called subscriber to redirect an incoming call to another number before answering, per 3GPP TS 24.072. Unlike call forwarding, CD is an on-demand action initiated by the subscriber during the alerting phase.

Call Deflection Sequence



Call Deflection Configuration

Call Deflection has no static configuration; it is invoked per call via the CD supplementary service during the alerting phase.

Multicall Configuration

Multicall allows a subscriber to maintain multiple simultaneous CS calls per 3GPP TS 23.135. This is distinct from MPTY (conference): in multicall, each call has independent audio. The subscriber switches between calls using the HOLD/RETRIEVE mechanism.

Multicall has no application-level configuration. The per-subscriber limit is an HLR/subscription value, `:max_calls`, supplied with the subscriber profile:

Parameter	Type	Default	Description
<code>:max_calls</code>	integer	2	Maximum number of simultaneous CS calls for the subscriber, from the HLR subscription. One call is active, the remainder are held. The value is capped at an absolute maximum of 7.

eMLPP (Enhanced Multi-Level Precedence and Pre-emption)

eMLPP provides priority call handling per 3GPP TS 24.067. Calls are assigned a priority level, and higher-priority calls may pre-empt lower-priority calls when resources are scarce.

Priority Levels

Seven priority levels are defined (numeric value, lower = higher priority):

Value	Name	Description
0	flash_override	Highest priority (Flash Override). Reserved for national emergency authorities.
1	flash	Flash. Reserved for senior government/military officials.
2	immediate	Immediate. High-priority government/military.
3	priority	Priority. General priority traffic.
4	routine	Routine. Standard subscriber calls (default).
5	spare_3	Spare level 3.
6	spare_4	Spare level 4.

eMLPP Configuration

eMLPP has no static configuration; the priority level (and any pre-emption) is applied per call from the subscriber's eMLPP subscription and the call's requested precedence.

AoCC (Advice of Charge - Charging)

AoCC provides real-time charge information to the subscriber during a call per 3GPP TS 24.086. The MSC sends charge rate information and accumulated charge indications to the mobile station.

AoCC Configuration

AoCC has no static configuration; the currency and charge amount are supplied per call as parameters to the AoCC session.

3GPP Specification References

Specification	Title	Feature
TS 24.084	Multi-Party (MPTY) Supplementary Service	MPTY / Conference calling
TS 24.091	Explicit Call Transfer (ECT) Supplementary Service	ECT
TS 24.093	Call Completion to Busy Subscriber (CCBS)	CCBS
TS 23.135	Multicall	Multicall, CCBS network procedures
TS 24.072	Call Deflection Supplementary Service	Call Deflection
TS 24.067	enhanced Multi-Level Precedence and Pre-emption (eMLPP)	eMLPP priority levels
TS 24.086	Advice of Charge (AoC) Supplementary Services	AoCC charging
TS 24.083	Call Waiting and Call Hold	Hold/Retrieve for multicall

REST API

This document describes the OmniMSC REST API, which provides programmatic access to subscriber data, active calls, routing configuration, SIP peers, media gateways, RAN connections, and system status. The API listens on port 8444 and serves an auto-generated OpenAPI 3 (OAS3) specification.

For the web-based control panel, see [Control Panel](#). For routing concepts referenced by the route endpoints, see [Routing Configuration](#).

OpenAPI Documentation

OmniMSC automatically generates an OpenAPI 3 specification from the API router. The interactive Swagger UI is available at `http://<host>:8444/api/docs` and provides a browsable, testable interface for all endpoints. The raw OAS3 specification is served at `http://<host>:8444/api/schema`.

Endpoints

All endpoints are served under the `/api` path prefix. Request and response bodies use JSON encoding.

Subscribers

Method	Path	Description
GET	/api/subscribers	List VLR subscribers. Supports an optional <code>search</code> query parameter that filters by IMSI or MSISDN (partial match).
GET	/api/subscribers/{id}	Retrieve full detail for a single subscriber, including identity, location, authentication state, service profile, and supplementary services.
DELETE	/api/subscribers/{id}	Purge a subscriber record from the local VLR (deletes the VLR record only; no MAP PurgeMS is sent to the HLR).
POST	/api/subscribers/{id}/actions	Execute an action on a subscriber, such as initiating a detach, forcing re-authentication, or triggering a location update.
POST	/api/subscribers/{id}/ss	Manage supplementary services for a subscriber, including activation, deactivation, and interrogation of call barring, call forwarding, and other services.

Calls

Method	Path	Description
GET	/api/calls	List all active CC FSM call transactions, including call reference, direction, parties, state, and duration.
GET	/api/calls/{id}	Retrieve full detail for a single call, including timing, codec, serving BSC/RNC, and CC FSM state history.
DELETE	/api/calls/{id}	Release an active call. Initiates network-side disconnect and BSSMAP CLEAR COMMAND.

SMS

Method	Path	Description
GET	/api/sms	List active SMS transactions with transaction ID, direction, subscriber, state, and SMS Centre address.

Routes

Method	Path	Description
GET	/api/routes	List all entries in the route table, including prefix, destination type, priority, and destination-specific parameters.
POST	/api/routes	Add a new route to the route table. The route takes effect immediately without restart.
DELETE	/api/routes/{prefix}	Delete a route from the route table by prefix.
GET	/api/routes/lookup	Look up the route that would be selected for a given called party number. Useful for verifying routing behaviour without placing a call.

SIP Peers

Method	Path	Description
GET	/api/sip/peers	List all configured SIP peers with address, transport, status, active calls, and capacity.
GET	/api/sip/peers/{name}	Retrieve full detail for a single SIP peer, including codec list, OPTIONS keepalive state, and call statistics.
PUT	/api/sip/peers/{name}	Trigger an immediate OPTIONS keepalive ping toward the peer. This does not modify the peer's configuration.

Media Gateways

Method	Path	Description
GET	/api/mgw	List configured media gateways with name, address, protocol (MGCP or Megaco), and reachability status.

RAN and STP

Method	Path	Description
GET	/api/ran/connections	List active RAN connections (SCCP connection-oriented sessions) with connection ID, subscriber IMSI, BSC/RNC, and state.
GET	/api/ran/bscs	List known BSCs with point code, global title, cell count, and last BSSMAP RESET timestamp.
GET	/api/stp	Get STP link status, including M3UA ASP state, SCTP association details, and traffic counters.

Paging

Method	Path	Description
POST	/api/paging	Initiate a paging request for a subscriber by IMSI or MSISDN. Sends BSSMAP PAGING to the appropriate BSCs.
GET	/api/paging	List pending paging requests with subscriber identity, target LAC, paging cause, and elapsed time.

Advice of Charge

Method	Path	Description
POST	/api/aoc	Send an Advice of Charge message to a subscriber during an active call. Supports AoCI (information) and AoCE (charging) per 3GPP TS 24.086.

Silent Call and SMS

Method	Path	Description
POST	/api/silent	Initiate a silent call or silent SMS toward a subscriber. Used for lawful intercept and network testing purposes.

Handover Cells

Method	Path	Description
GET	/api/handover/cells	List cells configured as handover targets, including cell identity, LAC, BSC, and handover priority.
POST	/api/handover/cells	Add a cell to the handover target list with cell identity, LAC, and priority parameters.

System

Method	Path	Description
GET	/api/health	Health check endpoint. Returns a simple status indicator suitable for load balancer probes.
GET	/api/status	System status including BEAM VM statistics, memory allocation, supervisor health, active alarm count, and MSC configuration summary.
GET	/metrics	Prometheus metrics scrape endpoint. Returns all OmniMSC telemetry counters and gauges in Prometheus exposition format. Note: <code>/metrics</code> is served by the Control Panel Phoenix endpoint on port 4000 , not by the REST API on port 8444. See Metrics and Monitoring .

Response Format

All endpoints return JSON responses. Successful requests return the requested data in a top-level object or array. Error responses include a JSON object with an `error` field containing a human-readable message.

Subscriber and call detail responses include nested objects for related data (identity, location, authentication, timing) matching the structure described in the [Control Panel subscriber detail](#) and [call detail](#) sections.

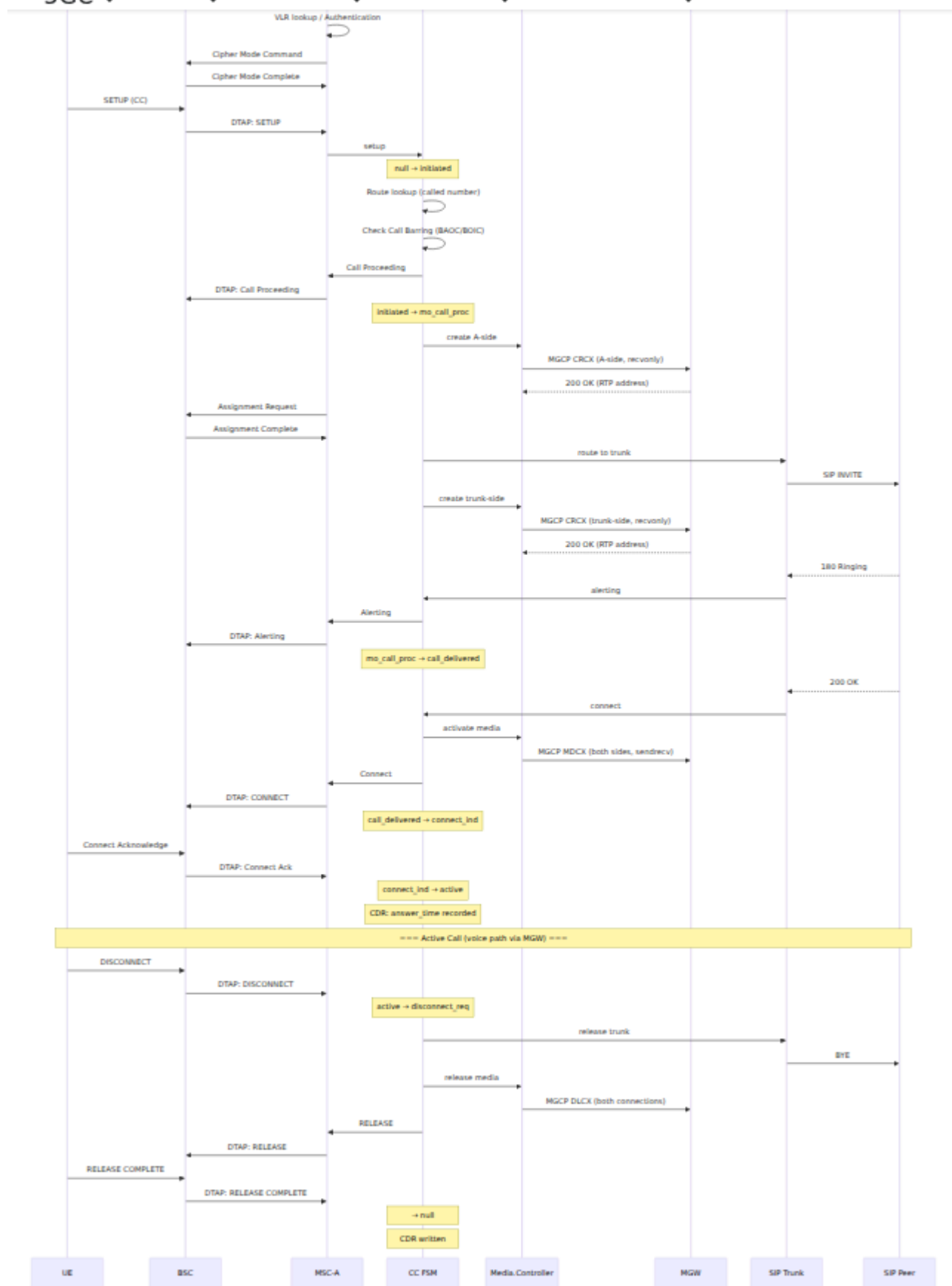
Call Flow Diagrams

This document contains sequence diagrams for all major call scenarios handled by OmniMSC. Each diagram shows the signaling flow between network elements.

For CC FSM state definitions, see [CC FSM State Diagram](#) below. For routing configuration, see [Routing Configuration](#). For SIP trunk signaling details, see [SIP Trunking](#). For ISUP trunk signaling, see [ISUP Trunking](#). For media gateway control during call setup, see [Media Control](#). For supplementary service flows (hold, MPTY, ECT), see [Supplementary Services](#).

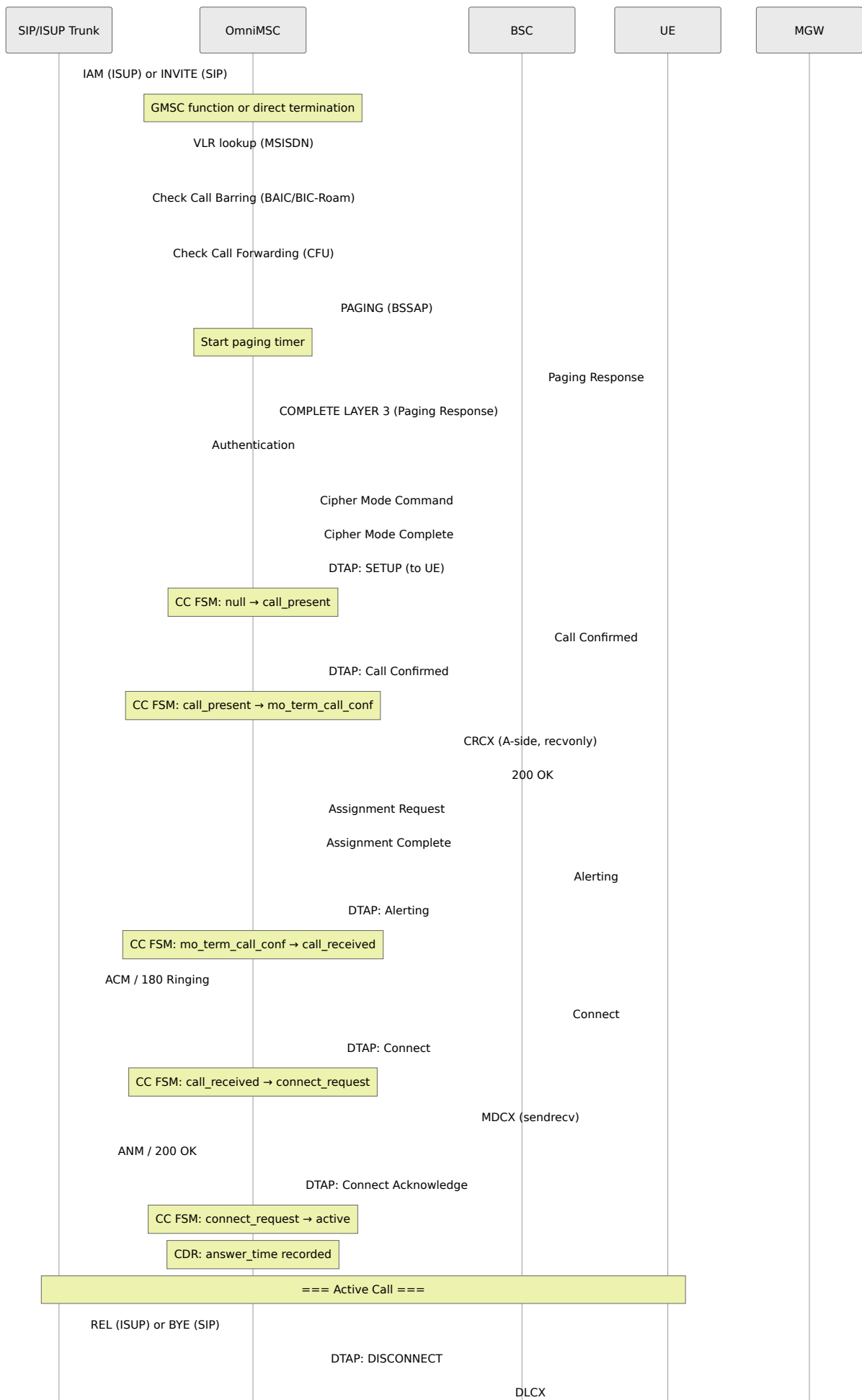
Mobile Originating (MO) Call

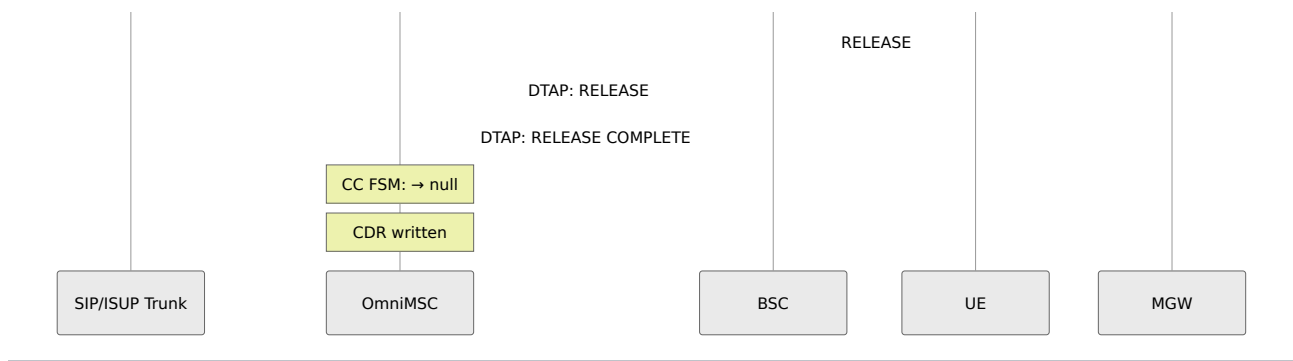
A subscriber initiates an outgoing call. The MSC handles call setup, authentication (if needed), cipher mode, assignment, and trunk allocation.



Mobile Terminating (MT) Call

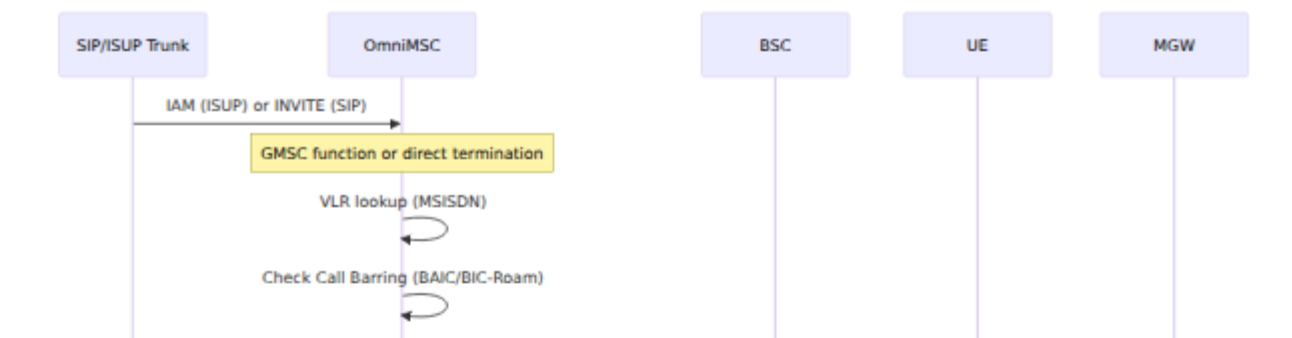
An incoming call arrives from the PSTN or a SIP peer. The MSC pages the subscriber, sets up the radio path, and connects the call. The trunk-side signaling may be SIP or ISUP depending on the route.



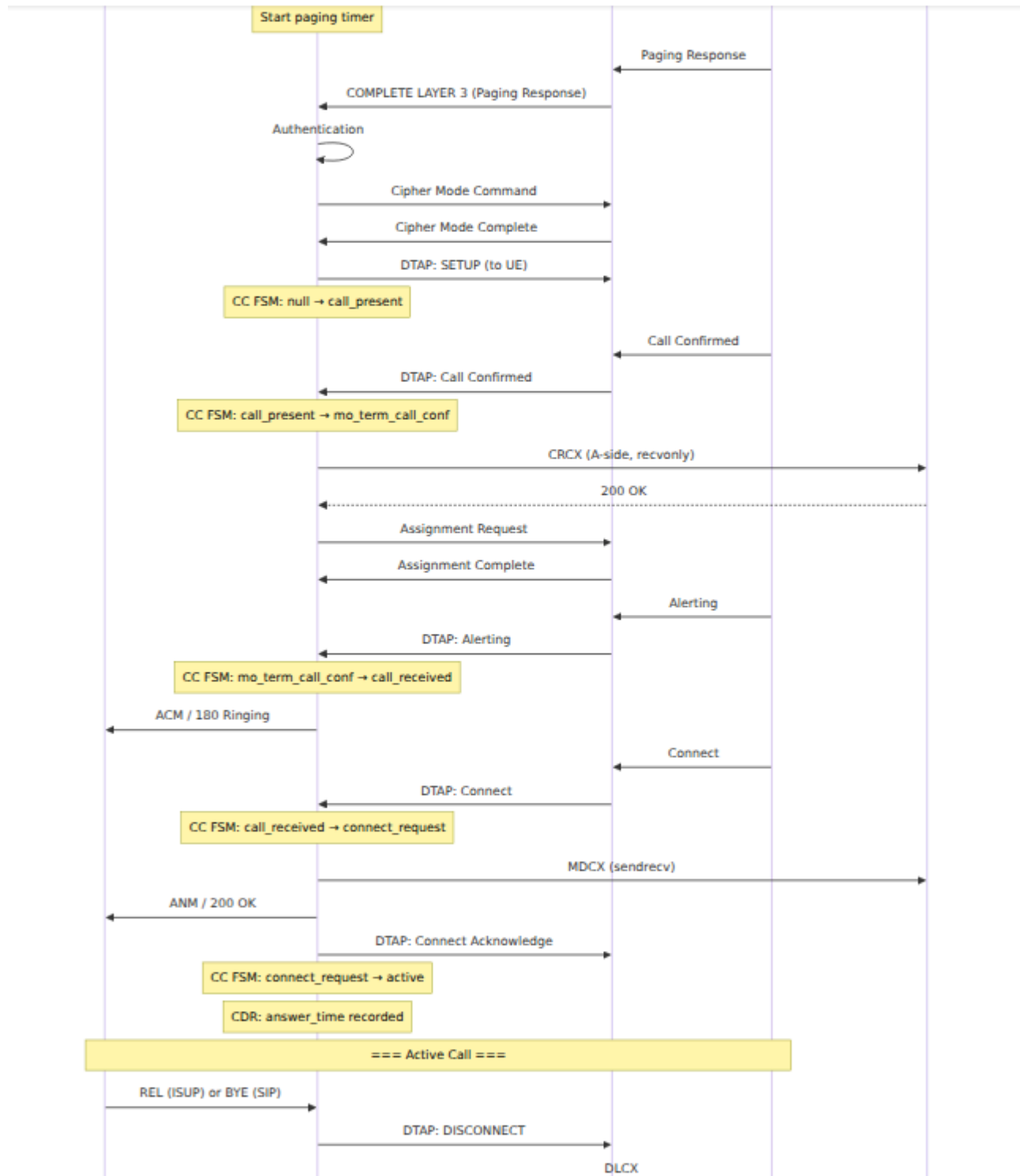


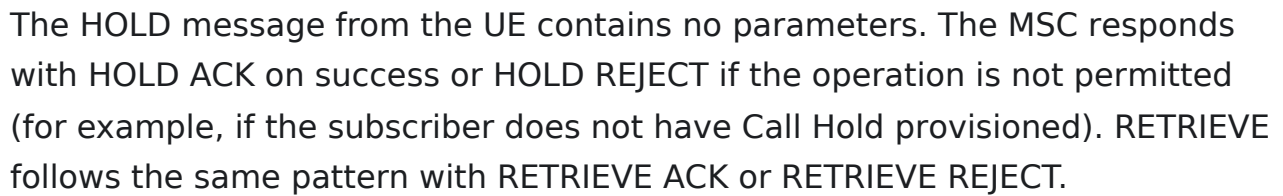
Call Hold and Retrieve

Call Hold and Retrieve allow a subscriber to suspend and resume an active call per 3GPP TS 24.083. While a call is held, the media gateway places the held leg into receive-only mode, silencing the audio path. The subscriber may establish a second call while the first is held.



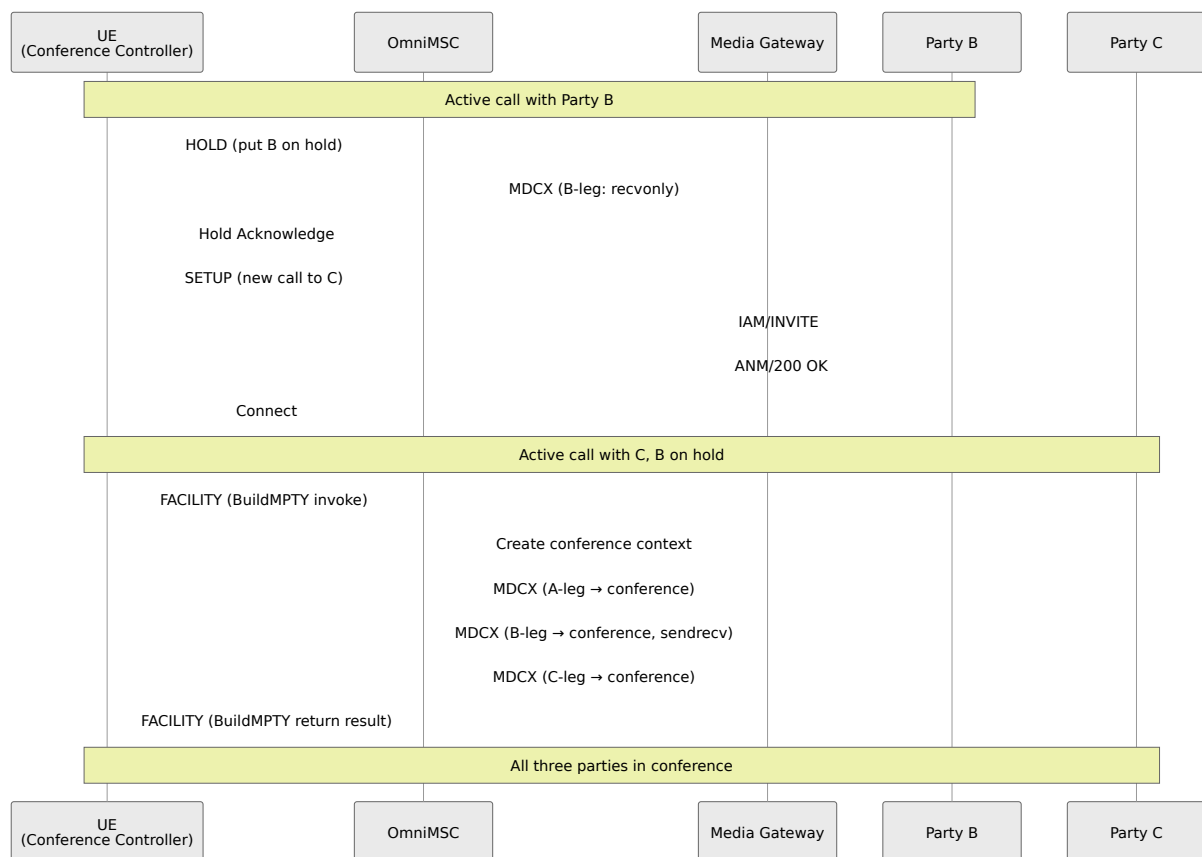
OmniCore 5GC OmniCall OmniRAN OmniCharge Platform English ▼





MPTY allows a subscriber to bridge multiple calls into a conference per 3GPP TS 24.084. The subscriber acts as the conference controller. All conference audio is mixed through a conference bridge on the media gateway.

BuildMPTY



HoldMPTY, RetrieveMPTY, SplitMPTY

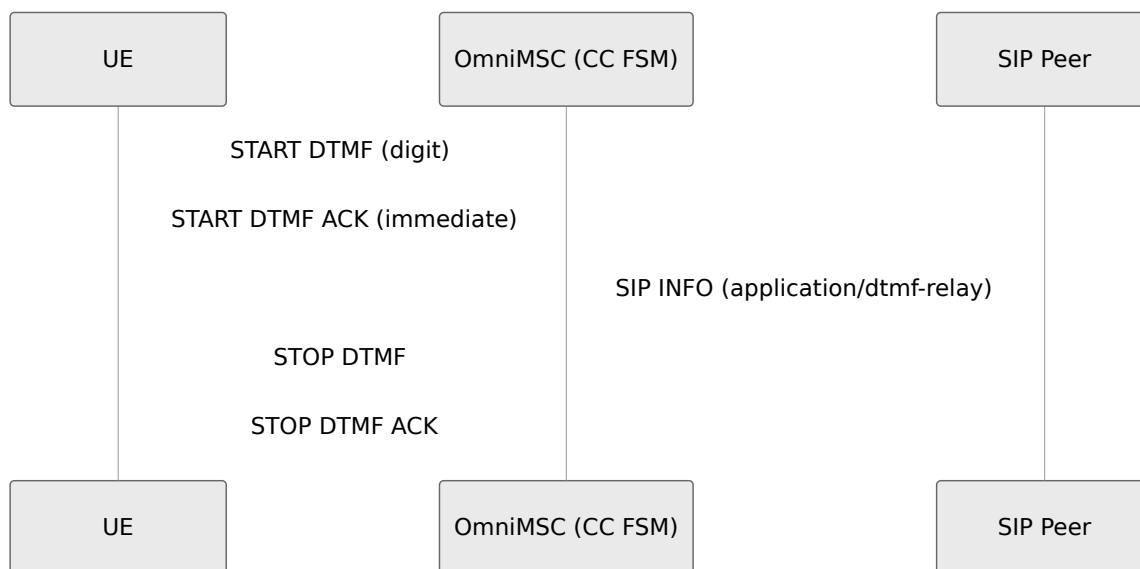
Once a conference is established, the controller has three additional operations available:

Operation	Effect
HoldMPTY	Places the entire conference on hold. All remote parties hear silence. The controller may establish a private call outside the conference.
RetrieveMPTY	Resumes a held conference. All parties are reconnected to the conference bridge.
SplitMPTY	Extracts one party from the conference into a separate held call. The remaining parties continue in conference. If only two parties remain after the split, the conference context is released and the call reverts to a normal point-to-point connection.

Each operation is invoked by the UE via a CC FACILITY message and acknowledged by the MSC with a corresponding return result or error.

DTMF Relay

OmniMSC relays DTMF tones from the radio interface to the trunk side. The UE sends a START DTMF message (3GPP TS 24.008) containing the digit. The CC FSM immediately acknowledges the UE and forwards the digit to the SIP peer.



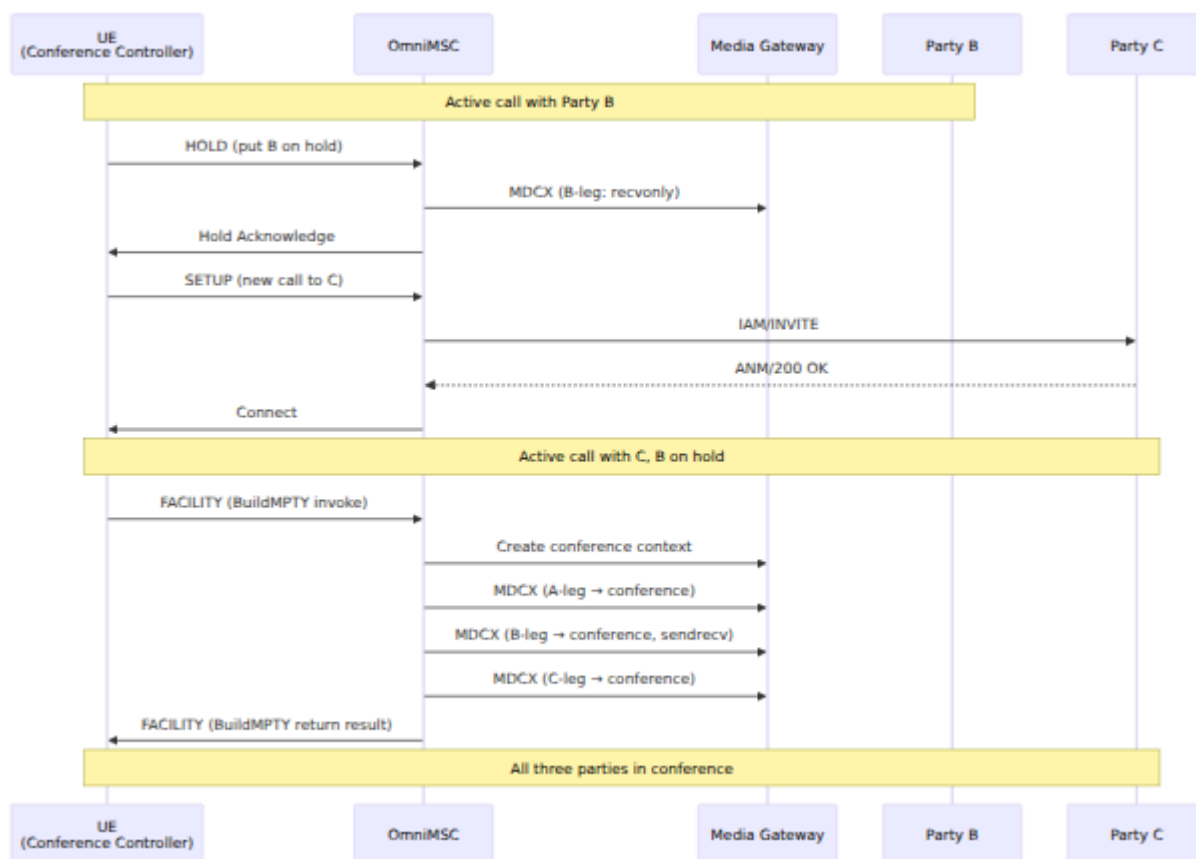
The SIP INFO body uses the `application/dtmf-relay` content type with Signal and Duration fields. The MSC sends START DTMF ACK immediately to the UE without waiting for the SIP peer's response, avoiding audio clipping on the radio path. DTMF relay is handled in any call state where a trunk-side connection exists.

Emergency Calls

Emergency calls receive priority handling. The MSC detects emergency calls by the CC Emergency Setup message type (3GPP TS 24.008 §9.3.8, message type 0x0E) and the CM Service Request type (`:emergency`).

Authentication is attempted normally. If it succeeds, cipher mode is established and the subscriber's MSISDN is used as the calling party. If authentication fails, the call proceeds anyway — cipher mode is skipped and the IMEI is used as the calling party instead. Calls from UEs without a SIM are accepted.

Unlike regular CC Setup, the Emergency Setup message does not carry a Called Party BCD Number IE — the handset sends only an optional Bearer Capability and Emergency Service Category. The MSC uses the configured `psap_address` as the called number for route table lookup and the outgoing SIP INVITE Request-URI. See [Configuration Reference](#) for emergency parameters.



CC FSM State Diagram

The CC FSM (Call Control Finite State Machine) manages the lifecycle of a single circuit-switched call per 3GPP TS 24.008. The MO and MT paths share common states but enter through different transitions. Live call state, duration, codec, and serving BSC/RNC are visible in the Active Calls page of the control panel — see [Control Panel Guide](#).

MO Call States



null

MS SETUP received

initiated



Call Proceeding sent

mo_call_proc

Alerting (remote ringing)

call_delivered

Connect sent to MS

RELEASE COMPLETE

connect_ind

Connect Ack from MS

active

MS DISCONNECT

Network release

disconnect_req

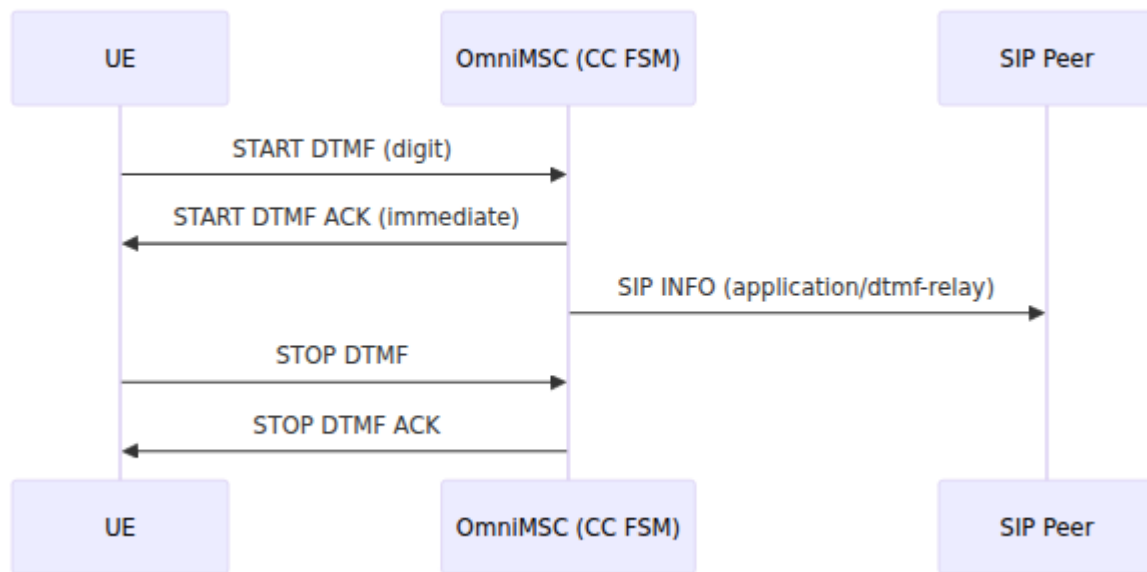
disconnect_ind

RELEASE sent

RELEASE sent

release_req

MT Call States



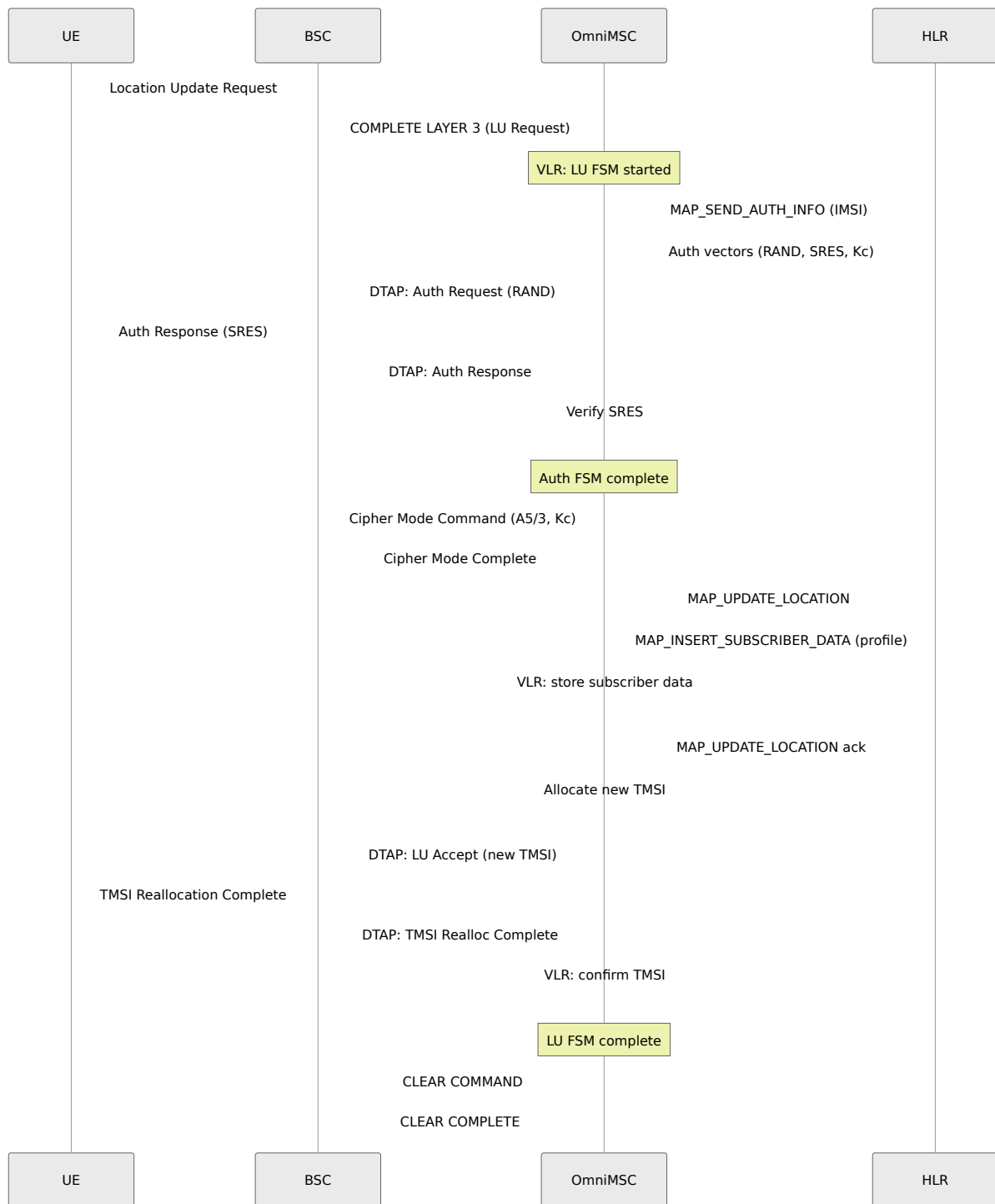
Connection Release

When the A-interface connection is lost (radio link failure, BSC clear, or transport failure), MSC-A sends a `connection_lost` event to all CC FSMs associated with that subscriber. Each CC FSM receiving this event releases its trunk-side resources (SIP BYE or ISUP REL) and media gateway connections (MGCP DLCX), then transitions to the null state and writes the CDR.

This ensures that no trunk or media resources are leaked when the radio path is unexpectedly lost. The CC FSM handles `connection_lost` in any state except null.

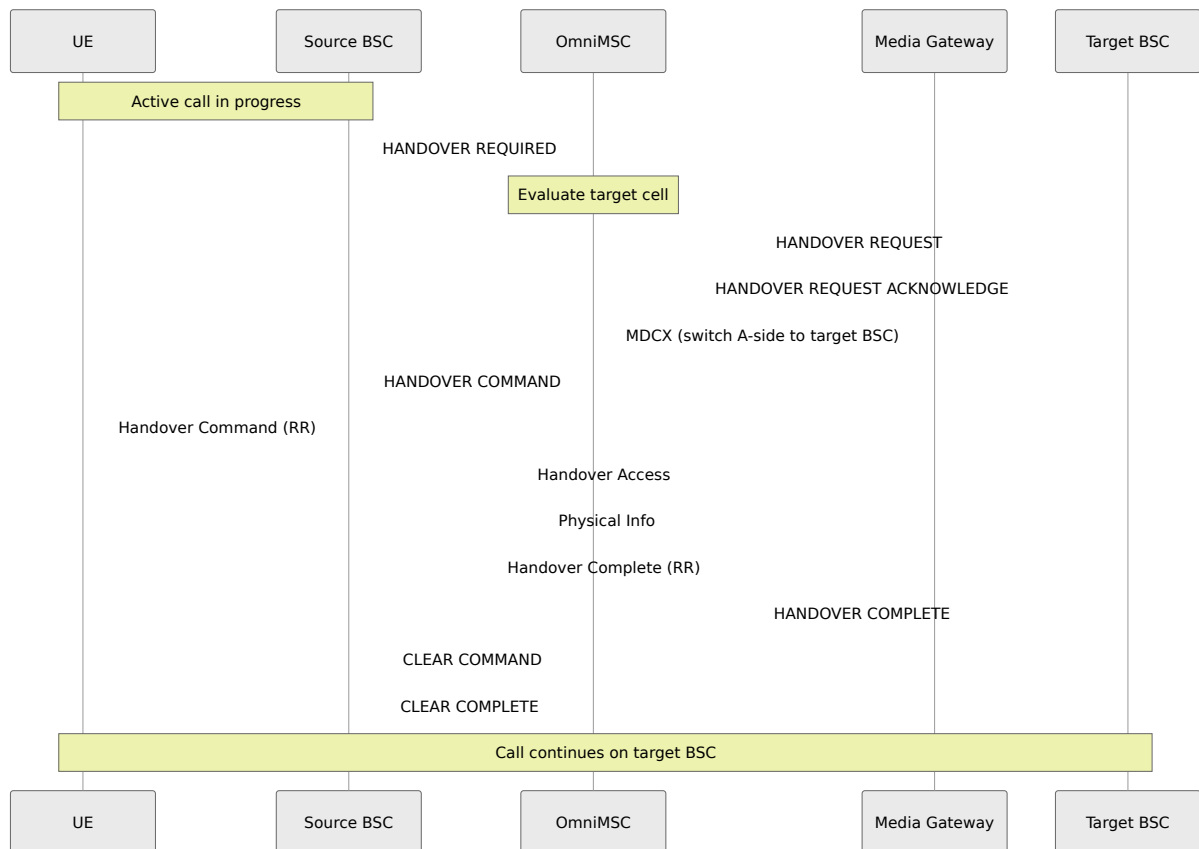
Location Update

Subscriber registers with the MSC. The MSC authenticates the subscriber and updates the HLR.



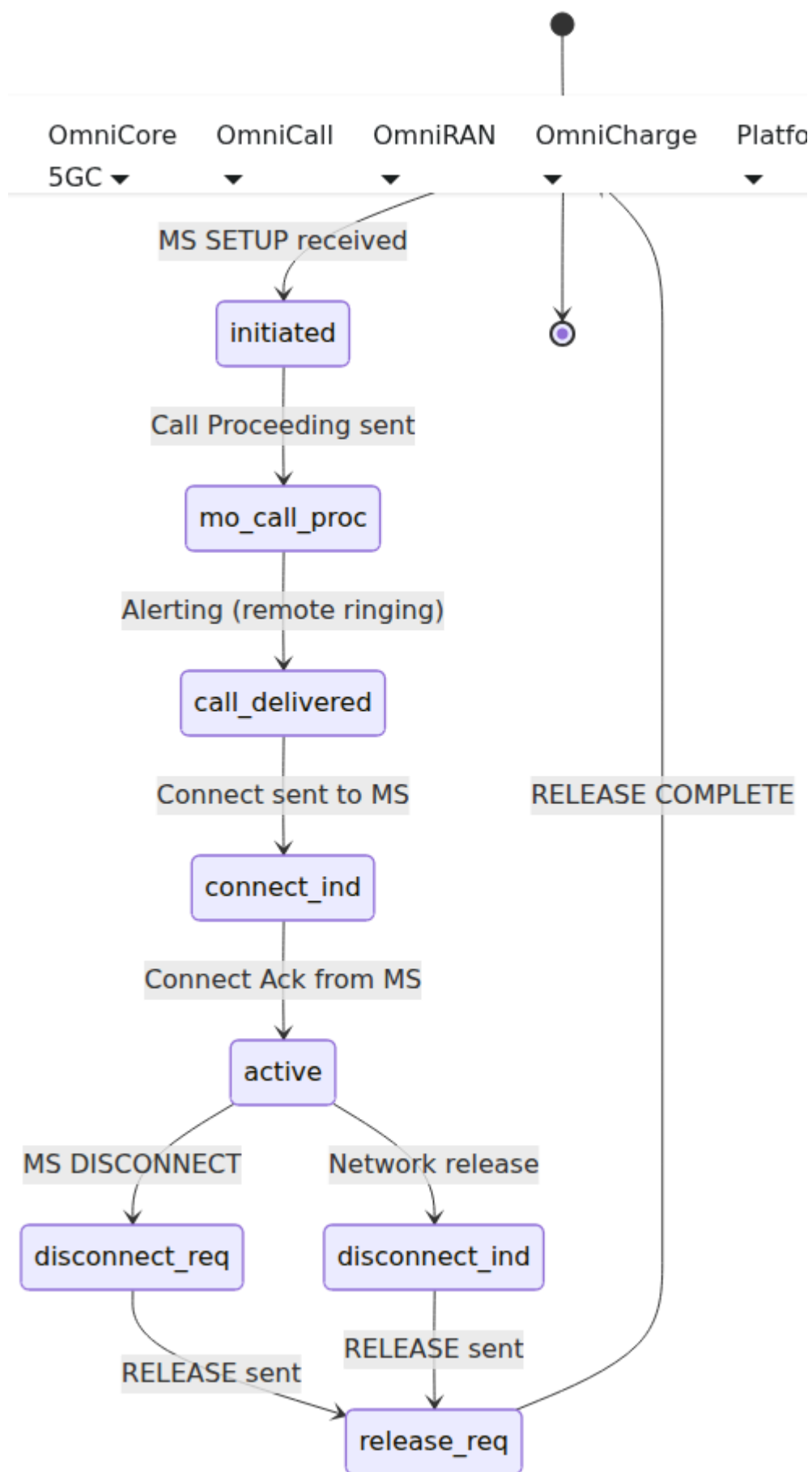
Intra-MSC Handover

Handover of an active call between two BSCs served by the same MSC.



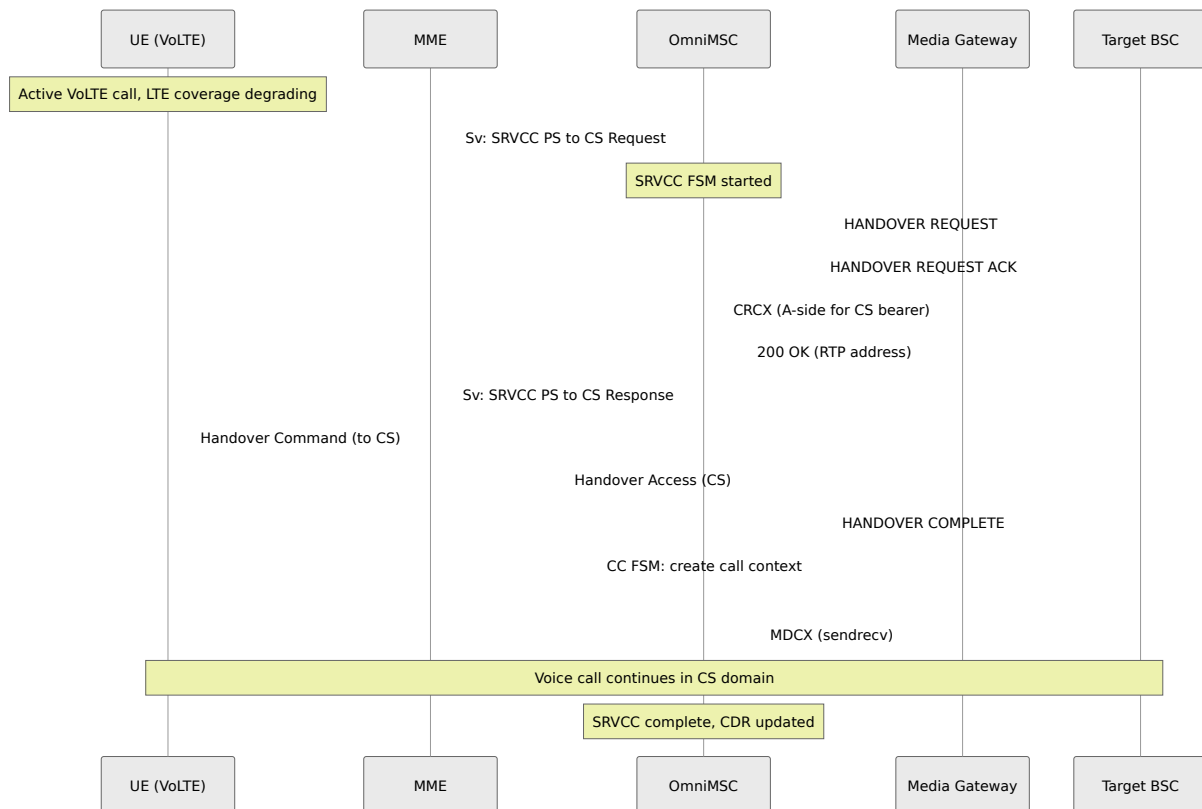
Inter-MS Handover

Handover of an active call from OmniMSC (MSC-A) to a target MSC (MSC-B).



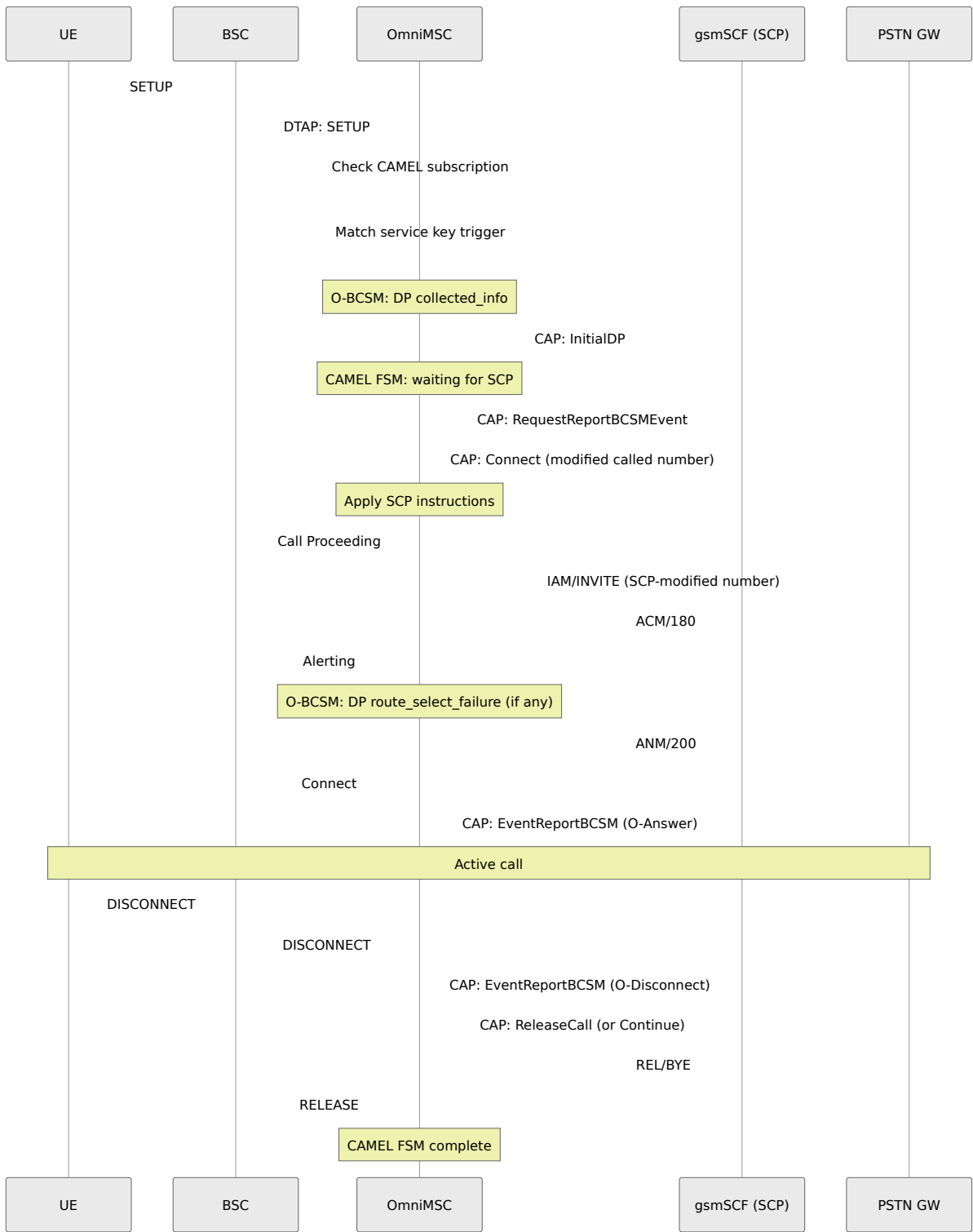
SRVCC (Single Radio Voice Call Continuity)

Handover of a VoLTE call from the IMS/LTE domain to the CS domain per 3GPP TS 23.216.



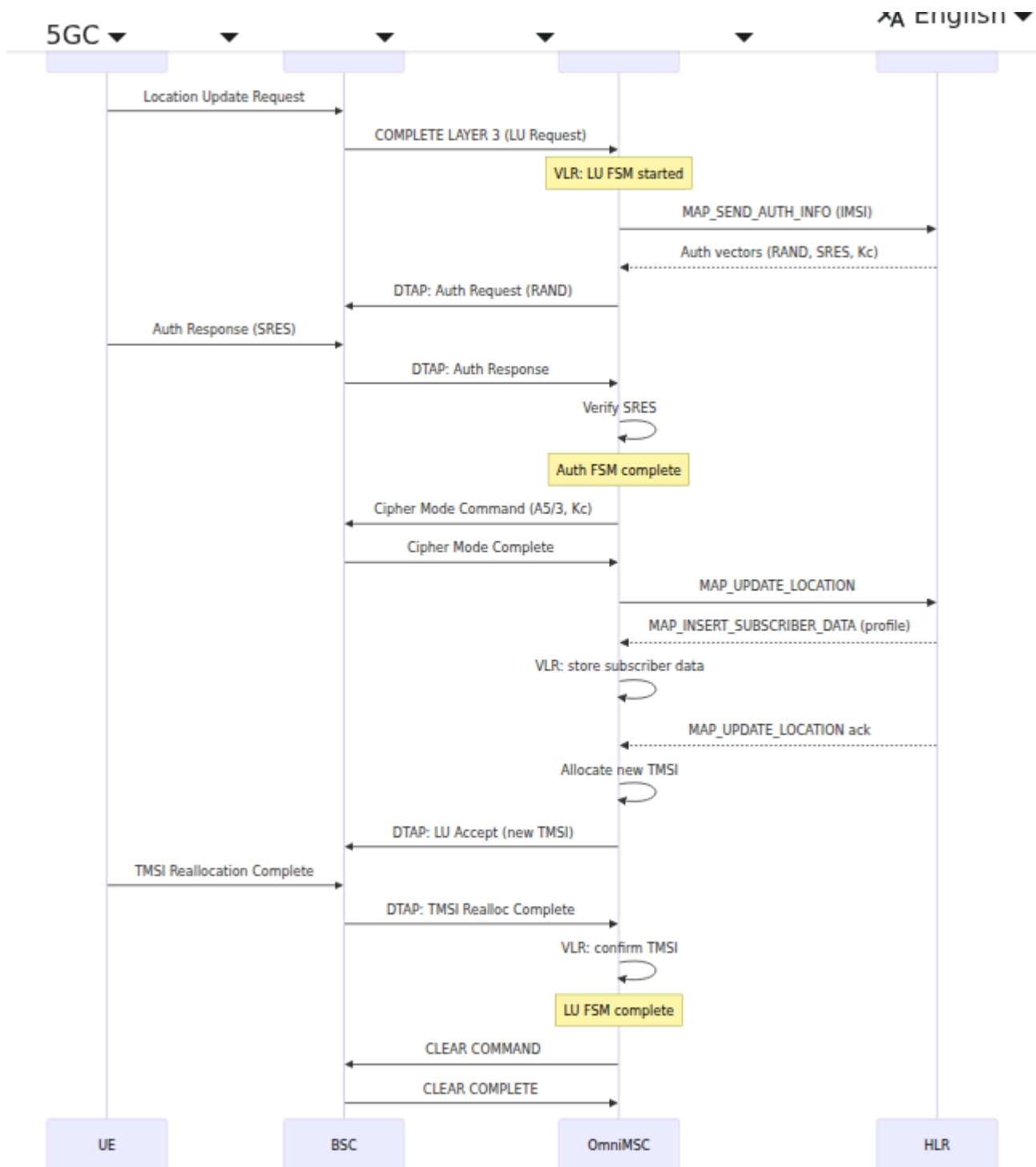
CAMEL-Triggered Call (SCP Interaction)

Call with CAMEL Originating BCSM (O-BCSM) interaction per 3GPP TS 23.078.



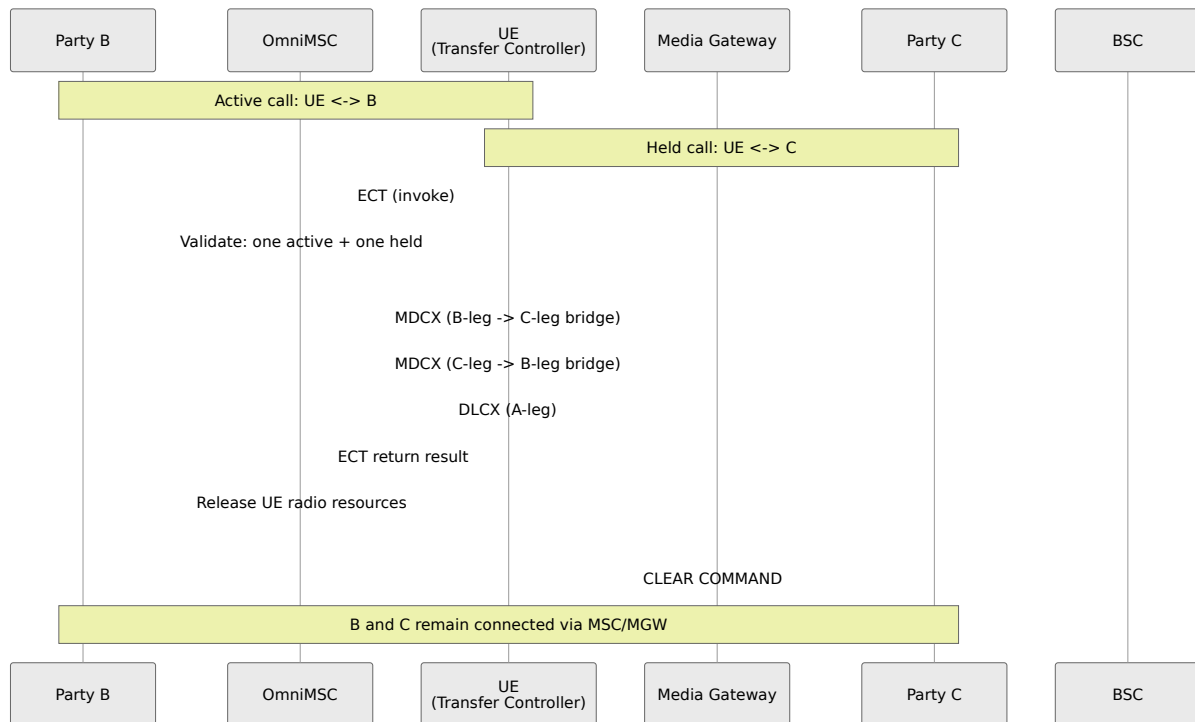
MPTY (BuildMPTY) Sequence Diagram

Multi-party conference call setup. The subscriber establishes two calls, then bridges them into a conference per 3GPP TS 24.084. For configuration, see [Advanced Call Features](#).



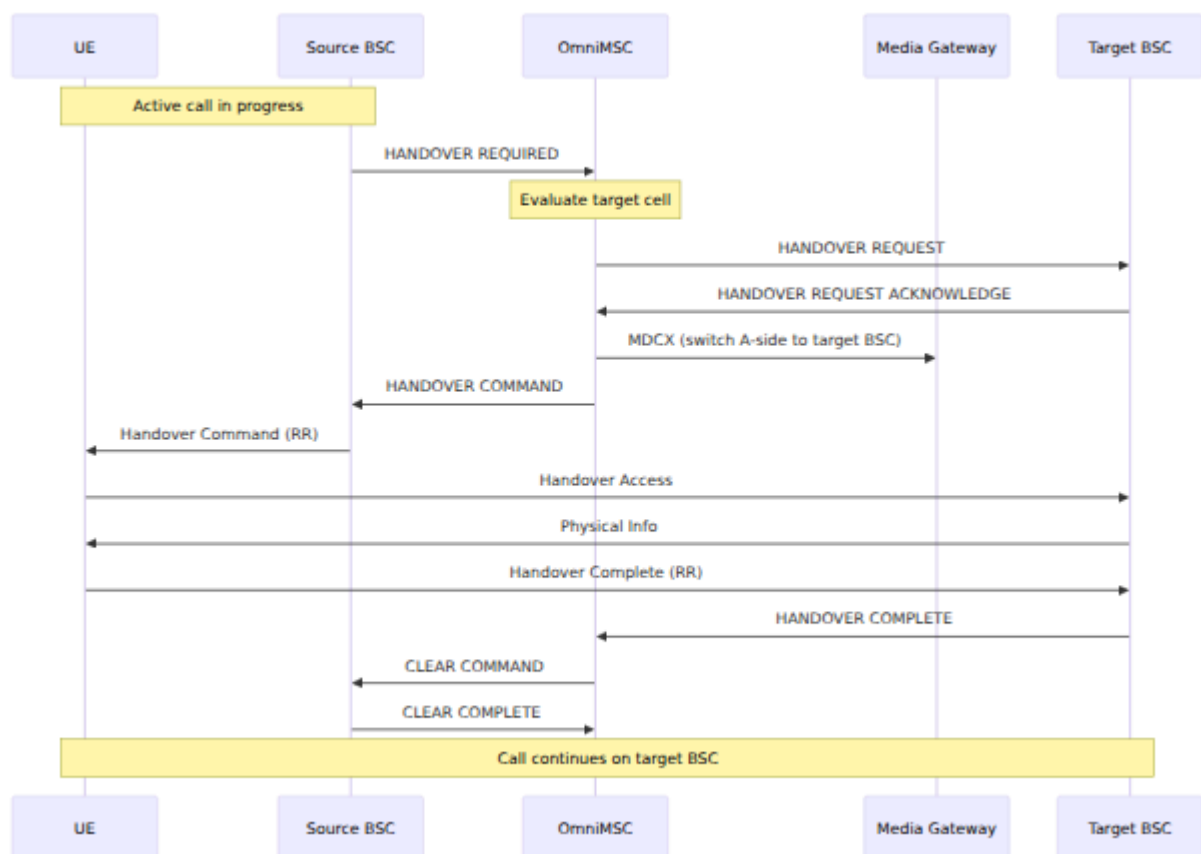
ECT (Explicit Call Transfer) Sequence Diagram

Explicit Call Transfer connects two remote parties and releases the transferring subscriber per 3GPP TS 24.091. For configuration, see [Advanced Call Features](#).



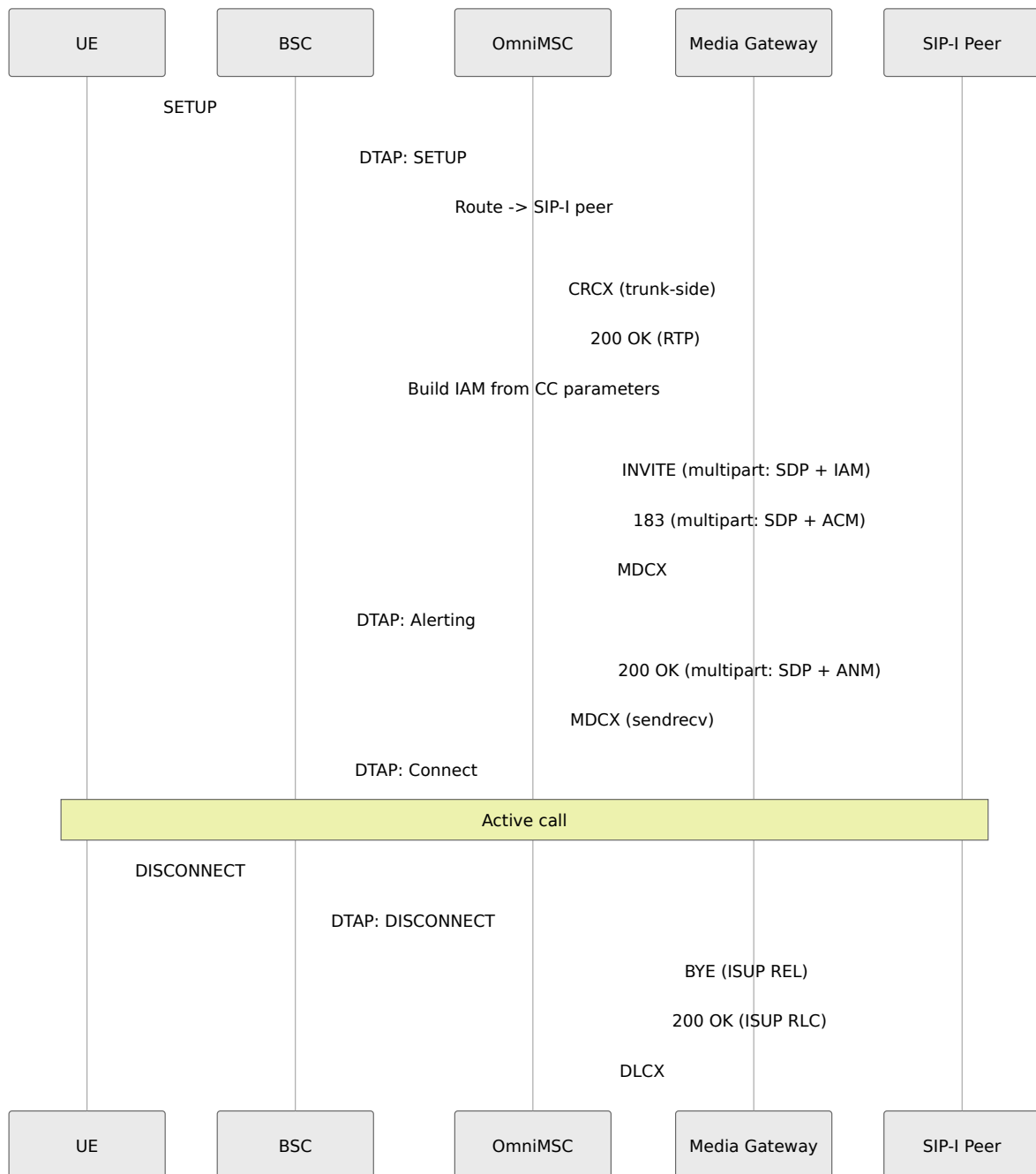
CSFB MT Call Sequence Diagram

Mobile-terminating call to an LTE-attached subscriber via Circuit-Switched Fallback per 3GPP TS 23.272. The MSC pages via the SGs interface, the UE falls back to 2G/3G, and the call proceeds over the A-interface. For SGs details, see [SGs Interface & CSFB](#).



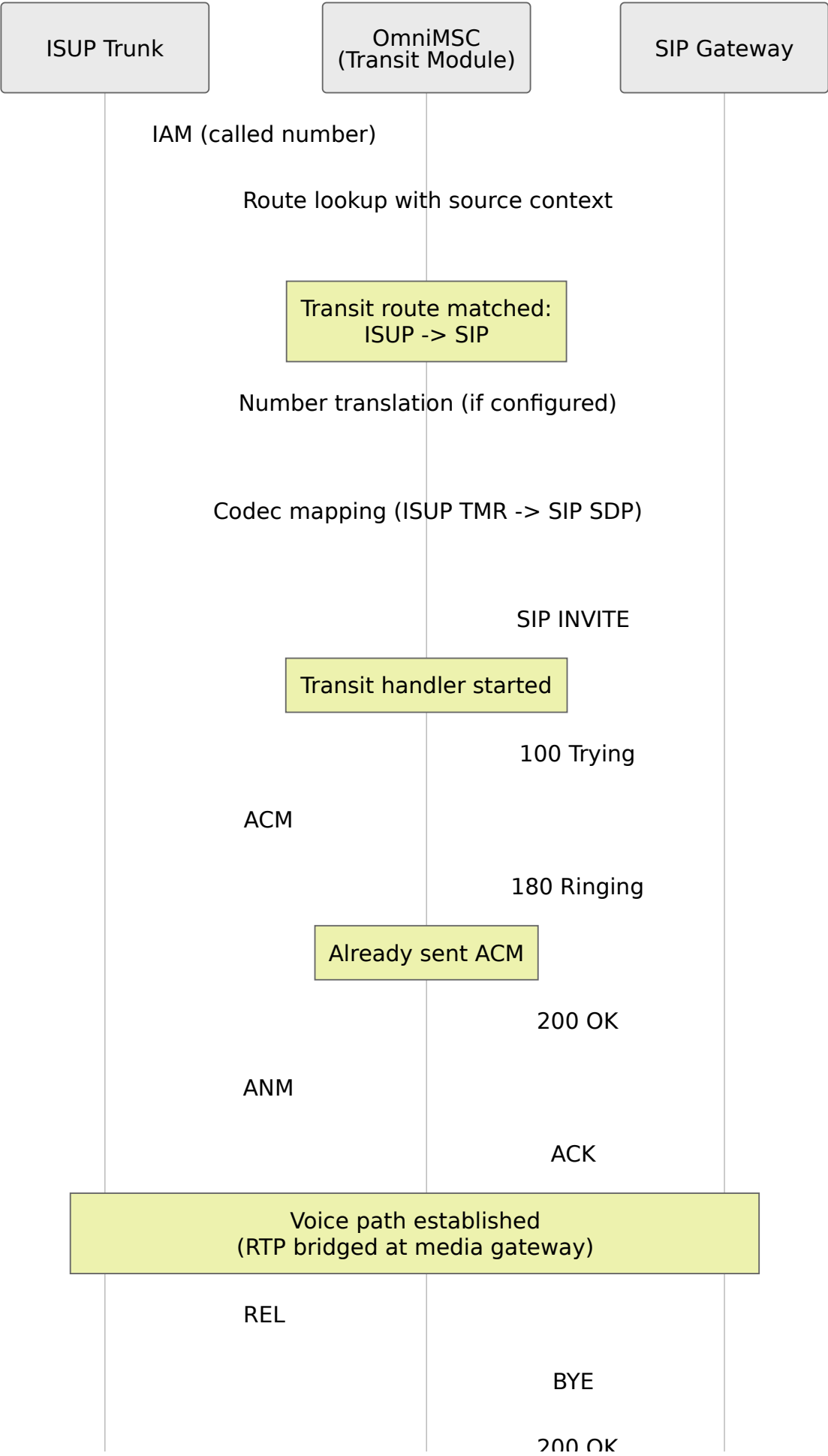
SIP-I Call Sequence Diagram

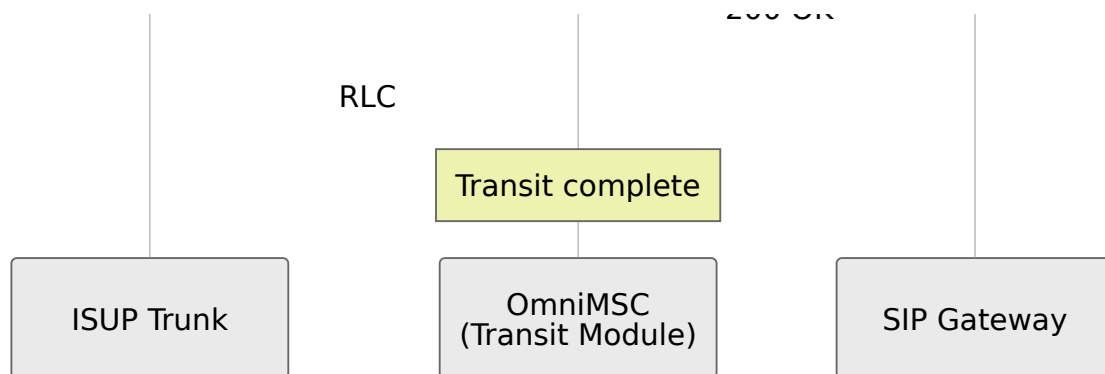
Outgoing call via SIP-I trunk with encapsulated ISUP per ITU-T Q.1912.5. The INVITE carries a multipart body containing SDP and the ISUP IAM. For SIP-I details, see [SIP-I Trunking](#).



ISUP-to-SIP Transit Call

Transit call interworking between an ISUP trunk and a SIP peer, bypassing the CC FSM.





CAMEL / CAP

This document describes the CAMEL (Customized Applications for Mobile Enhanced Logic) implementation in OmniMSC, including service key configuration, CAP dialogue handling, BCSM detection points, supported CAP operations, and TCAP transport.

For the full CAMEL-triggered call sequence diagram (InitialDP, Connect, EventReportBCSM), see [Call Flow Diagrams](#). For how CAMEL triggers fit into the routing pipeline (number analysis flow), see [Routing Configuration](#). For CAMEL-related CDR fields (FurnishChargingInformation, cause_for_term), see [Call Detail Records](#). For configuration of CAMEL service keys, see [Configuration Reference](#).

Overview

CAMEL provides a framework for mobile operators to deploy Intelligent Network (IN) services on top of the GSM/UMTS core network. OmniMSC acts as the gsmSSF (GSM Service Switching Function), interacting with an external gsmSCF (GSM Service Control Function, also known as the SCP) to provide real-time call control services such as prepaid charging, number translation, call screening, and virtual private networks.

The gsmSCF controls call processing by sending instructions to OmniMSC at defined detection points within the Basic Call State Model (BCSM). OmniMSC reports call events back to the gsmSCF and executes the received instructions (continue, connect to a different number, release the call, apply charging).

Service Key Configuration

Each subscriber may have one or more CAMEL subscriptions provisioned via MAP INSERT SUBSCRIBER DATA from the HLR. A CAMEL subscription includes a

service key, which identifies the IN service to invoke, and the gsmSCF address (Global Title) to contact.

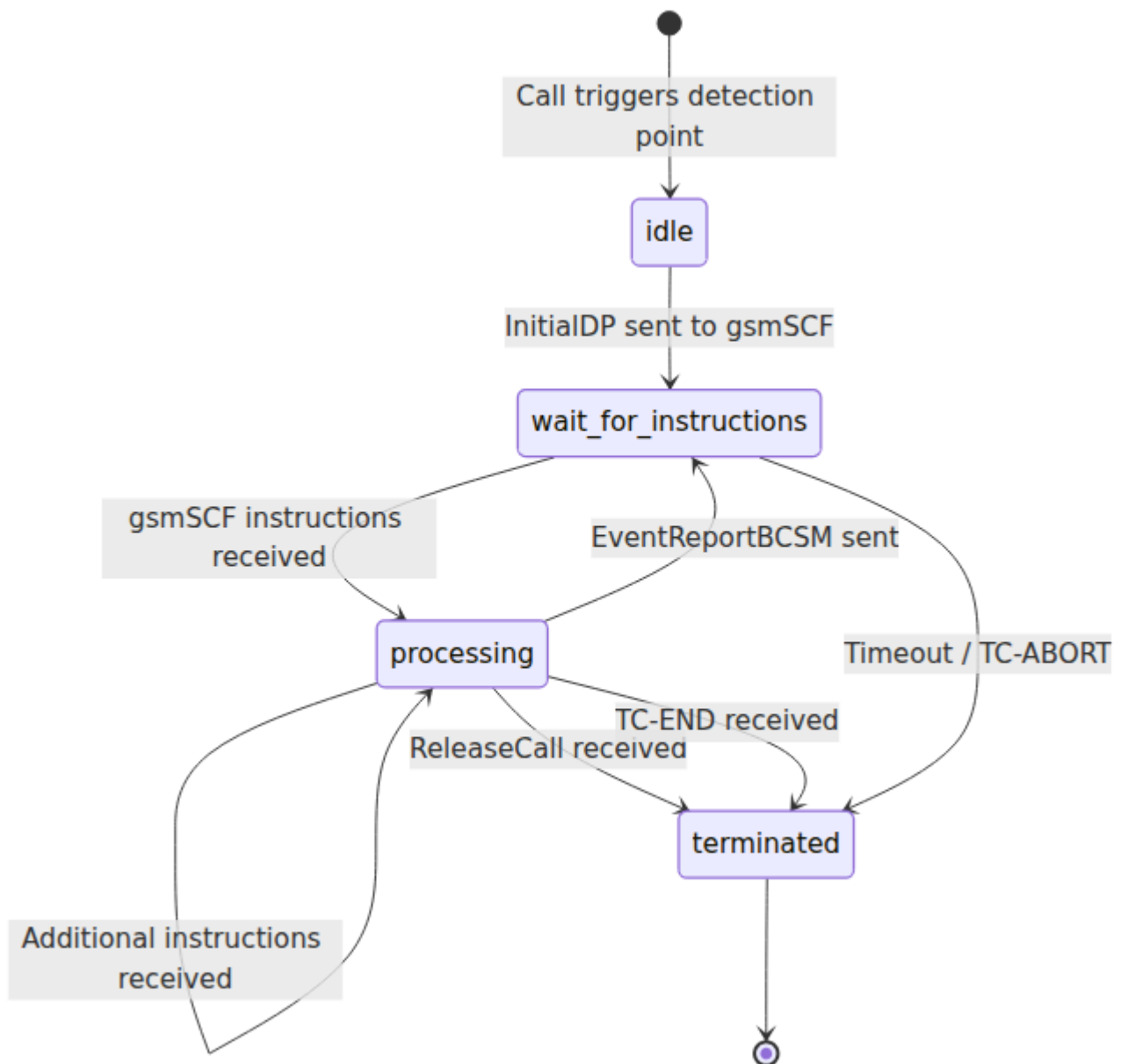
When a call triggers a CAMEL detection point (such as `collected_info` for MO calls or `terminating_attempt_authorized` for MT calls), OmniMSC checks the subscriber's CAMEL subscription data. If a matching service key is found, OmniMSC opens a CAP dialogue with the gsmSCF and sends an InitialDP operation.

Subscription Parameter	Description
Service key	Integer identifying the IN service (e.g., 1 for prepaid, 2 for VPN)
gsmSCF address	Global Title of the SCP to contact
Default call handling	Action if the SCP is unreachable: <code>:continue_call</code> or <code>:release_call</code>
TDP list	List of trigger detection points armed for this subscription
CAMEL phase	Supported CAMEL phase (Phase 1, 2, 3, or 4)

If the gsmSCF is unreachable or the TCAP dialogue fails, OmniMSC applies the default call handling action from the subscriber's CAMEL subscription data.

CAP Dialogue States

Each CAMEL interaction runs as an independent CAP dialogue within a TCAP transaction. The dialogue tracks the state of the SSF-SCF interaction from InitialDP through to termination.



State	Description
idle	Detection point triggered, preparing InitialDP
wait_for_instructions	InitialDP sent, awaiting gsmSCF response
processing	Executing gsmSCF instructions (Continue, Connect, ApplyCharging)
terminated	Dialogue complete, TCAP transaction closed

CAP Operations

OmniMSC supports the following CAP operations for CAMEL Phase 2 and Phase 3 service interaction.

SSF to SCF (OmniMSC to gsmSCF)

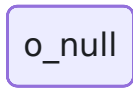
Operation	Description
InitialDP	Reports a triggered detection point with call parameters (service key, called/calling number, event type, location information)
EventReportBCSM	Reports a call event at an armed detection point (answer, disconnect, abandon, route select failure)
ApplyChargingReport	Reports the result of a charging operation (call duration, charge units consumed)
CallInformationReport	Reports call information requested by the gsmSCF (call duration, release cause)

SCF to SSF (gsmSCF to OmniMSC)

Operation	Description
Continue	Resume call processing at the current BCSM state
Connect	Route the call to a different destination number (number translation, VPN routing)
ReleaseCall	Release the call with a specified cause code
RequestReportBCSMEvent	Arm detection points for future event reporting (answer, disconnect, abandon)
ApplyCharging	Apply charging parameters (maximum call duration, charge advice)
FurnishChargingInformation	Provide free-format charging data to be included in the CDR
ResetTimer	Reset the SSF inactivity timer to prevent timeout during long SCP processing
SendChargingInformation	Send advice-of-charge information to the mobile station
CallInformationRequest	Request call information to be reported at call release

O-BCSM Detection Points

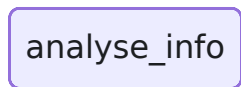
The Originating Basic Call State Model defines the detection points available for MO calls per 3GPP TS 23.078.



MO call initiated



Digits collected



Number analysis
complete



Remote party alerting



Remote party answers

Route select failure



Called party busy / no
answer

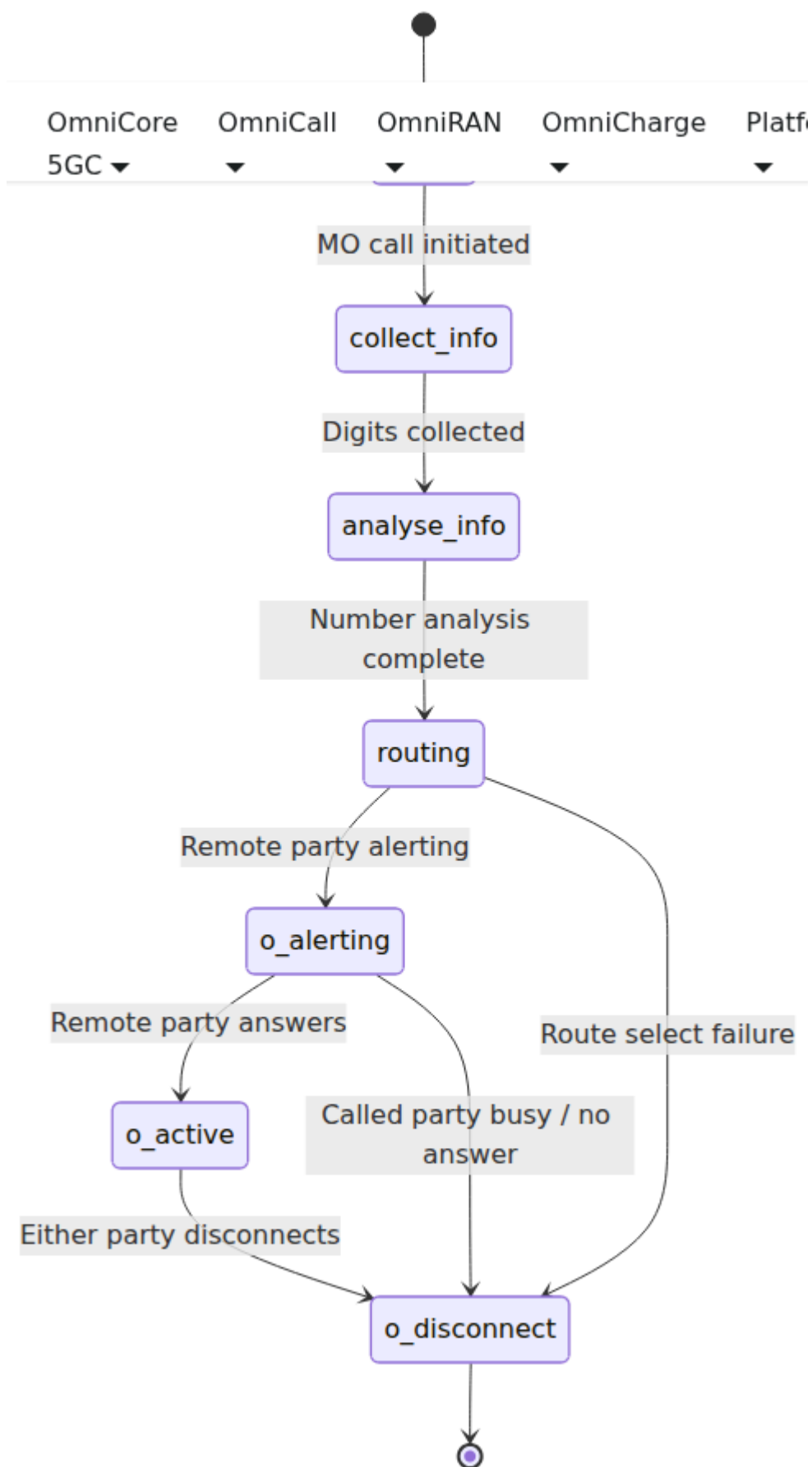
Either party disconnects



Detection Point	BCSM State	Trigger
collected_info (DP 2)	collect_info	Dialed digits available, before number analysis
analysed_info (DP 3)	analyse_info	Number analysis complete, before routing
route_select_failure (DP 4)	routing	Routing fails (no route, trunk busy, peer down)
o_called_party_busy (DP 5)	o_alerting	Called party busy
o_no_answer (DP 6)	o_alerting	Called party does not answer within timer
o_answer (DP 7)	o_active	Called party answers
o_disconnect (DP 9)	o_disconnect	Either party initiates disconnect

T-BCSM Detection Points

The Terminating Basic Call State Model defines the detection points available for MT calls.



Detection Point	BCSM State	Trigger
terminating_attempt_authorized (DP 12)	terminating_attempt_authorized	MT call received before paging
t_busy (DP 13)	t_alerting	Called subscriber busy
t_no_answer (DP 14)	t_alerting	Called subscriber does not answer within timer
t_answer (DP 15)	t_active	Called subscriber answers
t_disconnect (DP 17)	t_disconnect	Either party initiates disconnect

TCAP/CAP Transport

CAP operations are carried over TCAP (Transaction Capabilities Application Part) dialogues, which in turn use the SCCP/M3UA/SCTP transport stack. OmniMSC uses a generic BER decoder via the TcapDecoder module to parse incoming TCAP and CAP PDUs.

Transport Parameter	Value
SSN (remote, gsmSCF)	146
SSN (local, MSC/VLR/SSF)	8
TCAP dialogue type	Structured (TC-BEGIN, TC-CONTINUE, TC-END)
Encoding	ASN.1 BER (Basic Encoding Rules)
Application context	CAP v3 only: 0.4.0.0.1.0.50.1, 0.4.0.0.1.0.50.2, 0.4.0.0.1.0.50.3

The gsmSCF address is a Global Title, routed via SCCP Global Title Translation to the SCP node. OmniMSC maintains a TCAP transaction for the lifetime of each CAP dialogue, using TC-CONTINUE to exchange operations within the dialogue and TC-END to close it.

References

Reference	Title	Relevance
3GPP TS 23.078	CAMEL Phase 3 -- Stage 2	CAMEL architecture, BCSM model, detection points
3GPP TS 29.078	CAMEL Application Part (CAP) -- Stage 3	CAP protocol encoding, ASN.1 definitions
ITU-T Q.771-Q.775	Transaction Capabilities	TCAP dialogue and transaction handling
ITU-T Q.711-Q.716	SCCP	Signaling connection for TCAP transport
3GPP TS 22.078	CAMEL -- Service Description	CAMEL service requirements

Call Detail Records

This document describes the Call Detail Record (CDR) subsystem in OmniMSC by Omnitouch. CDRs are generated in compliance with 3GPP TS 32.298 and provide the charging and audit trail for all circuit-switched services handled by the MSC.

For CDR-related configuration parameters, see [Configuration Reference](#). For the CDR Statistics page in the web interface, see [Control Panel Guide](#). For CDR-related Prometheus metrics and alarm events, see [Metrics and Monitoring](#).

Overview

OmniMSC generates CDRs for voice calls, SMS transactions, location updates, and roaming events. Each CDR captures the subscriber identity, service details, timestamps, location, and termination cause for a single transaction. CDRs are collected in memory, buffered, and periodically flushed to files in ASN.1 BER format following the record structures defined in 3GPP TS 32.298.

The CDR subsystem consists of two components:

- **CDR Collector** -- receives events from the Call Control FSM, VLR location update procedures, and SMS handlers. It correlates events for active calls (setup, alerting, answer, release) into complete CDR records and manages per-record-type sequence numbers.
 - **CDR Writer** -- writes encoded CDR records to files on disk, handling file rotation based on size, record count, and time interval.
-

Record Types

OmniMSC supports the following CDR record types, each identified by a unique ASN.1 tag per TS 32.298.

ASN.1 Tag	Record Type	Description
0	MOCallRecord	Mobile Originated voice call. Generated when a subscriber originates a voice call.
1	MTCallRecord	Mobile Terminated voice call. Generated when a subscriber receives a voice call.
3	TransitRecord	Transit call. Generated for calls that transit the MSC without originating or terminating at a local subscriber.
5	MOSMSRecord	Mobile Originated SMS. Generated when a subscriber sends a short message.
6	MTSMSRecord	Mobile Terminated SMS. Generated when a subscriber receives a short message.
10	SSActionRecord	Supplementary service action. Generated when a subscriber invokes a supplementary service action.
13	LocUpdateHLRRecord	Location Update (HLR). Generated for location update procedures at the HLR level, tracking MSC/VLR changes.
14	LocUpdateVLRRecord	Location Update (VLR). Generated for location update procedures at the VLR level, tracking location area changes, authentication results, and TMSI allocation.
17	RoamingRecord	Roaming event. Generated for inter-MSC roaming events.

CDR Fields

Voice Call Records (MOCallRecord and

MTCallRecord)

Field	Description
served_imsi	IMSI of the subscriber who originated or received the call
served_msisdn	MSISDN (phone number) of the served subscriber
served_imei	IMEI of the mobile equipment used
calling_number	Calling party number (A-number)
called_number	Called party number (B-number), present in MO records
connected_number	Number of the party actually connected (may differ from called number due to forwarding)
recording_entity	Address of the MSC that generated the CDR
msc_address	E.164 address of the MSC
msc_incoming_tkgp	Incoming trunk group name
msc_outgoing_tkgp	Outgoing trunk group name
location	Subscriber location at time of call, including Location Area Code (LAC) and Cell Identity (CI)
basic_service	Bearer service or teleservice code identifying the service type
seizure_time	UTC timestamp when the call was initiated (setup message received)

Field	Description
answer_time	UTC timestamp when the call was answered (may be nil for unanswered calls)
release_time	UTC timestamp when the call was released
call_duration	Duration of the call in seconds, measured from answer to release. Zero for unanswered calls.
radio_chan_used	Radio channel type used (full rate or half rate)
cause_for_term	Reason for call termination (see Cause for Termination below)
diagnostics	Diagnostic information: GSM 04.08 cause code, MAP error code, or network-specific cause
call_reference	Unique call reference number
sequence_number	Per-record-type sequence number for gap detection by downstream billing systems
ms_classmark	Mobile station classmark information
system_type	Access network type: GERAN, UTRAN, or unknown
partial_record_type	For partial CDRs: indicates whether this is an intermediate or last partial record

SMS Records (MOSMSRecord and MTSMSRecord)

Field	Description
served_imsi	IMSI of the subscriber
served_msisdn	MSISDN of the subscriber
served_imei	IMEI of the mobile equipment
service_centre	Address of the SMS Service Centre
recording_entity	Address of the recording MSC
location	Subscriber location (LAC/CI)
message_reference	SMS message reference number (MO only)
destination_number	SMS destination number (MO only)
originating_number	SMS sender number (MT only)
origination_time	Timestamp of SMS origination (MO) or delivery (MT)
sms_result	Result of SMS delivery: success, delivery failure, or forwarded

Location Update Records

Field	Description
served_imsi	IMSI of the subscriber
served_msisdn	MSISDN of the subscriber (VLR records only)
recording_entity	Address of the recording entity
update_time	UTC timestamp of the location update
update_type	Type of update: normal location update, periodic location update, IMSI attach, or IMSI detach
old_location / new_location	Previous and new location information (VLR records: LAC/CI)
old_msc / new_msc	Previous and new MSC addresses (HLR records)
old_vlr / new_vlr	Previous and new VLR addresses (HLR records)
vlr_result / hlr_result	Outcome of the location update procedure
authentication_result	Authentication outcome: success, failure (no vectors), failure (auth mismatch), or not performed (VLR records only)
tmsi_allocated	New TMSI value if one was allocated during the procedure (VLR records only)

Cause for Termination

The `cause_for_term` field records why a call was terminated. The following values are defined per TS 32.298.

Cause	Integer Value	Description
normal_release	0	Normal call clearing by either party
partial_record	1	Partial CDR generated for a long-duration call (intermediate record)
partial_record_call_reestablishment	2	Partial record due to call re-establishment
unsuccessful_call_attempt	3	Call setup failed before answer (busy, no answer, routing failure)
abnormal_release	4	Abnormal release due to radio link failure, protocol error, or system error
CAMEL_init_call_release	5	Call released by the CAMEL service (SCP initiated release)
management_intervention	52	Call released by operator intervention

CDR Collector

The Collector is a GenServer that acts as the central collection point for CDR events. It receives event notifications from the Call Control FSM, VLR, and SMS handlers, and correlates them into complete CDR records.

Event Flow

For voice calls, the Collector receives a sequence of events over the call lifetime:

1. Call setup -- records the subscriber identity, called/calling numbers, direction (MO or MT), seizure time, and service type.
2. Call alerting -- logged for diagnostics but does not generate a CDR field.
3. Call answer -- records the answer timestamp and starts the partial CDR timer for long calls.
4. Call release -- calculates the call duration, selects the termination cause, generates the final CDR record, and buffers it for writing.

For SMS and location updates, the Collector generates a CDR record immediately from a single event notification.

Buffering and Flushing

CDR records are accumulated in an in-memory buffer. The buffer is flushed to the Writer under two conditions:

- A periodic flush timer fires (default interval: 5000 ms).
- The buffer reaches its maximum size (default: 1000 records), triggering an immediate flush.

Partial CDR Generation

For long-duration calls, the Collector generates intermediate partial CDR records at a configurable interval (default: 3600 seconds / 1 hour). Each partial CDR captures the call state up to that point. The final CDR record upon call release is marked as the last partial if any intermediate partials were generated. This ensures that downstream billing systems can reconstruct the complete call duration even if the MSC fails before the call ends.

Sequence Numbers

The Collector maintains independent sequence number counters for each record type (MO call, MT call, MO SMS, MT SMS, roaming, HLR location update, VLR location update). Sequence numbers increment monotonically and wrap at 10000. Downstream billing systems use sequence numbers to detect gaps indicating lost CDR records.

CDR File Naming

CDR files follow a naming convention that includes the MSC identity, timestamp, and sequence number:

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

Where:

- NodeID is the MSC name (from the recording_entity configuration).
- Date is in YYYYMMDD format.
- Time is in HHMMSS format.
- SeqNum is a zero-padded 4-digit sequence number (wraps at 10000).

For example: MSC01_20260329_143022_0001.dat

Files are written in ASN.1 BER format containing a sequence of CDR records as defined in TS 32.298.

File Rotation

CDR files are rotated (closed and a new file opened) when any of the following conditions are met:

- The file exceeds the configured maximum size (default: 10 MB).
- The file contains the configured maximum number of records (default: 100,000).

- The configured time interval has elapsed since the file was opened (default: 3600 seconds).
 - An explicit rotation is triggered via the API.
-

Configuration

The CDR subsystem is configured through the Collector and Writer startup parameters.

Collector Parameters

Parameter	Default	Description
recording_entity	(required)	Address or name of the recording MSC, written into every CDR record
msc_address	Same as recording_entity	E.164 MSC address included in call records
flush_interval	5000 ms	Interval between periodic buffer flushes to the Writer
buffer_size	1000	Maximum number of CDR records held in the buffer before a forced flush
partial_cdr_interval	3600 seconds	Interval for generating intermediate partial CDRs on long-duration calls

Writer Parameters

Parameter	Default	Description
output_dir	(required)	Directory where CDR files are written. Created automatically if it does not exist.
node_id	(required)	Network element identifier used in CDR file names
extension	.dat	File extension for CDR files
max_file_size	10,000,000 bytes (10 MB)	Maximum file size before rotation
max_records	100,000	Maximum number of records per file before rotation
rotation_interval	3600 seconds	Maximum time a file remains open before rotation. Set to nil to disable time-based rotation.

CDR Web UI

The CDR Statistics page in the Control Panel displays real-time information about the CDR subsystem.

CDR Statistics page showing writer status, buffer depth, active tracked calls, and per-type sequence numbers.

Field	Description
Records in File	Number of CDR records written to the current output file
Pending in Buffer	Number of CDR records buffered in memory awaiting the next flush
Active Calls Tracked	Number of calls with open CDR state (between setup and release)
Current File	Path of the current CDR output file, or "No file open" if idle
Sequence Numbers	Per-record-type sequence counters showing the next sequence number for each CDR type

The page auto-refreshes every 5 seconds via WebSocket.

3GPP Specification References

Specification	Title	Relevance
TS 32.298	Charging Data Record Encoding Rules	CDR record types, ASN.1 structure, field definitions
TS 32.205	Charging Data Description for CS Domain	CS domain charging principles and CDR content requirements
TS 32.015	Charging and Billing	Overall charging architecture context

Configuration Reference

This document covers every configuration parameter for OmniMSC. Configuration is specified in Elixir config files (`config.exs`, `dev.exs`, `runtime.exs`) and can be overridden at runtime via environment variables.

For a quick start example, see the [Operations Guide](#).

MSC Identity

```
config :omnimsc, :msc
```

Defines the MSC's SS7 network identity, used for SCCP addressing, MAP operations, Location Area identification, and CDR generation. The active MSC identity parameters are visible in the System page of the control panel — for more, see [Control Panel Guide](#).

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

Parameter	Type	Required	Default	Description
point_code	integer or [integer, integer, integer]	Yes	0	SS7 point code. May be specified as a flat integer in 14-bit ITU format [a, b, c] (encoded as $a*2048 + b*8 + c$).
global_title	string	Yes	"000000000000"	SCCP Global Title (E.164 number) for MAP routing to HLR, SMSc, and peer nodes.
name	string	Yes	"OMNIMSC01"	Logical MSC name. Used in CDR recording_engine field, alarm descriptions, and log messages.
msc_number	string	Yes	--	E.164 address of the MSC, sent to the HLR in MAP Update Location and used for MAP call routing.
vlr_number	string	Yes	--	E.164 address of the co-located VLR, sent to the HLR in MAP Update Location

Parameter	Type	Required	Default	Description
				Typically the same as <code>msc_number</code> .
<code>mcc</code>	<code>integer</code>	Yes	--	Mobile Country Code (3 digits). Combined with <code>mnc</code> and <code>lac</code> to form the Location Area Identity (broadcast in System Information).
<code>mnc</code>	<code>integer</code>	Yes	--	Mobile Network Code (2 or 3 digits).
<code>lac</code>	<code>integer</code>	Yes	--	Location Area Code (16-bit). Identifies the location area served by this MSC/VLR.
<code>allowed_a5</code>	<code>list(atom)</code>	No	<code>[:a5_1, :a5_3]</code>	Permitted A5 cipher algorithm for air-interface encryption. Valid values: <code>:a5_0</code> , <code>:a5_1</code> , <code>:a5_2</code> , <code>:a5_3</code> . Algorithm negotiation prefers A5/3 > A5/1 > A5/0 (see TS 48.008).

HLR

```
config :omnimsc, :hlr
```

Configures the remote HLR address for MAP operations (Send Authentication Info, Update Location, Insert Subscriber Data, Purge MS).

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

Parameter	Type	Required	Default	Description
<code>address</code>	<code>string</code>	Yes	--	HLR Global Title (E.164 number) for MAP routing.
<code>point_code</code>	<code>integer</code> or <code>[integer, integer, integer]</code>	No	--	HLR SS7 point code for direct MTP3 routing when Global Title Translation is not used. May be a flat integer or ITU 14-bit format <code>[a, b, c]</code> .

VLR

```
config :omnimsc, :vlr
```

Controls Visitor Location Register behavior including authentication policy, TMSI management, and lab/guest modes.

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


Parameter	Type	Required	Default	
<code>hlr_adapter</code>	<code>module</code>	No	<code>Omnimsc.VLR.HLR.Default</code>	H co ul 0 a 0 se on 0 pl si TI se 0 e:
<code>auth_required</code>	<code>boolean</code>	No	<code>true</code>	W A bo W U S
<code>tmsi_realloc</code>	<code>boolean</code>	No	<code>true</code>	W no st U st co
<code>num_auth_vectors</code>	<code>integer</code>	No	<code>1</code>	N ve H A po

Parameter	Type	Required	Default	
				H si m
lab_mode	boolean	No	false	W SI re te w th
guest_mode	boolean	No	false	W su th ra M do

M3UA / STP

`config :omnimsc, :m3ua_asp`

Configures the M3UA ASP (Application Server Process) connection to a Signalling Transfer Point. All SS7 signalling (A-interface, MAP to HLR/SMSc, ISUP) is routed through this link.

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

Parameter	Type	Required	Default	Description
<code>enabled</code>	<code>boolean</code>	No	<code>false</code>	Whether to start the M3UA ASP client. When <code>false</code> , no STP connection is established.
<code>local_ip</code>	<code>tuple</code>	No	<code>{0, 0, 0, 0}</code>	Local SCTP bind IP address as an Erlang tuple.
<code>local_port</code>	<code>integer</code>	No	<code>0</code>	Local SCTP bind port. Use <code>0</code> to let the OS assign an ephemeral port.
<code>remote_ip</code>	<code>tuple</code>	Yes	--	STP SCTP IP address as an Erlang tuple.
<code>remote_port</code>	<code>integer</code>	No	<code>2905</code>	STP SCTP port. Port 2905 is the IANA-assigned M3UA port.

Parameter	Type	Required	Default	Description
<code>routing_context</code>	<code>integer</code>	No	--	M3UA routing context value. Must match the STP's AS configuration for this ASP.
<code>receive_watchdog</code>	<code>boolean</code>	No	<code>true</code>	Whether to enable the M3UA heartbeat watchdog. When <code>true</code> , the ASP monitors for missing BEAT-Ack and triggers link recovery.
<code>receive_watchdog_idle</code>	<code>integer</code>	No	<code>15</code>	Idle interval in seconds before the receive watchdog considers the link stalled.

The local point code is taken from `:msc point_code`; a `point_code` set under `:m3ua_asp` is not read. The MTP3 network indicator is not configurable here.

Direct SCTP listeners (for BSC connections without an STP) are configured under `config :omnimsc, :sctp`:

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

Parameter	Type	Required	Default	Description
<code>name</code>	<code>atom</code>	Yes	--	Logical listener name for SCTP association lookups and control panel display.
<code>ip</code>	<code>tuple</code>	No	<code>{0, 0, 0, 0}</code>	Bind IP address. Use <code>{0, 0, 0, 0}</code> for all interfaces.
<code>port</code>	<code>integer</code>	No	<code>2905</code>	SCTP bind port.
<code>ppid</code>	<code>integer</code>	No	<code>3</code>	SCTP Payload Protocol Identifier. Value <code>3</code> indicates M3UA (RFC 4666).

Runtime override: Set `SCTP_LISTEN_IP` and `SCTP_LISTEN_PORT` environment variables.

SIP

```
config :omnimsc, :sip
```

Configures the SIP listener and SIP peer gateways for VoIP interconnection.

```

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

```

SIP Listener Parameters

Parameter	Type	Required	Default	Description
<code>signaling_address</code>	<code>string</code>	No	--	IP address used in SIP Contact headers and SDP <code>c=</code> lines. Must be reachable by SIP peers. Falls back to the SCTP listener address if not set.
<code>listen_ip</code>	<code>tuple</code>	No	<code>{0, 0, 0, 0}</code>	SIP listener bind address.
<code>listen_port</code>	<code>integer</code>	No	<code>5060</code>	SIP listener port.
<code>transport</code>	<code>atom</code>	No	<code>:udp</code>	Default transport protocol. One of <code>:udp</code> , <code>:tcp</code> , <code>:tls</code> .

SIP Peer Parameters

Each peer in the `peers` list accepts the following:

Parameter	Type	Required	Default	Description
<code>name</code>	<code>string</code>	Yes	--	Logical peer name. Referenced in route table entries with <code>:sip</code> .
<code>address</code>	<code>string</code>	Yes	--	Peer IP address or hostname.
<code>port</code>	<code>integer</code>	No	<code>5060</code>	Peer SIP port.
<code>transport</code>	<code>atom</code>	No	<code>:udp</code>	Transport for this peer: <code>:udp</code> , <code>:tcp</code> , or <code>:tls</code> .
<code>codecs</code>	<code>list(atom)</code>	No	<code>[:pcmu, :pcma]</code>	Supported audio codecs. Valid values are <code>:pcmu</code> , <code>:pcma</code> , <code>:g722</code> , <code>:g729</code> , <code>:amr_wb</code> .
<code>max_channels</code>	<code>integer</code>	No	<code>100</code>	Maximum concurrent calls to this peer. Calls exceeding <code>max_channels_reject</code> are rejected when the limit is reached.
<code>options_interval</code>	<code>integer</code> or <code>nil</code>	No	<code>nil</code>	Interval in seconds between SIP OPTIONS keep-alive probes. Peer state transitions to <code>:disconnected</code> if OPTIONS responses cease. Set to <code>nil</code> to disable.

For routing configuration that references these peers, see [Routing Configuration](#). For SIP OPTIONS keepalive behavior and peer health states, see [SIP Trunking](#).

MGCP / Media

`config :omnimsc, :mgcp` and `config :omnimsc, :media`

MGCP (Media Gateway Control Protocol, RFC 3435) is used to control media gateways for bearer path setup. The MSC acts as the MGCP Call Agent, issuing CRCX, MDCX, and DLCX commands to gateways. The `:media` key selects which media control protocol to use.

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

MGCP Parameters

Parameter	Type	Required	Default	Description
<code>listen_port</code>	<code>integer</code>	No	<code>2727</code>	Local UDP port for the MGCP Call Agent (RFC 3435 Sec 2.2). Set to <code>0</code> to disable the MGCP transport (e.g., in test).
<code>gateways</code>	<code>list(map)</code>	No	<code>[]</code>	List of managed media gateways.

Gateway Parameters

Parameter	Type	Required	Default	Description
<code>name</code>	<code>string</code>	Yes	--	Logical gateway identifier used for lookups and control panel display.
<code>address</code>	<code>string</code>	Yes	--	IP address of the media gateway.
<code>port</code>	<code>integer</code>	No	<code>2427</code>	MGCP port on the gateway.
<code>domain</code>	<code>string</code>	Yes	--	Gateway domain name used in endpoint naming (e.g., <code>aa1n/1@mgw</code>). Required — there is no default.
<code>endpoints</code>	<code>list</code>	No	<code>[]</code>	Pre-declared endpoint identifiers on the gateway.
<code>max_connections</code>	<code>integer</code>	No	<code>1000</code>	Maximum concurrent connections the MSC will place on this gateway.

Media Mode

Parameter	Type	Required	Default	Description
<code>gateway</code>	<code>string</code>	No	<code>"MGW-01"</code>	Name of the default gateway (must match a gateway <code>name</code> from the MGCP or Megaco config).
<code>mode</code>	<code>atom</code>	No	<code>:megaco</code>	Media control protocol: <code>:mgcp</code> for RFC 3435 or <code>:megaco</code> for ITU-T H.248. The compiled-in fallback when unset is <code>:megaco</code> ; the shipped <code>config.exs</code> sets <code>:mgcp</code> explicitly.

Megaco Transport

`config :omnimsc, :megaco`

Used when `:media mode` is `:megaco` (ITU-T H.248).

Parameter	Type	Required	Default	Description
<code>listen_port</code>	<code>integer</code>	No	<code>2944</code>	Local UDP port for the Megaco/H.248 Media Gateway Controller.

SMSc

`config :omnimsc, :smsc`

Configures the Short Message Service Centre address for MAP MT-ForwardSM and MO-ForwardSM operations.

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

Parameter	Type	Required	Default	Description
address	string	Yes	--	SMS Global Title (E.164 number) for MAP routing.

CDR

```
config :omnimsc, :cdr
```

CDR records are generated per 3GPP TS 32.250 by the CDR Collector and written to files in ASN.1 BER format (3GPP TS 32.298) by the CDR Writer. File naming follows the pattern `<NodeID>_<YYYYMMDD>_<HHMMSS>_<SeqNum>.dat`.

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

Parameter	Type	Required	Default	Description
<code>output_dir</code>	<code>string</code>	Yes	<code>"/tmp/omnimsc/cdr"</code>	Directory for CDR output files. Must be writable. BEAM will create automatically if it does not exist.
<code>max_file_size</code>	<code>integer</code>	No	<code>10,000,000</code>	Maximum file size in bytes (approx 10 MB) before a new file is created when the current one is exceeded.
<code>max_records</code>	<code>integer</code>	No	<code>100,000</code>	Maximum number of CDR records per file.
<code>rotation_interval</code>	<code>integer</code>	No	<code>3600</code>	Time interval in seconds for file rotation. A new CDR file will be created every 3600 seconds regardless of file size or record count.

Routes

```
config :omnimsc, :routes
```

Defines prefix-based routing rules that map dialed number prefixes to destinations. The route table uses longest-prefix match with priority as a tiebreaker.

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

Parameter	Type	Required	Default	Description
<code>prefix</code>	<code>string</code>	Yes	--	Number prefix to match. Empty string <code>"</code> acts as a catch-all default route.
<code>type</code>	<code>atom</code>	Yes	--	Destination type: <code>:local</code> , <code>:sip</code> , <code>:isup</code> , <code>:transit</code> , <code>:gmsc</code> , <code>:sip_i</code> , or <code>:sip_with_failover</code> .
<code>priority</code>	<code>integer</code>	No	<code>10</code>	Route priority. Higher values take precedence when multiple routes match the same prefix.
<code>peer</code>	<code>string</code>	Conditional	--	SIP peer name (required when <code>type</code> is <code>:sip</code> , <code>:sip_i</code> , or <code>:sip_with_failover</code>). Must match a peer <code>name</code> from the SIP configuration.
<code>trunk_group</code>	<code>string</code>	Conditional	--	ISUP trunk group name (required when <code>type</code> is <code>:isup</code>).
<code>point_code</code>	<code>[integer, integer, integer]</code>	Conditional	<code>[0, 0, 0]</code>	Destination point code for ISUP routing.
<code>cic_range</code>	<code>{integer, integer}</code>	No	<code>{1, 31}</code>	Inclusive range of Circuit Identification

Parameter	Type	Required	Default	Description
				Codes for ISUP trunks.
<code>transport</code>	<code>atom</code>	No	<code>:udp</code>	SIP transport override for this route.

Routes can also be managed at runtime via the REST API (`POST /routes`, `DELETE /routes`) and the Web UI. For detailed routing examples, see [Routing Configuration](#).

MM Information

```
config :omnimsc, :mm_info
```

Controls the MM INFORMATION message sent to the mobile station after Location Update Accept (3GPP TS 24.008 section 9.2.15a). Contains the network name, time, and timezone.

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

Parameter	Type	Required	Default	Description
network_name	string	No	"Omnitouch"	Full network name displayed on the handset. Encoded in GSM 7-bit default alphabet (3GPP TS 24.008 10.5.3.5a).
short_name	string or nil	No	nil	Short network name. Omitted from the MM INFORMATION message when nil.
timezone_offset	integer	No	0	UTC offset in quarter-hours. For example, UTC+5:30 (India) is 22, UTC-5 (US Eastern) is -20. Encoded in BCD per 3GPP TS 24.008 10.5.3.8.

MSC Pool

`config :omnimsc, :pool`

Configures MSC-in-Pool operation per 3GPP TS 23.236. Pool mode enables multiple MSC instances to share BSCs via A-Flex, providing load distribution and resilience.

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

Parameter	Type	Required	Default	Description
<code>enabled</code>	<code>boolean</code>	No	<code>false</code>	Whether to enable MSC pool operation. When <code>false</code> , the MSC operates in standalone mode.
<code>pool_id</code>	<code>string</code>	Conditional	<code>nil</code>	Pool area identifier. Required when <code>enabled</code> is <code>true</code> .
<code>nri_bitlength</code>	<code>integer</code>	No	<code>10</code>	Number of bits for the Network Resource Identifier field extracted from the TMSI. Must be identical across all pool members.
<code>nri_values</code>	<code>list(integer)</code>	Conditional	<code>[]</code>	NRI values owned by this MSC instance. Must not

Parameter	Type	Required	Default	Description
				overlap with other pool members. Required when <code>enabled</code> is <code>true</code> .
<code>null_nri</code>	<code>integer</code>	No	<code>0</code>	NRI value indicating an unassigned TMSI. Triggers NRI-based re-routing to the correct pool member.
<code>members</code>	<code>list(map)</code>	No	<code>[]</code>	Other MSC instances in the pool. Each member has <code>name</code> , <code>nri_values</code> , <code>address</code> , and <code>port</code> .

For pool architecture and NRI bit layout details, see [MSC Pool & NRI](#).

Overload

```
config :omnimsc, Omnimsc.Overload
```

Overload protection thresholds. When any threshold is exceeded, new service requests (calls, paging, Location Updates) are rejected with GSM cause 42 (switching equipment congestion). The `admit?/0` function provides lock-free reads via `persistent_term` for minimal overhead in the hot path.

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

Parameter	Type	Required	Default	Description
<code>max_calls</code>	<code>integer</code>	No	<code>10,000</code>	Maximum concurrent active calls before entering overload state.
<code>max_subscribers</code>	<code>integer</code>	No	<code>50,000</code>	Maximum VLR registered subscribers before overload.
<code>max_process_count</code>	<code>integer</code>	No	<code>500,000</code>	Maximum BEAM VM process count before overload. Monitors total VM process pressure.
<code>max_paging_rate</code>	<code>integer</code>	No	<code>1,000</code>	Maximum paging requests per second before overload.
<code>check_interval</code>	<code>integer</code>	No	<code>5,000</code>	Interval in milliseconds between overload threshold checks.

Overload state transitions emit telemetry events `[ :omnimsc, :overload, :state_change ]` for external monitoring. See [Metrics Reference](#).

SGs / CSFB

```
config :omnimsc, :sgs
```

Configures the SGs-AP interface for Circuit-Switched Fallback (CSFB) and SMS over SGs with LTE MMEs per 3GPP TS 29.118.

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


Parameter	Type	Required	Default	Description
<code>listen_port</code>	<code>integer</code>	No	<code>29118</code>	SCTP listen port for SGs AP connections from MMEs. Port 29118 is the 3GPP-assigned default. Set to <code>0</code> to disable SGs
<code>vlr_name</code>	<code>string</code>	No	<code>"vlr.omnimsc.local"</code>	VLR name (FQDN) sent to MMEs in SGs-AP Location Update Accept. The MME uses this to identify and route to this VLR instance.

For SGs protocol details, association states, and CSFB call flows, see [SGs / CSFB](#).

USSD

```
config :omnimsc, :ussd
```

Configures external USSD gateways for routing Unstructured Supplementary Service Data requests. Each gateway handles specific USSD service codes (e.g. `*100#` for balance). A gateway with `codes: :all` acts as the default fallback for unmatched codes.

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

USSD Gateway Parameters

Each gateway in the `gateways` list accepts the following:

Parameter	Type	Required	Default	Description
<code>name</code>	<code>string</code>	No	<code>"unnamed"</code>	Logical gateway name for logging and control panel display.
<code>address</code>	<code>string</code>	Yes	--	Gateway Global Title (E.164 number) for MAP USSD routing.
<code>ssn</code>	<code>integer</code>	No	<code>147</code>	SCCP Subsystem Number for the gateway. SSN 147 is the standard USSD SSN.
<code>codes</code>	<code>list(string)</code> or <code>:all</code>	No	<code>:all</code>	USSD service codes handled by this gateway (e.g. <code>["*100", "*101"]</code>). Set to <code>:all</code> for a catch-all default gateway.

For USSD protocol details and relay behavior, see [USSD](#).

Emergency

```
config :omnimsc, Omnimsc.Emergency
```

Configures emergency number detection, service category classification, and PSAP routing per 3GPP TS 22.101.

Emergency Setup messages (3GPP TS 24.008 §9.3.8) do not carry a Called Party BCD Number IE — unlike regular CC SETUP, the handset does not include the dialed digits. OmniMSC uses the configured `psap_address` as the called number for route table lookup and the outgoing SIP INVITE Request-URI. This value must match a prefix in the route table so that the call can be routed to the appropriate SIP peer or trunk.

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

Parameter	Type	Required	Default	Description
<code>numbers</code>	<code>list(string)</code>	No	<code>["112", "911", "999", "000", "110", "119"]</code>	Recognized emergency numbers. Call to these numbers bypass authentication, ciphering, and call barring.
<code>psap_address</code>	<code>string</code>	No	<code>"112"</code>	Called number used for emergency call routing. Because Emergency Setup messages carry no called number, this value is used as the called party for route table lookup and the outgoing trunk (SIP INVITE Request-URI or ISUP IAM Called Party Number). Set this to a number that matches an emergency

Parameter	Type	Required	Default	Description
				route prefix in the route table.
<code>allow_without_sim</code>	<code>boolean</code>	No	<code>true</code>	Whether to allow emergency calls from mobile stations with no SIM inserted (IMS absent). Per 3GPP TS 22.101, networks should permit this.

Node & Runtime

Top-level `config :omnimsc` keys that control node identity and the supervision tree.

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

Parameter	Type	Required	Default	Description
<code>node_id</code>	<code>string</code>	No	<code>"OMNIMSC01"</code>	Node identifier used in CDR <code>recording_entity</code> CDR filenames, and system sta
<code>point_code</code>	<code>integer</code>	No	<code>500</code>	Local SS7 point code used as the CDR collector's <code>local_msc_id</code> .
<code>max_restarts</code>	<code>integer</code>	No	<code>3</code>	Maximum restarts of the top-level supervisor within its restart window before the node shuts down.
<code>overload_monitor</code>	<code>boolean</code>	No	<code>true</code>	Whether to start the periodic overload/process count monitor. Set to <code>false</code> in tes

Paging

```
config :omnimsc, :paging
```

Controls the paging retry behavior for mobile-terminated procedures.

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

Parameter	Type	Required	Default	Description
<code>max_retries</code>	<code>integer</code>	No	<code>2</code>	Number of paging retransmissions before giving up on a mobile-terminated request.
<code>retry_interval_ms</code>	<code>integer</code>	No	<code>5_000</code>	Interval in milliseconds between paging retransmissions.

EIR

```
config :omnimsc, :eir
```

Configures Equipment Identity Register IMEI checking.

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


Parameter	Type	Required	Default	
<code>enabled</code>	<code>boolean</code>	No	<code>false</code>	V I C P V (e i v
<code>check_on</code>	<code>list(atom)</code>	No	<code>[:location_updating, :cm_service_request]</code>	F C I t
<code>backend</code>	<code>module</code>	No	<code>Omnimsc.EIR.Backend.Default</code>	E r u r s

Handover

```
config :omnimsc, :handover
```

Configures the Handover Number pool used for inter-MSC handover.

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

Parameter	Type	Required	Default	Description
ho_number_prefix	string	No	"8888"	Prefix for allocated Handover Numbers.
ho_number_count	integer	No	100	Number of Handover Numbers in the allocation pool.

SRVCC (Sv Interface)

```
config :omnimsc, :srvcc
```

Configures the Sv interface (SRVCC GTPv2-C) for Single Radio Voice Call Continuity.

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

Parameter	Type	Required	Default	Description
<code>sv_enabled</code>	<code>boolean</code>	No	<code>false</code>	Whether to start the SRVCC Sv (GTPv2-C) transport.
<code>sv_port</code>	<code>integer</code>	No	<code>2123</code>	UDP port for the Sv interface. Port 2123 is the GTP-C default.
<code>local_ip</code>	<code>tuple</code>	No	--	Local bind IP for the Sv transport as an Erlang tuple.

LCS

`config :omnimsc, :lcs`

Configures Location Services.

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

Parameter	Type	Required	Default	Description
<code>default_location</code>	<code>{number, number}</code>	No	<code>{0.0, 0.0}</code>	Fallback <code>{latitude, longitude}</code> in decimal degrees returned for a cell-based fix when no precise SMLC result is available.

Security

```
config :omnimsc, :security
```

Configures authentication-failure barring.

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

Parameter	Type	Required	Default	Description
<code>auth_failure_threshold</code>	<code>integer</code>	No	<code>3</code>	Number of consecutive authentication failures after which a subscriber is barred.

Routing (Number Analysis)

```
config :omnimsc, :routing
```

Configures number analysis for national/international prefix handling and emergency detection. This is distinct from the prefix-based route table (`:routes`).

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

Parameter	Type	Required	Default	Description
<code>international_prefix</code>	<code>string</code>	No	<code>"00"</code>	Dialing prefix indicating international number.
<code>national_prefix</code>	<code>string</code>	No	<code>"0"</code>	Dialing prefix indicating national (trunk) number.
<code>emergency_numbers</code>	<code>list(string)</code>	No	<code>["112", "911", "110"]</code>	Numbers classified emergency by number analysis.
<code>country_code</code>	<code>string</code>	No	<code>""</code>	Country code prepended when normalizing national numbers to E.164.
<code>area_code</code>	<code>string</code>	No	<code>""</code>	Area code used when normalizing subscriber local numbers.
<code>short_codes</code>	<code>list</code>	No	<code>[]</code>	Short-code entries as <code>{code,</code>

Parameter	Type	Required	Default	Description
				destination tuples.

SCCP

```
config :omnimsc, :sccp
```

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

Parameter	Type	Required	Default	Description
<code>local_subsystems</code>	<code>list(integer)</code>	No	<code>[7, 8]</code>	SCCP Subsystem Numbers that this node hosts locally (used by SCCP management for SSA/SSP handling).

CAMEL

Top-level `config :omnimsc` keys for CAMEL (Customized Applications for Mobile networks Enhanced Logic) service triggering.

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

Parameter	Type	Required	Default	Description
<code>camel_service_keys</code>	<code>map</code>	No	<code>%{}</code>	Map of CAMEL service key to SCP addressing overrides.
<code>camel_default_scp_address</code>	<code>string</code>	No	--	Default gsmSCF (SCP) Global Title used when a service key has no explicit address.
<code>camel_timers</code>	<code>map</code>	No	<code>%{}</code>	CAMEL timer overrides.

VLR Reaper

```
config :omnimsc, :vlr_reaper
```

Configures the periodic reaper that purges stale VLR subscriber records.


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

Parameter	Type	Required	Default	Description
scan_interval_ms	integer	No	60_000	Interval in milliseconds before scanning for new VLRs.
notify_hlr	boolean	No	true	Whether to notify the HLR with the VLR status.
hlr	module	No	Omnimsc.VLR.HLR.Default	HLR module to use for VLR status.

SIP-I

```
config :omnimsc, :sip_i
```

Configures SIP-I peers (SIP with encapsulated ISUP, ITU-T Q.1912.5) for inter-
MSC and PSTN interconnect.

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

Each peer in the `peers` list accepts the following:

Parameter	Type	Required	Default	Description
<code>name</code>	<code>string</code>	Yes	--	Logical peer name. Referenced in route table entries with type <code>:sip_i</code> .
<code>address</code>	<code>string</code>	Yes	--	Peer IP address or hostname.
<code>port</code>	<code>integer</code>	No	<code>5060</code>	Peer SIP port.
<code>transport</code>	<code>atom</code>	No	<code>:tcp</code>	Transport for this peer: <code>:udp</code> , <code>:tcp</code> , or <code>:tls</code> .
<code>isup_version</code>	<code>atom</code>	No	<code>:itu_t92</code>	ISUP variant carried in the encapsulated body: <code>:itu_t92</code> or <code>:ansi</code> .
<code>trunk_group_id</code>	<code>string</code> or <code>nil</code>	No	--	Trunk group identifier used for routing (e.g. "TG-InterMSC-01").
<code>point_code</code>	<code>[integer, integer, integer]</code> or	No	--	Remote SS7 point code for the ISUP

Parameter	Type	Required	Default	Description
	<code>integer</code> or <code>nil</code>			routing context.
<code>codecs</code>	<code>list(atom)</code>	No	<code>[:pcmu, :pcma]</code>	Supported audio codecs.
<code>max_channels</code>	<code>integer</code>	No	<code>100</code>	Maximum concurrent calls to this peer.

Web UI

```
config :omnimsc, OmnimscWeb.Endpoint
```

The web control panel is served by a Phoenix endpoint with LiveView. It provides real-time dashboards for subscribers, calls, connections, routing, and alarms.

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

Parameter	Type	Required	Default	Description
<code>http.ip</code>	<code>tuple</code>	No	<code>{0, 0, 0, 0}</code>	HTTP address to resolve locally
<code>http.port</code>	<code>integer</code>	No	<code>4000</code>	HTTP port for the pane
<code>url.host</code>	<code>string</code>	No	<code>"localhost"</code>	Host URL (Set to host's production)
<code>secret_key_base</code>	<code>string</code>	Yes	--	Phoenix signature. Generated by <code>mix phx.gen.secret</code> . Required for production from <code>SECRET_KEY_BASE</code> environment variable
<code>server</code>	<code>boolean</code>	No	<code>true</code>	Whether the H-Set to disable contr

Parameter	Type	Required	Default	Description
<code>check_origin</code>	<code>boolean</code>	No	<code>true</code> (prod) <code>false</code> (dev)	Whether to check the origin of the websockets head requests. Defaults to <code>false</code> in development and <code>true</code> in production.
<code>pubsub_server</code>	<code>atom</code>	No	<code>Omnimsc.PubSub</code>	PubSub server module. Defaults to <code>Omnimsc.PubSub</code> . LiveView broadcasts are sent via this module.
<code>live_view.signing_salt</code>	<code>string</code>	No	<code>"oMnImScLv"</code>	LiveView signing salt. Defaults to <code>"oMnImScLv"</code> .

Runtime override: Set `SECRET_KEY_BASE`, `PHX_HOST`, and `PORT` environment variables. In production, HTTPS with port 443 is configured automatically.

REST API

`config :api_ex`

The REST API is served by `api_ex` on a separate port, providing programmatic access to subscribers, calls, routes, SIP peers, connections, and system health.

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

Parameter	Type	Required	Default	Description
port	integer	No	8444	HTTP listen port for the REST API.
listen_ip	string	No	"0.0.0.0"	Bind IP address for the API listener.
product_name	string	No	"Omnitouch MSC"	Product name displayed in the Swagger UI.
title	string	No	"API - Omnitouch MSC"	Page title for the Swagger UI.
hostname	string	No	"localhost"	Hostname for API URL generation.
enable_tls	boolean	No	false	Whether to enable TLS for the API endpoint.

Available API Endpoints

Path	Methods	Description
GET /subscribers	GET, DELETE	List or remove VLR subscribers.
POST /subscribers/:id/actions	POST	Trigger subscriber actions (paging, detach).
GET /calls	GET, DELETE	List or release active calls.
GET /sms	GET	List SMS transactions.
GET /routes	GET, POST, DELETE	Manage the route table.
GET /routes/lookup	GET	Look up a route by dialed number.
GET /sip/peers	GET, PATCH	List or update SIP peer configuration.
GET /mgw	GET	List media gateway status.
GET /ran/connections	GET	List active RAN (A-interface) connections.
GET /ran/bscs	GET	List connected BSCs.
GET /stp	GET	Show STP connection status.
GET /health	GET	System health check.
GET /status	GET	System status summary.

Path	Methods	Description
POST /paging	POST	Trigger a paging request.
POST /silent	POST	Initiate a silent call or silent SMS.

Complete Production Configuration

Example

```
# config/runtime.exs
import Config

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

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

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

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

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

```

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

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

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

    config :omnimsc, :smc,
      address: "14155550300"

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

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

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

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

```

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

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

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

```
config :omnimsc, :ussd,  
gateways: []
```

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

Control Panel

This document describes the OmniMSC web-based control panel, a real-time monitoring and management interface built with Phoenix LiveView. The control panel is accessible at `http://<host>:4000` and provides live visibility into subscribers, calls, connections, routing, CDRs, and system health.

All pages auto-refresh via WebSocket push. Most pages refresh every 5 seconds; the Active Calls page refreshes every 2 seconds. No manual page reload is required. The auto-refresh toggle on each page allows pausing updates when inspecting a particular record.

For endpoint configuration (bind address, port), see [Configuration Reference](#). For the REST API, see [API Reference](#).

Dashboard

The dashboard is the main landing page, providing an at-a-glance summary of the entire MSC.

Summary Cards

The top row displays six real-time counters:

Card	Description
Subscribers	Number of subscribers currently registered in the VLR
Active Calls	Number of active CC FSM call transactions
Active SMS	Number of in-progress SMS transactions
RAN Connections	Count of BSCs and RNCs with ESTABLISHED SCTP associations
STP Link Status	M3UA ASP state toward the STP (ACTIVE, INACTIVE, DOWN)
System Uptime	Elapsed time since application start

SS7 Links Table

Displays the status of all configured SS7 signalling links, including M3UA ASP state and traffic mode.

Known BSCs Table

Lists each BSC by name, point code, cell count, and SCTP association state.

SIP Peers Table

Column	Description
Name	Peer logical name
Address	Peer IP address and SIP port
Calls	Current active call count on this peer
Status	Health state badge (Up, Down, Unknown)

Media Gateways Table

Lists configured media gateways with name, address, protocol (MGCP or Megaco), and reachability status.

Recent Events Feed

A scrolling feed of the most recent telemetry events, each tagged with an event type badge (CALL, LU, PEER, INFO) and UTC timestamp. Events are pushed in real time as they occur.

Subscribers

The Subscribers page provides a searchable list of all VLR subscriber records. Enter an IMSI or MSISDN (partial match supported) in the search box to filter the list in real time.

Subscriber List Columns

Column	Description
IMSI	International Mobile Subscriber Identity
MSISDN	Mobile Station ISDN Number
TMSI	Temporary Mobile Subscriber Identity allocated by the VLR
LAC	Location Area Code of the subscriber's current cell
State	VLR registration state
Auth	Authentication status
LU	Location Update completion status

Expandable Subscriber Detail

Clicking a subscriber row expands a detailed view organised into the following sections.

Identity

Field	Description
IMSI	International Mobile Subscriber Identity
MSISDN	Mobile Station ISDN Number
TMSI	Temporary Mobile Subscriber Identity
IMEI	International Mobile Equipment Identity (if available)
HLR Number	Address of the subscriber's home HLR

Location and State

Field	Description
LAC	Location Area Code
CI	Cell Identity
Serving BSC	Name of the BSC currently serving this subscriber
RAN Type	Radio access type (GERAN-A, UTRAN-lu, or SGs)
Usage Count	Number of active use count tokens held by this subscriber's MSC-A
Expires	VLR record expiry timestamp
State	Current subscriber state in the VLR
Roaming	Whether the subscriber is marked as roaming
SGs	SGs association state (if registered via MME for CSFB)

Authentication

Field	Description
Algorithm	Authentication algorithm in use (COMP128v1, COMP128v3, Milenage)
Tuples	Number of remaining authentication triplets
UMTS Quintuplet	Whether UMTS authentication quintuplets are available

Service Profile

Displays the circuit-switched services received from the HLR via MAP Insert Subscriber Data, including bearer service and teleservice subscriptions.

Supplementary Services

Lists all provisioned supplementary services with status badges:

Service	Description
BAOC	Barring of All Outgoing Calls
BOIC	Barring of Outgoing International Calls
BOIC-exHC	Barring of Outgoing International Calls except to Home Country
BAIC	Barring of All Incoming Calls
BIC-Roam	Barring of Incoming Calls when Roaming
CFU	Call Forwarding Unconditional
CFB	Call Forwarding on Busy
CFNRy	Call Forwarding on No Reply
CFNRc	Call Forwarding on Not Reachable
CW	Call Waiting
HOLD	Call Hold
MPTY	Multi-Party
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction

Each service displays an active/inactive status badge and, where applicable, the forwarded-to number and condition parameters.

MSC-A Connection

Displays the current MSC-A FSM state for any active connection associated with this subscriber, including the state name, active use count tokens, and elapsed time in state.

Connections

The Connections page provides visibility into all signalling links, RAN connections, and SIP peers.

STP Link (M3UA ASP)

Field	Description
Local IP	Local SCTP bind address
Remote	STP remote address and port
Association ID	SCTP association identifier
Status	M3UA ASP state badge (ACTIVE, INACTIVE, DOWN)

All signalling transport uses SCTP (Stream Control Transmission Protocol) for reliable, multi-homed delivery per RFC 4960.

Known BSCs

Column	Description
Point Code	BSC SS7 point code
Global Title	BSC global title address (if configured)
Last Reset	Timestamp of the most recent BSSMAP RESET exchange with this BSC

SIP Peers

Column	Description
Name	Peer logical name
Address	Peer IP address and SIP port
Transport	Protocol in use (UDP, TCP, or TLS)
Active Calls	Current number of active calls to this peer
Capacity	Maximum concurrent channels configured for this peer
Last OPTIONS	Timestamp of the most recent successful OPTIONS keepalive response
Status	Health state badge (Up, Down, Unknown)

Active Calls

The Active Calls page displays a live table of all CC FSM call transactions currently in progress.

Call Table Columns

Column	Description
Call Ref	Unique call reference number
Direction	MO (Mobile Originating) or MT (Mobile Terminating) badge
IMSI	Subscriber IMSI
Calling	Calling party number (A-number)
Called	Called party number (B-number)
State	CC FSM state with colour-coded badge
Duration	Elapsed time since call seizure
Codec	Negotiated speech codec
BSC/RNC	Name of the serving BSC or RNC

Expandable Call Detail

Clicking a call row expands a detailed view with two panels.

Call Details

Field	Description
Call Ref	Unique call reference
Direction	MO or MT
CC FSM State	Current state of the Call Control finite state machine
IMSI	Subscriber IMSI
MSISDN	Subscriber phone number
IMEI	Mobile equipment identity
Calling Party	A-number as presented on the signalling interface
Called Party	B-number as presented on the signalling interface

Timing and Resources

Field	Description
Duration	Elapsed call duration
Seizure Time	UTC timestamp of call setup start
Answer Time	UTC timestamp of call answer (blank if not yet answered)
Basic Service	Bearer service or teleservice associated with the call
Active CC Timer	Currently running CC protocol timer (if any)
BSC/RNC	Name of the serving BSC or RNC handling the radio side

Routes and Trunks

The Routes and Trunks page provides three tabbed views for managing call routing configuration at runtime.

Route Table Tab

Displays all prefix-based routing rules with search filtering by prefix or destination type.

Column	Description
Prefix	Number prefix (empty string indicates the catch-all default route)
Destination Type	Badge indicating route type: EMRG, SIP, SIP+FO, LOCAL, ISUP, TRANSIT, GMSC
Details	Destination-specific information such as peer name or trunk group
Priority	Numeric priority value (higher values take precedence)
Actions	Edit and Delete buttons for each route

The **Add Route** button opens a modal form supporting all destination types. Route changes take effect immediately without requiring a restart.

For detailed routing concepts and configuration, see [Routing Configuration](#).

ISUP Trunks Tab

Displays configured ISUP trunk groups with circuit availability and call counts.

SIP Peers Tab

Displays SIP peer status with address, transport, codec support, channel capacity, and active call counts.

SMS

The SMS page lists all active SMS transaction FSMs, showing transaction ID, subscriber IMSI, direction (MO or MT), transaction state, and SMS Centre address. Completed transactions are removed from the list automatically.

CDRs

The CDR Statistics page provides visibility into the Charging Data Record subsystem.

Summary Counters

Counter	Description
Records in File	Number of CDR records written to the current output file
Pending in Buffer	Number of CDR records buffered in memory awaiting the next write cycle
Active Calls Tracked	Number of calls with open (not yet finalised) CDR records

Writer Status

Field	Description
Current File Path	Filesystem path of the active CDR output file
Records Written	Total records written to the current file
Buffer Pending	Records queued in the write buffer

Sequence Numbers

Per-record-type sequence counters track the monotonically increasing sequence number for each CDR category:

Record Type	Description
LU HLR	Location Update toward HLR
LU VLR	Location Update in VLR
MO Call	Mobile Originating voice call
MT Call	Mobile Terminating voice call
MO SMS	Mobile Originating short message
MT SMS	Mobile Terminating short message
Roaming	Roaming event records

Pool

The Pool page is accessible when MSC pool mode is enabled. It displays the status of all MSC pool members, including member name, point code, NRI range, health state (Up, Down, or Draining), and last successful health probe timestamp. A subscriber distribution chart shows the NRI allocation across pool members.

For pool configuration and NRI-based routing, see [MSC Pool and NRI](#).

System

The System page provides detailed information about the BEAM VM, memory allocation, MSC identity, transport links, and supervision tree health.

BEAM VM

Field	Description
OTP Release	Erlang/OTP major version
Processes	Current process count and configured limit
Ports	Open port count
Atoms	Atom table size
Schedulers	Number of online schedulers
Uptime	BEAM VM uptime since boot

Memory

Field	Description
Total	Total memory allocated by the BEAM VM
Processes	Memory consumed by Erlang/Elixir processes
ETS	Memory consumed by ETS tables
Binary	Memory consumed by binary reference-counted data
Atom	Memory consumed by the atom table
System	Memory consumed by the runtime system (non-process)

MSC Configuration

Displays the active MSC identity parameters:

Field	Description
Name	MSC logical name
Point Code	Local SS7 point code
Global Title	MSC global title address
Allowed A5	Permitted A5 ciphering algorithms for GERAN

SCTP Transport

Field	Description
Link	Transport link name
Local IP	Local SCTP bind address
Remote	Remote STP address and port
Status	SCTP association state badge

Supervision Tree Health

Lists all children of the top-level OmniMSC supervisor (the count is computed dynamically), each displayed with:

Field	Description
PID	Erlang process identifier
Type	Process type (worker or supervisor)
Status	Health badge (Running, Restarting, or Stopped)

This view is useful for verifying that all subsystems are operational after startup or following a fault recovery event.

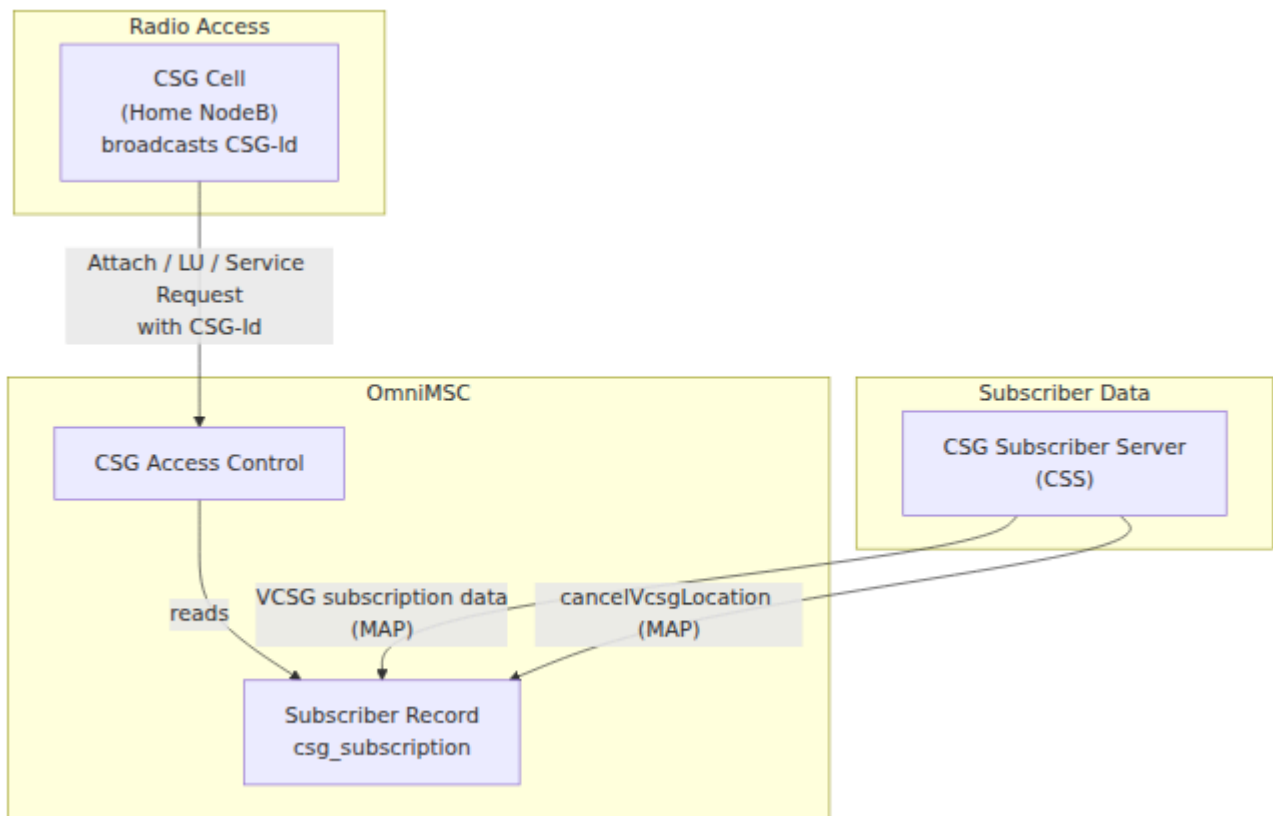
Closed Subscriber Groups (CSG / VCSG)

This document describes how OmniMSC handles Closed Subscriber Groups (CSG): the CSG subscription data held per subscriber, the access-control decision made when a subscriber attempts to use a CSG cell, and the MAP interaction with the CSG Subscriber Server (CSS) that keeps that subscription data current. For the general subscriber data model and how subscription data is downloaded from the HLR, see [MAP Operations](#). For Operator Determined Barring, a related access-control mechanism, see [Supplementary Services](#).

Overview

A **Closed Subscriber Group** identifies a set of subscribers permitted to access one or more CSG cells (for example a Home NodeB / femtocell serving a specific home, office, or campus). Each CSG is identified by a **CSG Identity** (a 27-bit value, coded per 3GPP TS 23.003). A CSG cell broadcasts its CSG Identity in system information; a subscriber camping on that cell receives normal service only when the subscriber is a member of that CSG and the membership has not expired (TS 22.011 Section 8).

The set of CSGs a subscriber may access is the **VCSG subscription data** (also called the Allowed CSG list). This data is held by the **CSG Subscriber Server (CSS)** and provided to the serving node (VLR / SGSN). OmniMSC stores it on the subscriber record and evaluates access at the point of use, in the same way Operator Determined Barring is enforced by the serving node rather than the HLR.



CSG Subscription Data

Each subscriber record carries a CSG membership list. Every entry describes one Closed Subscriber Group the subscriber belongs to and, optionally, when that membership expires.

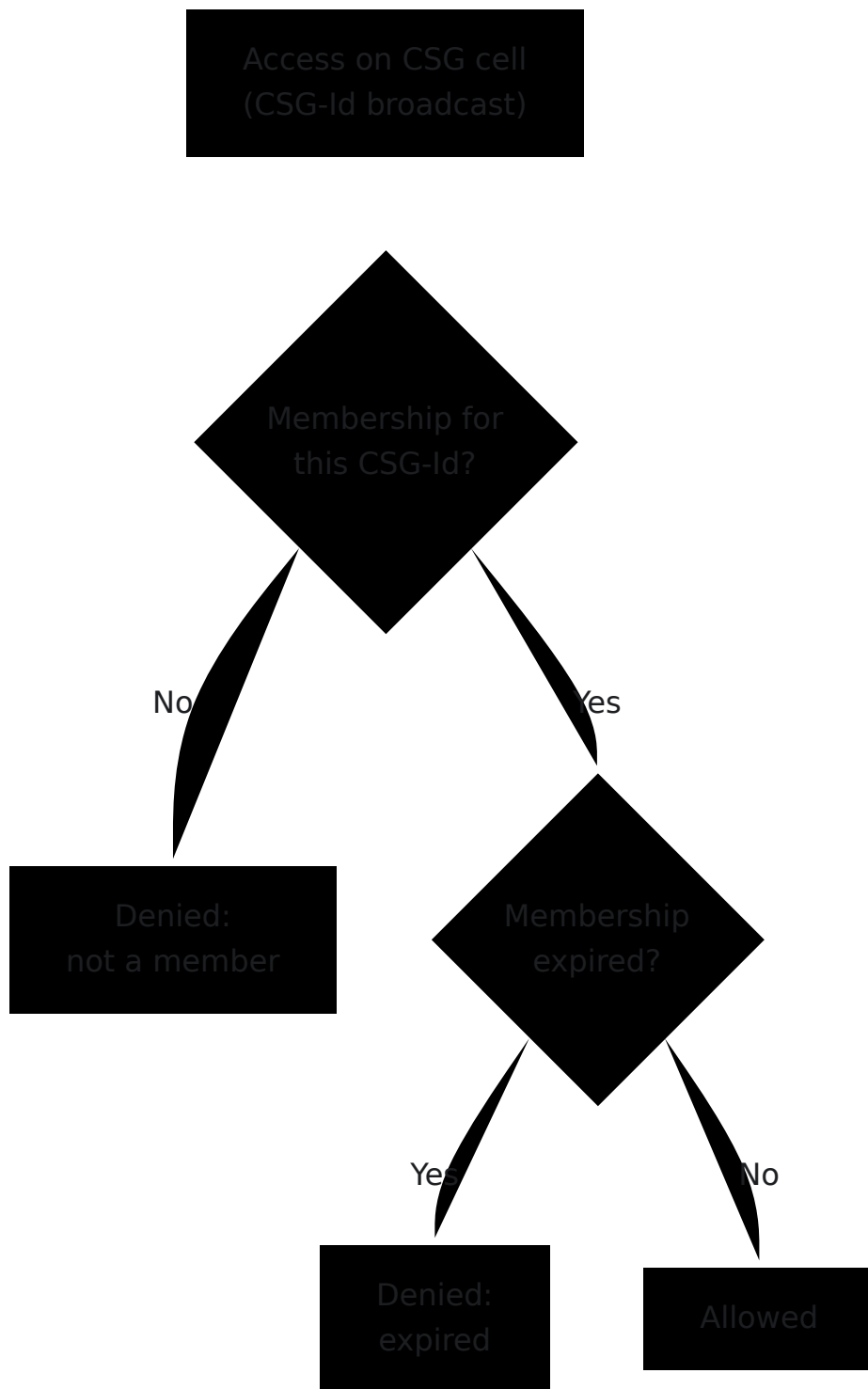
Field	Type	Description
csg_id	Integer	CSG Identity broadcast by the CSG cell. A 27-bit value coded per TS 23.003 .
expiry	DateTime / null	Membership expiry. A membership with <code>null</code> expiry never expires. Once the current time reaches or passes the expiry instant, the membership is treated as expired and access is denied.

The membership list is populated from the VCSG subscription data supplied by the CSS and is cleared by MAP `cancelVcsgLocation` (see [MAP Interaction](#)).

Removing only the CSG subscription data keeps the subscriber registered; other subscription data (basic services, supplementary services, CAMEL, Operator Determined Barring) is untouched.

Access Control

When a subscriber attempts to access a cell that broadcasts a CSG Identity, OmniMSC evaluates the subscriber's membership list against the broadcast CSG Identity. A cell that does not broadcast a CSG Identity is a normal (non-CSG) cell and is always accessible; the check below applies only to CSG cells.



The decision has three outcomes:

Outcome	Condition	Meaning
Allowed	The subscriber has a membership for the broadcast CSG Identity and it has not expired.	The subscriber receives normal service on the CSG cell.
Denied (not a member)	The subscriber has no membership for the broadcast CSG Identity (including the case where the subscriber has no CSG subscription data at all).	Access to the CSG cell is rejected.
Denied (expired)	The subscriber has a membership for the broadcast CSG Identity, but its expiry has passed.	Access to the CSG cell is rejected. The stale membership remains until the CSS updates or cancels it.

The expiry boundary is inclusive: when the current time equals the expiry instant, the membership is treated as expired.

MAP Interaction with the CSS

The CSG Subscriber Server maintains the master copy of a subscriber's VCSG subscription data and keeps the serving node in step using MAP operations (3GPP TS 29.002). OmniMSC handles the following.

Operation	Opcode	Direction	Effect
updateVcsgLocation	53	Serving node to CSS	Registers the serving node for VCSG service and retrieves the subscriber's CSG subscription data.
cancelVcsgLocation	36	CSS to serving node	Cancels this serving node's VCSG registration for the subscriber. OmniMSC removes all CSG subscription data while keeping the subscriber registered.

cancelVcsgLocation is sent by the CSS when the subscriber's VCSG registration is to be removed from this node (for example the subscriber's CSG membership was revoked, or the subscriber moved to another node). The argument carries the subscriber identity (IMSI). On receipt, OmniMSC clears the subscriber's CSG membership list and acknowledges the operation.

Parse error on line 9: ...er stays registered;
subsequent CSG- -----
 -----^ 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

CSG subscription data can also be withdrawn as part of MAP DeleteSubscriberData (the CSG data category), which removes the CSG membership list while leaving the subscriber registered and other data intact. See [MAP Operations](#) for the general DeleteSubscriberData procedure.

3GPP Specification References

Specification	Title	Relevance
TS 23.060	General Packet Radio Service (GPRS); Service description	CSG access control and VCSG location handling in the packet domain
TS 22.011	Service accessibility	CSG concept, Allowed CSG list, CSG membership and expiry
TS 23.003	Numbering, addressing and identification	CSG Identity coding (27-bit)
TS 29.002	Mobile Application Part (MAP) specification	updateVcsgLocation, cancelVcsgLocation, CSG subscription data, CSS interaction

ISUP Trunking

This document describes the ISUP (ISDN User Part) trunk interface implemented by OmniMSC, including trunk group management, circuit allocation, message encoding, timers, continuity check support, and integration with the route table and SIP-I.

For ISUP-SIP cause code mapping, see [SIP Trunking](#). For SIP-I (SIP with encapsulated ISUP), see [SIP-I Trunking](#). For routing configuration and the `:isup` route type, see [Routing Configuration](#). For call flow diagrams showing ISUP signaling in context (IAM/ACM/ANM, ISUP-to-SIP transit), see [Call Flow Diagrams](#).

ISUP Trunk Groups

OmniMSC organizes ISUP circuits into trunk groups. Each trunk group represents a bundle of voice circuits to a remote SS7 exchange, identified by a destination point code and a range of Circuit Identification Codes (CICs).

CIC Allocation

When a call is routed to an ISUP trunk group, the circuit manager allocates the first idle circuit found in the configured range. The allocated CIC is included in the outgoing IAM and reserved until the call is released.

Parameter	Type	Description
<code>name</code>	<code>string</code>	Unique trunk group identifier, referenced in route table entries
<code>dpc</code>	<code>integer</code>	Destination point code (encoded integer, e.g. <code>a*2048 + b*8 + c</code> for ITU 3-8-3)
<code>cic_range</code>	<code>{start, end}</code>	Inclusive range of CICs available for this trunk group

Circuit State Management

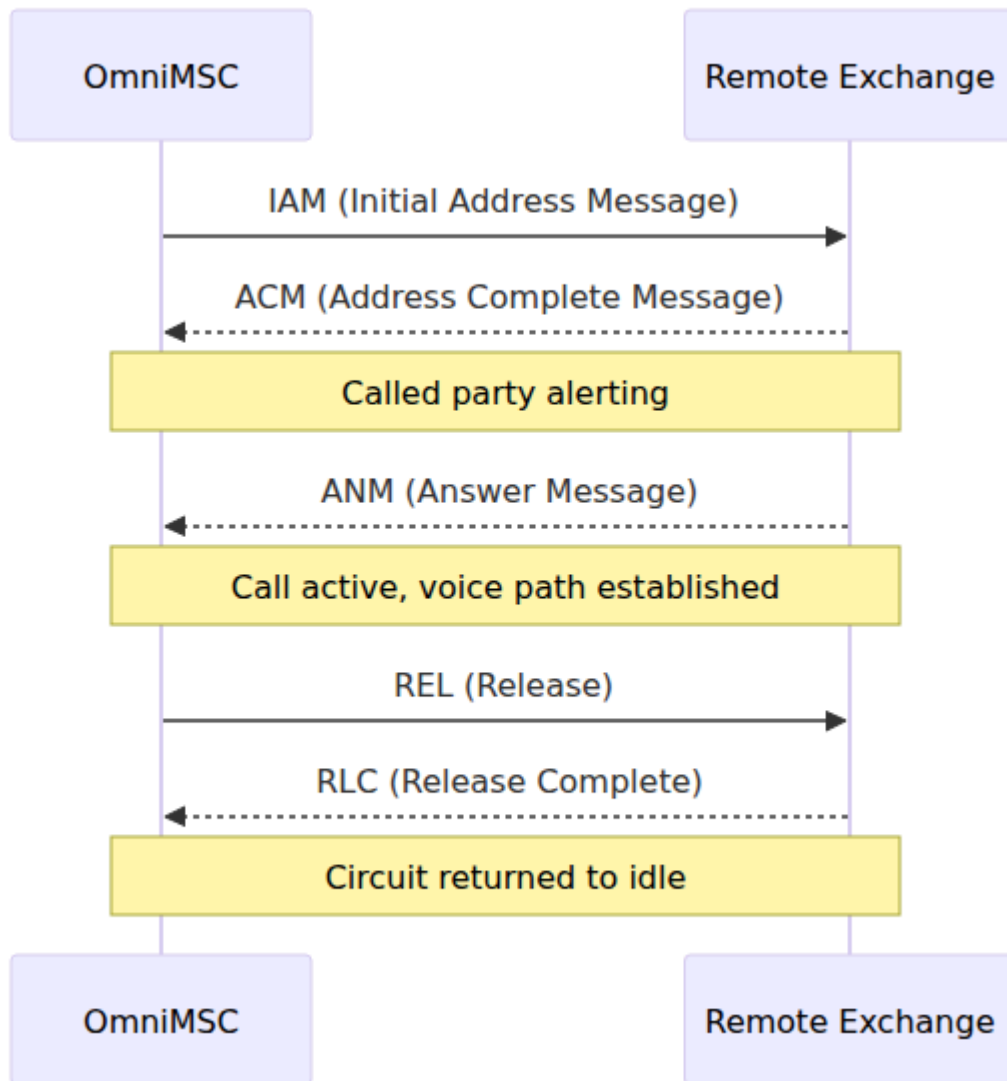
Each circuit within a trunk group tracks an independent state. The circuit manager handles blocking, unblocking, and group reset operations.

Circuit State	Description
<code>:idle</code>	Available for seizure
<code>:outgoing_busy</code>	Allocated for an outgoing call (IAM sent)
<code>:incoming_busy</code>	Reserved for an incoming call (IAM received)
<code>:blocked</code>	Blocked via BLO, unavailable for seizure
<code>:unblocked_pending</code>	Unblock (UBL) sent, awaiting acknowledgement
<code>:reset_pending</code>	Circuit reset in progress (RSC/GRS), awaiting acknowledgement

Circuit blocking (BLO) and unblocking (UBL) are performed per-circuit only. Group reset (GRS/GRA) resets all circuits in a range to idle and clears any blocking state; a single circuit can also be reset with RSC.

ISUP Message Flow

The standard ISUP signaling sequence for a successful call follows the IAM-ACM-ANM-REL-RLC pattern.

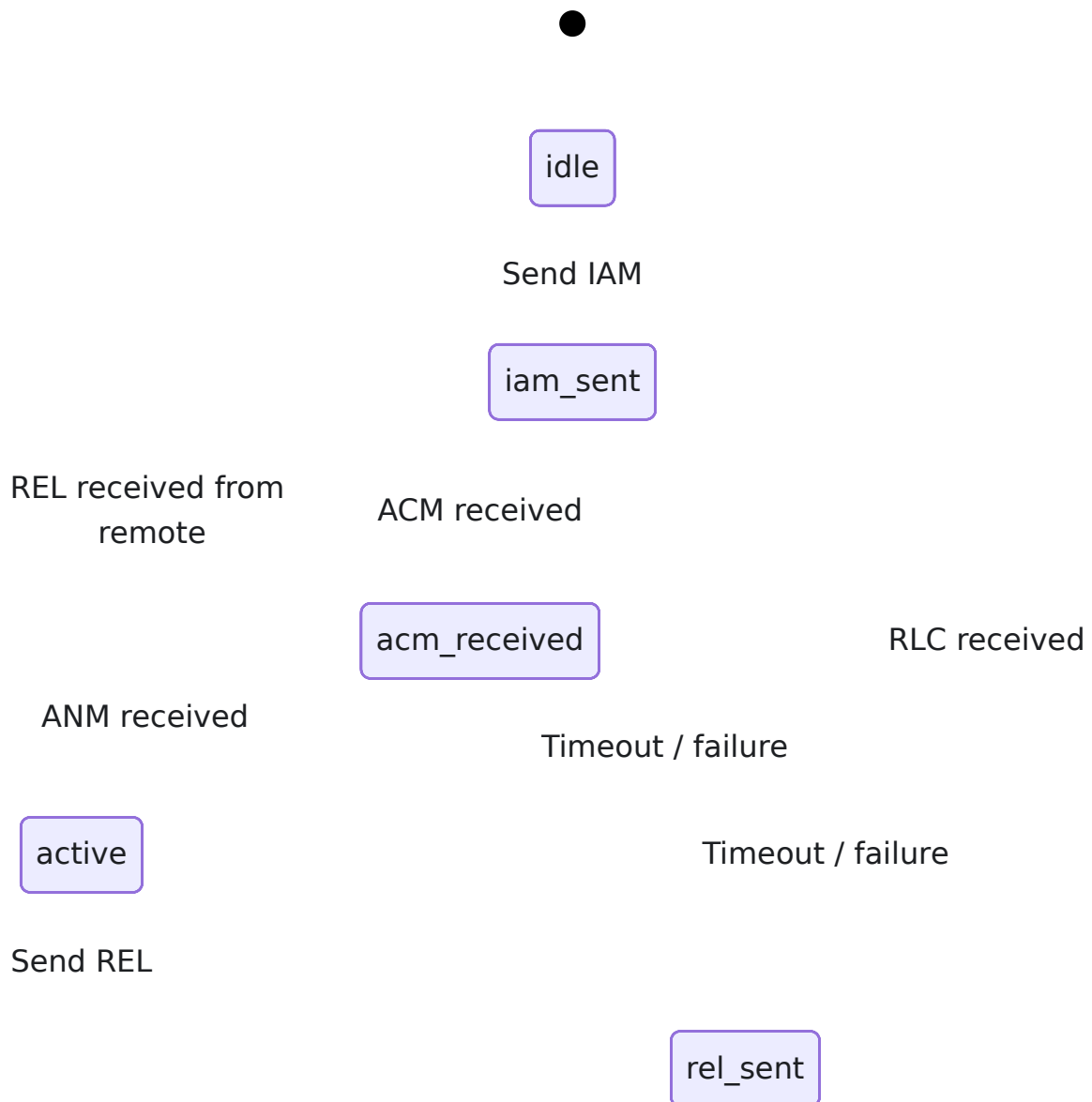


For incoming calls, the directions are reversed: IAM arrives from the remote exchange, and OmniMSC sends ACM and ANM as the call progresses through alerting and answer.

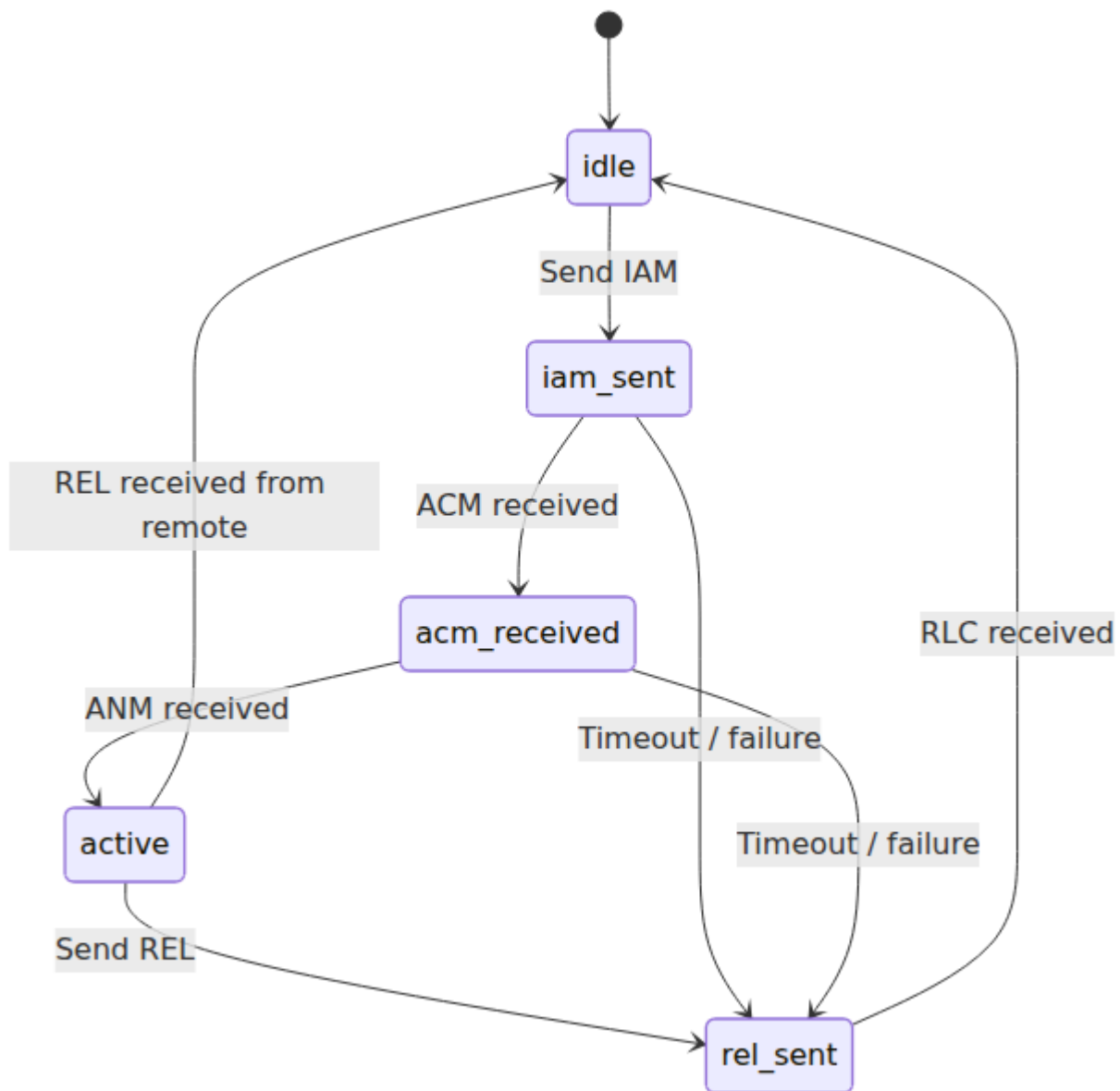
ISUP Handler States

The ISUP handler maintains per-call state that tracks the signaling progress for each circuit.

Outgoing Call States



Incoming Call States



ISUP Timers

OmniMSC implements the standard ISUP timers defined in ITU-T Q.764. These timers guard against signaling failures and ensure circuits are not left in indeterminate states.

Timer	Duration	Started After	Expires When	Action on Expiry
T1	20s	REL sent	RLC not received	Retransmit REL
T5	300s	T1 first expiry	RLC still not received	Send maintenance alert, reset circuit
T7	25s	IAM sent	ACM not received	Release call, send REL
T9	180s	ACM received	ANM not received	Release call, send REL

When T7 expires without receiving an ACM, OmniMSC sends a REL with cause 16 (normal call clearing) and notifies Call Control with cause 31 (normal, unspecified). When T9 expires without an ANM, OmniMSC sends a REL with cause 19 (no answer from user).

ISUP Message Encoding

OmniMSC implements a codec for encoding and decoding the five core ISUP message types used in call setup and release. All messages follow the ITU-T Q.763 format with mandatory fixed, mandatory variable, and optional parameter sections.

Message	Type Code	Direction	Key Parameters
IAM	0x01	Originating	Nature of Connection, Forward Call Indicators, Calling Party Category, Transmission Medium Requirement, Called Party Number, Calling Party Number
ACM	0x06	Terminating	Backward Call Indicators, Optional Backward Call Indicators, Cause Indicators
ANM	0x09	Terminating	Backward Call Indicators
REL	0x0C	Either	Cause Indicators
RLC	0x10	Either	(none -- acknowledgement only)

Additional messages supported for circuit maintenance:

Message	Type Code	Purpose
BLO	0x13	Block a circuit (local maintenance)
UBL	0x14	Unblock a circuit
RSC	0x12	Reset a single circuit
GRS	0x17	Group reset of a circuit range
GRA	0x29	Group reset acknowledgement
COT	0x05	Continuity check result
CPG	0x2C	Call Progress (mid-call event/progress indication)

Continuity Check

OmniMSC supports the ISUP continuity check procedure for verifying the bearer path before connecting a call. When the Forward Call Indicators in an outgoing IAM request a continuity check, the following sequence occurs:

1. OmniMSC seizes the circuit and sends IAM with the continuity check indicator set.
2. A loopback is applied at the far end of the circuit.
3. OmniMSC sends a test tone and verifies the return.
4. On success, OmniMSC sends COT (continuity check successful) and the call proceeds.
5. On failure, OmniMSC sends COT (check failed) and may re-attempt on an alternate circuit.

For incoming calls, when OmniMSC receives an IAM with the continuity check indicator, it applies a loopback on the specified circuit and waits for the COT message before proceeding with call setup.

Route Table Integration

Routes with type `:isup` in the route table direct calls to an ISUP trunk group. The route entry specifies the trunk group name, destination point code, and CIC range.

Route Parameter	Description
<code>type</code>	<code>:isup</code>
<code>trunk_group</code>	Trunk group name matching a configured trunk group
<code>dpc</code>	Destination point code (encoded integer)
<code>cic_range</code>	CIC range as <code>{start, end}</code>

When routing selects an ISUP destination, the trunk router requests a free circuit from the circuit manager. If no circuits are available in the primary trunk group, the system attempts overflow trunk groups to the same destination point code.

For route configuration examples, see [Routing Configuration](#).

SIP-I Support

SIP-I (SIP with encapsulated ISUP) provides an IP-based transport for ISUP messages. Routes with type `:sip_i` carry the full ISUP message (IAM, ACM, ANM, REL) as an `application/ISUP` MIME body within SIP signaling per ITU-T Q.1912.5 and RFC 3204.

SIP-I peers are configured separately from pure SIP peers. The ISUP encoder/decoder used for native ISUP trunks is shared with SIP-I for encoding and decoding the encapsulated ISUP bodies.

For SIP-I configuration, call flows, and header mapping, see [SIP-I Trunking](#).

SIP with ISUP Failover

Routes with type `:sip_with_failover` attempt the call via a SIP peer first. If the SIP route fails (peer unreachable, 5xx response, or timeout), the trunk

router automatically retries via the configured ISUP trunk group.

Failover Trigger	Description
Peer status :down	SIP peer is unreachable (OPTIONS keepalive failed)
SIP 5xx response	Server error from the SIP peer
SIP timeout	No response within the SIP transaction timer
max_channels exceeded	SIP peer has no available capacity

On failover, the trunk router allocates a CIC from the ISUP trunk group and sends an IAM. The CC FSM remains in the same state throughout the failover -- the retry is transparent to the radio-side signaling.

For failover route configuration, see [Routing Configuration](#).

References

Reference	Title	Relevance
ITU-T Q.761	Functional Description of the ISUP	ISUP overview and architecture
ITU-T Q.762	General Function of Messages and Signals of the ISUP	Message definitions
ITU-T Q.763	Formats and Codes of the ISUP	Message encoding and parameter formats
ITU-T Q.764	Signaling Procedures of the ISUP	Call setup/release procedures, timer definitions
ITU-T Q.850	Usage of Cause and Location in ISDN	Cause code definitions used in REL
RFC 3204	MIME Media Type for ISUP and QSIG Objects	ISUP encapsulation in SIP-I
ITU-T Q.1912.5	Interworking between SIP and BICC or ISUP	SIP-I protocol definition

MAP Operations

This document describes the MAP (Mobile Application Part) operations implemented by OmniMSC, including dialogue management, subscriber location procedures, authentication, SMS forwarding, USSD, and error handling. For configuration, see [Configuration Reference](#). For the SMS-layer view of MO-ForwardSM and MT-ForwardSM, including CP/RP protocol details, see [SMS](#). For authentication vector handling and the Auth FSM, see [Security](#). For how InsertSubscriberData populates the subscriber profile visible in the control panel, see [Control Panel Guide](#).

MAP Client

OmniMSC operates a MAP client that manages dialogues with remote MAP peers (HLR, SMS Sc, USSD gateway). The MAP client handles dialogue lifecycle, TCAP transaction correlation, and dialogue timeout supervision.

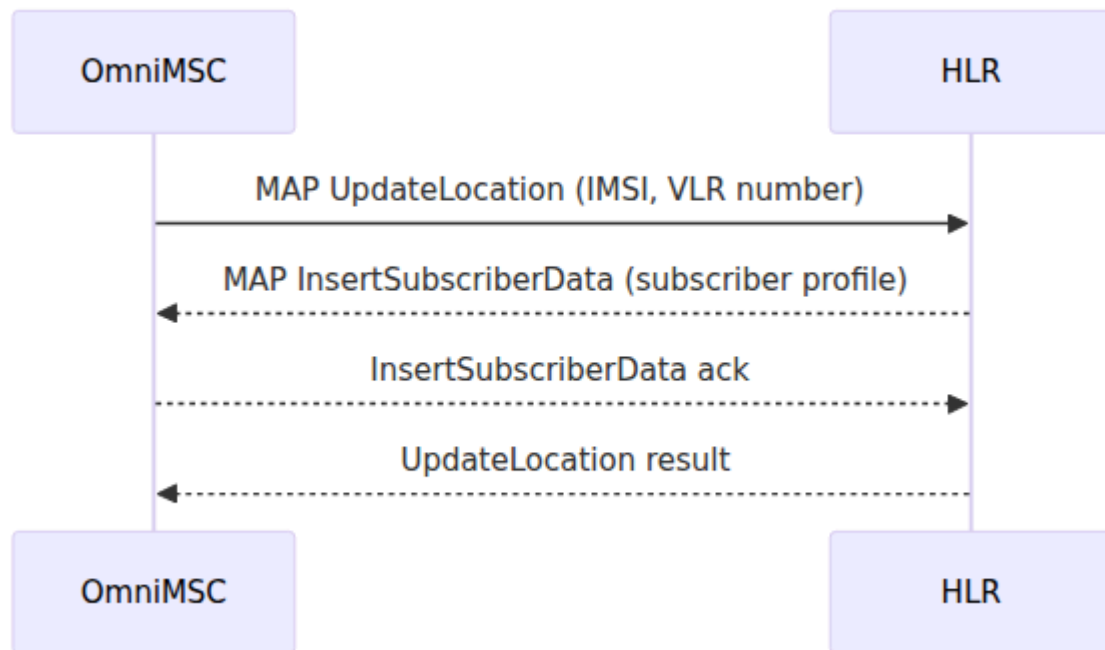
When a subsystem (VLR, SMS handler, SS handler) needs to invoke a MAP operation, it requests a new dialogue from the MAP client. The client allocates a local transaction ID (otid), opens a TCAP BEGIN towards the peer, and monitors the dialogue for a fixed 30-second timeout period. If the peer does not respond within the timeout, the client aborts the dialogue and notifies the requesting subsystem of the failure.

For incoming MAP dialogues initiated by remote peers (such as InsertSubscriberData from the HLR or MT-ForwardSM from the SMS Sc), the MAP client accepts the TCAP BEGIN, correlates it with the remote transaction ID (dtid), spawns a handler process, and supervises the dialogue until completion.

UpdateLocation

The MSC sends MAP UpdateLocation to the HLR when a subscriber performs a Location Update. The message carries the subscriber IMSI and the VLR number

(the E.164 address of this MSC/VLR). The HLR uses the VLR number to route future MT transactions (calls, SMS, USSD) to the correct MSC.



On receiving the UpdateLocation result, the VLR marks the Location Update as complete and the LU FSM proceeds to TMSI allocation. If the HLR returns an error (unknown subscriber, roaming not allowed), the MSC rejects the Location Update towards the mobile station with the appropriate cause.

InsertSubscriberData

The HLR sends MAP InsertSubscriberData to the MSC during the UpdateLocation procedure, and also proactively when the subscriber profile changes (e.g., supplementary service activation via the HLR provisioning interface). The message carries the subscriber profile including:

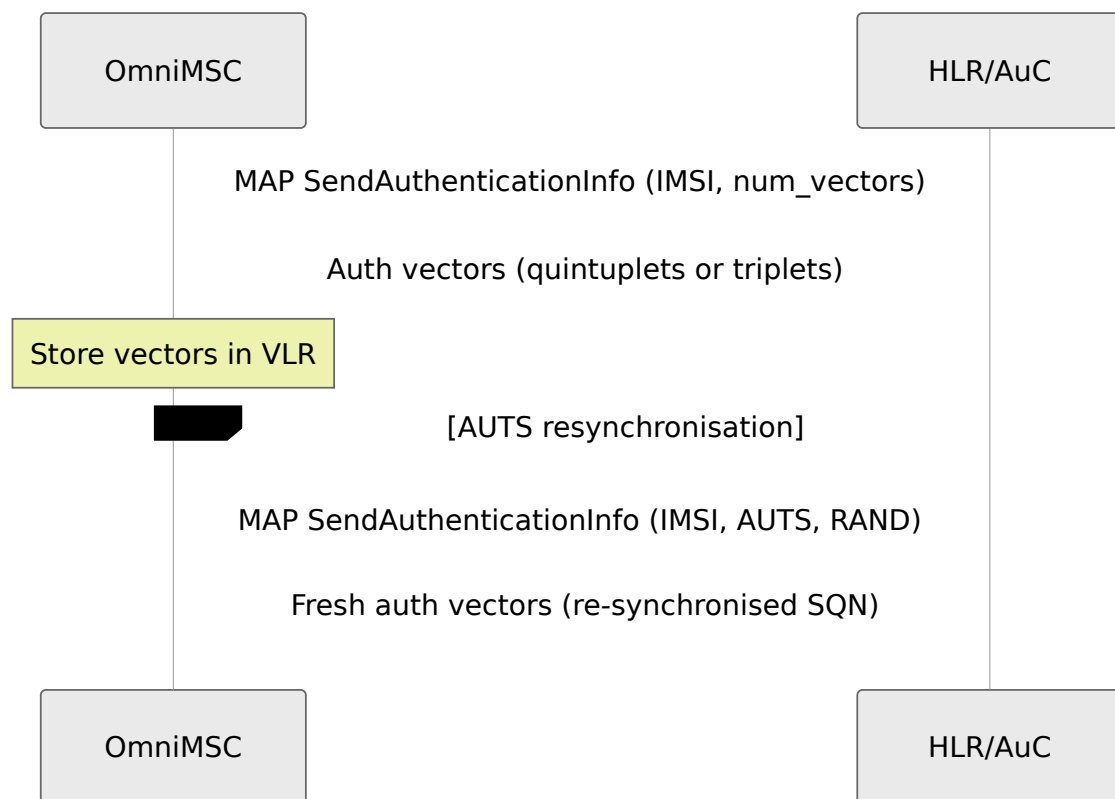
- MSISDN (the subscriber's directory number)
- CS bearer services and teleservices
- Operator Determined Barring (ODB) categories
- Supplementary service data (call forwarding numbers, barring status, CLIR mode, CW status)
- CAMEL subscription information (service keys, gsmSCF addresses)

The VLR stores this data in the subscriber record. Subsequent call setup, SMS delivery, and SS operations reference this locally cached profile to avoid round-trips to the HLR.

SendAuthenticationInfo

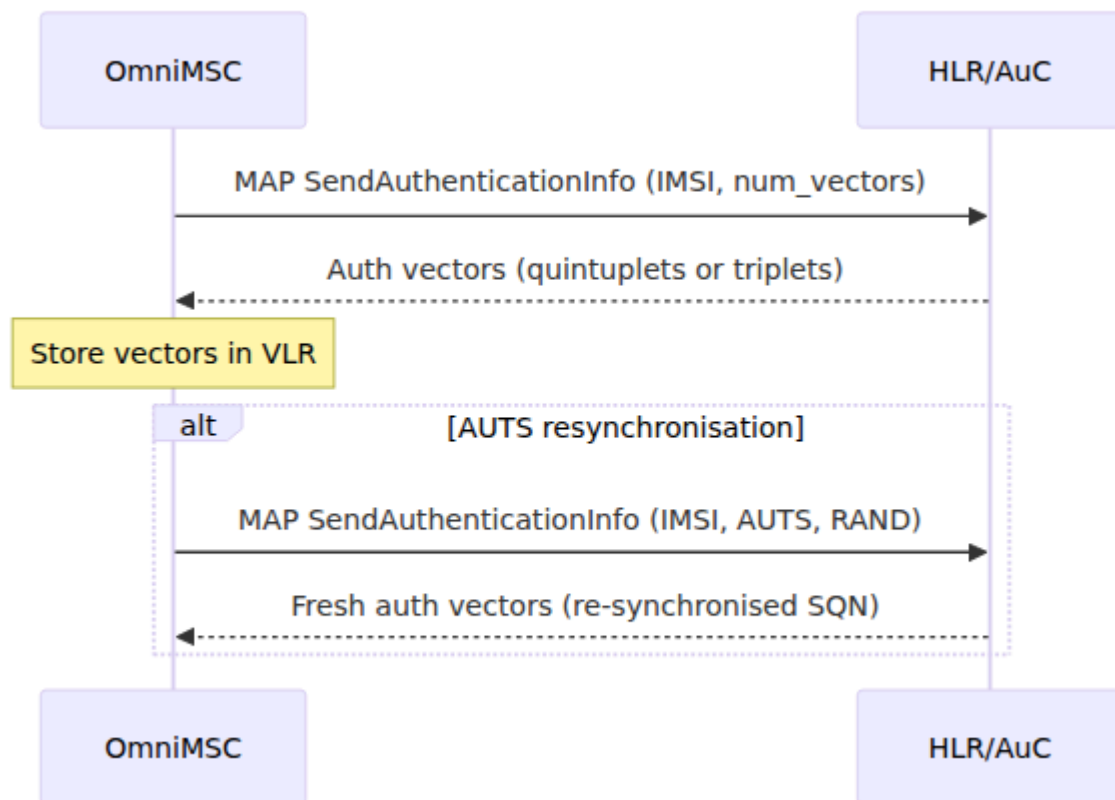
The MSC sends MAP SendAuthenticationInfo to the HLR to fetch authentication vectors for a subscriber. The request carries the IMSI, the number of requested vectors, and optionally re-synchronisation data (AUTS) if the UE reported a sequence number failure.

The HLR returns authentication vectors from the AuC: quintuplets (RAND, XRES, CK, IK, AUTN) for UMTS-capable subscribers or triplets (RAND, SRES, Kc) for GSM-only subscribers. The MSC stores the vectors in the VLR and uses them for subsequent authentication attempts without contacting the HLR again until the vector supply is exhausted.



PurgeMS

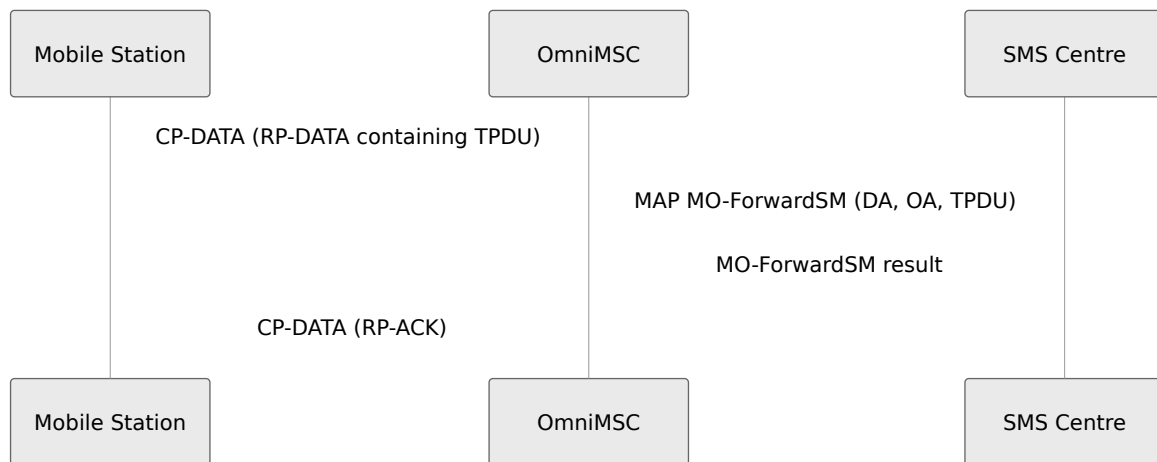
The MSC sends MAP PurgeMS to the HLR when a subscriber performs an IMSI detach. The message carries the IMSI and the VLR number. On receiving PurgeMS, the HLR clears the VLR address from the subscriber record. This ensures correct T-ADS (Terminating Access Domain Selection) routing: without a valid VLR address, the HLR knows the subscriber is not reachable via CS domain and can route MT services accordingly (e.g., trigger the MNRF flag for SMS, return absent subscriber for MT calls).



MO-ForwardSM

The MSC sends MAP MO-ForwardSM to the SMS Centre for mobile-originated short messages. The message carries the SM-RP-DA (destination, typically the SMSc address), SM-RP-OA (originator, the subscriber MSISDN), and the SM-RP-UI (the TPDU containing the SMS payload).

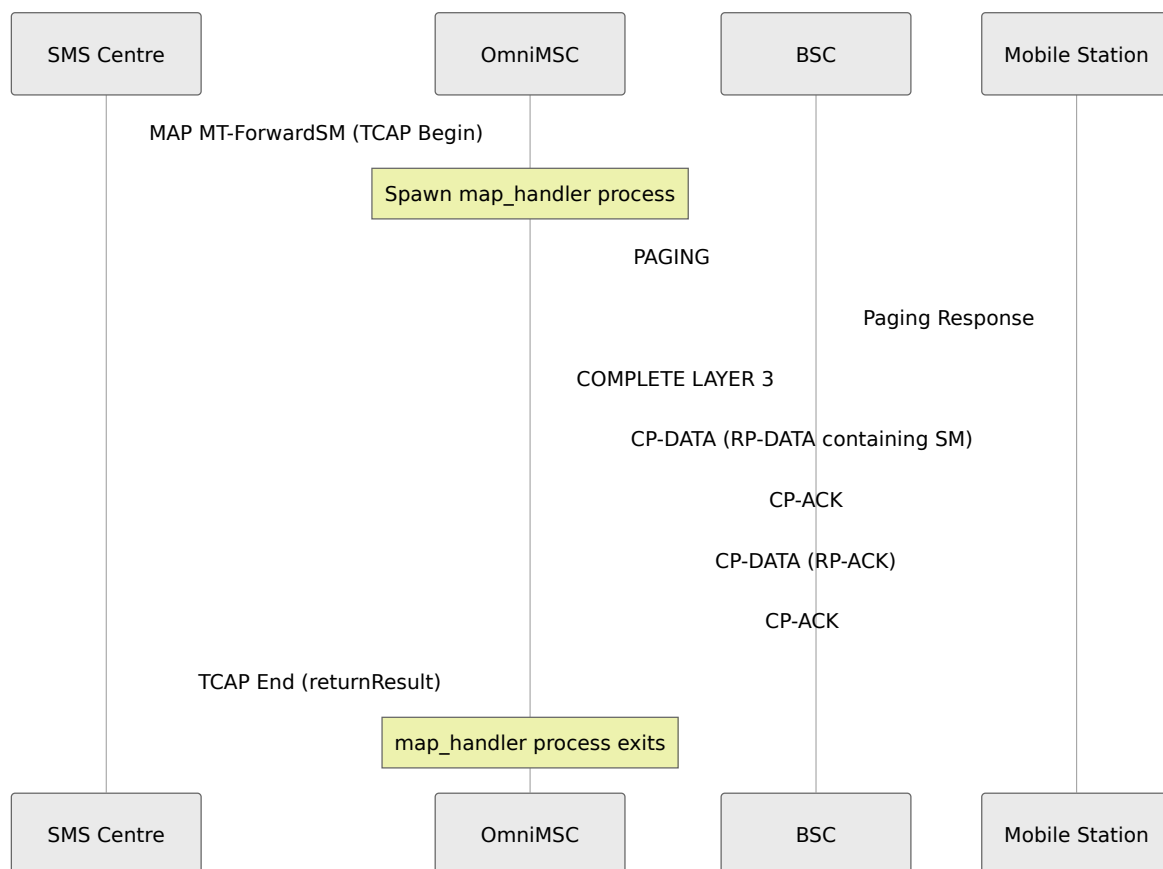
The SMSc acknowledges with a return result on successful acceptance, or a return error if the message cannot be processed (e.g., SMSc congestion, invalid destination).



MT-ForwardSM

The SMS Centre sends MAP MT-ForwardSM to the MSC for mobile-terminated short message delivery. On receiving this operation, OmniMSC spawns a dedicated map_handler process that manages the delivery attempt and holds the MAP dialogue open until the outcome is known.

The handler looks up the subscriber in the VLR, pages if necessary, and delivers the SM via DTAP. Once the mobile station acknowledges delivery (RP-ACK) or reports failure (RP-ERROR), the handler sends a TCAP End containing either a returnResult (successful delivery) or a returnError (delivery failure with cause) back to the SMSc.



If delivery fails (subscriber absent, memory exceeded, protocol error), the handler returns the appropriate MAP error:

Error	Cause
Absent Subscriber	Subscriber not reachable (not registered or no paging response)
SM Delivery Failure	MS returned RP-ERROR (memory full, unspecified error)
System Failure	Internal processing error

ProcessUnstructuredSS-Request

OmniMSC relays USSD requests to the HLR via MAP ProcessUnstructuredSS-Request when the USSD string targets a service that requires HLR processing

(e.g., supplementary service management, balance queries). The MSC forwards the USSD string and DCS (data coding scheme) to the HLR, which processes the request and returns a response string to be displayed on the mobile station.

For operator-defined USSD codes that are handled by an external USSD gateway rather than the HLR, the MSC routes the MAP dialogue to the configured gateway address instead.

TCAP Transaction Management

MAP dialogues are carried within TCAP transactions. OmniMSC maintains a transaction table that correlates local and remote transaction identifiers across the dialogue lifecycle.

TCAP Message	MAP Dialogue Phase	Description
TC-BEGIN	Opening	Initiator sends first invoke; carries originating transaction ID (otid)
TC-CONTINUE	Active	Both parties exchange components; response carries destination transaction ID (dtid) matching the peer's otid
TC-END	Closing	Final message; carries result or error components; dialogue terminated
TC-ABORT	Abort	Abnormal termination; protocol error or timeout

The MAP client tracks each active dialogue by its otid/dtid pair. When a TCAP CONTINUE or END arrives, the client matches the dtid to a local otid to locate the corresponding handler process. This correlation is essential for multiplexing many concurrent MAP dialogues over a single SCCP connection.

Dialogue Timeout

Each MAP dialogue has a fixed 30-second timeout. If the remote peer does not respond within the timeout period, the MAP client sends a TC-ABORT (locally initiated) and notifies the requesting subsystem. This prevents resource leaks from unresponsive peers.

MAP Error Handling

OmniMSC handles MAP errors at both the component level (return error within a dialogue) and the dialogue level (abort, provider error).

Common MAP Errors

Error	Typical Operation	MSC Handling
Absent Subscriber	MT-ForwardSM, SendRoutingInfo	Report delivery failure to SMSc; set MNRF in VLR
SM Delivery Failure	MT-ForwardSM	Forward TP failure cause to SMSc
Unknown Subscriber	UpdateLocation	Reject Location Update
Roaming Not Allowed	UpdateLocation	Reject Location Update with appropriate cause
System Failure	Any	Retry or report failure to requesting subsystem
Data Missing	SendAuthenticationInfo	Authentication cannot proceed; reject service
Unexpected Data Value	InsertSubscriberData	Log and reject the offending parameter

Dialogue-Level Failures

When a TCAP ABORT is received or a dialogue times out, the MAP client determines which subsystem initiated the dialogue and delivers a failure notification. The subsystem then applies its own recovery logic (e.g., the LU FSM rejects the Location Update, the SMS handler returns a delivery failure to the SMSc).

Point Code Routing

When OmniMSC receives an incoming MAP dialogue (e.g., MT-ForwardSM from the SMSc, InsertSubscriberData from the HLR), the M3UA layer records the originating point code from the incoming message's routing information. When the MSC sends the response (TCAP Continue or End), it uses this recorded point code as the destination point code (DPC) for the outgoing M3UA message.

This mechanism ensures that responses are routed back to the correct originating node, even when multiple HLRs or SMSes with different point codes are reachable via the same STP. The routing_info from the incoming M3UA association is stored per-dialogue and used for all subsequent messages within that dialogue.

Additional Supported Operations

Beyond the operations described in detail above, the MAP encoder implements the following operations, identified by their MAP local opcode:

Operation	Opcode	Purpose
CancelLocation	3	HLR instructs the previous VLR to cancel a subscriber's location
SendRoutingInfo	22	GMSC requests routing information (MSRN) for an MT call
SendRoutingInfoForSM	45	GMSC requests routing information for MT SMS delivery
ReportSM-DeliveryStatus	47	Report MT SMS delivery outcome to the HLR (MWD/MNRF handling)
SendIdentification	55	Retrieve IMSI and auth vectors from the previous VLR (pool relay)
RestoreData	57	Restore subscriber data from the HLR
UnstructuredSS-Request	60	Network-initiated USSD request toward the subscriber
AlertServiceCentre	64	Notify the SMSc that a subscriber is again reachable
ReadyForSM	66	Inform the HLR that the subscriber is ready to receive SMS

3GPP Specification References

Specification	Title	Relevance
TS 29.002	Mobile Application Part (MAP) Specification	All MAP operations, error codes, dialogue procedures
ITU-T Q.771-Q.775	Transaction Capabilities Application Part (TCAP)	TCAP transaction management, component handling
ITU-T Q.711-Q.716	Signalling Connection Control Part (SCCP)	SCCP addressing and routing for MAP dialogues
RFC 4666	MTP3 User Adaptation Layer (M3UA)	M3UA transport, point code routing

Media Control

This document describes media gateway control in OmniMSC, covering MGCP and Megaco/H.248 gateway protocols, the Media Controller state machine, codec negotiation, conference bridging, and SDP generation.

For call flow diagrams showing media setup in context, see [Call Flow Diagrams](#). For SIP trunk codec configuration, see [SIP Trunking](#). For media gateway configuration parameters, see [Configuration Reference](#). For MPTY conference bridging from the supplementary services perspective, see [Supplementary Services](#).

MGCP Gateway Control

OmniMSC controls media gateways using the Media Gateway Control Protocol (MGCP) per RFC 3435. The MGCP Call Agent issues three primary commands to manage RTP connections on the gateway.

Commands

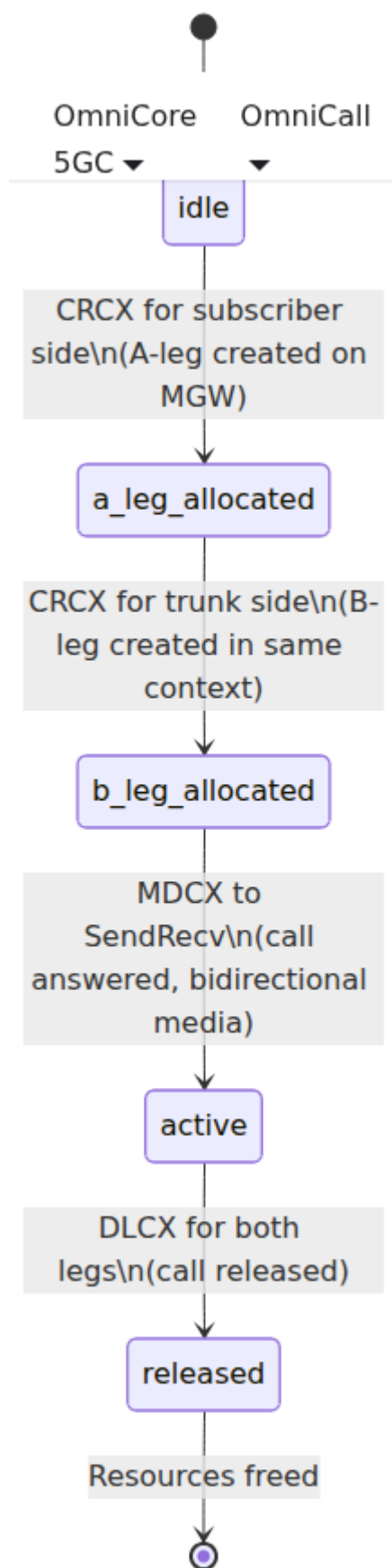
Command	Purpose	Description
CRCX	Create Connection	Allocates a new RTP endpoint on the media gateway and returns the local IP address, port, and SDP for that endpoint.
MDCX	Modify Connection	Updates an existing connection's parameters, such as switching the media mode from receive-only to send-and-receive when a call is answered.
DLCX	Delete Connection	Tears down an RTP connection and releases the associated endpoint resources on the gateway.

Endpoint Naming

Media gateway endpoint paths are caller-supplied rather than generated to a fixed pattern. When an endpoint path lacks an @, it is qualified with the gateway's configured domain, producing a fully qualified endpoint such as `ds/ds1-1/1@mgw01.local`. Each call leg occupies one endpoint within a connection context on the gateway.

Media Controller States

The Media Controller manages the lifecycle of media resources for each call. It progresses through the following states as the call is established and released.



A-Leg (Subscriber Side)

The A-leg represents the media path between the media gateway and the subscriber's radio access bearer via the BSC or RNC.

When a call is initiated, the Media Controller sends a CRCX command to the media gateway to allocate the A-leg endpoint. The initial connection mode is set to **RecvOnly**, meaning the gateway accepts incoming media from the subscriber side but does not transmit. This prevents clipping and echo during the alerting phase.

When the call is answered, the Media Controller sends an MDCX command to change the A-leg mode to **SendRecv**, enabling bidirectional media flow.

B-Leg (Trunk Side)

The B-leg represents the media path between the media gateway and the remote trunk (SIP peer or ISUP circuit).

The B-leg is allocated via a second CRCX command within the same MGW connection context as the A-leg. By placing both legs in the same context, the media gateway internally bridges the two RTP streams, enabling voice path continuity without hairpinning media through the MSC.

Codec Negotiation

OmniMSC negotiates speech codecs based on the capabilities reported by the BSC in the BSSMAP Assignment Request response (speech version list) and the codec preferences of the outbound trunk.

Supported Codecs

Payload types are statically assigned (not dynamically negotiated): GSM-FR uses the standard static type 3, PCMU/PCMA use the standard static types 0/8,

and the 3GPP speech codecs are fixed to types 96-101.

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

The codec offer list is constructed from the intersection of the BSC's reported speech version capabilities and the MSC's configured codec preferences. The resulting SDP is included in the outbound SIP INVITE to the trunk peer, allowing the remote side to select the preferred codec from the offered set.

Conference Bridge (Multi-Party)

OmniMSC supports multi-party (MPTY) conference calls per 3GPP TS 24.083 by leveraging the media gateway's conference bridging capability.

When a subscriber invokes the MPTY supplementary service, the Media Controller allocates a conference context on the media gateway. Individual call legs are then added to or removed from the conference as participants join or leave.

Conference Operations

Operation	Description
Create Conference	Allocates a new conference context on the media gateway with a dedicated mixing endpoint.
Add to Conference	Moves an existing call leg into the conference context via MDCX, connecting the participant to the conference mixer.
Remove from Conference	Moves a call leg out of the conference context back to a point-to-point connection.

The conference mixer on the media gateway handles media mixing for all participants. The MSC controls conference membership through signalling only and does not process media directly.

SDP Generation

OmniMSC generates SDP (Session Description Protocol) for outbound SIP messages using the following conventions:

SDP Field	Value
Origin (o=)	OmniMSC as the session originator username
Connection (c=)	IP address returned by the media gateway in the CRCX response
Media (m=)	RTP port returned by the media gateway, with codec payload types from the negotiated offer
Attributes (a=)	Codec-specific parameters such as fmtp for AMR octet-align mode

The connection address and port in the SDP always reflect the media gateway's allocated endpoint, ensuring that RTP flows directly between the media gateway and the remote peer without traversing the MSC signalling path.

Megaco/H.248 Support

As an alternative to MGCP, OmniMSC supports media gateway control via the Megaco/H.248 protocol per ITU-T Recommendation H.248. The choice between MGCP and Megaco is a single global setting — the `media mode` option (default `:megaco`) — and applies to all media gateways, not per gateway.

Megaco uses a transaction-based command model with Add, Modify, Subtract, and Move commands that map conceptually to the MGCP CRCX, MDCX, and DLCX operations. The Megaco Controller manages H.248 transactions, context allocation, and termination lifecycle on the gateway.

Both MGCP and Megaco transports use UDP by default. The Media Controller abstracts the protocol differences so that the CC FSM and other call-handling components interact with a unified media control interface regardless of the underlying gateway protocol.

Gateway Configuration

Each media gateway is defined with the following identity parameters:

Parameter	Description
Name	Logical gateway name used for identification in logs and the control panel
Address	IP address of the media gateway
Port	MGCP or Megaco listening port on the gateway
Domain	Gateway domain name used in MGCP endpoint addressing (the @mgw portion of endpoint names)

For the full set of media configuration parameters, see [Configuration Reference](#).

References

- **RFC 3435** -- Media Gateway Control Protocol (MGCP) Version 1.0
- **ITU-T H.248** -- Gateway Control Protocol (Megaco)
- **3GPP TS 24.083** -- Call Waiting and Call Hold supplementary services (MPTY)
- **RFC 4566** -- Session Description Protocol (SDP)

Metrics and Monitoring

This document describes the telemetry, metrics, alarms, and health endpoints provided by OmniMSC. For overload threshold configuration, see [Configuration Reference](#). For troubleshooting alert conditions, see [Troubleshooting Guide](#). For the real-time dashboard view of active calls and subscriber count, see [Control Panel Guide](#).

Telemetry Overview

OmniMSC emits Erlang/Elixir telemetry events for all significant operational activities. These events are exported as Prometheus metrics, available at the `/metrics` endpoint on the Phoenix HTTP port. All metric names are namespaced under `omnimsc_` to avoid collisions with other applications. The System page in the control panel provides a real-time view of BEAM VM statistics including process count, memory, and scheduler load — see [Control Panel Guide](#).

The metric definitions below reflect the metrics OmniMSC exposes. Any Prometheus-compatible scraper (Prometheus, Grafana Agent, Datadog, Victoria Metrics) can collect these metrics at the standard scrape interval.

Metrics Reference

Metric	Type	Labels	
<code>omnimsc_active_calls_count</code>	Gauge	--	Cu voi
<code>omnimsc_vlr_subscribers_count</code>	Gauge	--	Sul reg
<code>omnimsc_sccp_connections_count</code>	Gauge	--	Act (A/
<code>omnimsc_sms_sent_count</code>	Counter	--	Tot ser
<code>omnimsc_location_update_complete_count</code>	Counter	<code>type</code>	Loc cor nor
<code>omnimsc_auth_failure_count</code>	Counter	<code>reason</code>	Aut
<code>omnimsc_auth_skipped_count</code>	Counter	--	Aut exi cor
<code>omnimsc_handover_attempt_count</code>	Counter	<code>type</code>	Ha (int int suc
<code>omnimsc_paging_attempt_count</code>	Counter	<code>result</code>	Pa (dis tim

Metric	Type	Labels	
<code>omnimsc_peer_status</code>	Gauge	<code>peer</code>	SIP (1=
<code>omnimsc_ss_operation_count</code>	Counter	<code>operation</code> , <code>ss_service</code>	Sup ope
<code>omnimsc_ss_error_count</code>	Counter	<code>reason</code>	SS
<code>omnimsc_ussd_request_count</code>	Counter	<code>routing</code>	US hlr
<code>omnimsc_map_dialogue_duration</code>	Histogram	<code>operation</code>	MA tim
<code>omnimsc_call_release_count</code>	Counter	<code>type</code>	Cal

Label Values

omnimsc_location_update_complete_count -- the `type` label distinguishes location update types per 3GPP TS 24.008:

Value	Description
<code>imsi_attach</code>	IMSI attach (subscriber powering on)
<code>normal</code>	Normal location update (subscriber moved to new location area)
<code>periodic</code>	Periodic location update (T3212 timer expiry)
<code>guest</code>	Guest subscriber accepted (unknown IMSI, local guest provisioning)

omnimsc_auth_failure_count -- the `reason` label identifies the failure cause. The authentication FSM currently emits a single value:

Value	Description
<code>auth_failed</code>	Authentication failed (SRES/RES mismatch or MS-reported failure)

omnimsc_paging_attempt_count -- the `result` label tracks paging outcomes:

Value	Description
<code>dispatched</code>	Paging sent to BSC(s)
<code>success</code>	Subscriber responded to paging
<code>timeout</code>	Max retries exhausted without response

omnimsc_peer_status -- the `peer` label identifies the remote peer by its configured name (e.g., Default-GW, International-GW, MSC-02).

omnimsc_ss_operation_count -- the `operation` label identifies the SS operation (register, erase, activate, deactivate, interrogate) and the `ss_service` label identifies the target service (cfu, cfb, cfnry, cfnrc, cw, clip, clir, baoc, baoc).

omnimsc_ussd_request_count -- the `routing` label distinguishes between locally handled SS requests and those relayed to the HLR:

Value	Description
<code>local_ss</code>	Request handled locally by the MSC
<code>hlr_relay</code>	Request relayed to the HLR via MAP

omnimsc_call_release_count -- the `type` label distinguishes call direction:

Value	Description
mo	Mobile-originated call released
mt	Mobile-terminated call released
unknown	Direction not determined at release time

Example PromQL Queries

The following queries are useful starting points for dashboards and alerting rules.

Active call monitoring -- current call load on the MSC:

```
omnimsc_active_calls_count
```

Call rate -- calls released per second, averaged over five minutes:

```
rate(omnimsc_call_release_count[5m])
```

Auth failure ratio -- authentication failures per second by reason:

```
rate(omnimsc_auth_failure_count[5m])
```

Peer availability -- identify any peers that are currently down:

```
omnimsc_peer_status
```

SMS throughput -- SMS messages per second:

```
rate(omnimsc_sms_sent_count[5m])
```

Location update rate by type -- breakdown of LU activity:

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

SS operation rate by service -- supplementary service activity:

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

USSD routing breakdown -- local vs HLR-relayed USSD requests:

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

Alarm System

OmniMSC raises and clears alarms for conditions that require operator attention. Each alarm has a severity level and a unique identifier.

Alarm Types

Alarm	Severity	Description
sctp_link_down	Critical	SCTP association to STP lost
hlr_unreachable	Critical	HLR not responding to MAP operations
cdr_write_failure	Major	CDR file write error
overload	Major	System overload threshold exceeded

Alarm Telemetry Events

The alarm subsystem emits telemetry events that can be consumed by external monitoring systems or attached to Prometheus metrics:

Event	Description
<code>[:omnimsc, :alarm, :raised]</code>	Emitted when an alarm condition is detected. Metadata includes alarm_id, severity, source, and descriptive text.
<code>[:omnimsc, :alarm, :cleared]</code>	Emitted when an alarm condition is resolved. Metadata includes alarm_id, severity, and source.

Alarms remain active until the underlying condition is resolved, at which point the cleared event is emitted. Multiple raises of the same alarm_id without an intervening clear are deduplicated.

Health Endpoint

OmniMSC exposes a health check endpoint for use by load balancers and orchestration systems.

GET /api/health returns the overall system health status. The response indicates whether the MSC is operational and accepting traffic. A healthy response confirms that core subsystems (VLR, CC, MAP client, SIP stack) are running. An unhealthy response indicates that one or more critical subsystems have failed.

This endpoint is suitable for Kubernetes liveness and readiness probes, or for load balancer health checks in traditional deployments.

Status Endpoint

GET /api/status returns detailed system information including active call count, registered subscriber count, peer link states, alarm summary, BEAM process count, and uptime. This endpoint provides a comprehensive snapshot for operational dashboards and diagnostic purposes.

The status response includes all the information needed to assess system capacity and identify degraded components without requiring Prometheus access.

Overload Protection

OmniMSC includes a configurable overload protection mechanism that prevents the system from exceeding safe operating limits. The overload module continuously monitors four metrics and compares them against configurable thresholds.

Overload Thresholds

Metric	Default Threshold	Description
Active calls	10,000	Maximum concurrent CS calls
Registered subscribers	50,000	Maximum subscribers in the VLR
BEAM process count	500,000	Maximum Erlang processes
Paging rate	1,000/sec	Maximum paging requests per second

When any threshold is exceeded, the overload module rejects new service requests with GSM cause 42 (switching equipment congestion). Calls already in progress are not affected. The overload state is reflected in the `[ :omnimsc, :overload, :state_change ]` telemetry event and the `overload` alarm.

Overload protection applies to location updates, call setup requests, and SMS transactions. Emergency calls bypass overload protection regardless of system load, per 3GPP TS 22.101.

For threshold configuration, see [Configuration Reference](#).

MSC Pool and NRI

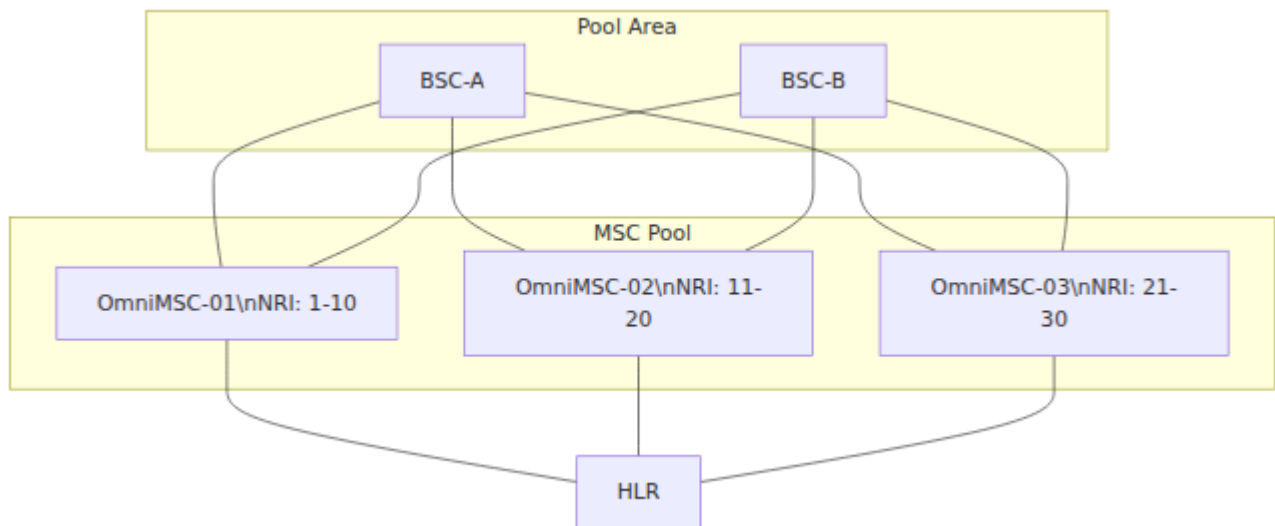
This document describes the MSC-in-Pool architecture implemented by OmniMSC by Omnitouch per 3GPP TS 23.236. Pooling allows multiple MSC servers to share a common pool area, providing load distribution across MSCs and resilience against individual MSC failures.

For pool-aware routing behavior, see [Routing](#). For the Pool page in the web interface, see [Control Panel Guide](#). For configuration parameters, see [Configuration Reference](#). For TMSI allocation details including the no-rollback design and NRI embedding, see [Security](#).

MSC-in-Pool Concept

In a traditional architecture, each BSC connects to a single MSC. If that MSC fails, all subscribers served by its BSCs lose service. MSC pooling addresses this limitation by allowing BSCs to connect to multiple MSCs simultaneously via the A-Flex interface. Any MSC in the pool can serve any subscriber arriving from any BSC in the pool area.

The key mechanism enabling pool operation is the Network Resource Identifier (NRI), a bit field embedded in the TMSI that identifies which MSC allocated that TMSI. When a subscriber presents a TMSI to a BSC, the BSC extracts the NRI and routes the signalling to the correct MSC. If that MSC is unavailable, the BSC selects an alternative MSC from the pool, and the receiving MSC handles the subscriber locally.



Each BSC maintains SCTP associations to every MSC in the pool. For returning subscribers, the BSC uses the NRI in the TMSI to select the MSC that originally registered the subscriber. For new subscribers (no TMSI or null NRI), the BSC uses round-robin or load-based selection.

Network Resource Identifier (NRI)

The NRI is encoded within the 32-bit TMSI allocated by the MSC. The 8 most significant bits (bits 31-24) are reserved; the NRI field starts at bit 23 and extends downward for `nri_bitlength` bits. The remaining low-order bits (bit `23 - nri_bitlength` down to bit 0) are the random portion of the TMSI. The length of the NRI field is configurable and must be identical across all pool members.

TMSI Bit Layout

For a 10-bit NRI, the reserved field is bits 31-24 (8 bits), the NRI occupies bits 23-14 (10 bits), and the random portion is bits 13-0 (14 bits):

Bits 31-24	Bits 23-14	Bits 13-0
8 bits	10 bits	14 bits
Reserved	NRI	Random

The default NRI bit length is 10, supporting up to 1024 distinct NRI values. Smaller deployments may use fewer bits. The random portion is always `24 - nri_bitlength` bits wide.

NRI Bit Length	Maximum NRI Values	Remaining (Random) TMSI Bits
5	32	19
8	256	16
10	1024	14

The "null NRI" (default value 0, configurable via `null_nri`) indicates that the TMSI was not assigned by any pool member. A subscriber presenting a null NRI is treated as a new subscriber and accepted locally with a fresh TMSI allocation.

TMSI Allocation

When pool mode is active, OmniMSC embeds one of its assigned NRI values into every TMSI it allocates. The allocation process generates a random 32-bit base TMSI and then overwrites the NRI bit field with the MSC's designated NRI value. This ensures that any BSC in the pool area can determine which MSC owns a given subscriber by inspecting the TMSI. For general TMSI allocation and confirmation behavior (including the no-rollback design choice), see [Security](#).

The MSC uses its first configured NRI value as the default for new allocations. All NRI values assigned to the MSC are recognized as "local" when evaluating incoming TMSIs.

Configuration

Pool membership is configured under the pool key in the MSC configuration (see [Configuration Reference](#)). The essential parameters are:

Parameter	Default	Description
enabled	false	Master switch for pooling. Must be set to <code>true</code> for the pool configuration to take effect; when <code>false</code> (or absent) the MSC operates in standalone (non-pooled) mode.
pool_id	nil	Pool identifier. All MSCs in the same pool must share the same pool_id.
nri_bitlength	10	Number of bits used for the NRI field in the TMSI. Must be identical across all pool members. Valid range: 1 through 10.
nri_values	(empty list)	List of NRI values owned by this MSC instance. TMSIs allocated by this MSC will contain one of these values. NRI ranges must not overlap between pool members.
members	(empty list)	List of other MSC instances in the pool. Each member entry includes a logical name, address, port, and assigned NRI values. Used for NRI-based subscriber relaying and health monitoring.

Each member entry in the members list requires:

Parameter	Description
name	Logical name of the remote pool member
address	IP address or hostname of the remote MSC, used as the target of the health liveness probe
port	Signalling port on the remote MSC (default 2905), probed via a TCP or SCTP connection attempt to determine member health
nri_values	NRI values assigned to the remote member, used to identify which MSC owns a given TMSI

Foreign NRI Handling

When a subscriber presents a TMSI containing an NRI that belongs to a different pool member, the receiving MSC must decide how to handle the subscriber. This situation arises when the BSC's NRI-based selection function (NNSF) routes to the wrong MSC, or when the owning MSC is unavailable.

Bits 31-24 8 bits Reserved	Bits 23-14 10 bits NRI	Bits 13-0 14 bits Random

The Pool Manager always accepts the subscriber locally and reallocates the TMSI with a local NRI value. The decision on how to resolve the subscriber's identity depends on the owning MSC's health status:

Owning MSC Status	Behavior
Reachable	Send MAP SendIdentification to the owning MSC to retrieve the IMSI and authentication vectors, then continue the location update with the received identity
Unreachable	Request the IMSI directly from the UE via an Identity Request, then fetch authentication vectors from the HLR
Unknown	Same behavior as unreachable; request the IMSI from the UE

In all cases, the subscriber is re-registered at the receiving MSC with a new TMSI containing a local NRI value.

Pool Member Health Tracking

Each MSC in the pool monitors the health of other pool members. The health state is tracked per member and directly affects foreign NRI handling behavior.

Member State	Description	Effect on Foreign NRI Handling
Up	Member is responding to health probes	Foreign NRI subscribers are identified via MAP SendIdentification to the owning MSC
Down	Member has not responded within the timeout period	Foreign NRI subscribers are identified by requesting the IMSI from the UE
Unknown	Initial state before health probes have completed	Treated the same as Down
Draining	Member has announced a drain for maintenance	No new subscribers are relayed; existing sessions are maintained until completion

When a pool member restarts, it broadcasts MAP Reset to all pool members. Receiving MSCs mark all subscriber records originally belonging to the reset MSC for re-registration on next contact. Health state changes are broadcast to the Control Panel via PubSub for real-time visibility.

Rolling Upgrade Procedure

Pool architecture enables zero-downtime upgrades by draining and upgrading one MSC at a time.

1. Set the target MSC to draining state via the Control Panel or API. BSCs stop sending new subscribers to this MSC; existing sessions continue.
2. Wait for active calls to complete naturally. Monitor the active call count on the dashboard.
3. Issue Clear Command to any remaining BSC connections.

4. Stop the MSC process. Remaining subscribers will re-register on other pool members at next contact.
5. Apply the software update or configuration change.
6. Start the upgraded MSC. It establishes SCTP associations with BSCs and announces itself via MAP Reset.
7. The MSC begins accepting new subscribers. BSCs include it in their selection algorithm.
8. Verify health on the Pool page: member state is Up, NRI allocation is correct, subscribers are registering.

Repeat for each MSC in the pool.

Pool LiveView Page

The Pool page in the Control Panel displays:

- Pool identity: pool ID, local NRI values, NRI bit length.
 - Member status table: name, address and port, NRI range, health state (Up, Down, or Draining), last probe timestamp, and subscriber count per member.
 - NRI distribution chart: visual distribution of subscribers across NRI ranges.
 - Foreign NRI events: recent foreign NRI encounters showing the TMSI presented, owning MSC, and outcome (relayed via MAP SendIdentification, resolved via IMSI request, or failed).
 - Pool statistics: total pool subscribers, local versus foreign NRI ratio, relay success rate.
-

3GPP Specification References

Specification	Title	Relevance
TS 23.236	Intra-domain connection of RAN nodes to multiple CN nodes	MSC Pool architecture, NRI format, BSC selection
TS 23.012	Location Management Procedures	VLR interaction with pool operation
TS 29.002	MAP Specification	MAP SendIdentification, MAP Reset for pool coordination
TS 48.008	BSC-MSC Interface (A-Flex)	A-Flex extensions for pool-aware BSSAP signalling

Routing

This document describes how OmniMSC by Omnitouch analyses called numbers, selects routes, and delivers calls to their destinations. It covers the number analysis pipeline, the route table, supported destination types, the GMSC function, and route management interfaces.

For call flow diagrams showing how routing integrates with call setup, see [Call Flow Diagrams](#). For route table configuration parameters, see [Configuration Reference](#). For SIP peer health monitoring, see [SIP Trunking](#). For ISUP trunk group details, see [ISUP Trunking](#). For route management via the control panel, see [Control Panel Guide](#).

Number Analysis

When a call is initiated, OmniMSC classifies the called number to determine its type and normalize it to E.164 format. The classification follows a priority order and uses the routing configuration for the deployment (country code, national prefix, international prefix, emergency numbers, and short codes).

Classification Order

The number analysis engine evaluates the called number against the following categories in order. The first match wins.

Priority	Number Type	Detection Rule	Normalization
1	Emergency	Exact match against the configured emergency number list (default ["112", "911", "110"]); operator-configurable)	Unchanged; the route hint is set to :emergency
2	Short code	Exact match against the configured short code table, where each code maps to a service type (operator assistance, directory enquiry, etc.)	Unchanged; the route hint is set to the service type atom
3	International	Number begins with "+" or with the configured international prefix (default "00")	Stripped of the international prefix and prepended with "+" to produce E.164
4	National	Number begins with the configured national prefix (default "0")	National prefix is stripped, then the country code is prepended with "+" to produce E.164
5	Local	Any remaining number that does not match the above	Country code and area code are prepended with "+" to produce E.164

After classification, the normalized E.164 number is passed to the route table for longest-prefix matching.

Route Table

The route table is an ETS-backed data structure that maps number prefixes to destinations. It is the central decision point for all outbound call routing in OmniMSC.

Longest-Prefix Matching

When a number is presented for routing, the route table iterates from the full number length down to a single digit, checking for a matching prefix at each step. The first (longest) match found is used. If no prefix-specific match is found, the table falls back to the default route (prefix is the empty string). If no default route exists, the call fails with a no-route-to-destination error.

Priority Ordering

Each route entry carries a numeric priority value. Higher values take precedence. Priority is used when the route table is displayed and when managing overlapping entries. Emergency routes should be configured with the highest priority (e.g., 100) to ensure they are never shadowed by less-specific entries.

Example Route Table

The following table illustrates how the route table resolves different called numbers.

Prefix	Type	Destination	Priority	Purpose
000	:sip	SIP peer "Default-GW"	100	Emergency number — route must match <code>psap_address</code>
04	:local	VLR subscriber	50	Australian mobile numbers
0412	:sip	SIP peer "Mobile-GW"	50	Specific mobile prefix routed to a SIP gateway
001	:sip	SIP peer "International-GW"	10	International dialing prefix
07	:isup	Trunk group "Mobile-Interconnect"	10	Mobile interconnect via SS7
08	:sip_with_failover	Primary: SIP peer "Primary-SIP-GW", Failover: ISUP trunk "Backup-ISUP"	10	SIP with automatic ISUP fallback
09	:sip_i	SIP-I peer "MSC-02-SIP-I"	10	SIP with encapsulated ISUP to a peer MSC

Prefix	Type	Destination	Priority	Purpose
(empty)	:sip	SIP peer "Default-GW"	1	Catch-all default route

With this table in place:

Dialed Number	Matching Prefix	Destination	Reason
000	000	SIP: Default-GW	Exact match on emergency prefix
0412345678	0412	SIP: Mobile-GW	Longest match (4 digits beats the 2-digit "04" entry)
0498765432	04	Local VLR subscriber	Matches "04" but not "0412"
0011234567	001	SIP: International-GW	Longest match (3 digits)
0312345678	(empty)	SIP: Default-GW	No prefix match; falls to default

Route Types

OmniMSC supports the following destination types in the route table.

Emergency Calls

Emergency calls are not a separate route type. The MSC detects emergency calls from the CC Emergency Setup message type (3GPP TS 24.008 §9.3.8, message type 0x0E) and the CM Service Request type (:emergency).

Authentication is attempted but the call proceeds regardless of the outcome. Ciphering is established if authentication succeeds; otherwise the call proceeds without it.

Emergency Setup messages do not carry a Called Party BCD Number — the handset sends only an optional Bearer Capability IE and Emergency Service Category IE. The MSC uses the `psap_address` from the Emergency configuration as the called number for route table lookup. This number is then routed through the normal route table like any other call. The route entry it matches can be any type (:sip, :isup, :sip_i, etc.).

Example: To route emergency calls to a SIP peer named "Default-GW":

```
# Route table – psap_address "000" will match this entry
%{prefix: "000", type: :sip, peer: "Default-GW", priority: 100}

# Emergency config – psap_address is used as the called number
config :omnimsc, Omnimsc.Emergency,
  psap_address: "000"
```

If authentication fails, the caller's IMEI is used as the calling party number instead of the MSISDN. Emergency numbers are also detected during number analysis and can trigger emergency handling even before the route table is consulted.

:local

Routes the call to a subscriber registered in the local VLR. The MSC looks up the called MSISDN in the VLR, pages the subscriber via the appropriate BSC or RNC, and establishes the call over the A-interface or lu-CS interface.

:sip

Routes the call to a configured SIP peer by sending a SIP INVITE. The route entry specifies the peer by name; the peer's IP address, port, transport, and codec configuration are resolved from the SIP peer table. The Trunk Router verifies that the peer is reachable (status is not "down") and that the peer has available channels before routing.

:isup

Routes the call via an SS7 ISUP trunk group. The route entry specifies the trunk group name, destination point code, and CIC (Circuit Identification Code) range. The Trunk Router allocates an idle circuit from the trunk group, constructs an Initial Address Message (IAM), and sends it via the M3UA/SCTP transport to the remote exchange.

:sip_i

Routes the call to a SIP-I peer, where the full ISUP message is encapsulated within the SIP body. SIP-I preserves all ISUP information elements during interworking, avoiding the information loss that can occur with standard SIP-ISUP conversion. For protocol details, see [SIP-I Trunking](#).

:sip_with_failover

Attempts the call via a primary SIP peer first. If the SIP peer is unreachable, returns a 5xx error, or times out, the Trunk Router automatically retries the call via a configured ISUP failover trunk group. This destination type requires both a SIP peer name (primary) and an ISUP trunk group with point code (failover).

:gmsc

Invokes the Gateway MSC function. The MSC sends a MAP SendRoutingInfo request to the HLR to obtain the MSRN (Mobile Station Roaming Number) for the called subscriber, then routes the call to the serving MSC using the returned MSRN. See the GMSC Function section below for details.

:transit

Routes the call as a transit call between trunk types without instantiating a full Call Control FSM. Transit routes are used for ISUP-to-SIP gateway operation, SIP-to-ISUP interworking, ISUP-to-ISUP tandem switching, and SIP-to-SIP proxy transit. Transit routes include source context (the incoming trunk type and name) to match incoming calls from specific trunks.

Route Table Management

Web UI

The Routes and Trunks page in the OmniMSC Control Panel provides a tabbed interface for managing routes, ISUP trunk groups, and SIP peers. From the Route Table tab, operators can add, edit, and delete routes through modal forms. Route changes take effect immediately without requiring a restart. Routes loaded from configuration at startup can be overridden at runtime. For details on the web interface, see [Control Panel Guide](#).

REST API

Routes can also be managed programmatically through the REST API.

Method	Endpoint	Description
GET	/api/routes	List all routes in the table
POST	/api/routes	Add a route. Request body includes prefix, type, peer (for SIP types), and priority.
DELETE	/api/routes/{id}	Remove a route by its prefix (the <code>id</code> path parameter is the route prefix)

Route Lookup Testing

The route lookup endpoint allows operators and integration systems to test routing decisions without placing a call.

Method	Endpoint	Description
GET	/api/routes/lookup/:number	Returns the destination that would be selected for the given called number, or a no-route indication if no match exists

GMSC Function

When OmniMSC receives a call for a mobile subscriber who is not registered in the local VLR, it can act as a Gateway MSC (GMSC) per 3GPP TS 23.018. The GMSC function bridges the gap between the calling network and the visited MSC where the subscriber is currently registered.

MT Call Routing Flow

1. An incoming call arrives from a PSTN trunk or SIP gateway with the subscriber's MSISDN as the called number.
2. The route table lookup returns the :gmsc destination type for this prefix.
3. OmniMSC sends a MAP SendRoutingInfo (SRI) request to the subscriber's HLR, providing the called MSISDN.
4. The HLR identifies the serving VLR and instructs it to allocate a Mobile Station Roaming Number (MSRN).
5. The HLR returns the MSRN to OmniMSC in the SRI response.
6. OmniMSC routes the call to the serving MSC using the MSRN, either via an ISUP IAM or a SIP INVITE depending on the interconnect type.
7. The serving MSC pages the subscriber and completes the MT call setup.

MSRN Pool

OmniMSC maintains a pool of MSRN for allocation during MT call routing. When a subscriber is paged at the local MSC, an MSRN is allocated from the pool, associated with the subscriber's IMSI, and returned to the querying GMSC. The MSRN is released back to the pool once the incoming call arrives or the allocation times out.

Pool-Aware Routing

When MSC pool mode is active (see [MSC Pool and NRI](#)), the routing module considers the NRI embedded in the subscriber's TMSI during MT call routing. If a subscriber's TMSI contains a foreign NRI (belonging to another pool member), the MSC can relay the subscriber to the owning MSC via MAP SendIdentification, re-register the subscriber locally if the owning MSC is unreachable, or route MT calls to the owning MSC if the subscriber has not yet re-registered locally.

NRI-based routing is automatic when pool mode is enabled and does not require explicit route table entries.

Number Analysis Flow

The full routing decision flow, from called number to destination, proceeds through the following stages:

1. Call barring check -- if the subscriber is barred from this call type, the call is rejected with a GSM cause code.
2. CAMEL trigger check -- if a CAMEL service key matches, an InitialDP is sent to the SCP. The SCP may modify the called number, connect to a different destination, or release the call.
3. Number analysis -- the called number is classified and normalized as described above.
4. Route table lookup -- longest-prefix match against the route table.

5. Destination dispatch -- the call is handed to the appropriate handler based on the matched destination type.
 6. Failover (if applicable) -- for :sip_with_failover routes, a failed SIP attempt triggers automatic retry via the ISUP fallback trunk.
-

ISUP Trunk Groups

Each ISUP trunk group represents a bundle of voice circuits to a remote SS7 exchange. Trunk groups are identified by name and configured with a destination point code and CIC range. When routing selects an ISUP trunk group, the Trunk Router allocates the first idle circuit found in the trunk group and sends an IAM.

Trunk groups support priority levels: primary (first choice), overflow (used when primary circuits are exhausted), and last-resort. Only active trunk groups are selected for routing; inactive or congested trunk groups are skipped.

Each trunk group tracks seizure, answer, busy, congestion, and release counters for operational monitoring.

SIP Peer Selection

SIP peers represent remote VoIP gateways, IMS nodes, or SIP trunking providers. Each peer is configured with an address, port, transport (UDP, TCP, or TLS), supported codecs, and maximum concurrent channels.

Peer health is monitored via periodic SIP OPTIONS keepalives. If a peer stops responding, its status transitions to "down" and the peer is excluded from routing. When a route specifies a SIP peer by name, the Trunk Router verifies the peer is reachable and has available capacity before routing the call.

3GPP Specification References

Specification	Title	Relevance
TS 23.018	Basic Call Handling	GMSC function, MT call routing, number analysis
TS 29.002	MAP Specification	MAP SendRoutingInfo, MSRN allocation
TS 23.078	CAMEL Phase 4	CAMEL trigger handling in the routing flow

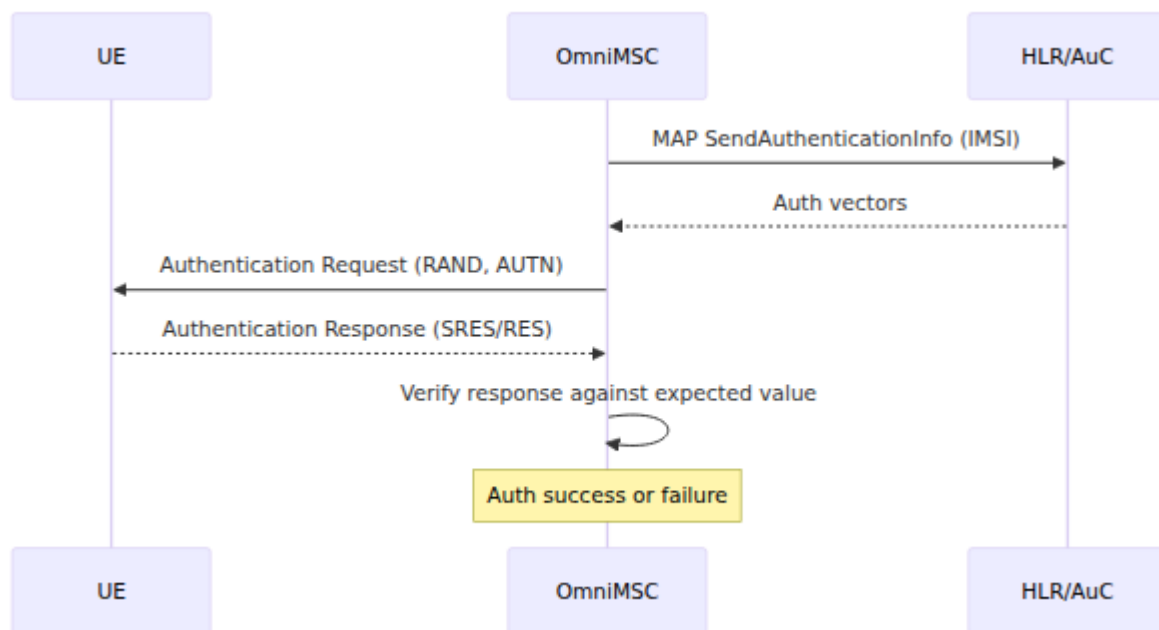
Security

This document describes the authentication, ciphering, and identity management mechanisms implemented by OmniMSC, including GSM and UMTS authentication, air-interface encryption, TMSI allocation, and identity request procedures. For configuration of cipher algorithms and security parameters, see [Configuration Reference](#). For the MAP operations that support authentication, see [MAP Operations](#). For TMSI allocation in MSC pool deployments with NRI encoding, see [MSC Pool and NRI](#).

Authentication Overview

OmniMSC supports both GSM (2G) and UMTS (3G) authentication as defined in 3GPP TS 33.102 and TS 24.008 Section 4.3. Authentication is performed during location updates and, optionally, during call setup and SMS transactions.

The MSC does not store long-term subscriber credentials (Ki). Authentication vectors are obtained from the HLR/AuC via MAP SendAuthenticationInfo (see [MAP Operations](#)). The MSC sends the IMSI to the HLR, which returns a set of authentication vectors. The MSC then challenges the UE and verifies its response. The subscriber's current authentication state and remaining tuple count are visible in the control panel — see [Control Panel Guide](#).



UMTS AKA (Authentication and Key Agreement)

UMTS Authentication and Key Agreement provides mutual authentication -- the network authenticates the subscriber and the subscriber authenticates the network. This is the preferred authentication method for USIM-equipped terminals.

The HLR returns quintuplets, each containing five values:

Field	Size	Description
RAND	128 bits	Random challenge generated by AuC
XRES	32-128 bits	Expected response, used by MSC to verify UE
CK	128 bits	Cipher key for air-interface encryption
IK	128 bits	Integrity key for air-interface integrity protection
AUTN	128 bits	Authentication token, used by UE to verify network

The MSC sends RAND and AUTN to the UE. The USIM verifies AUTN to authenticate the network, then computes RES, CK, and IK. The MSC compares the returned RES against XRES to authenticate the subscriber.

SQN Resynchronisation

AUTN contains a sequence number (SQN) that the USIM checks to prevent replay attacks. If the USIM determines that SQN is out of range (e.g., after a long period of inactivity or database restoration), it returns an Authentication Failure with cause "SQN failure" and includes an AUTS (resynchronisation token) of 112 bits. The MSC forwards AUTS to the HLR in a new MAP SendAuthenticationInfo request, allowing the AuC to resynchronise its SQN counter and return fresh vectors.

GSM AKA

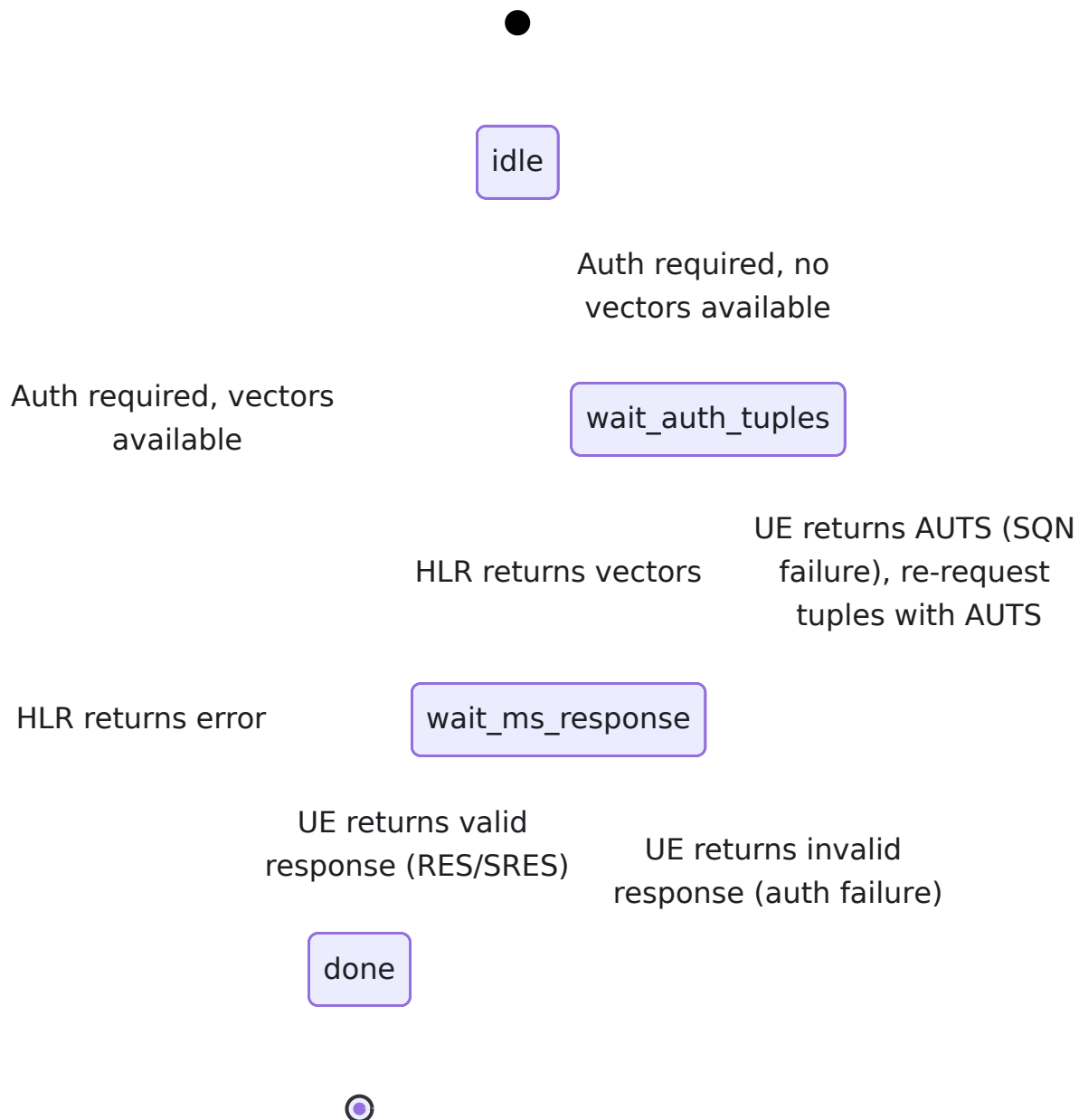
GSM authentication uses triplets for 2G-only subscribers (SIM without USIM application). Each triplet contains:

Field	Size	Description
RAND	128 bits	Random challenge
SRES	32 bits	Signed response, computed by SIM using A3(Ki, RAND)
Kc	64 bits	Cipher key, computed by SIM using A8(Ki, RAND)

GSM authentication is one-way: the network authenticates the subscriber, but the subscriber does not authenticate the network. The MSC sends RAND, the SIM computes SRES and Kc, and the MSC verifies SRES against the expected value from the triplet.

Auth FSM States

The authentication procedure is managed by a finite state machine within the VLR. The FSM tracks the progress of each authentication attempt.



In the `wait_auth_tuples` state, the MSC has sent MAP SendAuthenticationInfo and is awaiting vectors from the HLR. In `wait_ms_response`, the MSC has sent Authentication Request to the UE and is awaiting the response. When the UE reports a sequence number mismatch (AUTS), the FSM re-enters `wait_auth_tuples` — it re-requests fresh vectors from the HLR by sending MAP SendAuthenticationInfo carrying the AUTS resynchronisation token. There is no separate resync state; resynchronisation is handled as a return to `wait_auth_tuples`.

Ciphering

After successful authentication, the MSC initiates air-interface ciphering to protect signaling and user traffic on the radio path.

GERAN (2G/3G via BSC)

For the A-interface, the MSC sends a BSSMAP Cipher Mode Command to the BSC, carrying the cipher key (Kc) and the selected A5 algorithm. The BSC activates ciphering on the radio channel and returns Cipher Mode Complete.

Algorithm	Security	Description
A5/1	Moderate	Original GSM cipher, widely deployed
A5/3	Strong	KASUMI-based cipher, recommended for all deployments

UTRAN (3G via RNC)

For the Iu-CS interface, the MSC sends a RANAP Security Mode Command to the RNC, carrying CK, IK, and the selected UEA (encryption) and UIA (integrity) algorithms. The RNC activates ciphering and integrity protection and returns Security Mode Complete.

Allowed A5 Configuration

The operator configures the set of permitted A5 algorithms. The MSC selects the strongest algorithm supported by both the network configuration and the mobile station's reported capabilities.

The permitted algorithms are specified as a list: `allowed_a5: [:a5_1, :a5_3]`. The MSC intersects this list with the MS classmark capabilities and selects the highest-strength match. If no common algorithm exists and A5/0 is not permitted, the MSC rejects the connection.

TMSI Allocation

The MSC allocates a Temporary Mobile Subscriber Identity (TMSI) to each subscriber after a successful Location Update. The TMSI replaces the IMSI for subsequent paging and identification, reducing exposure of the permanent identity on the air interface.

Allocation and Confirmation

After completing authentication, ciphering, and the HLR UpdateLocation exchange, the MSC generates a new TMSI and sends it to the mobile station in the Location Update Accept message. The MS stores the TMSI and responds with TMSI Reallocation Complete.

If the TMSI Reallocation Complete is not received within the reallocation timer, the MSC confirms the new TMSI rather than rolling back. This design choice prevents a scenario where the MS has successfully stored the new TMSI but the confirmation was lost on the air interface -- rolling back would leave the MSC and MS with mismatched TMSIs, breaking subsequent paging.

TMSI in MSC Pool

When operating in an MSC pool (3GPP TS 23.236), the TMSI carries NRI (Network Resource Identifier) bits that allow the BSC to route returning subscribers to the correct MSC in the pool. The NRI is embedded in a configurable bit range within the TMSI. When a BSC receives a service request or paging response containing a TMSI, it extracts the NRI and routes the signaling to the MSC that owns that NRI range.

For MSC pool configuration and NRI assignment, see [MSC Pool & NRI](#).

Identity Request

When the MSC cannot resolve a subscriber's identity -- for example, when a TMSI is presented that is not found in the local VLR (after MSC restart, pool re-routing, or VLR overflow) -- the MSC sends an Identity Request to the mobile station requesting the IMSI.

The MS responds with an Identity Response containing its IMSI. The MSC then proceeds with authentication using the IMSI. This procedure is defined in 3GPP TS 24.008 Section 4.3.3.

Identity Request is also used to obtain the IMEI (International Mobile Equipment Identity) when equipment checking is required.

3GPP Specification References

Specification	Title	Relevance
TS 33.102	3G Security; Security Architecture	UMTS AKA, quintuplets, SQN resynchronisation, key hierarchy
TS 24.008	Mobile Radio Interface Layer 3	Authentication Request/Response (Sec 4.3), Identity Request (Sec 4.3.3), TMSI Reallocation (Sec 4.3.1)
TS 43.020	Security Related Network Functions	GSM A3/A8, A5 cipher algorithms
TS 48.008	MSC-BSS Interface (BSSMAP)	Cipher Mode Command/Complete
TS 25.413	UTRAN Iu Interface (RANAP)	Security Mode Command/Complete
TS 23.236	Intra-Domain Connection of RAN Nodes to Multiple CN Nodes	NRI allocation, TMSI structure for MSC pool
TS 29.002	MAP Specification	MAP SendAuthenticationInfo

SGs Interface and CSFB

This document describes the SGs interface and Circuit-Switched Fallback (CSFB) implementation in OmniMSC by Omnitouch per 3GPP TS 29.118. The SGs interface connects the MSC/VLR to the MME, enabling combined EPS/IMSI attach, CS paging via the LTE network, and SMS delivery without CS fallback.

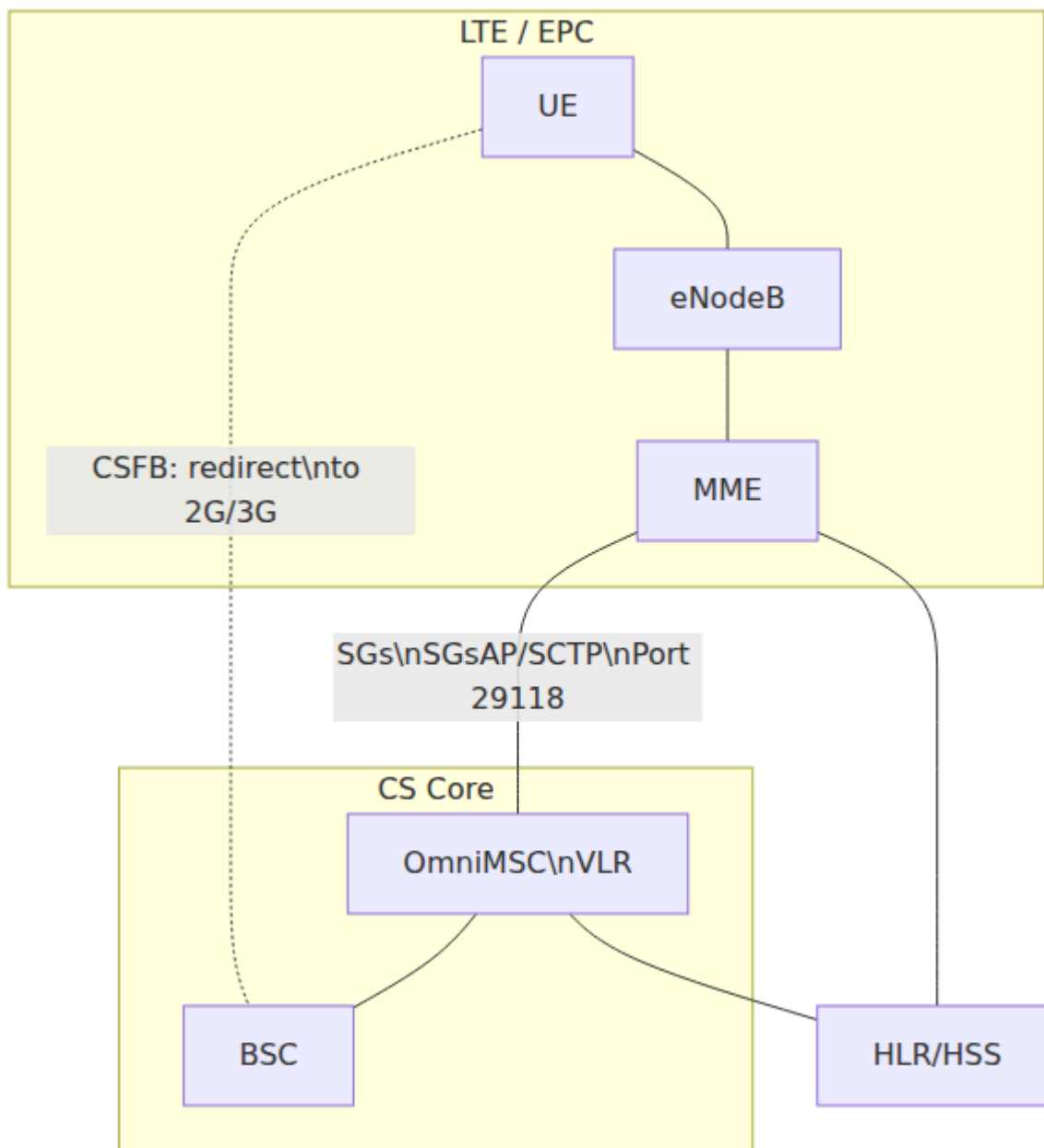
For the CSFB MT call sequence diagram, see [Call Flow Diagrams](#). For configuration parameters, see [Configuration Reference](#). For authentication during combined attach, see [Authentication & Security](#). For SMS over SGs, see [SMS](#). For MSC Pool considerations with CSFB, see [MSC Pool](#).

Overview

In LTE networks, the MME handles mobility management for packet-switched services. However, LTE does not natively support circuit-switched voice prior to VoLTE deployment. CSFB allows LTE-attached subscribers to receive and make CS voice calls and SMS by falling back to the 2G/3G CS domain.

The SGs interface is the signalling link between the MSC/VLR and the MME, carrying SGsAP messages over SCTP (default port 29118). Through SGs, the MSC can:

- Perform combined EPS/IMSI attach, registering a subscriber in both the EPC and CS domains simultaneously.
- Page LTE-attached subscribers for incoming CS calls, triggering a fallback to GERAN or UTRAN.
- Deliver SMS to LTE-attached subscribers without CSFB, tunnelling the NAS PDU through the SGs interface.



SGsAP Message Types

The SGs interface carries the following SGsAP message types per 3GPP TS 29.118.

Location Update

Message	Direction	Purpose
SGsAP-LOCATION-UPDATE-REQUEST	MME to MSC	Combined EPS/IMSI attach or periodic location area update
SGsAP-LOCATION-UPDATE-ACCEPT	MSC to MME	Location update accepted, includes new TMSI
SGsAP-LOCATION-UPDATE-REJECT	MSC to MME	Location update rejected with cause code

Paging and Service

Message	Direction	Purpose
SGsAP-PAGING-REQUEST	MSC to MME	Page subscriber for MT call or MT SMS
SGsAP-SERVICE-REQUEST	MME to MSC	Subscriber responding to CS paging (CSFB in progress)
SGsAP-SERVICE-ABORT-REQUEST	MSC to MME	Abort a CS fallback service request

SMS Tunnelling

Message	Direction	Purpose
SGsAP-DOWNLINK-UNITDATA	MSC to MME	MT SMS delivery: NAS PDU carried to UE via SGs
SGsAP-UPLINK-UNITDATA	MME to MSC	MO SMS submission: NAS PDU carried from UE via SGs

Detach

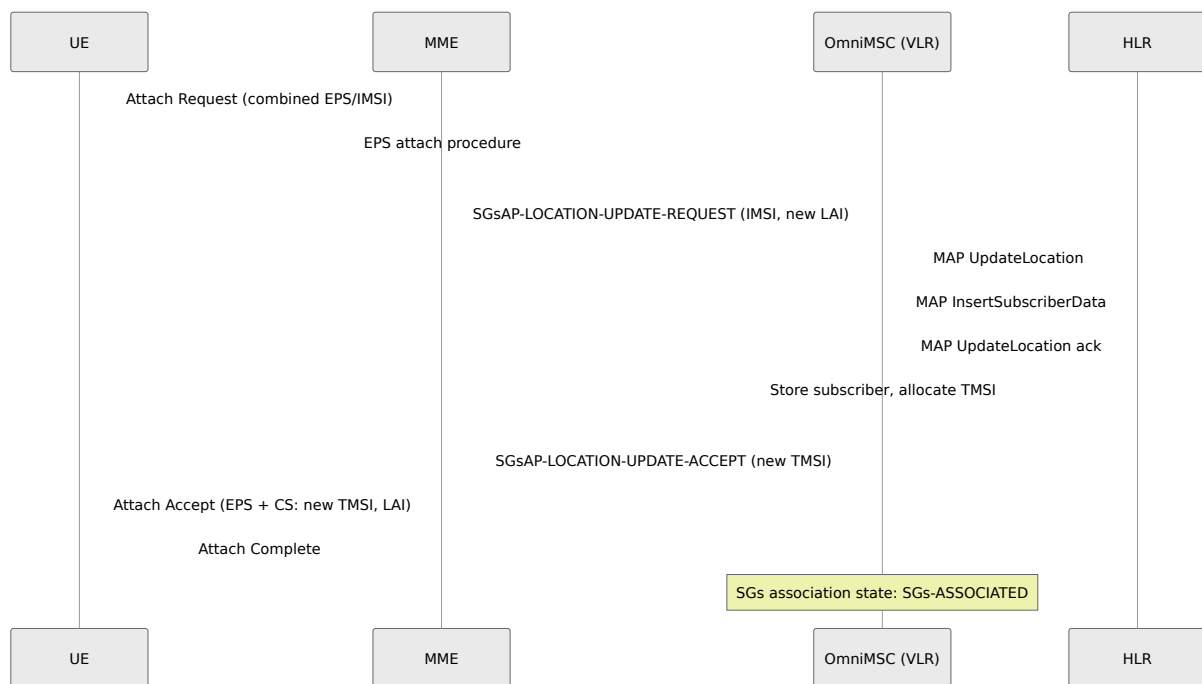
Message	Direction	Purpose
SGsAP-EPS-DETACH-INDICATION	MME to MSC	Subscriber detached from EPS
SGsAP-EPS-DETACH-ACK	MSC to MME	Acknowledge EPS detach
SGsAP-IMSI-DETACH-INDICATION	MME to MSC	Subscriber IMSI detach
SGsAP-IMSI-DETACH-ACK	MSC to MME	Acknowledge IMSI detach

Reset and Status

Message	Direction	Purpose
SGsAP-RESET-INDICATION	Either direction	Peer has restarted; receiver must re-register affected subscribers
SGsAP-RESET-ACK	Either direction	Acknowledge reset indication
SGsAP-STATUS	Either direction	Error indication with cause and erroneous message
SGsAP-MM-INFORMATION-REQUEST	MSC to MME	Network name and time zone information
SGsAP-ALERT-REQUEST	MSC to MME	Alert request after paging failure
SGsAP-ALERT-ACK	MME to MSC	Acknowledge alert
SGsAP-UE-ACTIVITY-INDICATION	MME to MSC	UE has become active
SGsAP-RELEASE-REQUEST	MSC to MME	Release SGs connection for this subscriber

Combined EPS/IMSI Attach

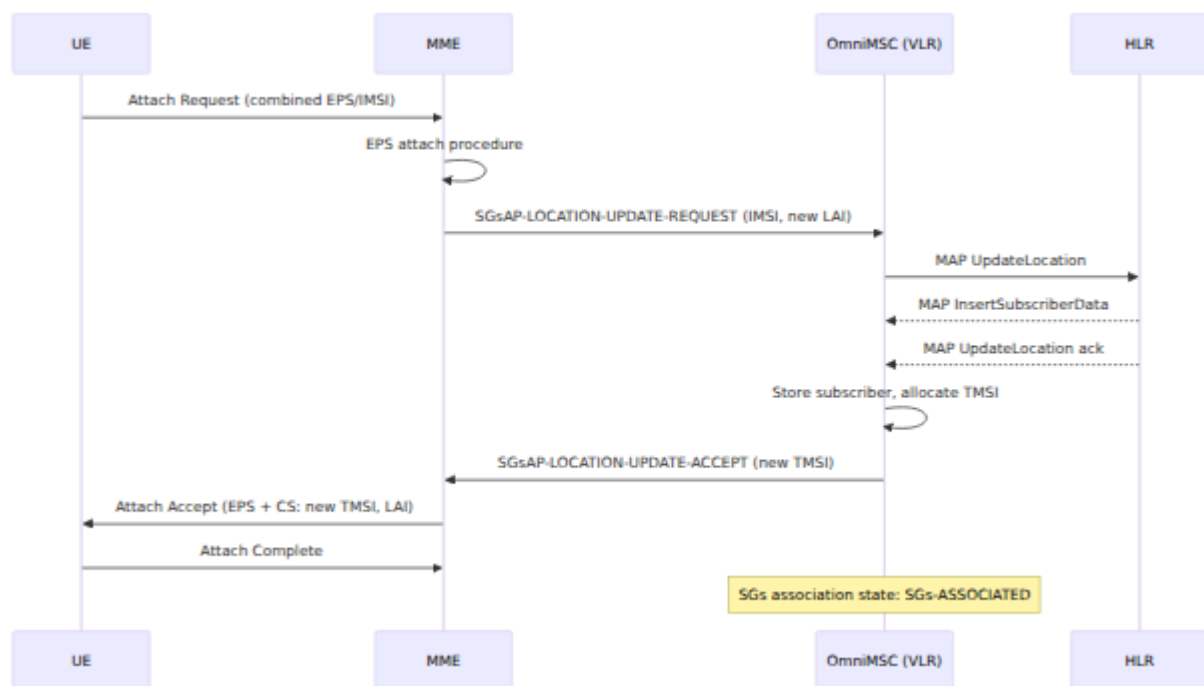
When a UE performs a combined EPS/IMSI attach in LTE, the MME sends an SGsAP-LOCATION-UPDATE-REQUEST to the MSC. The MSC performs a VLR location update, which may include HLR interrogation, and responds with acceptance or rejection. Upon acceptance, the subscriber is registered in both the EPC (via the MME) and the CS domain (via the MSC/VLR) simultaneously.



After a successful combined attach, the subscriber's SGs association state transitions to SGs-ASSOCIATED. The MSC can now page the subscriber via SGs and deliver SMS without CSFB.

MT Call Paging via CSFB

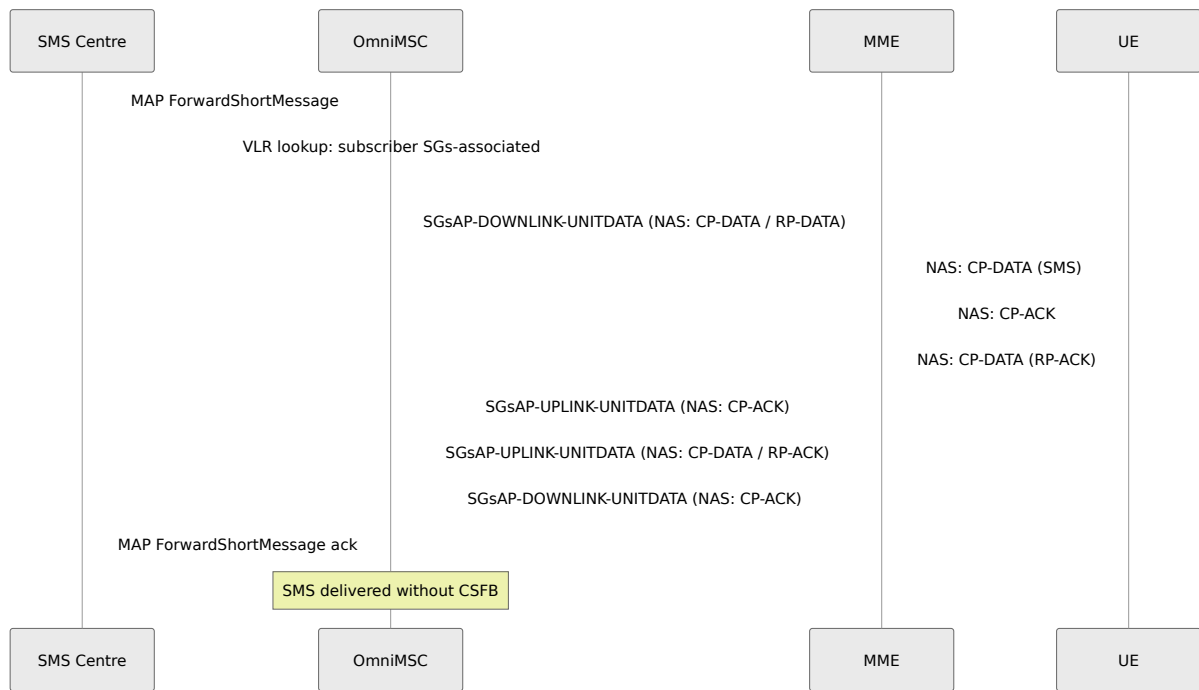
When an MT call arrives for a subscriber that is attached via LTE (SGs-associated), the MSC pages the subscriber through the MME rather than through BSCs. The MME instructs the UE to fall back to 2G or 3G, where the call proceeds over the A-interface or Iu-CS interface.



Once the UE has fallen back to the CS domain and sent a Paging Response via the BSC, the call proceeds as a normal MT call. The MSC-A state machine handles the E-UTRAN/SGs RAN type by omitting the Clear Complete step that would normally be expected from a BSC, since the SGs association does not use BSSMAP connection management.

MT SMS via SGs

SMS can be delivered to LTE-attached subscribers without requiring CSFB. The MSC tunnels the SMS NAS PDU through the SGs interface to the MME, which delivers it to the UE over the LTE air interface. This avoids the latency and radio resource cost of a CS fallback for a short message.

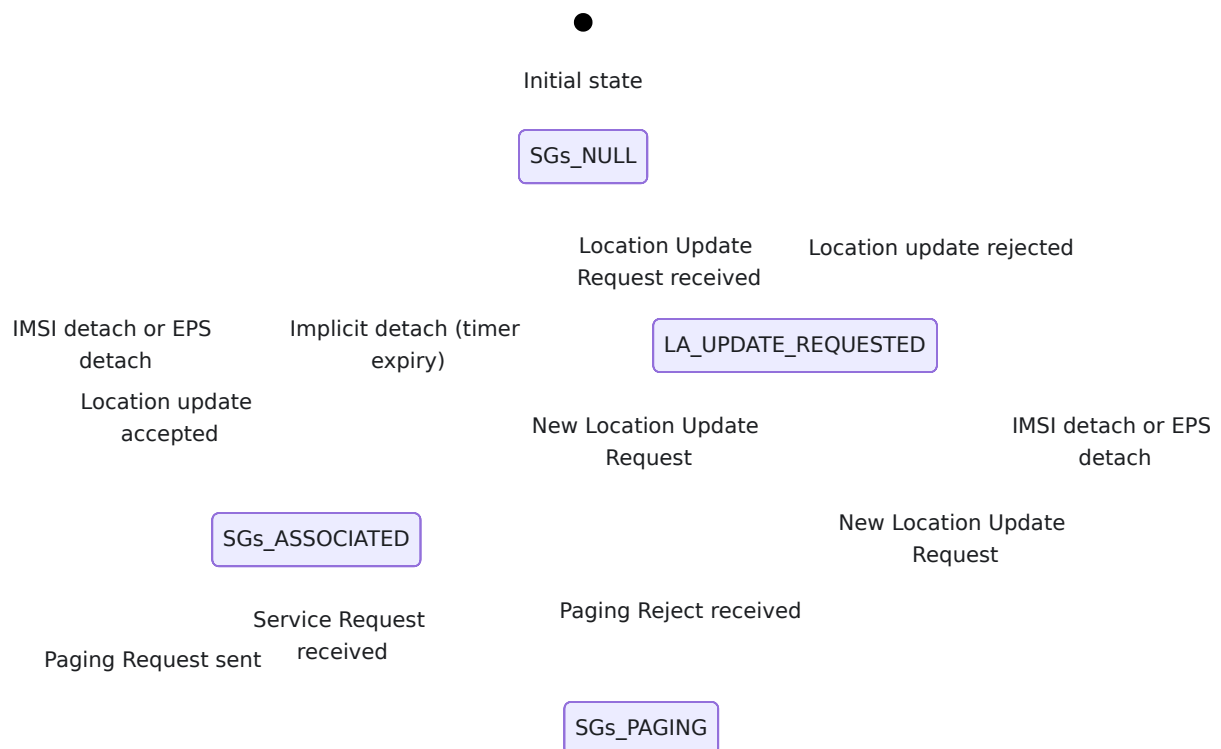


MO SMS follows the reverse path: the UE sends the SMS NAS PDU via the MME as SGsAP-UPLINK-UNITDATA, and the MSC forwards it to the SMS Centre.

SGs Association States

Each subscriber's SGs association is tracked as a state machine per 3GPP TS 29.118 Section 4.

State	Description
SGs-NULL	No SGs association exists. CS paging via SGs is not possible. This is the initial state.
LA-UPDATE-REQUESTED	A location update is in progress. The MSC has received a request from the MME but has not yet completed the HLR update.
SGs-ASSOCIATED	The subscriber has a valid SGs association. The MSC can page via SGs and deliver SMS without CSFB.
SGs-PAGING	A CS paging request has been sent to the MME and the MSC is awaiting the subscriber's response. Entered from SGs-ASSOCIATED on a paging request; returns to SGs-ASSOCIATED on a service request or paging reject.



MME Tracking

The SGs handler maintains a registry of known MMEs. Each MME is identified by its FQDN (the MME Name information element in SGsAP messages). For each MME, the handler tracks:

- The SCTP connection reference used for sending outbound messages.
- The set of IMSIs (subscribers) currently associated with that MME.

This per-MME subscriber registry enables targeted reset handling: when an MME fails, only the subscribers associated with that specific MME are affected.

MME Reset Handling

Reset procedures ensure state consistency when either the MSC or an MME restarts.

Scenario	Initiator	Action by Receiver
MSC restart	MSC sends SGsAP-RESET-INDICATION to all known MMEs	Each MME re-sends SGsAP-LOCATION-UPDATE-REQUEST for its associated subscribers, allowing the MSC to rebuild VLR state
MME restart	MME sends SGsAP-RESET-INDICATION to the MSC	MSC marks all subscribers associated with that MME as SGs-detached (SGs-NULL state) and clears the subscriber list for that MME
SGs link failure	Detected by either side	Both sides treat the failure as an implicit reset

When the MSC receives a Reset Indication from an MME, it iterates over all subscribers registered against that MME, transitions each to the SGs-NULL state, and clears the MME's subscriber set. On the next contact from any

affected subscriber (location update or paging response), the MSC performs a full re-registration.

SGsAP Codec

Encoding and decoding of SGsAP messages is provided by the shared `sgs_ex` library (`SgsEx.Codec`), which OmniMSC pulls in as an external dependency rather than an in-tree module. The codec handles the SGsAP messages per the formats defined in 3GPP TS 29.118, processing the binary SGsAP message type octet and information elements (IEs), supporting all mandatory and optional IEs for each message type. Encoded messages are transmitted over SCTP; decoded messages are dispatched to the SGs handler for processing.

Configuration

The SGs interface is configured under the `sgs` key in the MSC configuration.

Parameter	Default	Description
<code>listen_port</code>	29118	SCTP listen port for SGsAP connections from MMEs. Port 29118 is the 3GPP-defined port for SGs per TS 29.118. Setting <code>listen_port: 0</code> disables the SGs transport (no socket is opened), which is useful for test deployments.
<code>vlr_name</code>	(required)	VLR name in FQDN format, used in SGsAP messages. The MME uses this to identify the VLR. Must match the VLR name configured on the MME side.

RAN Type: E-UTRAN via SGs

The MSC-A state machine supports E-UTRAN via SGs as a distinct RAN type (:eutran_sgs). When a subscriber is SGs-associated, the MSC-A FSM adjusts its behavior for the SGs interface:

- No BSSMAP connection management is used; there is no Clear Command / Clear Complete exchange.
- Paging is performed via SGsAP-PAGING-REQUEST to the MME rather than via BSSMAP Paging to BSCs.
- SMS delivery uses SGsAP Downlink/Uplink Unitdata rather than DTAP over the A-interface.
- Once the subscriber falls back to GERAN or UTRAN (after CSFB), the connection transitions to the corresponding RAN type for the remainder of the call.

3GPP Specification References

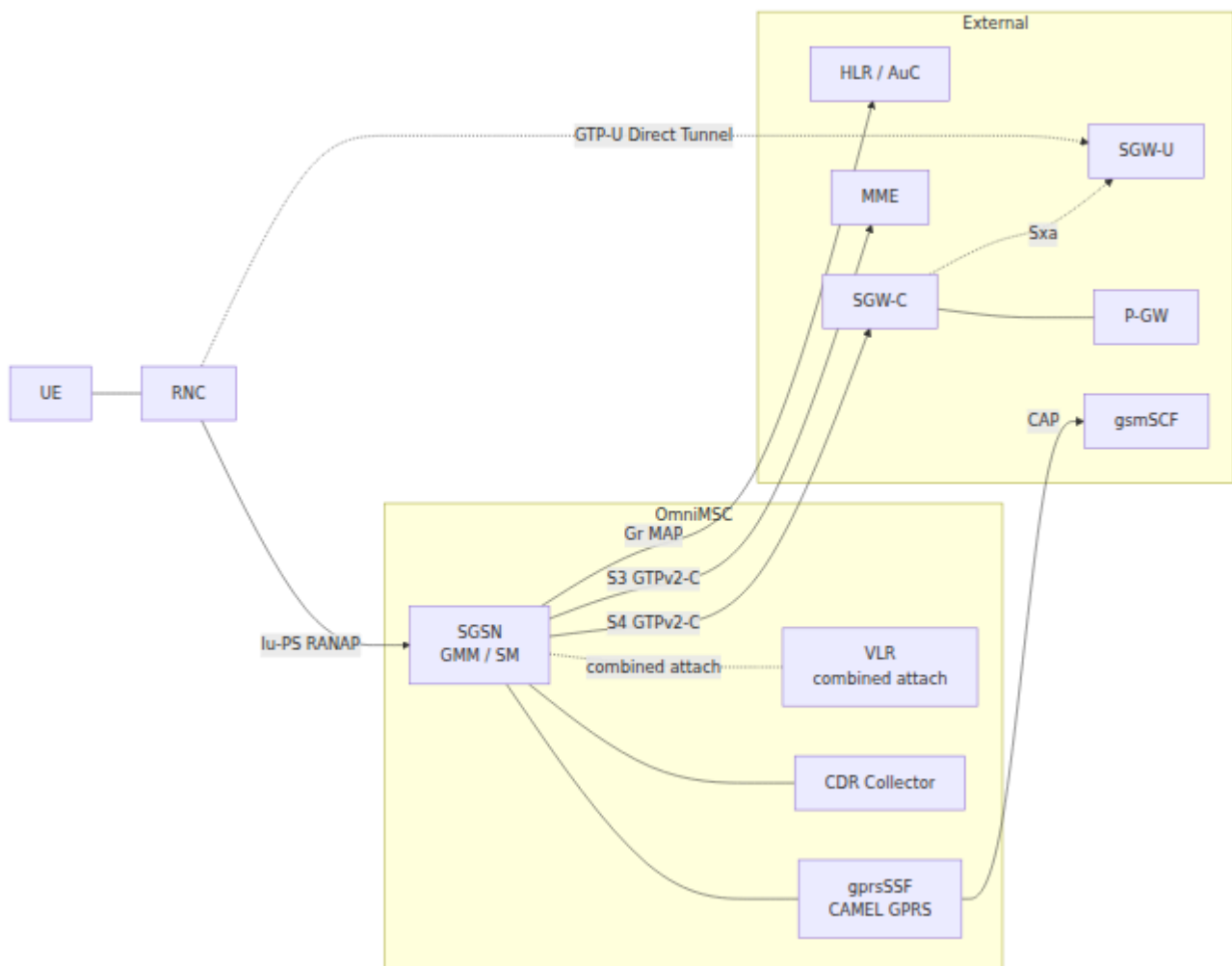
Specification	Title	Relevance
TS 29.118	MME-VLR SGs Interface Specification	SGsAP protocol, message formats, procedures
TS 23.272	Circuit Switched Fallback in EPS	CSFB architecture, call flows, SMS over SGs
TS 23.012	Location Management Procedures	VLR location update procedures used in SGs
TS 24.008	Mobile Radio Interface Layer 3	NAS messages tunnelled via SGs Unitdata

SGSN (Packet Domain)

OmniMSC includes an integrated **S4-SGSN** that serves the packet-switched (PS) domain for 3G (UTRAN) subscribers over **Iu-PS**, anchoring their data sessions on the same S-GW/P-GW as LTE. A single node serves both the CS domain (voice, SMS) and the PS domain (packet data) for a subscriber; combined attach is handled in-process between the SGSN and the VLR.

The SGSN is disabled by default and enabled per the [configuration](#) below. Most external dependencies are opt-in so a lab can run the packet core with a static peer and injected credentials before a full HLR/DNS estate exists.

Architecture



Direct Tunnel is used: the GTP-U user plane runs directly between the RNC and the S-GW-U. The SGSN brokers the tunnel endpoints during bearer setup but never carries user-plane packets. When the UE goes idle (PMM-IDLE) the SGSN re-anchors the downlink endpoint back on itself so the S-GW buffers and raises a Downlink Data Notification instead of sending to a released RNC (TS 23.060 §15.6).

Interfaces

Interface	Peer	Protocol	Purpose	Reference
Iu-PS	RNC	RANAP over SCCP/M3UA	NAS transport, RAB assignment, relocation	TS 25.413
Gr	HLR / AuC	MAP over TCAP/SCCP	Location update, auth vectors, subscription	TS 29.002
S4	S-GW (SGW-C)	GTPv2-C	Create / Modify / Delete Session, paging	TS 29.274
S3	MME	GTPv2-C	3G-PS to LTE inter-RAT mobility	TS 29.274 §7.3
Gn/Gp (CAP)	gsmSCF	CAP over TCAP/SCCP	CAMEL GPRS online charging / control	TS 29.078
GTP-U	RNC to S-GW-U	GTP-U (Direct Tunnel)	User plane (not through the SGSN)	TS 29.281

Iu-PS, Gr, S3 and CAP reuse the SS7 and GTPv2-C stacks the CS side already runs. S3 and Sv share the GTPv2-C server; the SRVCC Sv interface remains on its own socket.

Configuration

The SGSN reads `config :omnimsc, :sgsn` and, for the GTPv2-C interfaces, the shared `config :gtpc, :service` block.


```

config :omnimsc, :sgsn,
  enabled: true,
  # Routing area this SGSN serves (advertised to UEs)
  rai: %{mcc: "001", mnc: "01", lac: 1, rac: 1},
  # NRI width for P-TMSI allocation in a pool (0 = no pool)
  nri_bits: 6,
  # This SGSN's S4/S3 control-plane F-TEIDs advertised to the S-GW
  / MME
  s4_f_teid: %{teid: "0a0a0a0a", ipv4: "10.0.0.10"},
  s3_f_teid: %{teid: "0b0b0b0b", ipv4: "10.0.0.10"},
  # GTP-C recovery restart counter (TS 23.007 §18)
  recovery: 1,
  # Static packet-core peers (used unless DNS selection is
  enabled)
  sgw: %{ip: "10.179.1.25", port: 2123},
  pgw_c: "10.179.1.21",
  # Default APN-AMBR sent in Create Session when the subscription
  carries none
  default_apn_ambr: %{ul: 0, dl: 0},
  # APN-based P-GW/S-GW selection via DNS S-NAPTR (opt-in; default
  off)
  pgw_dns: false,
  sgw_dns: false,
  # Iu-release guard timer (ms) after an Iu Release Command
  iu_release_guard_ms: 5000,
  # GMM / SM retransmission timer overrides (ms)
  gmm_timers: %{t3350: 6000, t3360: 6000, t3370: 6000, t3312:
  3_240_000},
  sm_timers: %{t3395: 8000},
  # Subscription fallback when Gr Insert Subscriber Data is not
  wired
  subscribed_apns: ["internet"],
  default_apn: "internet",
  wildcard_apn: false

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

```

n3: 3

}

Core Parameters

Parameter	Type	Required	Default	Description
<code>enabled</code>	Boolean	No	<code>false</code>	Master serving the SGSN tree and identity.
<code>rai</code>	Map	Yes	-	Routing Area Identity (mcc/mnc) advertise and used serving network.
<code>nri_bits</code>	Integer	No	0	NRI field in the P-TMS with the I-RAT. 0 disable.
<code>s4_f_teid</code>	Map	Yes	-	SGSN S4 TEID (teid) (ip4) the address bearer signaling.
<code>s3_f_teid</code>	Map	No	-	SGSN S3 TEID advertise the MME RAT mobility.
<code>recovery</code>	Integer	No	0	GTP-C Restart counter. 23.007 §11.1.1 Increment restart.

Parameter	Type	Required	Default	Description
<code>sgw</code>	Map	No	<code>{ip: "10.179.1.25", port: 2123}</code>	Static S-C peer user <code>sgw_dns</code>
<code>pgw_c</code>	String	No	<code>"10.179.1.21"</code>	Static P-C address u <code>pgw_dns</code>
<code>default_apn_ambr</code>	Map	No	<code>{ul: 0, dl: 0}</code>	APN-AMB placed in Session w subscript supplies i avoids lal that rejec zero valu
<code>pgw_dns</code>	Boolean	No	<code>false</code>	Resolve t per reque via DNS S (TS 29.30 back to p any DNS
<code>sgw_dns</code>	Boolean	No	<code>false</code>	Resolve t per reque via DNS S Falls back on any DI
<code>iu_release_guard_ms</code>	Integer	No	5000	Time to w RANAP Iu Complete force-free

Parameter	Type	Required	Default	Description
				connectio 25.413 §8

Timer Parameters

Parameter	Type	Default (ms)	Description
<code>gmm_timers.t3350</code>	Integer	6000	Retransmit of Attach Accept / RAU Accept / P-TMSI Reallocation awaiting Complete (TS 24.008 §11.2.2).
<code>gmm_timers.t3360</code>	Integer	6000	Retransmit of Authentication & Ciphering Request awaiting Response.
<code>gmm_timers.t3370</code>	Integer	6000	Retransmit of Identity Request awaiting Identity Response.
<code>gmm_timers.t3312</code>	Integer	3240000	Mobile-reachable / periodic-RAU timer; on expiry (plus grace) the MM and PDP contexts are implicitly detached (TS 24.008 §4.7.2.2).
<code>sm_timers.t3395</code>	Integer	8000	Retransmit of a network-requested Deactivate PDP Context Request awaiting Accept (TS 24.008 §6.1.3.4.2).

All retransmission timers cap at 5 attempts before the procedure is abandoned.

Subscription and APN Parameters

Used to validate the requested APN when Gr Insert Subscriber Data has not populated a live subscription (see [Gr MAP](#)). When a real subscription is present it takes precedence over these static values.

Parameter	Type	Default	Description
<code>subscribed_apns</code>	List	<code>[]</code>	Allowed APN names. A requested APN outside this list is rejected with SM cause 33 (TS 24.008 §10.5.6.6). Empty disables enforcement (accept any).
<code>default_apn</code>	String	-	APN used when the UE requests none. Falls back to the sole subscribed APN if unset.
<code>wildcard_apn</code>	Boolean	<code>false</code>	When <code>true</code> , any requested APN is permitted (wildcard subscription).

Lab Injection Seams

These keys inject a function (or `{module, function}`) so the packet core can run before the SS7/HLR estate is complete. They are optional; when unset the SGSN skips the corresponding external round-trip and the procedure still completes.

Parameter	Type	Description
quintet_source	Function/{m, f}	Supplies a UMTS AKA quintet (imsi, resync) for the authentication challenge instead of a live Gr SendAuthenticationInfo.
gr_source	Function/{m, f}	Supplies the HLR UpdateGprsLocation / Insert Subscriber Data result at attach. When unset, attach proceeds without Gr registration.
purge_ms_sink	Function/{m, f}	Receives a Purge MS notification when the SGSN drops a subscriber.

GTP-C Service Parameters

Parameter	Type	Required	Default	Description
<code>name</code>	Atom	Yes	-	Service name; <code>:s3</code> for the SGSN mobility server.
<code>listen_ip</code>	String	Yes	-	Bind address for the GTPv2-C server.
<code>listen_port</code>	Integer	No	2123	GTP-C UDP port (TS 29.274).
<code>control_module</code>	Module	Yes	-	<code>Omnimsc.Gtpc.Router</code> routes peer-initiated S3/S4 messages into the SGSN.
<code>t3</code>	Integer	No	5000	GTP-C request retransmission timer (ms).
<code>n3</code>	Integer	No	3	GTP-C maximum retransmission attempts.

When both Sv (SRVCC) and the SGSN's GTPv2-C interfaces run on one host, bind them to distinct IP/port endpoints.

Mobility Management (GMM)

The SGSN runs a per-UE GMM state machine ([TS 24.008 §4.7](#)).



Deregistered

Attach (P-TMSI only)

Attach (IMSI)

IdentityPending

Identity Response

AuthPending

Auth success (lu)

Detach / implicit detach
(T3312)

WaitSecurityMode

Security Mode Complete

AttachInitiated

Attach Complete

Registered

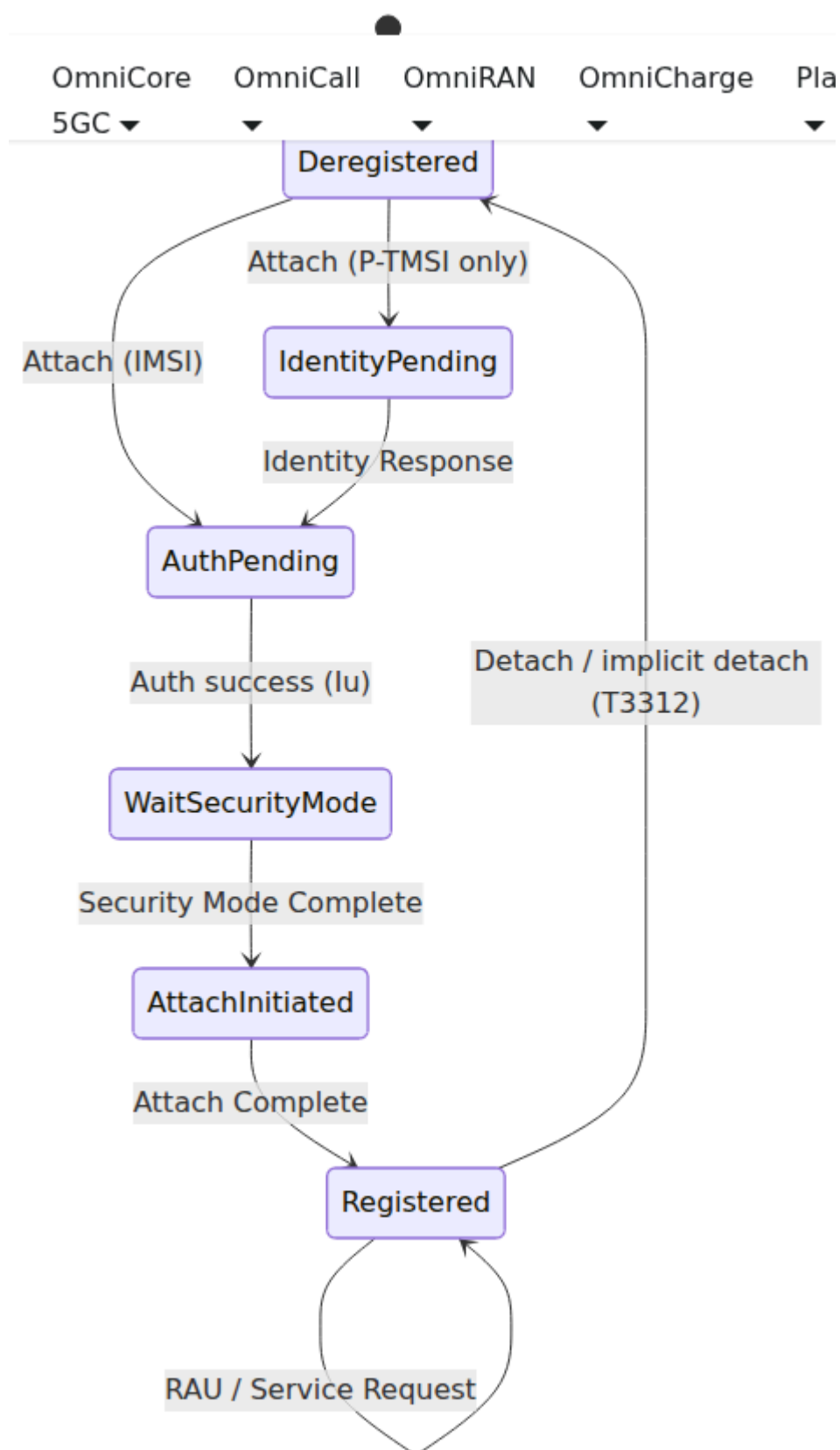
RAU / Service Request

Implemented GMM behaviour:

- **Attach / RAU / Detach / Service Request**, with combined (PS+CS) attach handled in-process with the VLR.

- **UMTS AKA** authentication with RES validation against XRES, including AUTS resynchronisation.
 - **P-TMSI allocation** and a **P-TMSI signature** authenticated on a later attach/RAU (TS 24.008 §10.5.5.8).
 - **Retransmission timers** T3350/T3360/T3370 and the **mobile-reachable timer** T3312 driving implicit detach.
 - **RANAP Common ID** sent to the RNC after Security Mode Complete (TS 25.413 §8.24).
 - **Identity procedure** requesting IMEISV during attach.
 - **GMM STATUS** on an unknown or erroneous GMM message, and **per-procedure reject causes** (not a single generic cause).
 - **Network-initiated (MT) Detach Request** so the network can detach a UE and prompt re-attach.
 - **PDP Context Status** handling on RAU / Service Request so the MS and SGSN PDP state cannot diverge.
 - **lu release** after a signalling-only procedure completes, with the guard timer above.
-

Session Management (SM / PDP)



Implemented SM behaviour:

- **PDP context activation** with APN, QoS and PDN address negotiation.
 - **NSAPI multiplexing / secondary PDP contexts**: a UE holds multiple concurrent contexts keyed by NSAPI (5-15); an NSAPI-in-use collision is resolved by locally deactivating the colliding context per [TS 24.008 §6.1.3.1.4](#).
 - **QoS negotiation** from requested and subscribed QoS into the S4 Bearer QoS and the NAS QoS IE.
 - **PDP types** IPv4, IPv6 and IPv4v6 end-to-end.
 - **Network-requested deactivation** with retransmission timer **T3395**.
 - **APN selection and subscription enforcement**: validate the requested APN against the subscription, resolve wildcard and default APNs, and reject a non-subscribed APN with the correct SM cause.
 - **SM STATUS** and NSAPI validation on protocol errors, with GTP-C cause mapped to the NAS SM cause.
-

Iu-PS and RANAP

The Iu-PS handler owns the SCCP connection-oriented section per UE and bridges NAS both ways over RANAP DirectTransfer.

- **InitialUE / DirectTransfer bridge** carrying GMM/SM NAS in each direction.
- **RAB Assignment** with parameters derived from the bearer/subscribed QoS, and reaction to the RAB Assignment Response **FailedList** (mapping the RANAP cause to an SM reject) and TEID-only modifications (relayed to the S-GW).
- **Iu Release** after signalling procedures, and on inbound SCCP release for a PS connection, with the guard timer.
- **RANAP RESET** from an RNC purging that RNC's stale Iu-PS connections and acknowledging.
- **RANAP Error Indication** emitted on a malformed / undecodable RANAP PDU ([TS 25.413 §8.27](#)).
- **SRNS relocation signalling** ([TS 25.413 §8.6-8.9](#)): all six Relocation PDUs, driving intra-SGSN relocation and re-anchoring Direct Tunnel on the target

RNC on completion. Inter-SGSN relocation over S3 is tracked as future work (see [Limitations](#)).

S4 and GTP-C

- **Create / Modify / Delete Session** toward the S-GW, with RAT type UTRAN and the S4-SGSN F-TEIDs.
 - **Direct Tunnel** endpoint brokering, and **downlink switch-back to the SGSN on PMM-IDLE** so the S-GW buffers and triggers paging instead of sending to a released RNC.
 - **Peer-initiated Delete / Update Bearer Request** from the S-GW/P-GW: acknowledged and relayed to the UE.
 - **GTP-C path management**: Echo Request/Response and Recovery restart-counter detection to invalidate stale sessions ([TS 23.007 §18](#)).
 - **DNS S-NAPTR P-GW/S-GW selection** per APN when enabled, with static fallback.
 - **MT-data paging**: an S4 Downlink Data Notification triggers RANAP Paging and is acknowledged ([TS 29.274 §7.2.11](#)).
-

S3 Mobility (to the MME)

- **Idle-mode context transfer**: Context Request / Response / **Acknowledge** ([TS 29.274 §7.3.7](#)).
 - **MM Context security mode** encoded as EPS (value 4) when carrying a KASME context ([TS 29.274 §8.38](#)).
 - **Forward Relocation transparent containers** (Source-to-Target / Target-to-Source RAN containers) carried end-to-end so the target radio can be set up ([TS 29.274 §7.3.1](#)).
-

Gr MAP (HLR Interface)

- **UpdateGprsLocation** registering the SGSN in the HLR at GPRS Attach ([TS 23.060 §6.5.3](#)).
- **Insert Subscriber Data** consumed into the subscriber context (allowed APNs, subscribed QoS, APN-AMBR, charging), feeding APN enforcement and QoS negotiation.
- **Cancel Location** purging the local MM and PDP contexts and tearing down the S4 session; **Purge MS** sent when the SGSN drops a subscriber.

The Gr round-trip is gated on `gr_source`; when unset, attach proceeds without Gr registration so the lab keeps working with an injected quintet.

Charging (PS CDRs)

The SGSN produces PS-domain call detail records routed to the shared CDR collector ([TS 32.251](#), [TS 32.298](#)):

- **S-CDR** (`SGSNPDPrecord`) opened on PDP activation and closed on deactivation.
- **M-CDR** (`SGSNMMRecord`) opened on Attach Complete and closed on Detach, with a change-of-location container on RAU.
- **Change-of-charging-condition** containers (QoS / RAT / tariff-time / Direct-Tunnel change) and **partial records** with an incrementing sequence number.

See [CDR documentation](#) for the collector and output format. Volume counting under Direct Tunnel depends on an S4 usage-report feed (see [Limitations](#)).

CAMEL GPRS (Online Charging and Control)

An opt-in gprsSSF drives CAMEL phase-3 GPRS control ([TS 23.078](#), [TS 29.078](#)). It is armed only when the subscription carries **GPRS-CSI**; without it, attach and PDP activation are unchanged.

- **gprsSSF state models** for Attach/Detach and PDP Context, with detection-point arming and event reporting.
 - **InitialDPGPRS** triggered at the Attach and PDP-Context-Establishment detection points.
 - **ApplyChargingGPRS / ApplyChargingReportGPRS** online-charging loop.
 - **Control operations** Connect/Continue/Release/Cancel/ActivityTest GPRS, the **Tssf** timer and **default GPRS handling** on gsmSCF error or timeout.
 - **FurnishChargingInformationGPRS** merged into the S-CDR and **SendChargingInformationGPRS** captured toward the SM layer.
-

Reference Tables

Common GMM Reject Causes (TS 24.008 §10.5.5.14)

Cause	Name	Typical trigger
2	IMSI unknown in HLR	Subscriber not provisioned
7	GPRS services not allowed	Subscription bars packet service
9	MS identity cannot be derived	RAU/Service Request P-TMSI not resolvable
11	PLMN not allowed	Roaming / PLMN restriction
17	Network failure	No authentication vectors from the HLR

Common SM (PDP) Reject Causes (TS 24.008 §10.5.6.6)

Cause	Name	Typical trigger
26	Insufficient resources	S-GW refused Create Session, or no RAB could be assigned
27	Missing or unknown APN	Requested APN cannot be resolved
31	Activation rejected, unspecified	RNC RAB setup failed
33	Requested service option not subscribed	APN not in the subscription

Metrics

Metric: omnimsc_sgsn_attach_count **Type:** Counter **Description:** GPRS attach outcomes. **Labels:**

- result - Attach result (for example accepted, rejected).

Metric: omnimsc_sgsn_pdp_count **Type:** Counter **Description:** PDP context activation outcomes. **Labels:**

- result - active or rejected.

Example queries:

```
# Attach acceptance rate
sum(rate(omnimsc_sgsn_attach_count{result="accepted"}[5m]))
  / sum(rate(omnimsc_sgsn_attach_count[5m]))

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

Troubleshooting

Attach rejected with cause 17 (network failure)

Symptoms: UE cannot attach to the packet domain; GMM Attach Reject cause 17.

Possible causes:

- No authentication vectors returned from the HLR over Gr.
- `quintet_source` unset in a lab with no live Gr.

Resolution:

1. Confirm the HLR returns vectors for the IMSI (SendAuthenticationInfo).
2. In a lab, set `quintet_source` to inject a known UMTS quintet.

PDP activation rejected with cause 26 (insufficient resources)

Symptoms: Activate PDP Context Reject cause 26.

Possible causes:

- The S-GW refused Create Session (for example a ULI or non-zero APN-AMBR it rejects).
- No RAB could be assigned by the RNC.

Resolution:

1. Check the S-GW accepts the Create Session; set `default_apn_ambr` to `%{ul: 0, dl: 0}` for S-GWs that reject a non-zero value.
2. Review the RAB Assignment Response for a FailedList entry.

PDP activation rejected with cause 33 (service option not subscribed)

Symptoms: Activate PDP Context Reject cause 33.

Possible causes:

- The requested APN is not in the subscription or in `subscribed_apns`.

Resolution:

1. Add the APN to the HLR subscription (Insert Subscriber Data) or to `subscribed_apns`.
2. Set `wildcard_apn: true` only if any APN should be permitted.

No downlink data

Symptoms: Uplink works but no downlink packets arrive.

Possible causes:

- Direct Tunnel not completed: the Modify Bearer did not carry the RNC F-TEID.
- Downlink still anchored on a released RNC after the UE went idle.

Resolution:

1. Confirm the Modify Bearer after RAB assignment carried the RNC F-TEID.
2. Confirm the downlink switch-back to the SGSN fired on PMM-IDLE so paging can bring the UE back.

RAU not routed to this SGSN

Symptoms: A UE's Routing Area Update lands on the wrong node.

Possible causes:

- The P-TMSI NRI does not match this SGSN's `nri_bits` / pool allocation.

Resolution:

1. Align `nri_bits` with the MSC/SGSN pool configuration.
-

Limitations

The following are implemented as seams or partial paths and are documented so operators know what is not yet end-to-end:

- **Volume counting under Direct Tunnel:** the SGSN sees no user plane, so S-CDR and CAMEL online-charging volumes require an S4 usage-report feed that is not yet wired. The record and reporting loops are complete; live volume decrement awaits that feed.
- **CAMEL Advice-of-Charge to the MS:** SendChargingInformationGPRS is captured toward the SM layer, but AoC delivery to the handset is not yet built.
- **Inter-SGSN Forward Relocation:** intra-SGSN SRNS relocation signalling is complete; driving the S3 hop to a peer SGSN (connected-mode PS handover completion) is tracked under the S3 interface epic.

SIP-I Trunking

This document describes the SIP-I (SIP with encapsulated ISUP) trunking interface implemented by OmniMSC. SIP-I enables transparent transport of ISUP messages within SIP signaling, preserving full ISUP information across IP-based trunk segments.

For pure SIP trunking, see [SIP Trunking](#). For routing configuration, see [Routing Configuration](#). For configuration parameters, see [Configuration Reference](#). For general operations, see [Operations Guide](#).

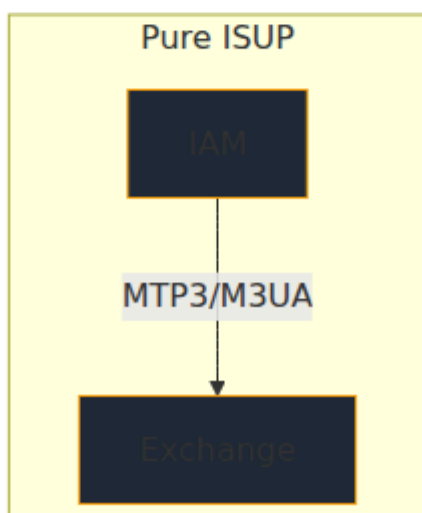
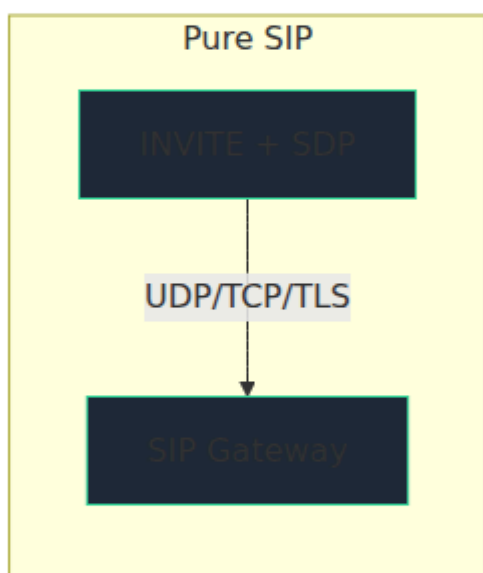
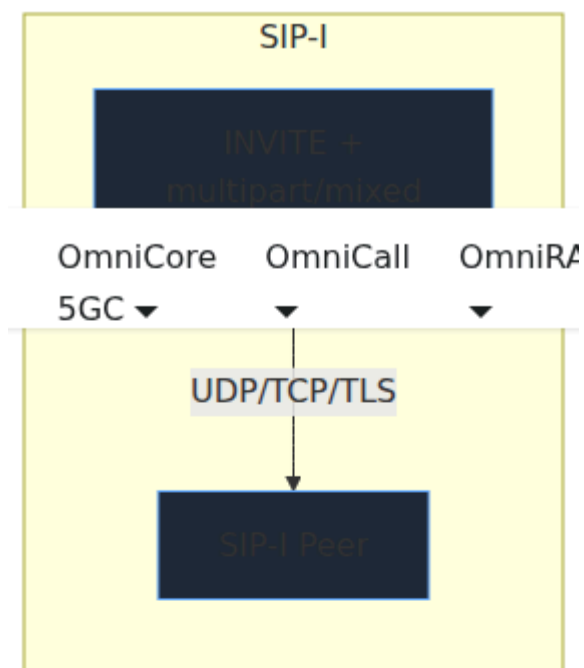
What Is SIP-I?

SIP-I (Session Initiation Protocol with encapsulated ISUP) is defined by ITU-T Q.1912.5 and uses the SIP protocol as a transport mechanism for ISUP messages. Unlike pure SIP trunking, which maps ISUP parameters to SIP headers (potentially losing information), SIP-I includes the complete ISUP message as a MIME body alongside the SDP, ensuring lossless interworking.

SIP-I is the standard trunking protocol used between MSC servers and media gateways in 3GPP IMS-based core networks and is widely deployed for PSTN interconnection.

The ISUP body is carried per RFC 3204 (MIME media type for ISUP) and RFC 3261 (SIP).

Protocol Comparison





Aspect	Pure ISUP	Pure SIP	SIP-I
Transport	MTP3/M3UA/SCTP	UDP/TCP/TLS	UDP/TCP/TLS
Signaling info	Full ISUP	Mapped to SIP headers	Full ISUP preserved
Media description	Bearer capability in IAM	SDP	SDP + ISUP bearer cap
Information loss	None	Possible (parameter mapping)	None
Codec negotiation	TMR in IAM	SDP Offer/Answer	SDP Offer/Answer
Use case	Legacy PSTN	VoIP interconnect	MSC-MSC, PSTN gateway

Multipart Body Format

SIP-I messages use a `multipart/mixed` MIME body containing two parts: the SDP offer/answer and the ISUP message encoded per RFC 3204.


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

```
--boundary42
```

```
Content-Type: application/sdp
```

```
v=0
```

```
o=0mniMSC 12345 12345 IN IP4 203.0.113.10
```

```
s=0mniMSC
```

```
c=IN IP4 203.0.113.10
```

```
t=0 0
```

```
m=audio 10042 RTP/AVP 0 8
```

```
a=rtpmap:0 PCMU/8000
```

```
a=rtpmap:8 PCMA/8000
```

```
--boundary42
```

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

```
<binary ISUP IAM>
```

```
--boundary42--
```

The `application/ISUP` content type is defined in RFC 3204. The `version` parameter identifies the ISUP variant (e.g., `itu-t92+` for ITU-T Q.767).

SIP-I Peer Configuration

SIP-I peers are configured under the `:sip_i` key, separately from pure SIP peers.

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

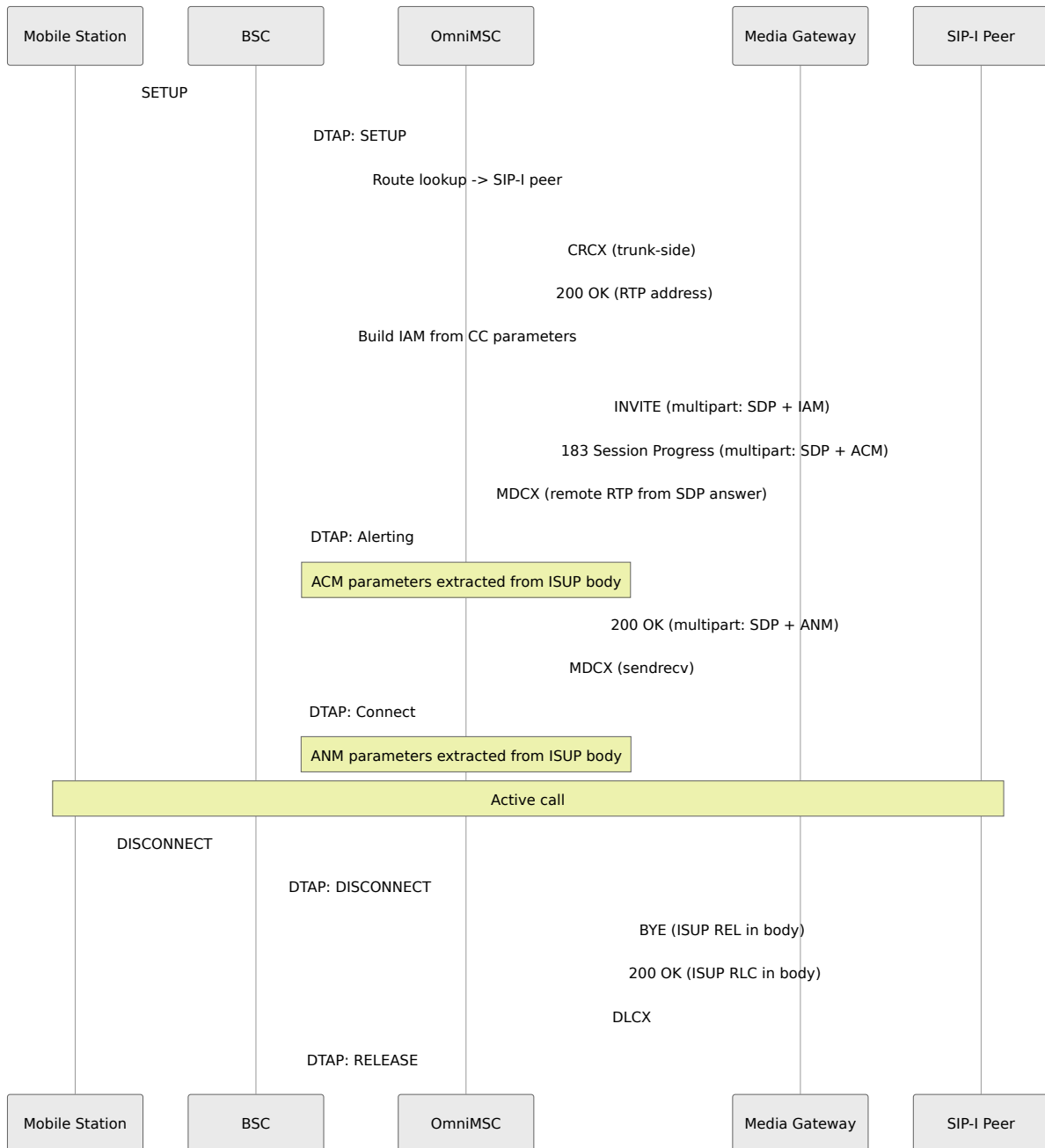
SIP-I Peer Parameters

Parameter	Type	Default	Description
<code>name</code>	<code>string</code>	-- (required)	Logical peer name. Referenced in <code>route table</code> entries with type <code>:sip_i</code> .
<code>address</code>	<code>string</code>	-- (required)	Peer IP address or hostname.
<code>port</code>	<code>integer</code>	<code>5060</code>	Peer SIP port.
<code>transport</code>	<code>atom</code>	<code>:tcp</code>	Transport protocol: <code>:udp</code> , <code>:tcp</code> , or <code>:tls</code> . TCP is recommended for SIP-I due to larger message sizes.
<code>isup_version</code>	<code>atom</code>	<code>:itu_t92</code>	ISUP encoding variant: <code>:itu_t92</code> (ITU-T Q.767) or <code>:ansi</code> (ANSI T1.113).
<code>codecs</code>	<code>list(atom)</code>	<code>[:pcmu, :pcma]</code>	Supported audio codecs for the SDP portion.
<code>max_channels</code>	<code>integer</code>	<code>100</code>	Maximum concurrent calls to this peer.
<code>trunk_group_id</code>	<code>string</code> or <code>nil</code>	<code>nil</code>	Trunk group identifier used for routing context.
<code>point_code</code>	<code>list</code> or <code>nil</code>	<code>nil</code>	Remote SS7 point code as <code>[a, b, c]</code> , used as ISUP routing context.

SIP-I peers do not have an OPTIONS keepalive configuration.

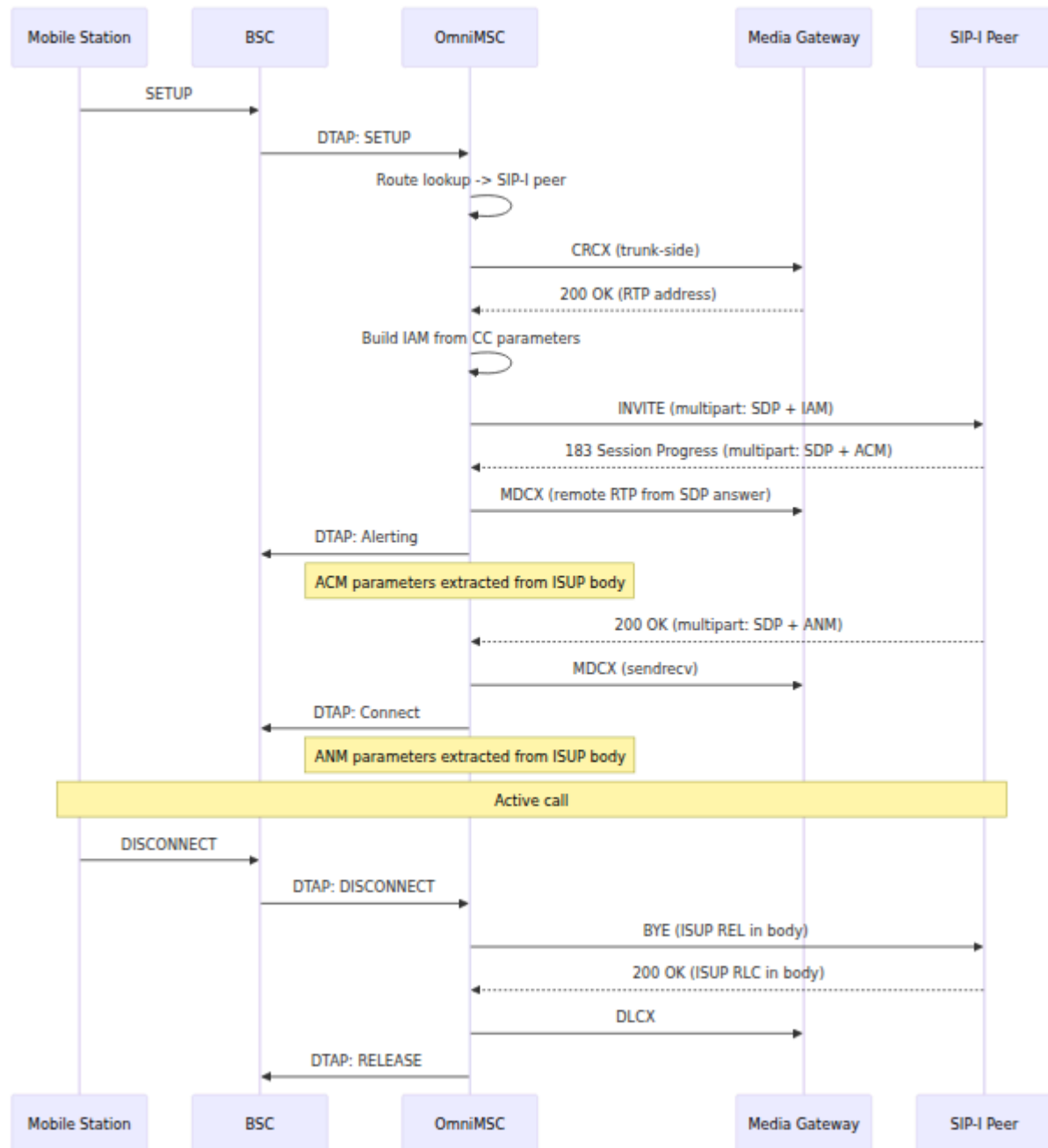
Outgoing Call (SIP-I)

When OmniMSC routes a call to a SIP-I peer, it constructs the SIP INVITE with a multipart body containing both SDP and the ISUP IAM.



Incoming Call (SIP-I)

When an INVITE arrives from a SIP-I peer with a multipart body, OmniMSC extracts the ISUP message and uses it to populate the CC FSM parameters.



ISUP-SIP Header Mapping

When interworking between the ISUP body and SIP headers, OmniMSC applies the following mapping. The ISUP body is authoritative; SIP headers are populated for the benefit of SIP-only intermediaries.

ISUP Parameter (IAM)	SIP Header	Notes
Called Party Number	Request-URI, To	E.164 format in <code>tel:</code> URI
Calling Party Number	From, P-Asserted-Identity	Presentation indicator controls <code>Privacy</code> header
Nature of Connection Indicators	Via	Satellite hop indicator
Forward Call Indicators	--	Encoded in ISUP body only
Calling Party Category	P-Asserted-Identity	Operator/priority category
Transmission Medium Requirement	SDP <code>m=</code> line	Speech, 3.1kHz audio, 64k unrestricted
User Service Information	SDP codec lines	Codec and rate mapping
Optional Forward Call Indicators	Supported	ISDN access indicator

ISUP Parameter (ACM/ANM)	SIP Response	Notes
Backward Call Indicators	183/200	Charge indicator, interworking flag
Cause Indicators (REL)	Reason header	Q.850 cause per RFC 3326
Optional Backward Call Indicators	--	Encoded in ISUP body only

Cause Code Mapping Reference

SIP-I preserves the full ISUP cause code in the ISUP body. Additionally, the SIP **Reason** header carries the Q.850 cause for intermediary nodes.

For call clearing, the ISUP REL message in the BYE body takes precedence over the SIP Reason header if both are present.

3GPP and ITU-T References

Reference	Title	Relevance
ITU-T Q.1912.5	Interworking between SIP and Bearer Independent Call Control (BICC) or ISUP	SIP-I protocol definition
RFC 3204	MIME Media Type for ISUP and QSIG Objects	application/ISUP content type
RFC 3261	SIP: Session Initiation Protocol	SIP transport
RFC 3264	Offer/Answer Model with SDP	SDP negotiation within SIP-I
RFC 3326	Reason Header Field	Cause code in SIP responses
ITU-T Q.767	Application of the ISUP	ISUP message encoding
ITU-T Q.850	Usage of Cause in ISDN	Cause code definitions
3GPP TS 29.163	Interworking between SIP-I based circuit-switched core and other networks	3GPP SIP-I profile

SIP Trunking

This document covers SIP peer configuration, OPTIONS keepalive monitoring, SDP codec negotiation, in-dialog re-INVITE handling, mid-call services (hold/resume, REFER transfer, UPDATE refresh), session timers, DTMF relay, and SIP trunk call states in OmniMSC.

For SIP-related routing, see [Routing Configuration](#). For SIP with encapsulated ISUP, see [SIP-I Trunking](#). For SIP trunk troubleshooting, see [Troubleshooting Guide](#). For call flow sequences showing SIP signaling in context, see [Call Flow Diagrams](#). For media gateway codec negotiation, see [Media Control](#). For SIP peer configuration parameters, see [Configuration Reference](#).

SIP Peer Configuration

Each SIP peer represents a remote endpoint such as a VoIP gateway, SBC, IMS node, or SIP trunking provider. Peers are defined in the `:sip` configuration block and referenced by name in the [route table](#).

Parameter	Type	Default	Description
<code>name</code>	<code>string</code>	-- (required)	Logical peer name. Referenced in route table entries.
<code>address</code>	<code>string</code>	-- (required)	Peer IP address or hostname.
<code>port</code>	<code>integer</code>	<code>5060</code>	Peer SIP port.
<code>transport</code>	<code>atom</code>	<code>:udp</code>	Transport protocol: <code>:udp</code> , <code>:tcp</code> , or <code>:tls</code> .
<code>codecs</code>	<code>list(atom)</code>	<code>[:pcmu, :pcma]</code>	Supported audio codecs for SDP negotiation.
<code>max_channels</code>	<code>integer</code>	<code>100</code>	Maximum concurrent calls to this peer.
<code>options_interval</code>	<code>integer</code> or <code>nil</code>	<code>nil</code>	Interval in seconds for SIP OPTIONS keepalive probes.

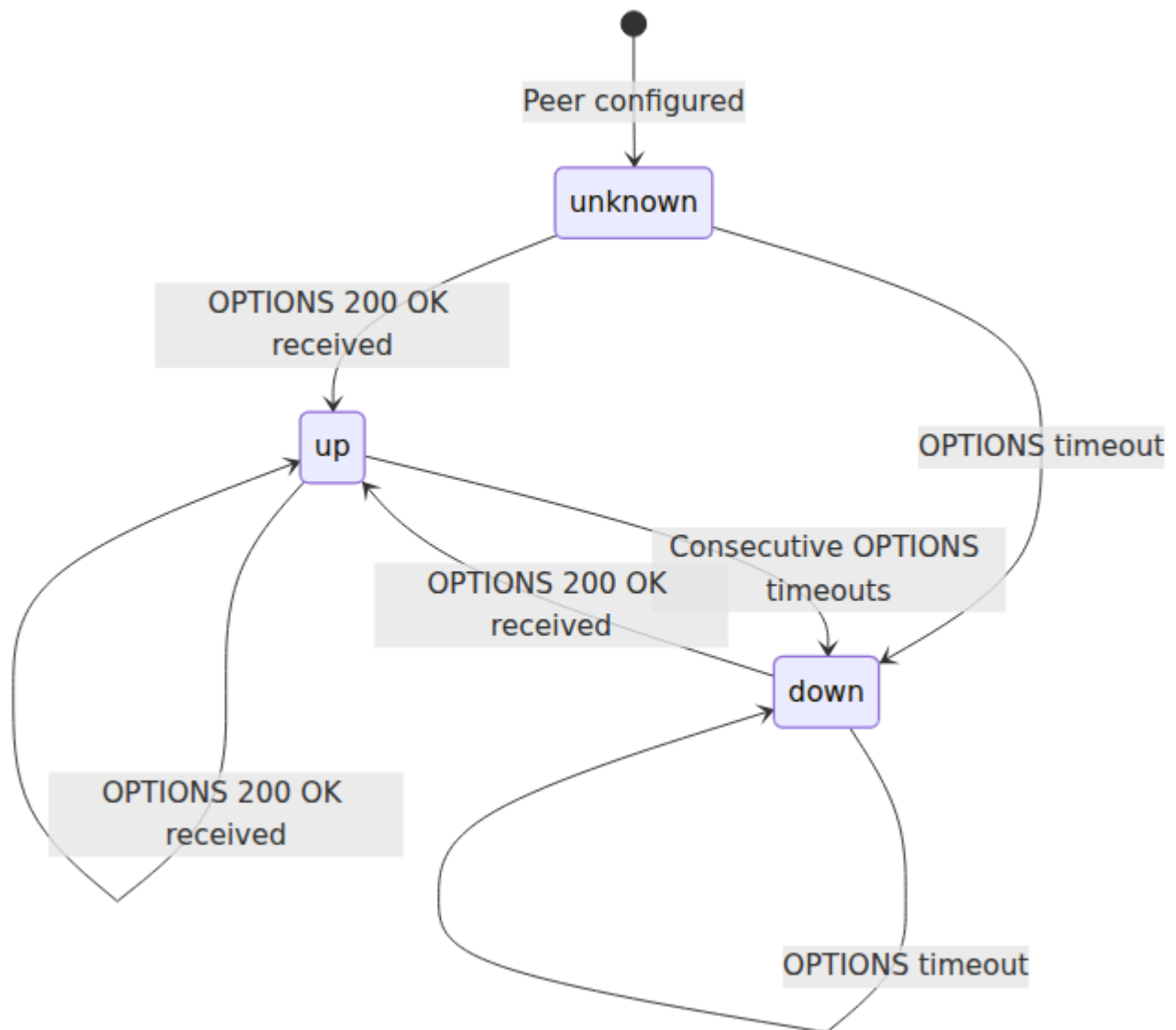
OmniMSC identifies itself with the User-Agent header `OmniMSC/0.1` in all outgoing SIP requests and responses.

SIP OPTIONS Keepalive

When `options_interval` is configured for a peer, the SIP Peer Manager sends periodic SIP OPTIONS requests to monitor peer health. The peer status determines whether the peer is eligible for call routing.

Peer Health States

Each peer tracks a status of `:up`, `:down`, or `:unknown`. On startup, all peers begin in the `:unknown` state.

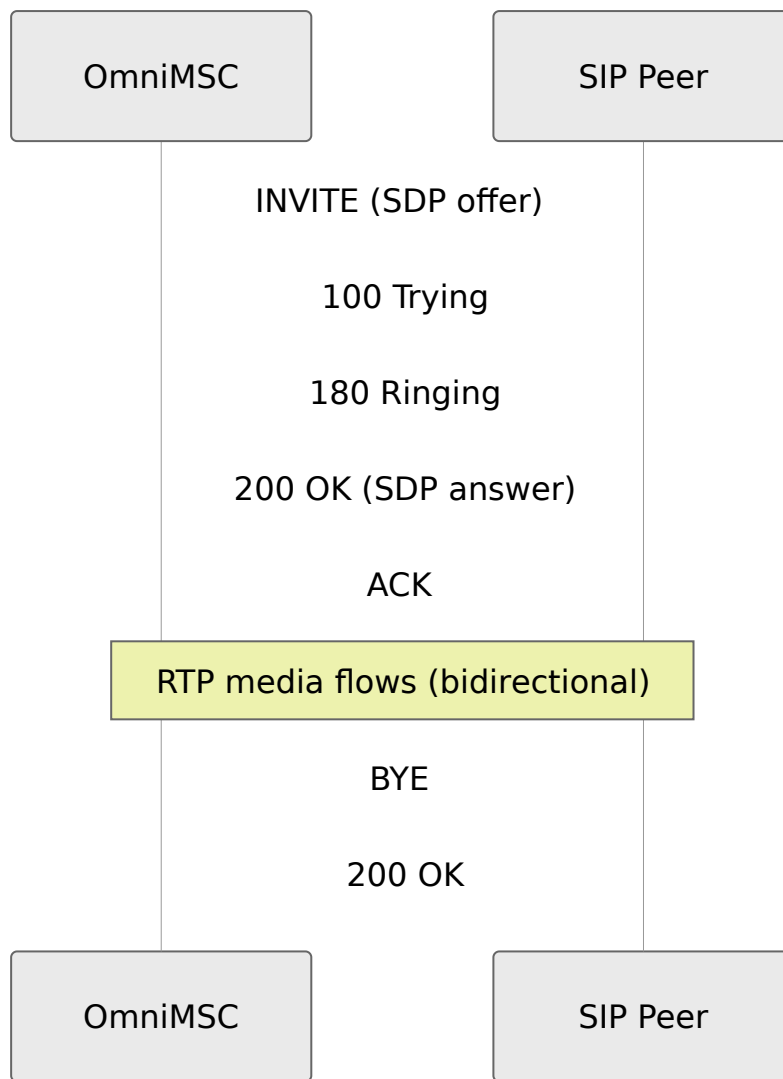


Event	Transition	Effect
OPTIONS 200 OK received	Any -> up	Peer eligible for routing
Consecutive OPTIONS timeouts	up/unknown -> down	Peer excluded from routing, alarm raised
OPTIONS 200 OK after down	down -> up	Peer re-eligible, alarm cleared
<code>max_channels</code> reached	up -> up (soft limit)	New calls rejected for this peer, existing calls unaffected

For SIP peer monitoring in the control panel, see [Control Panel Guide](#).

MO Call SIP Flow

When OmniMSC routes a mobile-originating call to a SIP peer, the following SIP signaling exchange takes place between OmniMSC and the remote peer.



The INVITE carries an SDP offer with codecs based on the peer configuration and BSC capabilities. The 200 OK contains the SDP answer with the selected codec and remote RTP address. After ACK, the RTP media path is established through the media gateway.

In-Dialog Re-INVITE Handling

A SIP peer may send a re-INVITE within an established dialog for several purposes: call hold, resume, codec change, or session refresh. OmniMSC accepts any in-dialog re-INVITE with a 200 OK using the current session SDP. If the re-INVITE carries an SDP body, the remote SDP is updated from it.

The re-INVITE is answered the same way regardless of purpose (200 OK with the current session SDP). OmniMSC does not send 488 Not Acceptable Here in

response to a re-INVITE, and does not renegotiate the codec on a re-INVITE. The existing dialog and media session remain in place. In addition, OmniMSC inspects the offered SDP for a hold/resume transition and signals it to the Call Control (CC) FSM (see Mid-Call Services below).

Mid-Call Services

OmniMSC handles three in-dialog mid-call procedures on an established SIP trunk leg: call hold/resume, REFER call transfer, and UPDATE session refresh. All three apply only in the `active` call state; requests received outside `active` are ignored or rejected as appropriate.

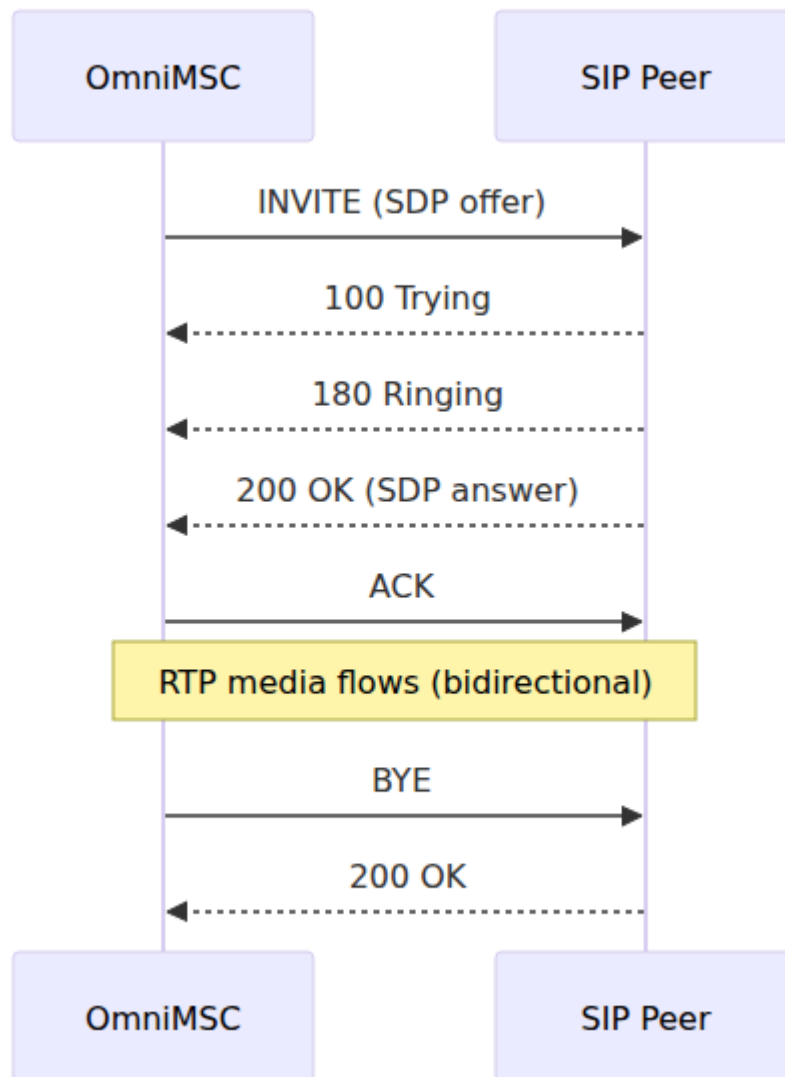
Call Hold and Resume

A remote peer places the call on hold by sending a re-INVITE (or UPDATE) whose SDP marks the media stream as inactive. OmniMSC recognises both the modern and the legacy hold encodings (RFC 3264 section 5.1, TS 29.163 Annex B):

Hold encoding	SDP marker	Notes
Direction attribute	<code>a=sendonly</code> or <code>a=inactive</code>	Preferred (RFC 3264). Media-level attribute overrides session-level
Zeroed connection	<code>c=0.0.0.0</code>	Legacy RFC 2543 hold offer
Resume	<code>a=sendrecv</code> (or no direction attribute) and a non-zero <code>c=</code>	Returns the stream to active

On a transition into hold, OmniMSC answers 200 OK and signals `hold_ind` to the CC FSM; the FSM marks the call held and propagates the condition toward

the mobile station (a NOTIFY with a remote-hold indicator) and the MNCC layer. On a transition back to active, `retrieve_ind` is signalled and the held state is cleared. Repeated offers with an unchanged direction (for example a session refresh that keeps the call held) are idempotent and do not re-signal a transition.

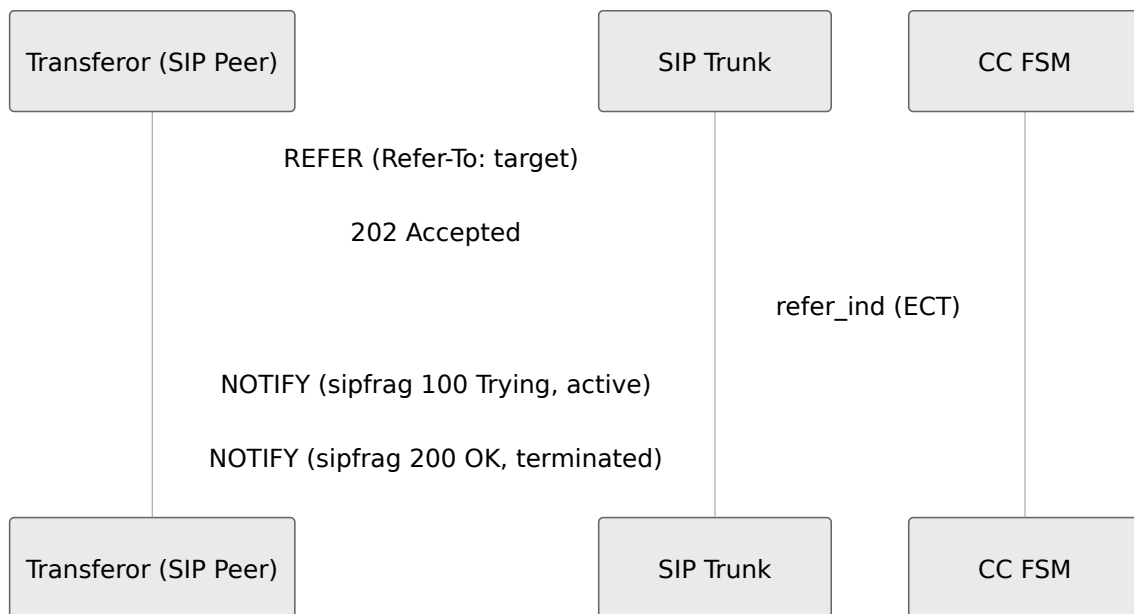


REFER Call Transfer (RFC 3515)

A peer can transfer the call by sending an in-dialog REFER whose `Refer-To` header names the transfer target. OmniMSC accepts the REFER with a 202 Accepted (establishing the implicit refer event subscription), reports the transfer to the CC FSM as an ECT (Explicit Call Transfer, TS 24.091) indication carrying the `Refer-To` URI, and reports progress back to the transferor through sipfrag NOTIFY messages (RFC 3515 section 2.4.5). A REFER without a usable `Refer-To` is rejected with 400 Bad Request.

The progress NOTIFYs carry a `message/sipfrag` body with the status line of the far-leg transaction and a `Subscription-State` header:

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



Session Timer (RFC 4028)

OmniMSC supports SIP session timers per RFC 4028 to detect and clean up orphaned SIP sessions. Session timers ensure that both endpoints periodically refresh the session, preventing stale call state after network failures.

Parameter	Value	Description
Session-Expires	1800s (default)	Maximum time between session refreshes
Min-SE	90s	Minimum acceptable Session-Expires value
Refresher	UAC or UAS	Determined during negotiation
session_refresh_method	:invite (default) or :update	Method used to send the periodic refresh

Session Timer Negotiation

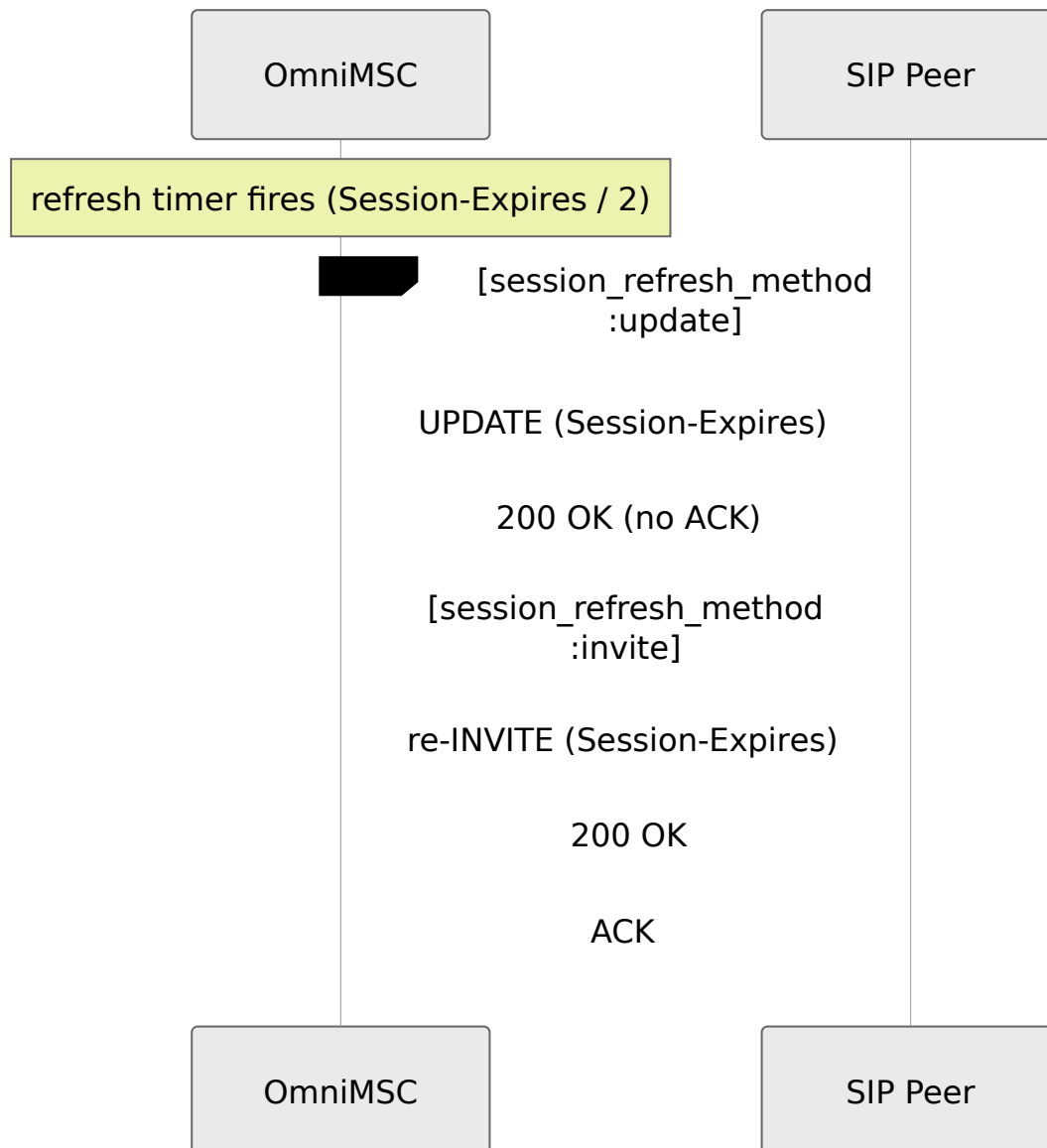
OmniMSC includes the `Session-Expires` and `Min-SE` headers in outgoing INVITE requests. When OmniMSC receives a 422 Session Interval Too Small in response to an outgoing INVITE, it acknowledges the 422, extracts the peer's Min-SE, and retries the INVITE with an updated Session-Expires that is at least the peer's minimum.

The refresh is sent at half the negotiated Session-Expires interval. If no refresh arrives before the session expires, OmniMSC sends BYE to tear down the call and releases all associated resources.

Refresh Method: re-INVITE or UPDATE (RFC 3311)

By default the refresh is sent as a re-INVITE. When a trunk is configured with `session_refresh_method: :update`, OmniMSC refreshes the session with an UPDATE (RFC 3311) instead. UPDATE is lighter-weight: it is a standalone transaction that does not disturb the offer/answer and requires no ACK. An UPDATE 200 OK is therefore never acknowledged, whereas a re-INVITE 200 OK is ACKed as usual.

OmniMSC also answers a peer-initiated UPDATE. When the UPDATE carries an SDP offer, OmniMSC echoes its current SDP as the answer; the 200 OK advertises the negotiated `Session-Expires`. An UPDATE carrying a hold offer drives the same hold/resume signalling to the CC FSM as a re-INVITE.



DTMF Relay

OmniMSC relays DTMF tones using SIP INFO messages per the `application/dtmf-relay` content type. This method is used when the peer does not support RFC 2833 telephone-event RTP payload or when out-of-band DTMF is preferred.

Field	Description	Example
Content-Type	MIME type for DTMF relay	application/dtmf-relay
Signal	DTMF digit (0-9, *, #, A-D)	Signal=5
Duration	Tone duration in milliseconds	Duration=160

When DTMF events are detected from the radio side (via the media gateway), OmniMSC generates a SIP INFO message toward the SIP peer with the corresponding signal and duration. In the reverse direction, incoming SIP INFO DTMF events are forwarded to the media gateway for playout toward the mobile station.

SDP Codec Negotiation

OmniMSC generates SDP offers based on the intersection of the peer's configured codec list and the BSC-reported speech codec capabilities. Codecs are offered in preference order.

Supported Codecs

Codec	RTP Payload Type	Clock Rate	fmtp Parameters
PCMU	0	8000	--
PCMA	8	8000	--
AMR (narrowband)	dynamic (96)	8000	octet-align=1
AMR-WB (wideband)	dynamic (97)	16000	octet-align=1

The default codec list is `[ :pcmu, :pcma]` (PCMU payload 0 and PCMA payload 8). AMR is offered with `octet-align=1` (RFC 4867) for interoperability with 3GPP access networks. The GSM full-rate speech version maps to PCMA (payload 8) on the SIP side. AMR and AMR-WB are offered when the BSC indicates support for these codecs in the speech version list during assignment.

Codec Selection

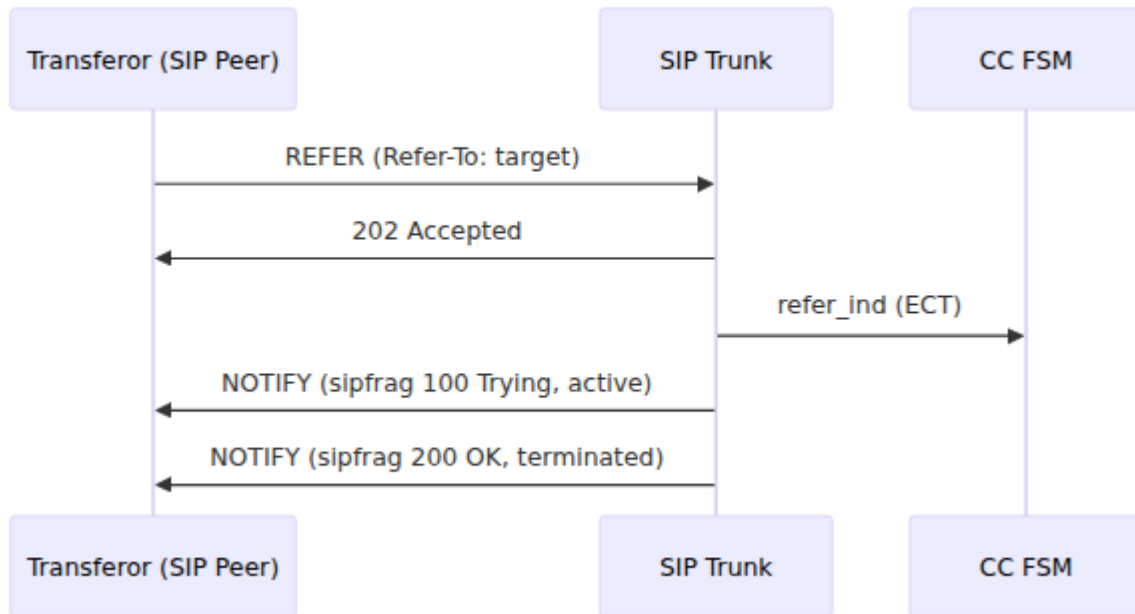
The codec selection follows the SDP Offer/Answer model (RFC 3264):

1. OmniMSC builds the SDP offer from the peer codec list, filtered by BSC speech capabilities.
2. The remote peer responds with an SDP answer containing one or more accepted codecs.
3. OmniMSC selects the first common codec from the original offer order.
4. The media gateway is instructed (via MDCX) with the selected codec and RTP parameters.

If no common codec exists, OmniMSC responds with or receives 488 Not Acceptable Here.

SIP Trunk Call States

Outgoing Call States



Incoming Call States



idle

INVITE received

invite_received

Send 180 Ringing

ringing

Send 200 OK

answered

Reject (4xx/5xx)

ACK received

CANCEL received

active

BYE received Send BYE

terminated



References

Reference	Title	Relevance
RFC 3261	SIP: Session Initiation Protocol	Core SIP signaling
RFC 4028	Session Timers in SIP	Session-Expires, Min-SE, refresh mechanism
RFC 3311	The SIP UPDATE Method	UPDATE-based session refresh
RFC 3515	The SIP Refer Method	REFER call transfer, sipfrag NOTIFY progress
RFC 2833	RTP Payload for DTMF Digits	Telephone-event RTP payload type
RFC 3264	Offer/Answer Model with SDP	SDP codec negotiation, hold/resume markers
RFC 4867	RTP Payload Format for AMR and AMR-WB	AMR octet-align parameter
RFC 3326	Reason Header Field	Cause code in BYE/CANCEL
TS 29.163	Interworking between IMS and CS networks	Annex B: hold/resume interworking

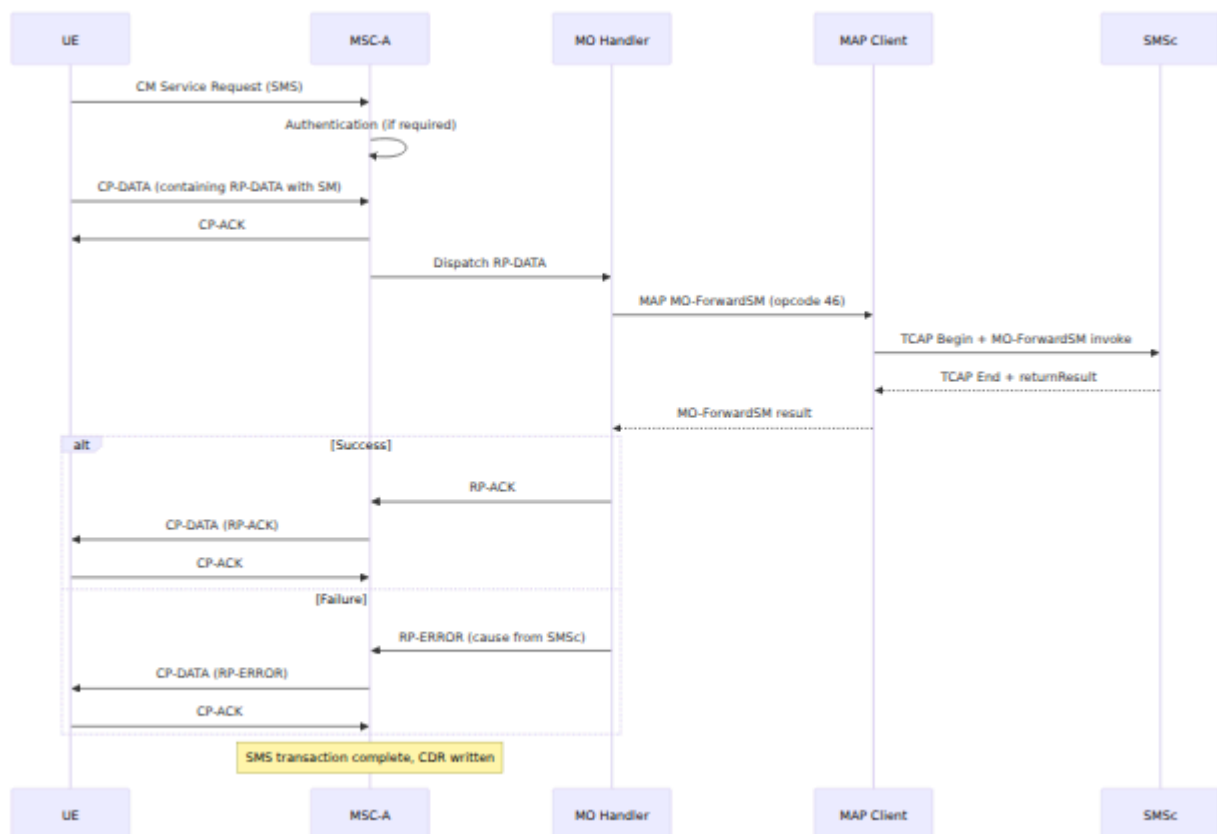
SMS

This document describes the Short Message Service implementation in OmniMSC, covering mobile-originating and mobile-terminating SMS flows, DTAP transaction identifier allocation, A-interface SAPI handling, MAP response routing, and the SMS codec layers.

For call flow diagrams that include SMS alongside voice, see [Call Flow Diagrams](#). For MAP interface details covering MO-ForwardSM and MT-ForwardSM operations, see [MAP Operations](#). For SMSc address and point code configuration, see [Configuration Reference](#). For common SMS delivery issues, see [Troubleshooting — SMS Issues](#).

MO-SMS (Mobile Originating SMS)

A subscriber sends a short message via the MSC to the SMS Centre (SMSc). The MSC acts as a relay, receiving the SM from the air interface and forwarding it to the SMSc using MAP MO-ForwardSM.



The MO Handler extracts the SM-RP-DA (destination address, typically the SMSc address) and SM-RP-OA (originating address, the subscriber MSISDN) from the RP-DATA, then constructs the MAP MO-ForwardSM request. The MAP response determines whether the MSC sends RP-ACK or RP-ERROR back to the UE.

MT-SMS (Mobile Terminating SMS)

The SMSc delivers a short message to a subscriber via the MSC. The SMSc sends a MAP MT-ForwardSM (opcode 44) to the MSC, which pages the subscriber if necessary and delivers the SM over the air interface.

For MT-SMS, the network allocates the Transaction Identifier (TI). Per 3GPP TS 24.007, the TI flag distinguishes the originator:

Direction	TI Flag	Meaning
Network → UE (CP-DATA)	0	Network originated this transaction
UE → Network (CP-ACK, RP-ACK)	1	UE responding to network-originated transaction

The MSC sets TI flag=0 in the CP-DATA sent to the UE. The UE mirrors the TI value but sets flag=1 in all responses (CP-ACK, CP-DATA containing RP-ACK). This convention allows both sides to distinguish between multiple concurrent SMS transactions.

SAPI 3

SMS NAS PDUs (CP-DATA, CP-ACK, CP-ERROR) are carried on SAPI 3 of the A-interface per 3GPP TS 48.006. The DLCI (Data Link Connection Identifier) byte in the BSSAP DTAP header is set to 0x03, indicating SAPI=3.

SAPI 3 provides a separate logical channel from the main signaling channel (SAPI 0), which carries CC and MM messages. This separation allows SMS delivery to occur concurrently with an active voice call without interfering with call control signaling.

MAP Response Routing

When an MT-ForwardSM arrives from the SMSc, the MSC must route the TCAP End response back to the correct originating point code. The ingress module captures the OPC (Originating Point Code) from the incoming M3UA transfer message and stores it as `routing_info[:opc]`.

When constructing the TCAP End response, the MSC uses this stored OPC as the DPC (Destination Point Code) for the outgoing M3UA message. This ensures the response reaches the correct SMSc, which is important in networks where

multiple SMS Sc instances use different point codes, or where an STP routes based on point code rather than SCCP global title.

The OPC/DPC swap follows the standard M3UA convention: the response OPC is the MSC's own point code (the incoming DPC), and the response DPC is the SMS Sc's point code (the incoming OPC).

SMS Codec

The SMS codec handles two protocol layers per 3GPP TS 24.011:

CP Layer (Connection Management Sublayer)

Message	Direction	Description
CP-DATA	Both	Carries an RP message as payload
CP-ACK	Both	Acknowledges receipt of CP-DATA
CP-ERROR	Both	Reports a CP-layer error (cause value included)

CP-DATA contains a single RP-layer PDU. Each CP-DATA must be acknowledged with a CP-ACK before the next CP-DATA can be sent on the same transaction.

RP Layer (Relay Protocol)

Message	Direction	Description
RP-DATA	Both	Carries the SM-TP-DU (the actual short message) along with RP-DA and RP-OA addresses
RP-ACK	Both	Confirms successful RP-DATA delivery
RP-ERROR	Both	Reports an RP-layer error (cause value from TS 24.011 table 8.4)

For MO-SMS, the RP-DATA from the UE contains the SM-RP-DA (SMSc address) and SM-RP-OA (subscriber address). For MT-SMS, the MSC constructs RP-DATA with SM-RP-DA (subscriber IMSI) and SM-RP-OA (SMSc address).

References

Specification	Title	Relevance
TS 24.011	Point-to-Point Short Message Service support on mobile radio interface	CP and RP protocol layers, message formats, cause codes
TS 29.002 Section 12	MAP Specification - Short Message Service procedures	MAP MO-ForwardSM (opcode 46), MT-ForwardSM (opcode 44), routing info for SM
TS 23.040	Technical realization of SMS	SM-TP layer encoding, validity period, status reports
TS 48.006	Signalling transport mechanism specification for the BSC-MSC interface	DLCI/SAPI assignment for A-interface DTAP
TS 24.007	Mobile radio interface signalling layer 3 - General aspects	Transaction Identifier allocation and TI flag conventions

Supplementary Services

This document describes the supplementary services implemented in OmniMSC, covering the SS dispatch mechanism, call forwarding, call barring, call waiting, line identification, call hold, multi-party conferencing, and HLR interaction. For call flow sequences, see [Call Flow Diagrams](#). For configuration parameters, see [Configuration Reference](#). For advanced call features such as ECT and CCBS, see [Advanced Call Features](#). For the MAP operations used to relay SS changes to the HLR (RegisterSS, ActivateSS), see [MAP Operations](#). For MPTY conference bridge details at the media layer, see [Media Control](#).

SS Dispatch Overview

A mobile station interacts with supplementary services by sending DTAP messages from the SS message group: SS REGISTER, SS FACILITY, and SS RELEASE COMPLETE, as defined in 3GPP TS 24.010. Each message carries a facility information element containing ASN.1-encoded component(s) with an operation code and SS code that identify the target service. The provisioned supplementary services for each subscriber, along with their status badges, are visible in the Subscribers page of the control panel — see [Control Panel Guide](#).

When OmniMSC receives one of these messages, the CC/SS dispatcher extracts the SS code from the facility IE and routes the request to the appropriate service handler. The SS code is a single-byte value defined in 3GPP TS 29.002 that uniquely identifies the supplementary service being invoked.

SS Operations

Every supplementary service supports a subset of the five standard operations:

Operation	Description
Register	Provision the service with parameters (e.g., forwarded-to number, no-reply timer)
Erase	Remove a previously registered service
Activate	Enable a registered service so that it takes effect
Deactivate	Disable an active service without removing the registration
Interrogate	Query the current status and parameters of a service

The MS encodes these operations using invoke components within the facility IE. OmniMSC processes the request, determines whether HLR involvement is required, and returns a return result or return error component in the response.

Call Forwarding

OmniMSC implements the four 3GPP call forwarding variants defined in TS 24.082. Each variant can be provisioned per subscriber via MAP INSERT SUBSCRIBER DATA from the HLR, or managed by the subscriber using SS Register, Activate, Deactivate, Erase, and Interrogate operations.

Variant	SS Code	Trigger	3GPP Reference
Call Forwarding Unconditional (CFU)	0x21	All incoming calls	TS 24.082 Sec 4.1
Call Forwarding on Busy (CFB)	0x29	Called subscriber busy	TS 24.082 Sec 4.2
Call Forwarding on No Reply (CFNRy)	0x2A	No answer within timer	TS 24.082 Sec 4.3
Call Forwarding on Not Reachable (CFNRc)	0x2B	Subscriber not reachable	TS 24.082 Sec 4.4

CFU (Call Forwarding Unconditional)

All calls to the subscriber are unconditionally forwarded to the configured forwarded-to number. When CFU is active, the MSC does not page the subscriber. CFU takes priority over all other forwarding variants.

CFB (Call Forwarding on Busy)

Calls are forwarded when the subscriber is busy (all traffic channels occupied or user-determined user busy). The MSC detects the busy condition from either the radio interface (UDUB) or the CC FSM state.

CFNRy (Call Forwarding on No Reply)

Calls are forwarded when the subscriber does not answer within a configurable timer (default 20 seconds, range 5-30 seconds per 3GPP TS 24.082). The no-reply timer starts when the paging response or alerting indication is received.

CFNRc (Call Forwarding on Not Reachable)

Calls are forwarded when the subscriber cannot be reached: IMSI detached, no paging response, or radio link failure. The MSC determines reachability from the VLR subscriber state and paging outcome.

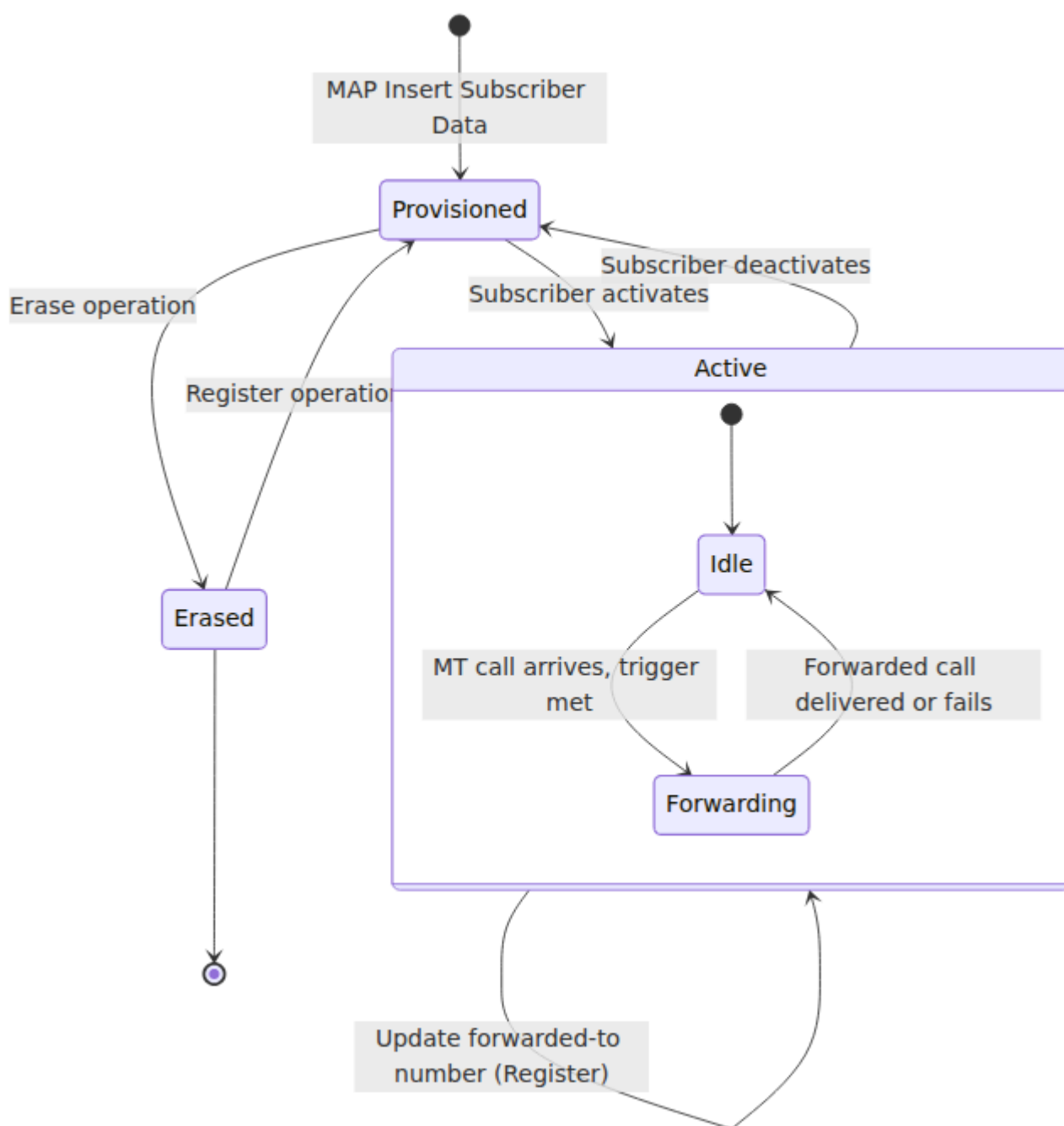
Call Forwarding Operations

A subscriber manages call forwarding through the standard SS operations:

Operation	Effect
Register	Store forwarded-to number and optional no-reply timer; implicitly activates the service
Erase	Remove forwarded-to number and deactivate the service
Activate	Enable a previously registered forwarding variant
Deactivate	Disable forwarding without removing the registered number
Interrogate	Return current status (active/inactive) and forwarded-to number

Registration and erasure operations are relayed to the HLR via MAP, since the forwarding data is part of the subscriber profile. Activation, deactivation, and interrogation can be handled locally from VLR data when the information is already available, or relayed to the HLR otherwise.

Call Forwarding State Diagram



Call Barring

OmniMSC implements call barring services per 3GPP TS 24.088. Barring categories are provisioned by the HLR via MAP INSERT SUBSCRIBER DATA and are enforced by the MSC during call setup. The subscriber cannot override operator-provisioned barring.

Call barring uses the canonical MAP SS-Code space defined in 3GPP TS 29.002. Individual barring categories and their enclosing group codes are:

Category	SS Code	Direction	Effect
Barring of All Outgoing Calls (BAOC)	0x92	MO	Block all outgoing calls
Barring of Outgoing International Calls (BOIC)	0x93	MO	Block international outgoing calls
Barring of Outgoing International Calls except to Home Country (BOIC-exHC)	0x94	MO	Block international outgoing calls except to home PLMN country
Barring of All Incoming Calls (BAIC)	0x9A	MT	Block all incoming calls
Barring of Incoming Calls when Roaming (BicRoam)	0x9B	MT	Block incoming calls when subscriber is roaming outside HPLMN

Group SS-Codes address multiple categories at once:

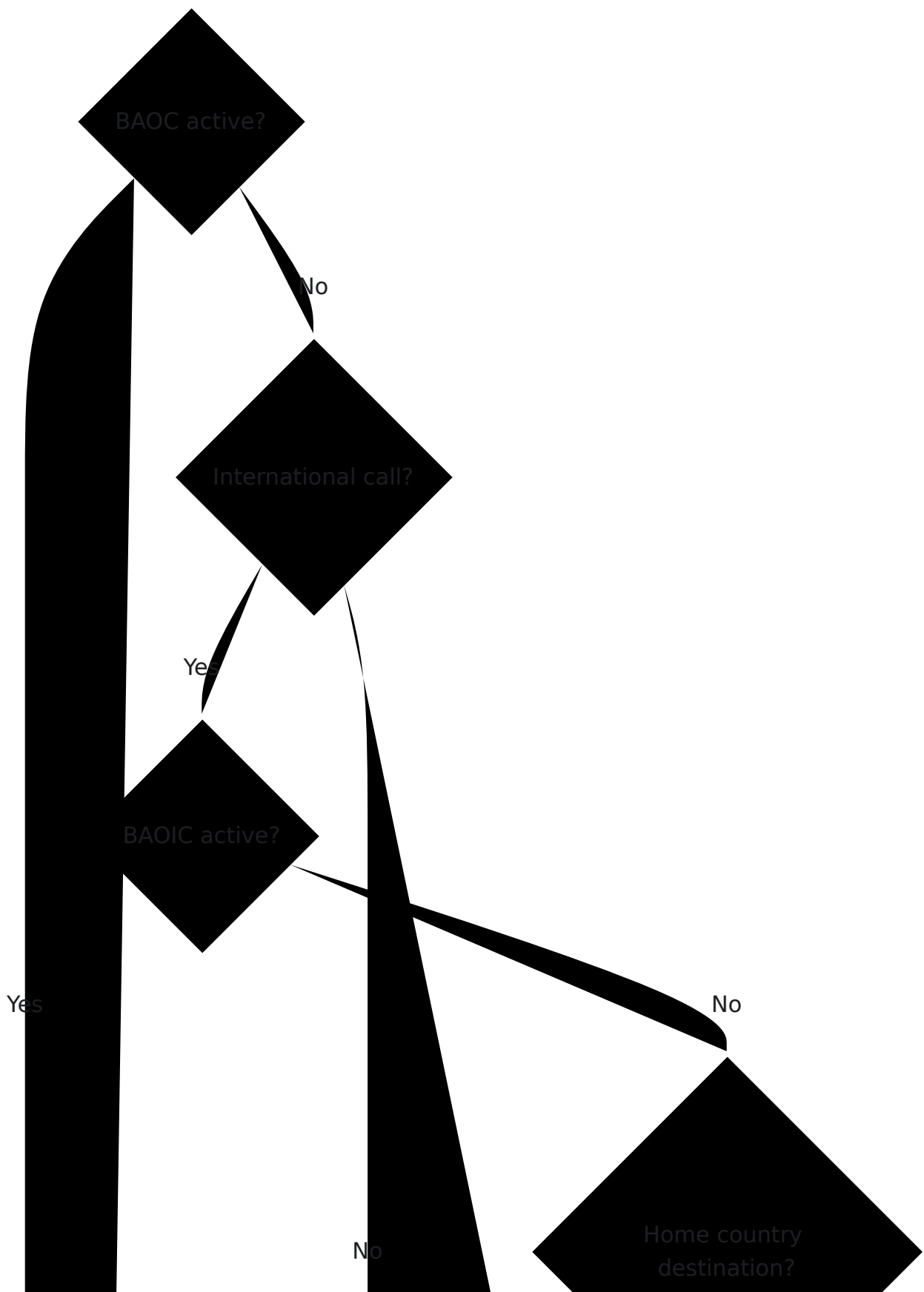
Group	SS Code	Covers
All Barring Services	0x90	All outgoing and incoming barring
Barring of Outgoing Calls	0x91	BAOC, BOIC, BOIC-exHC
Barring of Incoming Calls	0x99	BAIC, BicRoam

Barring Provisioning

Call barring data arrives from the HLR as part of the subscriber profile in the MAP INSERT SUBSCRIBER DATA operation during Location Update. The VLR stores the active barring categories and the MSC evaluates them at call setup time. Since barring is operator-controlled, activation and deactivation by the subscriber require HLR authorization via a barring password.

Barring Evaluation -- Outgoing Calls

MO Call Setup





Barring Evaluation -- Incoming Calls

MO Call Setup

BAOC active?

No

OmniCore
5GC ▼

OmniCall ▼

OmniRAN ▼

OmniCharge ▼

Platform ▼

English ▼

International call?

Yes

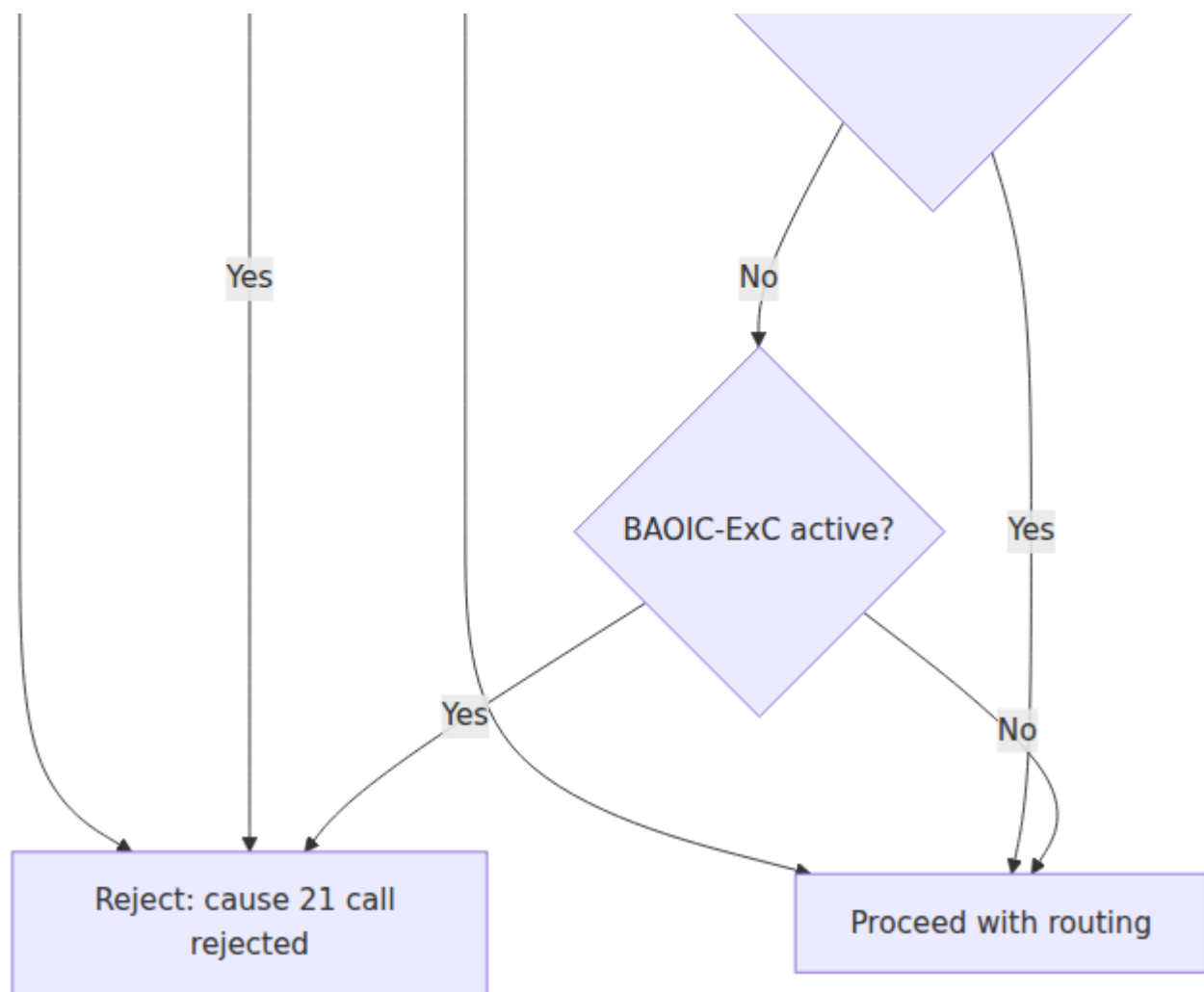
BAOIC active?

Yes

No

No

Home country
destination?



Subscriber call-barring supplementary services (BAOC/BOIC/BAIC) release the call with GSM cause 21 (call rejected). This is distinct from operator determined barring (ODB, TS 23.015), which is evaluated first and releases with GSM cause 8 (operator determined barring).

Operator Determined Barring and Closed User Group at MO Setup

Beyond the subscriber-controlled call barring services above, OmniMSC enforces two operator-controlled restrictions during the VLR mobile-originated call procedure (TS 23.018 Sec 7.1.2): Operator Determined Barring (ODB, TS 23.015) and Closed User Group (CUG, TS 24.085). Both are provisioned by the HLR via MAP INSERT SUBSCRIBER DATA, stored on the VLR subscriber, and checked by the MSC at MS SETUP before the call is offered to the network. A barred call is released toward the MS with RELEASE COMPLETE carrying the

appropriate GSM 04.08 cause and no charging record is raised for a connected call.

The three outgoing checks are applied in a fixed order and the first that bars releases the call:

1. Operator Determined Barring (ODB)
2. Closed User Group (CUG)
3. Subscriber call-barring supplementary services (BAOC/BOIC/BOIC-exHC)

Operator Determined Barring Categories

ODB categories are stored on the subscriber as `odb_categories`. The following mobile-originated categories are enforced from number analysis, all releasing with GSM cause 8 (operator determined barring):

Category	Effect	Release Cause
<code>barring_all_outgoing</code>	Bar every MO call	8 (operator determined barring)
<code>barring_outgoing_international</code>	Bar MO calls to international numbers	8 (operator determined barring)
<code>barring_outgoing_international_except_home</code>	Bar international MO calls except to the HPLMN country	8 (operator determined barring)
<code>barring_premium_rate_information</code>	Bar MO calls to a configured premium-rate information prefix	8 (operator determined barring)
<code>barring_premium_rate_entertainment</code>	Bar MO calls to a configured premium-rate entertainment prefix	8 (operator determined barring)

Premium-rate prefixes are network-specific and have no default. Configure them under the `:odb` key:

```
config :omnimsc, :odb,  
  premium_rate_information_prefixes: ["1900"],  
  premium_rate_entertainment_prefixes: ["1901"]
```

The `barring_outgoing_international_except_home` category compares the dialled E.164 country code against the HPLMN country code supplied to the CC layer as `home_country_code`. With no configured home country code the except-home check fails open (does not bar).

Closed User Group

CUG restricts which destinations a member may call. The subscriber's CUG subscription is stored as `cug_info`:

Field	Description
<code>groups</code>	List of CUG indexes (interlock codes) the subscriber is a member of
<code>outgoing_access</code>	Whether the subscriber may originate calls outside any CUG (default <code>false</code>)
<code>preferential_cug</code>	CUG index used when the MS signals no explicit index (optional)

On an MS SETUP the MS may include a CUG index in the CUG facility (`cug_index`). The VLR evaluates membership and access rights:

Condition	Outcome	Release Cause
No CUG subscription, plain call (no index)	Allowed	--
No CUG subscription, MS selects an index	Barred	87 (user not member of CUG)
MS selects an index the subscriber is a member of	Allowed	--
MS selects an index the subscriber is not a member of	Barred	87 (user not member of CUG)
Plain call, subscriber has outgoing access	Allowed	--
Plain call, subscriber has no outgoing access	Barred	55 (incoming calls barred within the CUG)

MO Setup Check Flow

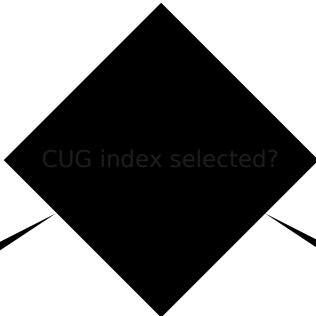
MS SETUP received at
VLR/MSC



Yes

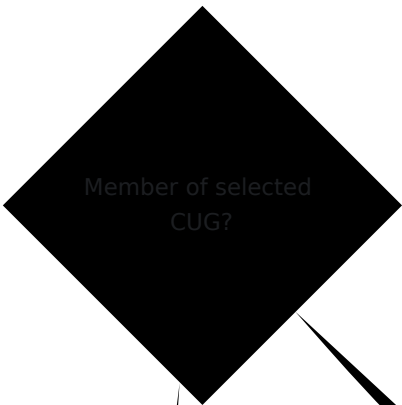
No

Release: cause 8
operator determined
barring



Yes

No



No

Yes

Release: cause 87 user
not member of CUG

Continue to call-barring
SS checks

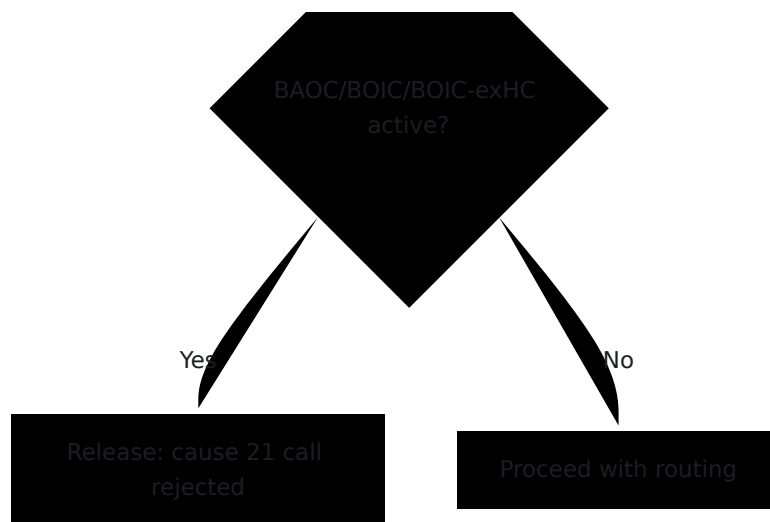


Yes

No

Release: cause 55
incoming calls barred
within CUG



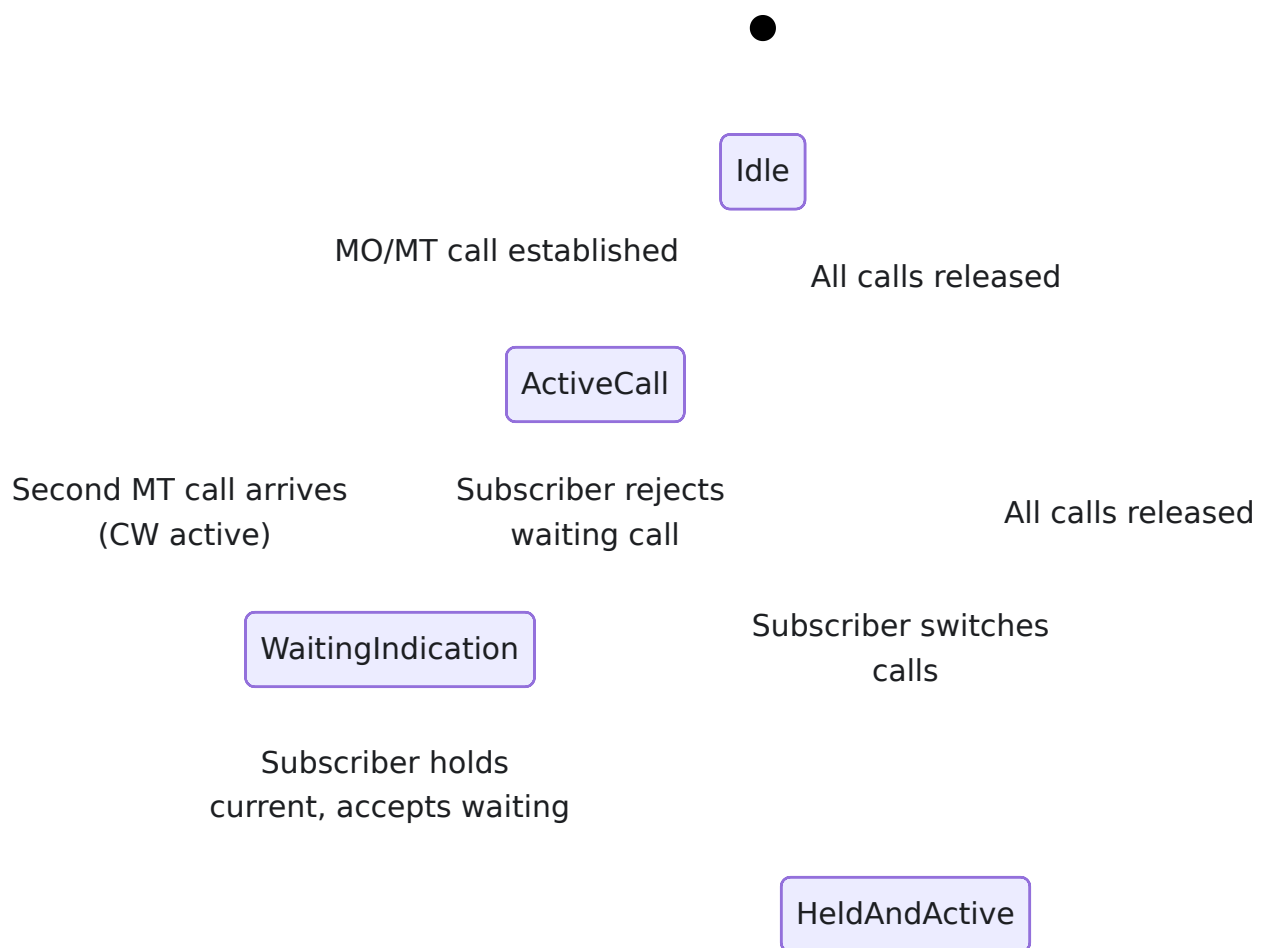


Call Waiting

OmniMSC implements Call Waiting (CW) per 3GPP TS 24.083. Call Waiting has SS code 0x41. The subscriber can activate or deactivate Call Waiting using the standard SS Activate and Deactivate operations.

When a subscriber with CW active is engaged in a call and receives a second incoming call, the MSC includes a Signal information element in the SETUP message sent to the mobile station. The Signal IE instructs the MS to play a call-waiting tone, alerting the subscriber to the incoming call. Without CW active, the MSC returns a busy indication to the second calling party, which may trigger CFB if configured.

The subscriber may then accept the waiting call by placing the current call on hold (HOLD message) and answering the new call, or reject the waiting call, which proceeds to normal busy handling.



Line Identification

OmniMSC implements Calling Line Identification Presentation (CLIP) and Calling Line Identification Restriction (CLIR) per 3GPP TS 24.081 and TS 24.083.

CLIP (Calling Line Identification Presentation) - - SS Code 0x11

CLIP provides the called party with the calling party number. The MSC includes the calling number in the SETUP message sent to the mobile station on the MT leg, and in the IAM or SIP INVITE on the outgoing trunk for MO calls. CLIP is a network-provisioned service: when CLIP is provisioned for the called subscriber, the network presents the calling number subject to CLIR restrictions of the calling party.

CLIR (Calling Line Identification Restriction) -- SS Code 0x12

CLIR allows the calling party to restrict presentation of their number to the called party. The HLR provisions the default CLIR mode, and the subscriber can invoke per-call overrides where permitted.

Mode	Behavior
Permanent	Number is always restricted; per-call override not available
Temporary (default restricted)	Number restricted unless subscriber invokes per-call presentation
Temporary (default allowed)	Number presented unless subscriber invokes per-call restriction

The MSC evaluates the CLIR setting of the calling subscriber when populating the Calling Party Number in outgoing signaling. A network operator override can force presentation regardless of CLIR setting, for scenarios such as lawful intercept and emergency callback.

Call Hold

OmniMSC handles Call Hold per 3GPP TS 24.083. The mobile station places an active call on hold by sending a HOLD message and retrieves it by sending a RETRIEVE message. Both are CC messages handled directly by the CC FSM within the MSC.

When the MSC receives a HOLD message, the CC FSM transitions the call leg to the held state, instructs the media gateway to set the held leg to receive-only, and sends a HOLD ACKNOWLEDGE back to the MS. On RETRIEVE, the CC FSM reverses the process: the media gateway leg returns to send-receive mode, and the MSC responds with RETRIEVE ACKNOWLEDGE.

Call Hold is a prerequisite for several other supplementary services including Call Waiting (accepting a second call), Multi-Party conference (bridging held and active calls), and Explicit Call Transfer (connecting held and active remote parties).

Multi-Party (MPTY) Conference

OmniMSC implements Multi-Party calling per 3GPP TS 24.084. MPTY allows a subscriber to bridge multiple calls into a conference. The conference bridge is hosted on the media gateway, with the MSC controlling participation through CC FACILITY invoke and return result exchanges.

MPTY Operations

Operation	SS Code	Description
BuildMPTY	0x51	Create or extend the conference by merging the held and active calls
HoldMPTY	0x52	Place the entire conference on hold
RetrieveMPTY	0x53	Retrieve a held conference
SplitMPTY	0x54	Extract one party from the conference into a private call

BuildMPTY Flow

The subscriber first establishes two calls (one active, one held) using normal call setup and the HOLD procedure, then sends a BuildMPTY invoke in a CC FACILITY message. OmniMSC creates a conference context on the media gateway, redirects all call legs into the conference bridge, and returns a BuildMPTY return result to the MS. Subsequent calls can be added to the

conference by repeating the hold-and-dial pattern followed by another BuildMPTY invoke.

HoldMPTY and RetrieveMPTY

HoldMPTY places all conference legs into receive-only mode on the media gateway, allowing the subscriber to make a private call outside the conference. RetrieveMPTY reverses this, restoring all legs to send-receive mode and reconnecting the subscriber to the conference.

SplitMPTY

SplitMPTY extracts a single party from the conference into a private two-party call with the subscriber. The remaining conference participants are placed on hold. The MS identifies the party to be split by call reference in the SplitMPTY invoke.

Conference Bridge on MGW

The media gateway maintains the conference context with one termination per participant. OmniMSC uses CRCX to create terminations and MDCX to add or remove them from the conference context. The gateway performs audio mixing for all participants in the context.

HLR Relay

Several SS operations require interaction with the HLR, since the subscriber profile is the authoritative source for supplementary service state. When the MSC receives an SS operation that modifies persistent state (Register, Erase, Activate, Deactivate for forwarding, barring password verification), the request is relayed to the HLR via the appropriate MAP operation. The HLR processes the request, updates the subscriber profile, and returns the result, which the MSC forwards to the mobile station.

Operations relayed via MAP include:

- RegisterSS / EraseSS for call forwarding numbers
 - ActivateSS / DeactivateSS for service state changes that must persist beyond the current VLR registration
 - RegisterPassword for call barring password management
 - InterrogateSS when the VLR does not hold the requested data
-

Local Interrogation

When the VLR already holds current supplementary service data (received during Location Update via INSERT SUBSCRIBER DATA), interrogation requests can be answered locally without contacting the HLR. This reduces signaling load and response time. The MSC queries the VLR subscriber record for the requested SS code and returns the current status directly to the mobile station.

Local interrogation is used for status queries where the VLR data is known to be fresh, such as immediately after a Location Update or after a successful Register/Activate/Deactivate operation that updated the local VLR copy.

3GPP Specification References

Specification	Title	Relevance
TS 24.010	Mobile Radio Interface Layer 3 -- Supplementary Services	SS message structure, facility IE, component types
TS 24.080	Mobile Radio Interface Layer 3 SS Specification -- Formats and Coding	ASN.1 encoding of SS operations and components
TS 24.081	Line Identification Supplementary Services	CLIP, CLIR
TS 24.082	Call Forwarding Supplementary Services	CFU, CFB, CFNRy, CFNRc
TS 24.083	Call Waiting and Call Hold Supplementary Services	CW, HOLD, RETRIEVE
TS 24.084	Multi-Party Supplementary Services	BuildMPTY, HoldMPTY, RetrieveMPTY, SplitMPTY
TS 24.085	Closed User Group Supplementary Services	CUG membership and access rights at MO setup
TS 24.088	Call Barring Supplementary Services	BAOC, BAOIC, BAOIC-ExC, BAIC, BAIC-Roam
TS 23.015	Technical Realization of Operator Determined Barring	ODB categories enforced at call setup

Specification	Title	Relevance
TS 23.018	Basic Call Handling	VLR MO-call procedure (Sec 7.1.2), ODB/CUG enforcement point
TS 29.002	MAP Specification	SS code assignments, MAP operations for SS provisioning

Troubleshooting Guide

This document covers common operational issues encountered with OmniMSC deployments and their resolution steps. For configuration reference, see [Configuration Reference](#). For system metrics and alerting, see [Metrics Reference](#). For real-time status and subscriber inspection, see [Control Panel Guide](#).

SS7 Connectivity

STP Link Down

Symptoms: No new calls are established, location updates do not complete, the `sctp_link_down` alarm is raised, and `omnimsc_peer_status` shows 0 for the affected STP peer.

Investigation: Verify that the SCTP association to the STP is established. Check that the remote IP address and port match the STP configuration. Confirm that SCTP protocol 132 is permitted through any firewalls between the MSC and STP. Verify the STP routing context matches the value configured in OmniMSC. Check that the M3UA ASP state machine has progressed through ASPUP and ASPAC to the ACTIVE state. If the association establishes but M3UA does not reach ACTIVE, check the M3UA logs for ERR chunks indicating a routing context or traffic mode mismatch.

Resolution: Correct the SCTP endpoint configuration (IP, port), firewall rules, or M3UA routing context as indicated by the investigation. Once the SCTP association re-establishes and M3UA reaches ACTIVE, the alarm clears automatically and signaling resumes.

MAP Dialogue Timeout

Symptoms: Location updates hang without completing, SMS delivery fails, the `hlr_unreachable` alarm may be raised. MAP operations time out without

receiving a TC-CONTINUE or TC-END from the HLR.

Investigation: Confirm that the HLR is reachable at the network level. Verify that point codes are correctly configured on both ends. Check that Global Title translation is correctly configured if GT-based SCCP routing is in use. Verify that M3UA has an active route to the HLR point code. Inspect logs for TC-BEGIN messages being sent without corresponding TC-CONTINUE responses.

Resolution: Correct point code or Global Title configuration as needed. If the HLR is reachable but not responding, the issue is on the HLR side. Verify that the HLR has a return route to the MSC point code.

Wrong DPC for MAP Responses

Symptoms: The SMSc never receives the MT-SMS acknowledgement. MAP ForwardSM responses are sent but do not arrive at the originating SMSc. The MT-SMS delivery appears to complete from the MSC perspective but the SMSc retransmits the request.

Investigation: Check the Destination Point Code (DPC) in the M3UA DATA message carrying the MAP response. The response DPC must match the Originating Point Code (OPC) from the incoming MAP request, which is the SMSc point code. If the response is being sent to the STP or HLR point code instead of the SMSc, the routing_info OPC is not being used for the response DPC.

Resolution: Ensure that the MAP response uses the OPC from the incoming routing_info as the DPC for the return message. This guarantees the response reaches the correct SMSc point code rather than a default route.

Call Issues

One-Way Audio

Symptoms: Call is established (both parties hear ringing and answer) but audio flows in only one direction, or not at all.

Investigation: Verify that the MGCP CRCX (Create Connection) and MDCX (Modify Connection) messages are being sent to the media gateway and that the gateway responds with 200 OK. Check that the MGW is reachable and healthy. Inspect the SDP connection address (c= line) in the SIP 200 OK to confirm it contains a routable IP address, not a private or loopback address. Verify that the `signaling_address` SIP config key is set to the address that remote SIP peers should use for signaling and SDP contact — the SIP listener advertises this value as the signaling address in outgoing messages. Confirm that the RTP port range is open in both directions through any firewalls.

Resolution: Correct the MGW connectivity, SDP address configuration, or firewall rules as identified. For deployments where the MSC must advertise a specific reachable address, set the `signaling_address` key in the SIP configuration to that address.

SIP BYE Not Sent on Call Clear

Symptoms: When the A-interface connection is released (e.g., radio link failure, BSC clear), the SIP peer is not notified. The remote SIP endpoint keeps the session open until its own timer expires.

Investigation: Verify that the `connection_lost` event is being sent to the CC FSMs when MSC-A releases the connection. Each active call transaction must receive the release indication so that the CC FSM can trigger SIP BYE on the outgoing leg.

Resolution: Ensure that the MSC-A release handler iterates all active transactions and delivers the `connection_lost` event. The CC FSM should transition to the release state and send SIP BYE upon receiving this event.

Assignment Complete to Wrong CC FSM

Symptoms: A new call in an existing connection (e.g., a second MO call while the first is held) receives the Assignment Complete for the wrong transaction, causing call state corruption.

Investigation: Verify that the `active_trans` reference is updated when a new call starts while the connection is already in the communicating state. The

Assignment Complete is delivered to whatever transaction is marked as active_trans at the time of receipt.

Resolution: Ensure that the MSC-A process updates active_trans to the new transaction when processing the second CM Service Request or call setup in the communicating state.

DTMF Not Working

Symptoms: In-call DTMF tones are not recognized by the remote party or IVR system. The subscriber presses digits but no action occurs.

Investigation: Verify that SIP INFO messages are being sent with content type application/dtmf-relay when DTMF events are received from the radio side. Confirm that the SIP peer supports the INFO method for DTMF relay. Check the SIP peer configuration for DTMF handling preferences.

Resolution: Ensure SIP INFO-based DTMF relay is enabled and that the peer is configured to accept it. If the peer requires RFC 2833 telephone-event RTP packets instead of SIP INFO, adjust the DTMF relay method accordingly.

SMS Issues

MT-SMS Delivery Timeout (TC1)

Symptoms: MT-SMS delivery initiated by the SMS Sc times out. The MAP ForwardSM operation does not complete within the TC1 timer. The SMS Sc retransmits the delivery attempt.

Investigation: Check that the register_mt_sms operation uses a synchronous call to ensure the DTAP CP-DATA is sent before the MAP response. Verify that the DTAP Transaction Identifier (TI) is correctly allocated for the MT direction. Confirm that SMS PDUs are being sent on SAPI 3 (the dedicated signaling channel for SMS) rather than SAPI 0.

Resolution: Ensure synchronous MT-SMS registration, correct TI allocation with the TI flag set for network-originated transactions, and SAPI 3 usage for SMS DTAP messages.

MT-SMS Re-Delivery Loop

Symptoms: The MT-SMS handler process crashes and restarts repeatedly, causing the same SMS to be re-delivered in a loop. The subscriber may receive duplicate messages.

Investigation: Check the `child_spec` of the MT-SMS handler process in the supervision tree. If the restart strategy is set to permanent, the supervisor will restart the handler unconditionally after every termination, including normal completion. This causes re-delivery because the restarted handler re-initiates the delivery.

Resolution: Set the MT-SMS handler `child_spec` to `restart: :temporary` so that normal termination does not trigger a restart. Only abnormal crashes should cause a restart, and the SMSc will handle re-delivery via its own retry mechanism.

MAP Response Not Reaching SMSc

Symptoms: MT-SMS delivery completes on the radio side (subscriber receives the message) but the SMSc does not receive the MAP ForwardSM response. The SMSc treats the delivery as failed and may re-deliver.

Investigation: Check the DPC in the M3UA DATA message carrying the MAP ForwardSM response. The DPC must match the SMSc point code, which is the OPC from the incoming MAP request (`routing_info[:opc]`). If the response is routed to the wrong point code, the SMSc never sees it.

Resolution: Ensure the MAP response DPC is derived from `routing_info[:opc]` of the incoming request, not from a default or HLR-associated point code.

Authentication

Auth Failure -- MAC Mismatch

Symptoms: Subscriber authentication fails with reason mac_failure. The UE sends Authentication Failure with cause "MAC failure" indicating the network authentication check failed on the USIM.

Investigation: This indicates a mismatch between the subscriber key (Ki/K) stored in the USIM and the key stored in the HLR/AuC. The authentication vector generated by the AuC does not match what the USIM computes. This can occur after SIM replacement, HLR migration, or provisioning errors.

Resolution: Verify that the subscriber key in the HLR/AuC matches the key programmed into the USIM. Re-provision the subscriber profile in the HLR if necessary. This is not an MSC-side issue -- the MSC faithfully relays vectors from the HLR.

Auth Resync Loop

Symptoms: The subscriber enters an authentication resynchronization cycle that repeats without resolution. The UE sends Authentication Failure with cause "SQN failure" and an AUTS parameter. The MSC relays the resync to the HLR, but subsequent authentication attempts also fail with SQN failure.

Investigation: OmniMSC permits a maximum of 2 resynchronization attempts per authentication cycle. Check whether the resync count has been exceeded. Verify that the HLR correctly processes the AUTS parameter and advances the SQN. If the HLR SQN is significantly out of range from the USIM SQN, a single resync may not be sufficient.

Resolution: If the resync loop persists after 2 attempts, the subscriber must be re-provisioned in the HLR. The HLR SQN must be reset to align with the USIM SQN. Contact HLR operations to resolve the SQN discrepancy.

Subscriber Issues

TMSI Unknown on Paging Response

Symptoms: A subscriber responds to paging using a TMSI that is not recognized by the MSC. This can occur after MSC restart or TMSI table corruption.

Investigation: When the MSC receives a Paging Response with an unknown TMSI, it does not reject the subscriber. Instead, the MSC sends an Identity Request to obtain the IMSI directly from the mobile station. This is normal recovery behavior per 3GPP TS 24.008.

Resolution: No action required. The MSC automatically resolves the unknown TMSI by requesting the subscriber's IMSI. If this occurs frequently, investigate whether TMSI reallocation is functioning correctly during location updates.

CM Service Request for Unknown IMSI

Symptoms: A subscriber sends a CM Service Request but is not registered in the VLR. The MSC does not have subscriber data for this IMSI.

Investigation: OmniMSC triggers an implicit location update when it receives a CM Service Request from an unregistered subscriber. The MSC initiates the full location update procedure (authentication, ciphering, MAP UPDATE LOCATION to HLR) before proceeding with the requested service.

Resolution: No action required. The implicit location update is automatic. If the location update itself fails (HLR unreachable, authentication failure), the CM Service Request is rejected and the subscriber must retry.

Subscriber Stuck in VLR

Symptoms: A subscriber record remains in the VLR despite the subscriber being unreachable or having moved to another MSC. Paging attempts for this subscriber consistently fail.

Investigation: Check whether the subscriber has completed a location update at another MSC (the HLR would have sent a MAP CANCEL LOCATION, which removes the VLR record). If the cancel was missed or the VLR record is otherwise stale, manual removal may be necessary.

Resolution: Use the DELETE /api/subscribers/{id} endpoint to purge the subscriber record from the VLR. The subscriber will re-register via location update when they next access the network.

Performance

Overload Rejection

Symptoms: New calls and location updates are rejected with GSM cause 42 (switching equipment congestion). The `overload` alarm is active.

Investigation: Check the current overload thresholds and the system metrics that are exceeding them. The four monitored metrics are: active calls (default max 10,000), registered subscribers (default max 50,000), BEAM process count (default max 500,000), and paging rate (default max 1,000/sec). Determine which metric is triggering the overload condition.

Resolution: If the thresholds are appropriate for the hardware, investigate the source of the overload: abnormal call volume, paging storms, or process leaks. If the thresholds are too conservative for the deployment, increase them in the overload configuration. See [Configuration Reference](#).

High Memory Usage

Symptoms: BEAM memory consumption grows over time or spikes unexpectedly. The system may become unresponsive if memory is exhausted.

Investigation: Check ETS table sizes for the major in-memory stores: VLR subscriber table, MPTY conference contexts, and TCAP transaction table. Large numbers of stale entries in any of these tables can cause memory growth. Also

check for process leaks -- a rising BEAM process count without corresponding subscriber or call growth indicates processes that are not terminating correctly.

Resolution: Identify and resolve the source of the growth. Stale VLR entries can be purged via the subscriber API. TCAP transaction timeouts should clean up abandoned dialogues automatically. If process leaks are identified, investigate the supervision tree for processes with incorrect restart strategies or missing timeout handling.

SIP Issues

For SIP peer configuration and OPTIONS keepalive details, see [SIP Trunking](#).

SIP Peer Showing UNKNOWN Status

Symptoms: A SIP peer appears with UNKNOWN status in the control panel or metrics, rather than UP or DOWN.

Investigation: OmniMSC determines SIP peer status via periodic OPTIONS keepalive messages. If OPTIONS keepalive is not configured for the peer, or if the peer has never responded to an OPTIONS request, the status remains UNKNOWN. Check whether the peer configuration includes keepalive settings. Verify that the peer is reachable and responds to SIP OPTIONS with 200 OK.

Resolution: Enable OPTIONS keepalive for the peer in the SIP configuration. If keepalive is enabled but the peer does not respond, investigate network connectivity and confirm the peer supports the OPTIONS method.

re-INVITE Retransmissions from Peer

Symptoms: A SIP peer sends re-INVITE requests during an established call (for codec renegotiation, session refresh, or hold/unhold) and retransmits them because the MSC does not respond. The peer may eventually terminate the call due to the unanswered re-INVITE.

Investigation: Verify that the MSC SIP stack handles in-dialogue re-INVITE messages when the call is in the active state. If the re-INVITE arrives during a state transition or is not matched to the correct dialogue, it may be silently dropped.

Resolution: Ensure the SIP transaction layer correctly matches in-dialogue re-INVITE to the existing call leg and that the CC FSM processes the re-INVITE in the active state. The MSC should respond with 200 OK containing an updated SDP answer.

Session Timer Expiry

Symptoms: Established calls are unexpectedly disconnected after a fixed interval (typically 1800 seconds). The SIP peer sends BYE with reason "Session Timer Expired."

Investigation: SIP session timers (RFC 4028) require periodic re-INVITE or UPDATE to keep the session alive. Check the Session-Expires header negotiation during call setup. Verify that the MSC respects the Min-SE (Minimum Session Expires) value proposed by the peer. If the MSC is the refresher, confirm that it sends re-INVITE or UPDATE before the session timer expires.

Resolution: Ensure the MSC participates in session timer negotiation and performs session refresh as required by the negotiated role (refresher or refreshee). If session timers are not needed in the deployment, the peer may need to be configured to not require them.

3GPP Specification References

Specification	Title	Relevance
TS 24.008	Mobile Radio Interface Layer 3	Authentication, identity, DTAP procedures
TS 29.002	MAP Specification	HLR operations, point code routing
TS 48.008	MSC-BSS Interface (BSSMAP)	Assignment, cipher mode, paging
TS 23.018	Handover Procedures	Inter-MSC handover
TS 22.101	Service Principles	Emergency call, overload

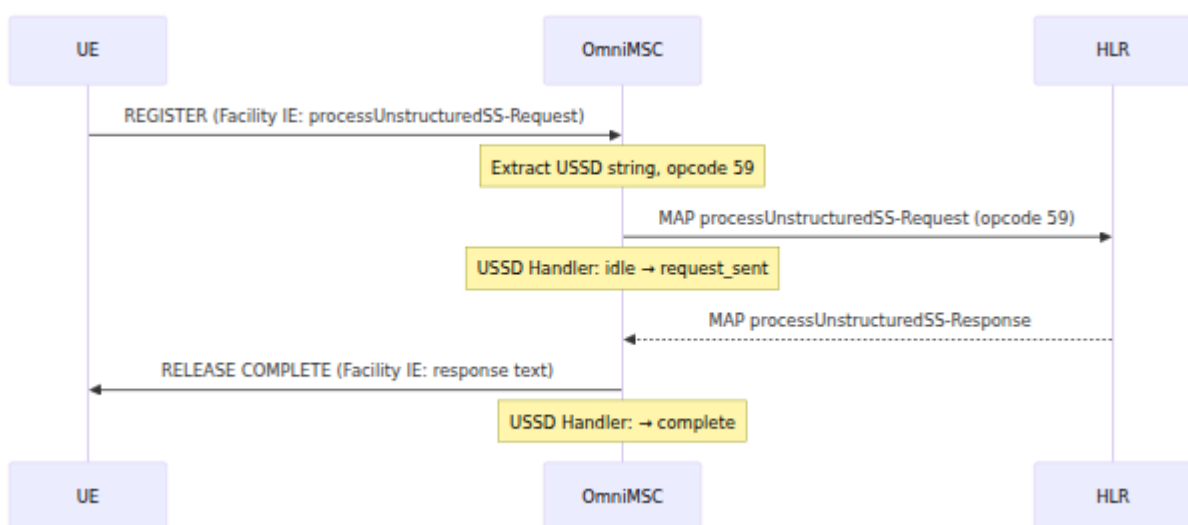
USSD

This document describes the Unstructured Supplementary Service Data (USSD) implementation in OmniMSC, covering HLR relay, local handling, the diagnostic easter egg menu, the USSD codec, and the SS message flow.

For supplementary service codes handled via USSD (call forwarding MMI codes, call barring, call waiting), see [Supplementary Services](#). For the MAP ProcessUnstructuredSS-Request operation and dialogue management, see [MAP Operations](#). For USSD-related Prometheus metrics, see [Metrics and Monitoring](#). For USSD gateway configuration, see [Configuration Reference](#). For troubleshooting USSD issues, see [Troubleshooting](#).

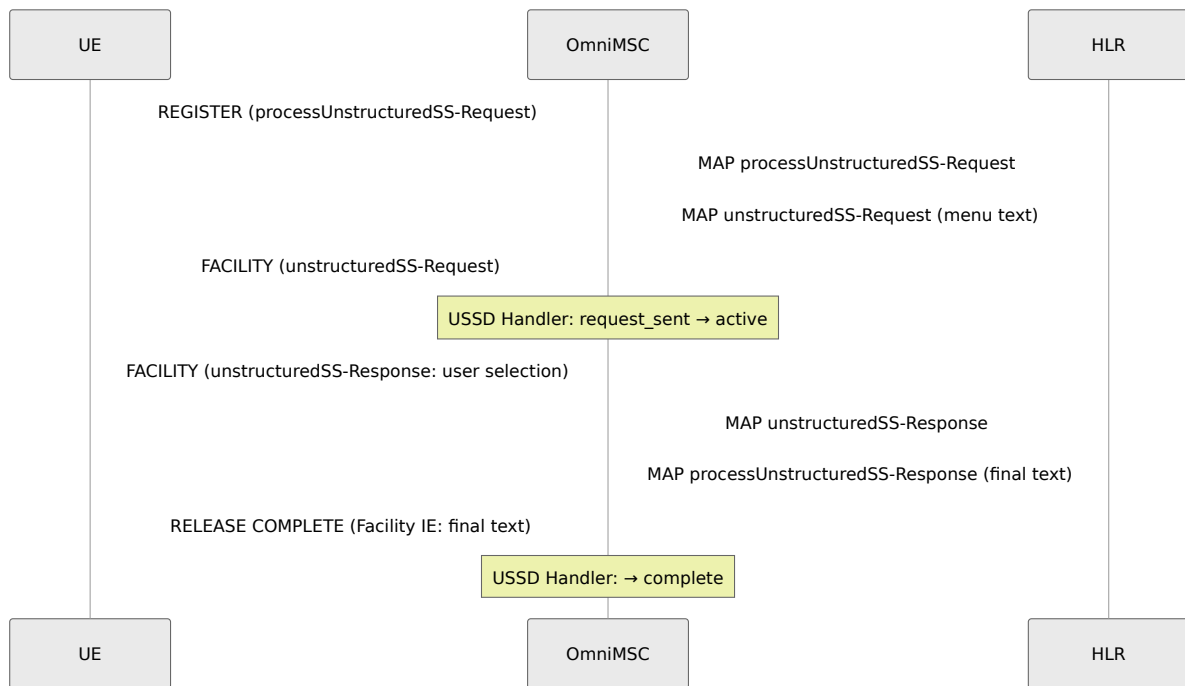
USSD Relay to HLR

When a subscriber sends a USSD string that is not handled locally by the MSC, the request is relayed to the HLR via MAP. The MS sends a REGISTER message containing a Facility IE with a processUnstructuredSS-Request (opcode 59). The MSC extracts the USSD string and forwards the request to the HLR using the same MAP operation. The MSC extracts the USSD string and forwards the request to the HLR using the same MAP operation.



For multi-step interactive sessions, the HLR responds with an unstructuredSS-Request (opcode 60) instead of a final response. The MSC relays this to the UE as a FACILITY message, and the UE's reply is forwarded back to the HLR. This

dialogue continues until the HLR sends a final processUnstructuredSS-Response.



Local USSD Handling

The MSC can handle certain USSD codes locally without forwarding to the HLR or an external gateway. Local handling is used for:

- Supplementary service activation/deactivation codes (CFU, CFB, CFNR, CFNRC, CLIP, CLIR, Call Barring, Call Waiting) using the standard MMI format defined in 3GPP TS 22.030
- Operator-defined diagnostic codes handled internally by the MSC

When a USSD string matches a locally handled service code, the USSD Handler routes it to the SS Handler or the appropriate internal module. The response is sent directly to the UE without MAP signaling.

For codes not handled locally, the USSD Gateway module routes the request to an external USSD gateway. Routing is purely prefix-based: each configured gateway declares a list of `codes` prefixes, and the first gateway whose prefix list matches the service code handles the request. A gateway configured with

codes: :all acts as a default/catch-all, receiving any code not matched by a more specific gateway. If no gateway matches and no :all default is configured, the request is rejected.

Easter Egg: System Diagnostic Menu

OmniMSC includes a hidden diagnostic menu accessible by dialing *#6664# (which spells *#0MNI# on a phone keypad). The MSC recognizes several keypad variants of this code and responds with an interactive USSD menu.

The main menu provides the following options:

Key	Menu Item	Information Displayed
1	System Status	Uptime, registered subscribers, active connections, active calls, memory usage, scheduler count
2	VLR	Registered subscriber count, active LU FSMs, active Auth FSMs
3	Active Calls	Count and summary of active calls (direction, calling/called numbers)
4	SS7 Stack	SCCP connection count, TCAP transaction count, pending paging requests
5	BEAM VM	Process count/limit, run queue depth, reduction count, memory breakdown (total, ETS, binary)
6	About	OmniMSC version info, OTP release, Omnitouch Network Services branding
9	Sales Enquiry	Contact information
0	Exit	Ends the session

Each submenu displays a "0. Back" option that returns to the main menu. The diagnostic data is gathered from live system metrics at the time of the request.

The easter egg is handled entirely within the MSC without any MAP signaling. The USSD Handler detects the magic code, routes it to the EasterEgg module, and manages the multi-step menu dialogue using network-initiated unstructuredSS-Request messages to the UE.

USSD Codec

The USSD codec handles encoding and decoding of USSD protocol elements per 3GPP TS 24.080 and TS 24.090.

Facility IE Structure

The Facility IE (tag 0x1C) wraps an ASN.1 BER-encoded component:

Component Type	ASN.1 Tag	Usage
Invoke	0xA1	Carries a request (processUnstructuredSS-Request, unstructuredSS-Request, unstructuredSS-Notify)
ReturnResultLast	0xA2	Carries a response (processUnstructuredSS-Response, unstructuredSS-Response)

Each component contains an invoke ID, an operation code, and an optional parameter SEQUENCE with the USSD data coding scheme and USSD string.

MAP Operation Codes

Opcode	Operation	Direction
59	processUnstructuredSS-Request	MO: UE → MSC → HLR
60	unstructuredSS-Request	MT: HLR → MSC → UE (interactive menu step)
61	unstructuredSS-Notify	MT: HLR → MSC → UE (notification, no response expected)

GSM 7-bit Encoding

USSD strings are encoded using the GSM 7-bit default alphabet defined in 3GPP TS 23.038. Each character is represented as a 7-bit septet, and septets are packed into octets (8 septets fit into 7 bytes). The data coding scheme byte (DCS=0x0F) indicates GSM 7-bit encoding.

For strings requiring characters outside the GSM 7-bit alphabet, UCS-2 encoding (DCS=0x48) is used, where each character occupies two bytes in big-endian UTF-16.

The maximum USSD string length is 182 characters for GSM 7-bit encoding (160 bytes packed) or 80 characters for UCS-2 (160 bytes).

SS REGISTER and RELEASE COMPLETE Message Flow

USSD sessions use the Supplementary Service (SS) message types defined in 3GPP TS 24.010:

Message	Direction	Purpose
REGISTER	UE → MSC	Initiates a new SS transaction. Contains a Facility IE with the USSD request.
FACILITY	Both	Carries mid-session data (interactive menu steps). Used for multi-step USSD dialogues.
RELEASE COMPLETE	Both	Ends the SS transaction. May contain a Facility IE with the final response.

A simple USSD request-response uses REGISTER (from UE) followed by RELEASE COMPLETE (from MSC). An interactive multi-step session uses REGISTER, then one or more FACILITY exchanges, then RELEASE COMPLETE.

The session has a configurable guard timeout (default 30 seconds). If neither the UE nor the gateway responds within this window, the MSC terminates the session with RELEASE COMPLETE.

References

Specification	Title	Relevance
TS 24.090	Unstructured Supplementary Service Data (USSD)	USSD procedures, session management
TS 29.002 Section 14	MAP Specification - Supplementary service operations	MAP processUnstructuredSS-Request (opcode 59), unstructuredSS-Request (opcode 60), unstructuredSS-Notify (opcode 61)
TS 24.080	Mobile radio interface layer 3 SS specification - Formats and coding	Facility IE structure, component encoding
TS 23.038	Alphabets and language-specific information	GSM 7-bit default alphabet, septet packing
TS 22.030	Man-Machine Interface (MMI)	Service code format, USSD string syntax
TS 24.010	Mobile radio interface layer 3 SS specification - General aspects	REGISTER, FACILITY, RELEASE COMPLETE message types

Voice Group Call Service and Voice Broadcast Service

This document describes the Voice Group Call Service (VGCS) and Voice Broadcast Service (VBS) group and broadcast call control implemented in OmniMSC by Omnitouch. VGCS follows 3GPP TS 43.068 and VBS follows 3GPP TS 43.069. The MAP group-call operations exchanged with the Group Call Register (GCR) and the relay MSCs follow 3GPP TS 29.002 clause 17.6.7.

For point-to-point call control, see [Call Flows](#). For the underlying MAP and TCAP procedures, see [MAP Operations](#). For enhanced Multi-Level Precedence and Pre-emption used to prioritise talkers, see [Supplementary Services](#). For configuration parameters, see [Configuration Reference](#).

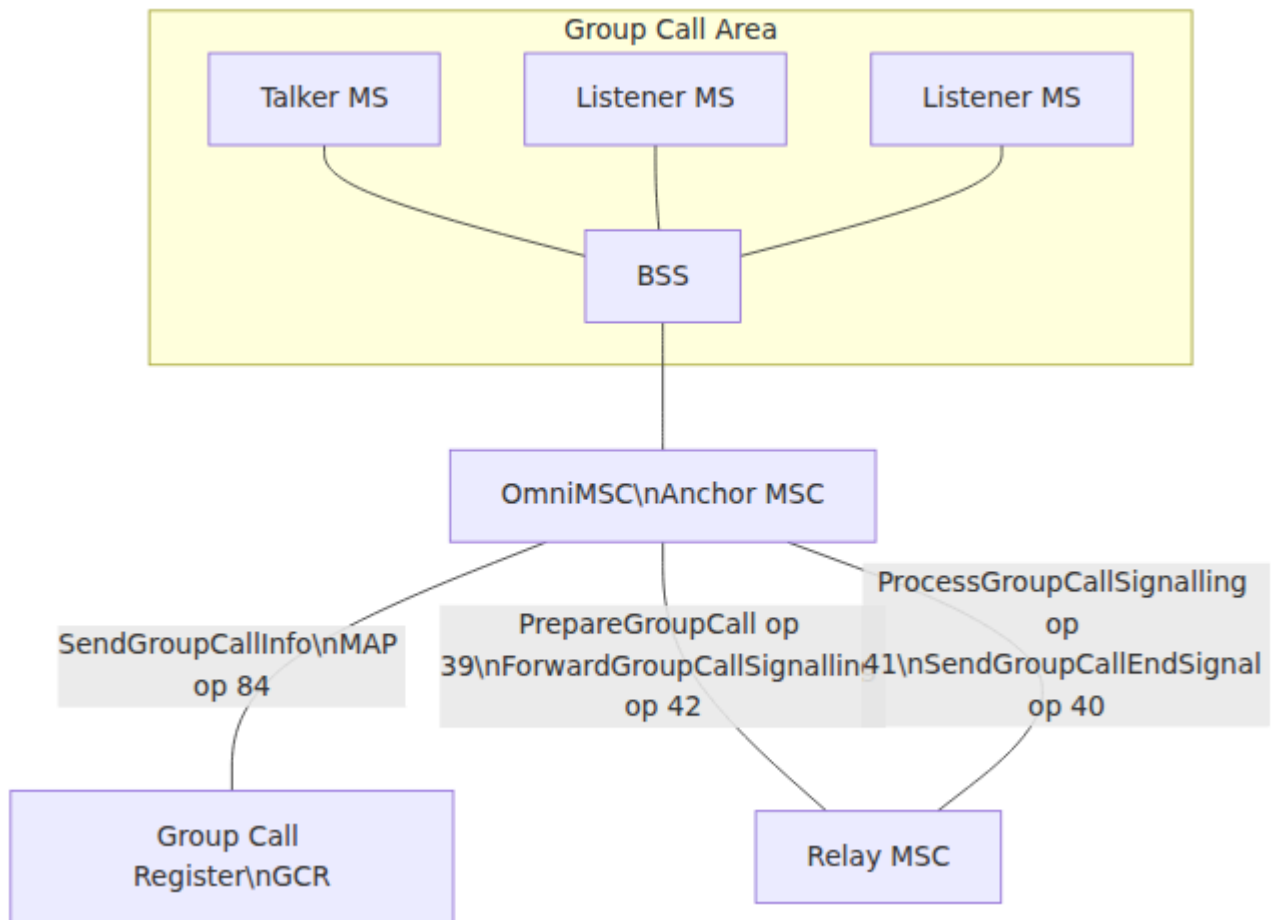
Overview

VGCS and VBS are ASCI (Advanced Speech Call Items) services used primarily in railway (GSM-R) and public-safety networks. They allow a single talker to be heard by many listeners in one or more group-call areas.

- VGCS (TS 43.068) is a bidirectional group call. Any service subscriber in the group-call area may become the talker by seizing the uplink. Only one talker holds the uplink at a time.
- VBS (TS 43.069) is a unidirectional broadcast. Only the broadcast originator (a dispatcher or a designated subscriber) transmits on the downlink. There is no uplink contention.

A group or broadcast call is anchored at a serving MSC, the anchor MSC. The anchor MSC interrogates the Group Call Register (GCR) to resolve the group attributes and the ASCI call reference, then prepares group-call channels in the

relevant cells through the relay MSCs. The group is identified by a Group Id (VGCS) or a broadcast Group Id (VBS).



MAP Group-Call Operations

OmniMSC implements the five MAP group-call operations of TS 29.002 clause 17.6.7. The operations are carried in TCAP over SCCP using the compiled ASN.1 codec (module `MAP-Group-Call-Operations` and data types `MAP-GR-DataTypes`).

Operation	Opcode	Direction	Confirmed	Purpose
SendGroupCallInfo	84	Anchor MSC to GCR	Yes	Interrogate the Group Call Register for the anchor-MSC address and ASC call reference
PrepareGroupCall	39	Anchor MSC to relay MSC	Yes	Ask a relay MSC to allocate group-call channel resource and return the group call number
SendGroupCallEndSignal	40	Relay MSC to anchor MSC	Yes	Release group-call leg
ForwardGroupCallSignalling	42	Anchor MSC to relay MSC	No	Carry downlink uplink-control commands (grant, reject,

Operation	Opcode	Direction	Confirmed	Purpose
				seize, release)
ProcessGroupCallSignalling	41	Relay MSC to anchor MSC	No	Carry uplink-control indicatio (uplink request, uplink release, call release)

The teleservice code distinguishes the service. VGCS uses voiceGroupCall (0x91) and VBS uses voiceBroadcastCall (0x92), per TS 22.003 and the MAP-TS-Code module.

Talker priority

The uplink-control operations carry a talker priority (TS 43.068 and the MAP TalkerPriority type):

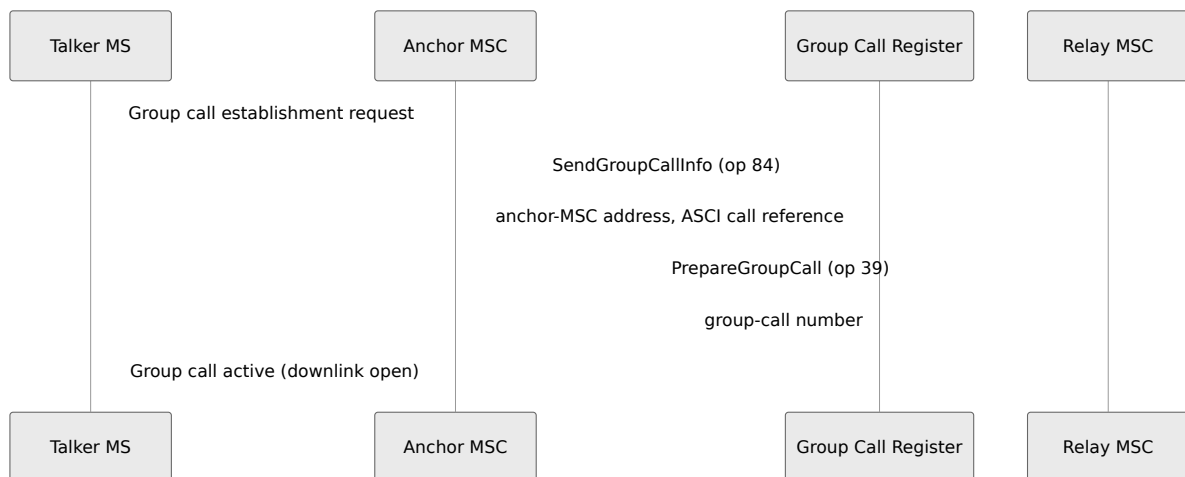
Priority	Value	Meaning
normal	0	Standard service subscriber
privileged	1	Privileged subscriber, may pre-empt normal talkers
emergency	2	Emergency talker, highest precedence

Group-Call Control State Machine

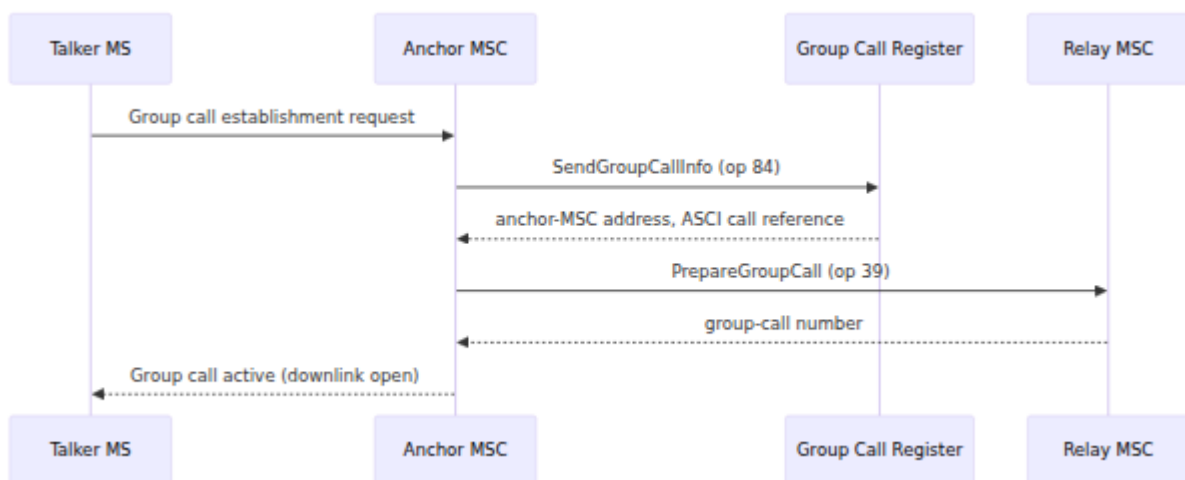
The anchor-MSD group-call control is a state machine (`Omnimsc.VGCS.FSM`) that mirrors the point-to-point call-control FSM. It manages a single group or broadcast call through establishment, the active phase, VGCS uplink contention, and release.

State	Meaning
null	No group call in progress
establishment	An establishment request has been accepted; the GCR is being interrogated (<code>SendGroupCallInfo</code>)
group_channel_setup	The anchor MSC is preparing group-call channels in the relay MSCs (<code>PrepareGroupCall</code>)
active	The group or broadcast call is established; the downlink is open. For VGCS the uplink is initially free
uplink_busy	VGCS only. A talker has seized the uplink. Further uplink requests are rejected until the uplink is released
release	The call is being torn down (<code>SendGroupCallEndSignal</code>) before returning to null

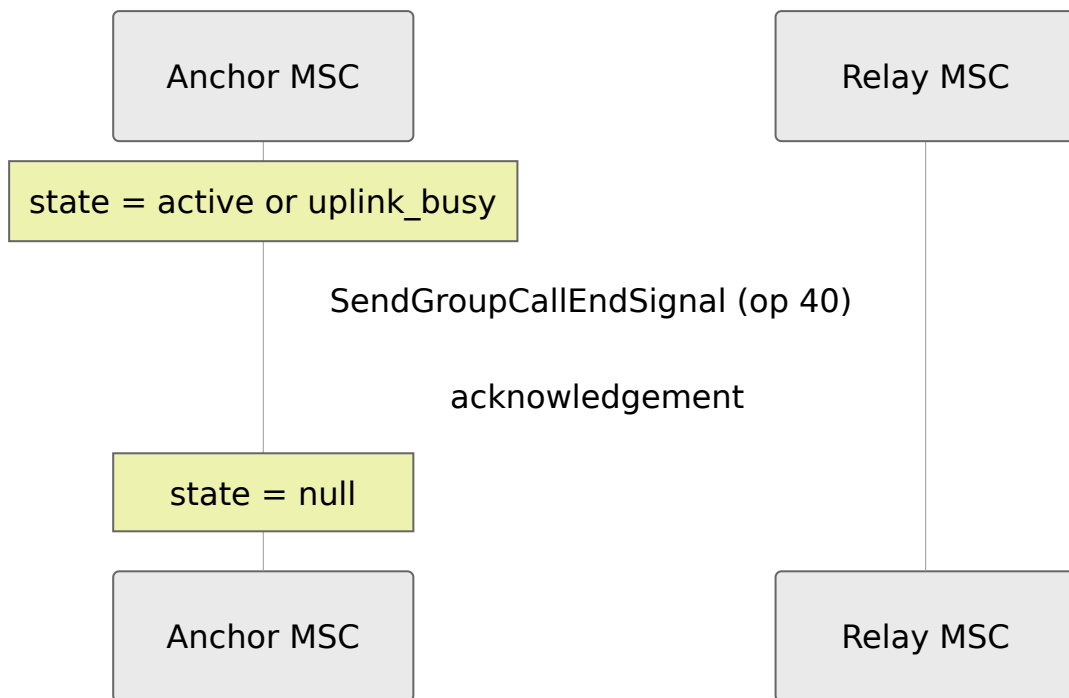
Establishment flow



VGCS uplink control flow



Release flow



Configuration

The group-call control layer runs under the `Omnimsc.VGCS.Supervisor` and requires no mandatory configuration to accept incoming group-call operations. The following optional parameters tune the relay-MSC behaviour.

Parameter	Location	Default	Description
group_call_number	<code>config :omnimsc,</code> <code>Omnimsc.VGCS.Handler</code>	MSC global title	E.164 number returned in the PrepareGroupCall response when acting as a relay MSC
global_title	<code>config :omnimsc,</code> <code>:msc</code>	none	Anchor-MSC address advertised in the SendGroupCallInfo response

Example:

```
config :omnimsc, Omnimsc.VGCS.Handler,
  group_call_number: "14155559000"
```

Implemented and Deferred

The following are implemented in this release.

- Group-call control state machine for VGCS and VBS, covering establishment, the active phase, VGCS uplink seize, reject and release, and call release, with a guard timer safety net.
- Encoders for all five MAP group-call request operations (SendGroupCallInfo, PrepareGroupCall, SendGroupCallEndSignal, ForwardGroupCallSignalling, ProcessGroupCallSignalling), each producing a complete TCAP message via the compiled ASN.1 codec.
- Decoders that normalise the group-call operation arguments into OmniMSC representations.

- Ingress routing of incoming group-call operations (opcodes 39, 40, 41, 42, 84) to the group-call handler, which correlates them to the running group-call state machine by Group Id and answers the confirmed operations with a TCAP acknowledgement.

The following are deferred.

- Encoding of the confirmed-operation result bodies (the group-call number in the PrepareGroupCall response and the anchor-MSI address and ASCII call reference in the SendGroupCallInfo response). The compiled TCAP codec in the SS7 dependency wires the group-call operation arguments into its ROS Invokable object set but does not wire the results into the Returnable object set. As a result these responses are currently sent as an empty (invoked-only) TCAP returnResult, which is a valid acknowledgement per the ROS ReturnResult definition (the result sequence is optional), but does not carry the result payload. The request-direction operations, argument decoding, and the peer-side result decoders are unaffected. This is tracked against the SS7 dependency exposing the group-call results in Returnable.
- The radio-side group-call channel establishment in the BSS (the VGCS/VBS channel and notification procedures of TS 44.068 and TS 44.069) is out of scope for the core network control layer described here.

Related Documentation

- [Call Flows](#) for point-to-point voice call sequences
- [MAP Operations](#) for the MAP and TCAP transport
- [Supplementary Services](#) for eMLPP precedence and pre-emption
- [Configuration Reference](#) for all configuration parameters

