NewNet Mobile Messaging
RTR R04.11.04

Operator Manual

Release 17.4 Revision A
February 2019

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

1.1 About this Document

This document discusses the operation and administration of the NewNet Mobile Messaging Router (RTR) product.

The RTR is a product from the NewNet Mobile Messaging product family of SS7 message routing and network querying products.

This document contains a description of the general operations and maintenance aspects of the NewNet Mobile Messaging system. Because the available functions are licensed and depend on the specific NewNet Mobile Messaging implementation, not all functions and/or applications contained in this document may be relevant or applicable to the NewNet Mobile Messaging system you will be working with. Actual screen presentation may differ from the screens presented in this document due to software changes or browser configurations.

1.2 Scope

This document describes the functionality of the NewNet Mobile Messaging RTR component.

This document does not describe the functionality of the RTR's Firewall (FWL) feature. For information about the FWL, refer to the NewNet Mobile Messaging Firewall Guide.

1.3 Intended Audience

This document is intended for everyone interested in how the RTR can best be used, but mainly for:

- Implementation Engineers who are responsible for the pre-installation, on-site installation, and configuration of the RTR in the end-user environment.
- Maintenance and Support Engineers who are responsible for maintaining the total system environment of which the RTR is a part, or just the devices.
- Network Operators who are in charge of the daily operation of the RTR systems and infrastructure.

1.4 Documentation Conventions

Typeface or Symbol	Meaning	Example
Bold	Refers to part of a graphical user interface.	Click **Cancel**.
`Courier`	Refers to a directory name, file name, command, or output.	The `billing` directory contains...

Typeface or Symbol	Meaning	Example
`<pointed brackets>`	Serves as a placeholder for text that the user will replace, as appropriate in context.	The file is called `MGRdata.xml.<ip>.gz`, where `<ip>` is the server's IP address.
`[square brackets]`	Indicates an optional command.	`[--validateonly]`
Note:	Indicates information alongside normal text, requiring extra attention.	**Note:** Ensure that the configuration...
\ (Unix)	Denotes line continuation; the character should be ignored as the user types the example, and ENTER should only be pressed after the last line.	`% grep searchkey \` `data/*.dat`

1.5 Locate Product Documentation on the Customer Support Site

Access to NewNet's Customer Support site is restricted to current NewNet customers only. This section describes how to log into the NewNet Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the NewNet Customer Support site.

   Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Chapter 2

System Overview

Topics:

2.1 Introduction

The Router (RTR) allows you to route SMS traffic from anywhere to virtually everywhere. The RTR can be used to distribute SMS traffic over various SMSCs using weighted load distribution and (guaranteed) throughput control.

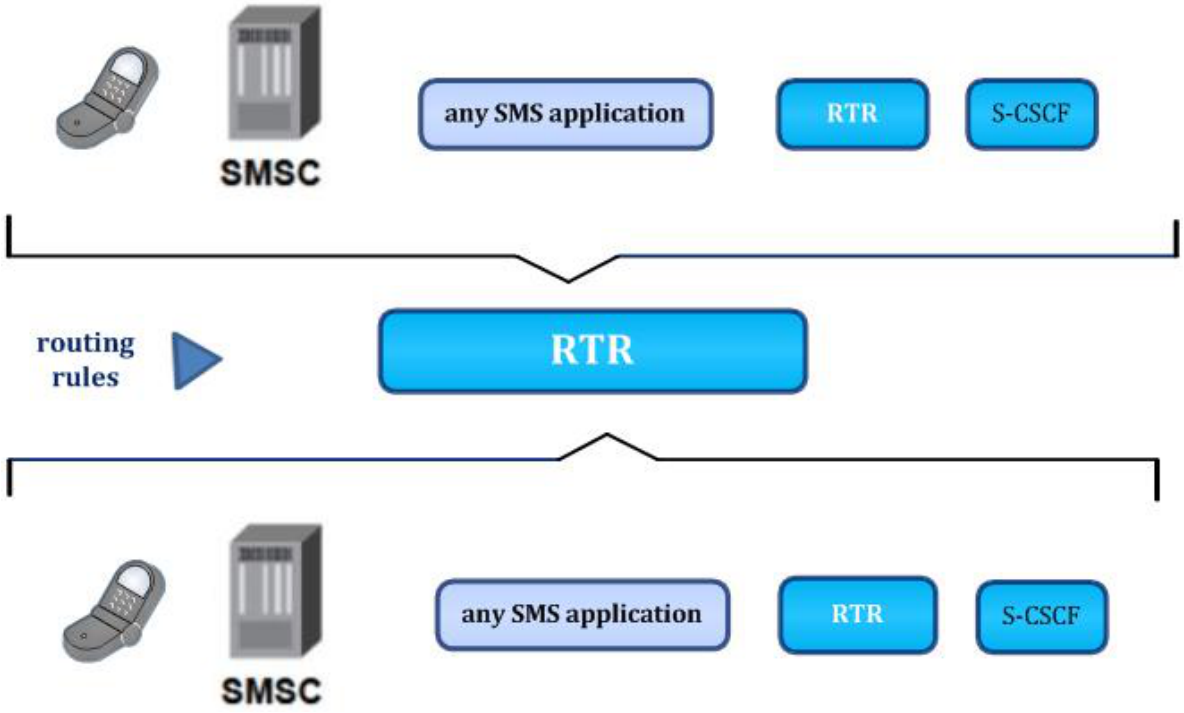


Figure 1: Traffic through the RTR

The RTR allows routing mobile-originated SMS traffic destined to interactive/voting applications directly to the related application. This will reduce the SMS bottlenecks and improve overall quality of service of SMS services. This enables optimized use of the existing SMS network infrastructure. Routing SMS traffic directly to your applications and even perform a delivery attempt without going through the SMSC are possible. For example, SMS voting or vehicle tracking are mainly one-way applications where the information is sent via a short message to the application. These type of short messages do not need to go via the SMSC, but can be delivered directly by the RTR to the SMS application.

Examples of how the RTR can be used are:

- Routing mobile-originating (MO) SMS traffic to SMSCs using advanced load distribution and throughput control.
- Routing MO SMS traffic to SMS applications directly, without going through an SMSC first.
- Routing application-originating (AO) SMS traffic directly to a mobile phone (a single delivery attempt).
- Routing IMS-originating SMS traffic to a mobile phone in GSM domain.
- Routing MO SMS messages directly to a mobile phone, creating instant SMS (mobile-to-mobile).
- Routing MO SMS messages directly to a device in IMS domain.

This chapter describes the RTR functionality, discusses how the RTR addresses the challenges of SMS operators today, and describes the RTR's architecture, hardware platform, components, and interfaces.

2.2 System Context

The following system context diagram illustrates the RTR's context spaces and functional interfaces.

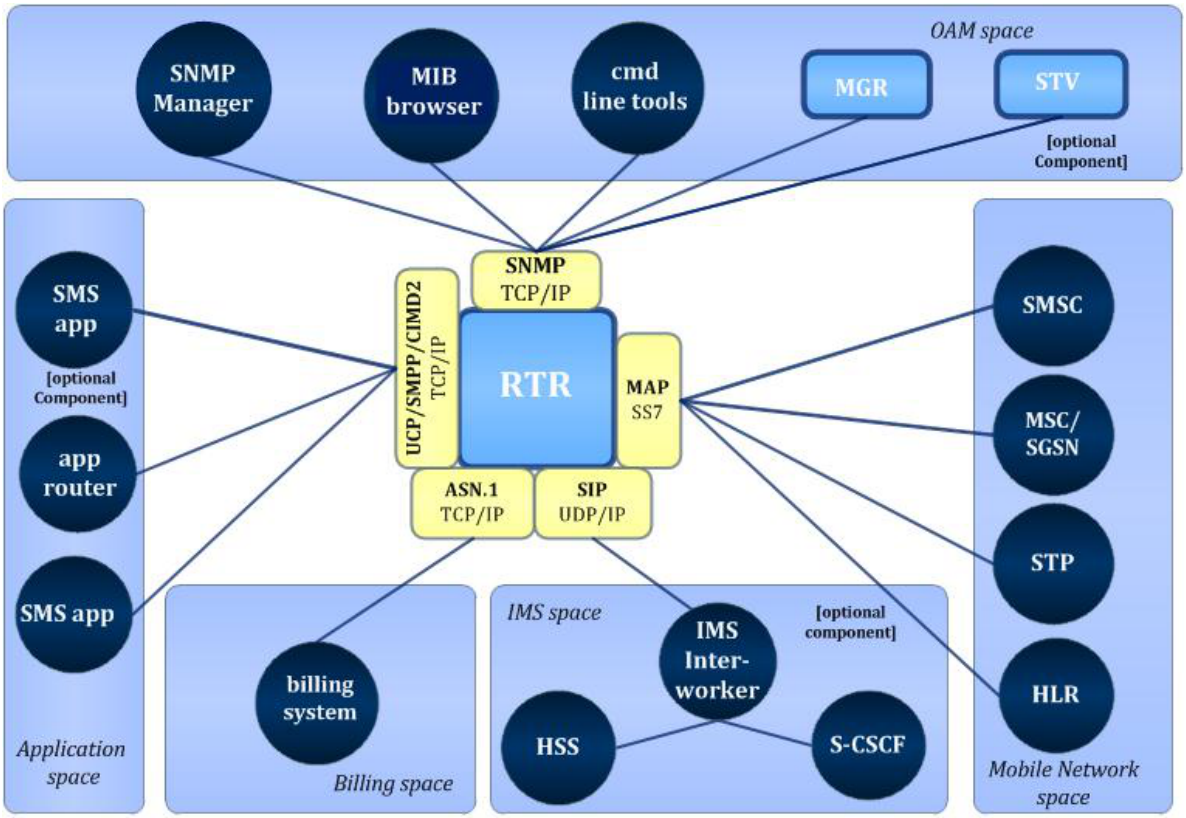


Figure 2: RTR system context

The high level overview contains applications that connect to the RTR to receive MO traffic from the network, using UCP, SMPP, or CIMD2 over TCP/IP. The RTR is connected to the relevant network component(s) via the signaling network to receive the MO traffic sent by the mobile subscribers. The RTR is connected to the IMS network (via the IIW) to receive the IMS Originated traffic and send the IMS Terminated traffic.

2.2.1 Mobile Network Space

The PLMN interface (that is, the MAP/SS7 interface toward the mobile network) is arranged entirely by the hardware and RTR firmware/software. The following components are part of the mobile network space:

- SMSC—The default destination of all traffic.
- MSC/SGSN—The originating point in the PLMN of the MoForwardSm messages that is subject to routing by the RTR.
- STP—The Signalling Transfer Point.
- HLR—The RTR uses the Home Location Register (HLR) to query subscriber information (such as the destination MSC for an SMS delivery).

Note: This document does not address all components in the mobile network space that are required for end-to-end SMS traffic (such as mobile subscribers, mobile stations, the radio network, and IN systems).

2.2.2 Application Space

The following components may be part of the application space:

- SMS application—The application responsible for receiving the SMS traffic for one short number through the SMPP, UCP, or CIMD2 protocol over TCP/IP. It is connected via the HUB as the application interface.
- Application router—An SMPP, UCP, or CIMD2 concentrator acting as a proxy for all sessions from SMS applications and handling authentication and session control of all sessions toward the RTR. The HUB is an example of an application router.

Note: This document does not address all components in the data network that are required for end-to-end SMS traffic (such as IP routers, switches, and firewalls).

2.2.3 Operations, Maintenance, and Provisioning Space

The operations, maintenance, and provisioning (OAM) space represents the interface among operations and maintenance software, including the Manager (MGR) and SNMP tools. All provisioning commands, management actions, and alarms pass through this space. The following optional components may be part of the OAM space:

- SNMP manager—Various SNMP-based network management tools that may be available. This system is responsible for capturing and processing all SNMP alarms.
- MIB browser—An application that can be used to view and modify the contents of the SNMP variables that are defined in the MIB file.
- Command-line tools—Tools and utilities that can be used on the command line of the RTR host machine.
- MGR—Web-based application used to manage the configuration of the RTR in the SMS network configuration.

2.2.4 Billing Space

The billing space is the interface that provides ASN.1-formatted Call Detail Records (CDRs) to the billing system or to the mediation system. The RTR can produce SMSC-compatible CDRs in a

configurable directory on the system. These CDRs are made available in the RTR billing directory for transport to a remote system.

A billing system performs charging of subscribers, while a mediation system performs post-processing (such as reformatting) of CDRs in preparation for processing by the billing system.

2.2.5 IMS Space

The following components may be part of the IMS space:

- IMS Inter-Worker - An IMS Inter-Worker handles the Diameter Sh interface with HSS and IMS Originated and IMS Terminated messages via I-CSCF. The IIW is an IMS Inter-Worker.
- S-CSCF - The S-CSCF is the heart of the IMS core network. The S-CSCF acts as a registrar server, and it is the central point for IMS service control over the ISC reference point. Moreover, the S-CSCF facilitates the routing path for mobile originated or mobile terminated messages. It is connected via the IIW.
- HSS - The HSS plays the role of a location server in IMS. The HSS also serves as a single point of provisioning for IMS subscribers and their services. It is connected via the IIW.
- RCS Server - The RCS Server allows an operator to deploy the Rich Communication Services. In our case RCS server is Krypton.

Note: This document does not address all components in the data network that are required for end-to-end SMS traffic (such as IP routers, switches, I-CSCF, RCS Server etc.).

2.3 SMS Routing Functionality

The RTR can route SMS messages in many ways. The following diagram depicts the available routing entities and the types of messages that these entities can send to or receive from the RTR.

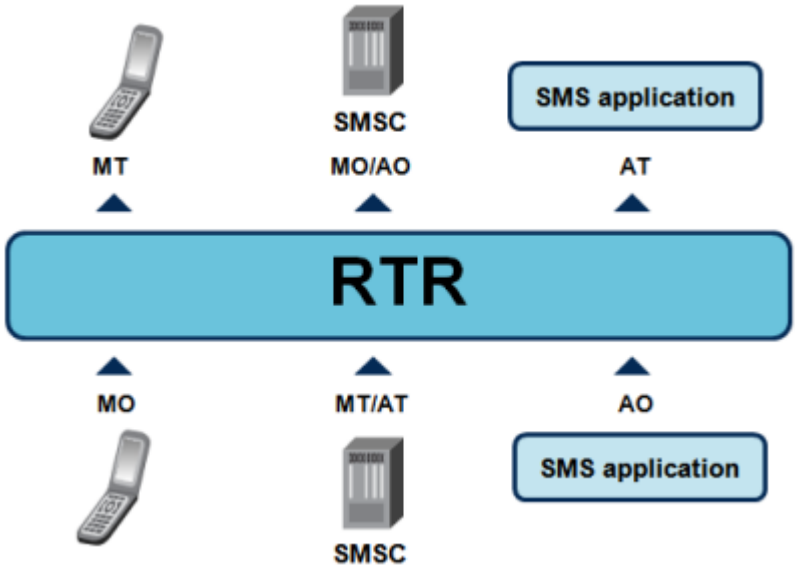


Figure 3: Routing entities and message types

2.4 Rule Sets

The RTR supports sets of rules that are evaluated against messages. Each rule set consists of rules that:

- Have a specific purpose
- Are evaluated against a certain type of message
- Apply to either inbound or outbound messages

Rule Set Purposes

Each rule set has a specific purpose:

- To route messages
- To count messages and rule evaluation results
- To request evaluation by an external application

The routing rule sets, abbreviated with an R, route messages. Inbound routing rules determine where each message should be routed. Outbound rules block or filter messages that have certain characteristics and are bound toward certain destinations.

The counting rule sets, abbreviated with a C, count messages and count the results of rule evaluations. Inbound counting rules count how the RTR responds to messages. Outbound counting rules count the types of responses to outbound messages that the RTR received.

The external condition rule sets, abbreviated with an X, request evaluation by external condition (EC) applications. EC applications can perform a variety of actions, but they always respond to the RTR's request with "true" or "false". If the response is negative, the external condition rule can reject or block the message.

Message Types

The RTR can evaluate rule sets for short messages (SMs) or for MAP-layer SendRoutingInfoForSm (SRI-SM) operations.

For inbound messages, the rule sets are:

Message Type	Routing Rule Set	Counting Rule Set	External Condition Rule Set
MO	MOR	MOC	MOX
AO	AOR	AOC	AOX
MT	MTIR	MTIC	MTIX
AT	ATIR	ATIC	ATIX
Internally generated SM	IGMR	IGMC	IGMX
SRI-SM request	SRIQR	Not applicable	Not applicable
SRI-SM response	SRIPR	Not applicable	Not applicable

For outbound messages, the rule sets are:

Message Type	Routing Rule Set	Counting Rule Set	External Condition Rule Set
MO	Not applicable	Not applicable	Not applicable
AO	Not applicable	Not applicable	Not applicable
MT	MTOR	MTOC	MTOX
AT	ATOR	ATOC	ATOX
SRI-SM request	MTOR	MTOC	MTOX
SRI-SM response	MTOR	MTOC	MTOX

2.5 Rule Evaluation

A rule consists of:

- A set of conditions, and
- A set of actions or counters

For a rule to match a message, the message must meet all conditions in the rule. The message may also need to meet certain parameters that are related to the rule's action.

Logically, all of a rule's conditions are combined by an AND operation. You can achieve OR logic by defining multiple rules. Also, certain types of conditions have intrinsic OR capabilities.

Evaluating Routing Rules

Every routing rules has a priority. When the RTR processes a set of routing rules, it starts with the rule that has the highest priority. If that rule does not match the message, the RTR continues to evaluate the rule with the next lowest priority. If multiple rules are defined with the same priority, the evaluation order is unspecified.

The evaluation process stops at the first rule that matches the message, and the RTR applies that rule's action to the message. If no routing rule matches a message, the RTR applies the default behavior of the rule set to the message.

Evaluating Counting Rules

Counting rules do not have a priority. All rules in a set of counting rules are evaluated, and the counters of all matching rules are updated. Therefore, the evaluation of a large counting rule set requires more processing power than the evaluation of an equally large routing rule set.

If no counting rule matches a message, the RTR does not update any counters.

Evaluating External Condition Rules

Every external condition rule has a priority. When the RTR processes a set of external condition rules, it starts with the rule that has the highest priority. If that rule does not match the message, the RTR continues to evaluate the rule with the next lowest priority. In case multiple external condition rules have the same priority, the order of evaluation is unspecified.

If a rule matches a message, the rule is appended to a list of matching rules. After the RTR has evaluated all external condition rules, the RTR processes the list of matching rules by evaluating the "external condition" for each rule. The evaluation of the external condition normally requires the RTR to send an external condition interface (ECI) request to an external application. The application will reply with an ECI response.

Prior the evaluation of the external condition and sending the ECI request, the RTR can modify the set of 32 external attributes (refer to *External Condition Attributes*). The **External Attribute Setting** option in the external condition rule provides a mechanism to configure these Boolean attributes individually. The configured values are set in the `externalAttribute` field of the ECI evaluation request sent to the EC application.

Important: In case the RTR is configured to use certain external attribute values that would be either set or checked by specific EC applications (such as PBC, XS-CPY, XS-FWD, XS-TIE, etc.), please ensure that the relevant attribute values for a particular application are not modified or overwritten while configuring the **External Attribute Setting** option in an EC rule that is not associated with the same application.

After the RTR receives a result that will lead to the rejection or blocking of the message, it ignores all lower-priority rules that are in the list of matching rules. If no external condition rule matches a message, the evaluation of the rule set does not affect any further processing of the message.

Note:

1. In case of MTOX rules, for incoming application originated message (e.g. AO-MT path), while evaluating the **Originator** condition, the source application is considered as the originating application.
2. In case of ATOX rules, for incoming application originated message (e.g. AO-AT path), while evaluating the **Originator** condition, the originating application is determined on the basis of the received SM. The source application category is a separate condition in the ATOX rule that can be used to evaluate the originating application category.
3. The **Application Category** configured under **Originator** condition is considered matched when at least one of the configured bit matches with the originating application.

2.6 Application Routers (HUBs)

As an optional component in the SMS routing domain, a special application can reside that behaves as a concentrator and load balancer of SMS application traffic. Such an application can be referred to as a HUB, multiplexer, concentrator, or application router; from now on referred to as HUB.

Depending on the mechanisms available in the HUB used and the applicable routing paths, the connections between the application and the HUB are independent of the connections between the HUB and the RTR.

HUBs can provide security, scalability, and maintainability benefits for SMS networks. If required, the MGR can facilitate common configuration parameters to be shared with a HUB.

When routing AO traffic through HUBs, the main functions of the HUB are:

- Distribute and load balance traffic over RTRs and SMSCs
- Regulate throughput

When routing AT traffic through HUBs, the main functions of the HUB are:

- Managing sessions between RTRs and/or SMSCs and the application
- Distributing (concentrating) traffic toward the application
- Regulate throughput

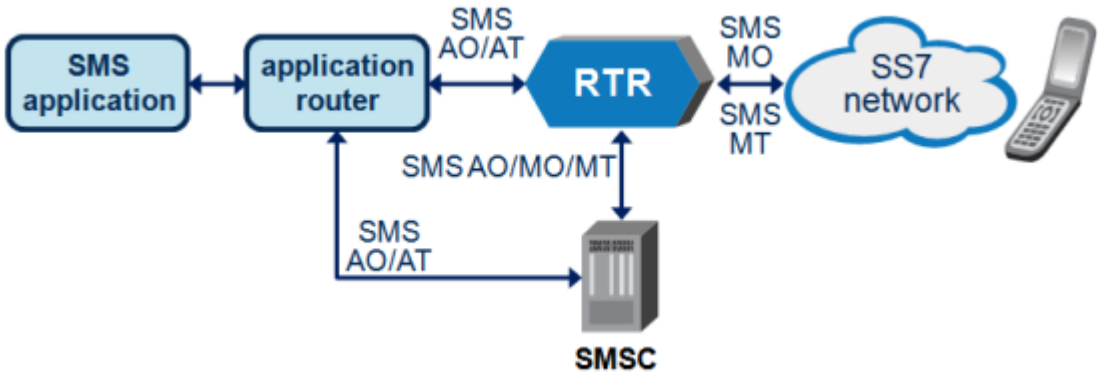


Figure 4: Role of the application router (HUB)

2.7 Software Overview

2.7.1 Software Architecture

The RTR's software architecture is modular. Depending on the network environment, protocol layers can be replaced by required protocols. The following diagram illustrates how the RTR is logically connected to the GSM network and how messages are processed when they arrive at the RTR interface.

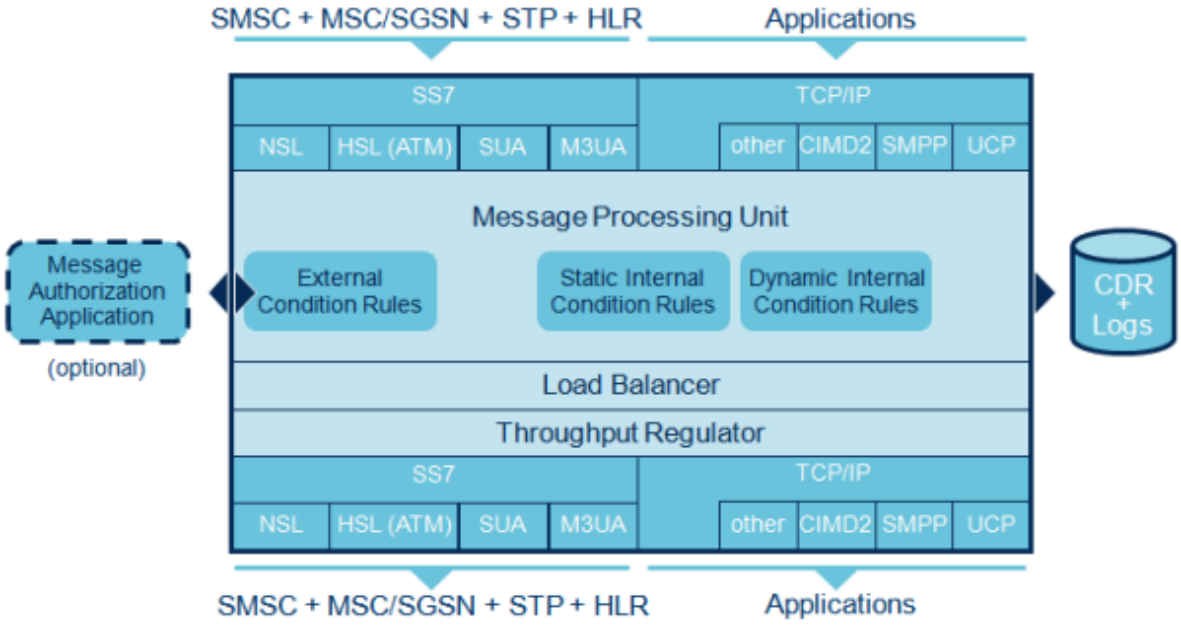


Figure 5: RTR software architecture

The RTR uses the operating system TCP/IP stack.

The GSM SS7 layer consists of an SMS-optimized stack containing MTP3(b), M3UA, SUA, SCCP, TCAP, and MAP functionality (MTP1 and MTP2 is provided in the firmware of the RTR SS7 interface card).

2.7.2 Software Processes

The RTR engine consists of the message processing unit and its supporting layers for message formatting, load balancing, and throughput regulation.

The RTR software that runs on the RTR host server consists of two executables:

- One instance of the RTR process, which contains the RTR kernel and the optimised SS7 stack
- One instance of the watchdog process, which monitors the RTR process and restarts and configures the RTR, if required

Routing rules and SNMP counter settings are maintained in the rule base and read and updated by the message processing unit.

CDR files are written in ASN.1-formatted CDR files by the billing module of the message processing unit.

2.7.3 System Software Components

The layered system software components used in the RTR are:

- Red Hat Enterprise Linux operating system
- Perl scripting language
- net-snmp, SNMP library, and utilities
- expat XML parser
- zlib
- gdbm
- openssl
- Apache Web server (for the Manager)
- mod_perl
- c-ares

For more information about the operating system software configuration and software versions, refer to the Red Hat Enterprise Linux documentation at *http://www.redhat.com/docs*.

2.8 Hardware Overview

The RTR hardware platform consists of the following main components:

- Host computer

Note: Please contact your account manager for the most up-to-date hardware recommendations.

2.9 Quality Characteristics

The RTR provides carrier-grade quality behaviour. This quality behaviour is a result of the RTR's architecture and design.

The RTR's most important quality design aspects are partially based on the ISO 9126 quality attributes. They are:

- High system performance, ensuring efficient use of available resources
- High availability, ensuring maximum service availability without outage
- Scalability, ensuring investment protection and virtually unlimited growth
- Modularity, providing possibility to co-locate other functionality from the NewNet product suite
- Flexibility, ensuring easy adjustment to changing market requirements
- Reliability, ensuring correctness, completeness, consistency, and no loss of data
- Security, providing access control, fraud prevention and data protection
- Manageability, providing full system control, alarming, and reporting
- Interoperability, providing solutions with different hardware versions of the RTR
- Usability, providing easy-to-use command-line and GUI access
- Traceability and auditability, ensuring that all system activity can be diagnosed
- Accuracy, ensuring correct billing and providing revenue assurance

2.10 Operator Personnel Working with the RTR

Different aspects of the RTR's interfaces with related systems may require different operator personnel to interact with it. The following table summarizes personnel tasks and the type of application or tool that they would use.

Management Function	Carried Out By ...	Using ...
Configuring system set-up	System administrator	Command-line tools
Configuring network elements	OAM, planning, and design personnel	Command-line tools
Configuring networks, countries, and devices	OAM, planning, and design personnel	MGR
Identifying and configuring SNMP alarms	OAM personnel	MIB
Configuring SMS applications	Provisioning personnel	MGR
Configuring routing and counting rules	Provisioning personnel	MGR
Activating routing and counting rules	Authorized provisioning personnel	MGR

Management Function	Carried Out By ...	Using ...
Troubleshooting and tracing	OAM personnel	OS host and RTR command-line tools
View statistical counters	OAM, planning, and design personnel	MGR and STV (if available)
View audit logs	System administrator and security personnel	OS host command-line tools

2.11 Multi-Instance Support

Multi instance feature allows multiple NMM users (up to 10, including the existing `'textpass'` user) be created on the same node, each of whom will be able to run one instance of RTR.

Note: A separate LICENSE is required for each NMM user.

Chapter 3

Routing Entities

Topics:

3.1 Introduction

There are several entities that can be used as operands of the routing, counting, and external condition rules:

- Application-related entities:
  - Application—SMS application that can send and/or receive SMS messages
  - Group—Enables advanced throughput control per group of applications
  - Category—Enables application labelling across groups
  - Service class—Enables quality of service differentiation.
  - External condition application—Enables advanced message management
- SMSC-related entities:
  - Service centre specification of SS7 parameters
  - Service centre groups for load balancing over SS7
  - Service centre specification of IP parameters
  - Service centre node specification
  - Termination point specification per service centre node
- Country
- Network

Configure these entities using the MGR.

3.2 Application Group Entity

The application group entity is the RTR's grouping mechanism for SMS applications. It enables throughput control across all applications in the group. If differentiated application group throughput control is not required, all applications can be placed in a single default application group.

An application can only be a member of one application group.

For more information about configuring application groups, refer to the MGR Operator Manual.

Up to 1000 application group entities can be defined in the RTR.

In case the Throughput AT Maximum parameter is configured as zero (0) for all the member applications of an application group and the semi-static parameter discardoutboundatmsgwhenmaxthroughputiszero is set to "true", then all outbound AT messages and notifications destined for that application group will be immediately discarded by the RTR with a permanent error.

This logic would also apply when an AT message or notification is supposed to be first stored in the AMS, which would subsequently initiate a delivery attempt towards an application group. In such a case, before attempting to store the message or notification in the AMS the RTR will first check whether the maximum AT throughput values of all member applications of the destination application group are set to 0 and whether the parameter discardoutboundatmsgwhenmaxthroughputiszero is set to "true". If both these conditions are met, the RTR will immediately discard the AT message or notification with a permanent error instead of storing it in the AMS.

3.3 Service Class Entity

The service class entity is the RTR's quality-of-service mechanism for applications. The service class links outside listeners and/or applications to termination points (TCP connect ports) and protocol types. The service class also introduces an extra level of throughput control across applications within a service class. If differentiated quality of service is not required, all applications can be placed in a single default service class.

At least one service class must be defined before applications can be defined. An application must be a member of one or multiple service classes.

For more information about configuring service classes, refer to the MGR Operator Manual.

Up to 1000 service class entities can be defined in the RTR.

3.4 Category Entity

The category entity allows labelling of applications across application groups. Categories can be used in all types of rules to refer to a cross-group selection of applications. The category is an optional entity.

An application can be associated with multiple categories.

For more information about configuring categories, refer to the MGR Operator Manual.

Up to 1000 category entities can be defined in the RTR.

3.5 Application Entity

The application entity is the RTR and HUB's definition of an application. Before routing rules can route messages to an application, it must be defined and activated. You can create application templates for flexible default assignments.

UCP, SMPP, and CIMD2 applications are available.

Note: License settings determine which application types are available on a system.

The originator address of Incoming application-originated (AO) messages is typically a short number; however, it may be alphanumeric. To associate incoming AO messages with defined applications, you can set up to 10 alphanumeric aliases for each application (using the MGR). The RTR/HUB can then match a message to an application using the short number or the alias. This functionality ensures that these AO messages are handled correctly and that the RTR can accurately update counters for the application.

For more information about configuring applications, refer to the MGR Operator Manual.

Up to 1000 application entities can be defined. With an extended application license, up to 10,000 applications can be defined.

The HUB has two separate outside window size configuration options "**Outside SMPP Transmit window size**" and "**Outside SMPP Receive window size**". The range for both window size values is between 1 to 1024.

The default value for both Outside SMPP window size values is 255.

The range for Inside SMPP window size is from 1 to 1024.

In case the Throughput AT Maximum parameter is configured as zero (0) for an application and the semi-static parameter `discardoutboundatmsgwhenmaxthroughputiszero` is set to "true", then all outbound AT messages and notifications destined for that application will be immediately discarded by the RTR with a permanent error.

This logic would also apply when an AT message or notification is supposed to be first stored in the AMS, which would subsequently initiate a delivery attempt towards an application. In such a case, before attempting to store the message or notification in the AMS the RTR will first check whether the maximum AT throughput values of the destination application is set to 0 and whether the parameter `discardoutboundatmsgwhenmaxthroughputiszero` is set to "true". If both these conditions are met, the RTR will immediately discard the AT message or notification with a permanent error instead of storing it in the AMS.

3.6 SMSC Entity

The SMSC entity is the RTR's definition of an SMSC. Before routing rules can route messages to an SMSC, it must be defined and activated.

The following types of SMSCs are available:

- SMSC (SS7)—Service centre specification of SS7 parameters
- SC (IP)—Service centre specification of IP parameters:
  - Service centre (IP)
  - Service centre node
  - Termination point per service centre node
- SMSC group—For load balancing SC (IP) traffic

For information about configuring SMSCs, refer to the MGR Operator Manual.

This section provides more detailed information about the SMSC entity and SMSC load balancing.

3.6.1 SMSC (SS7)

The SMSC (SS7) entity allows definition of SS7 SMSCs.

For information about configuring SS7 SMSCs, refer to the MGR Operator Manual.

Up to 500 SS7 SMSCs can be defined in the RTR.

3.6.2 Service Centre (IP)

Service centres (IP) are used with the HUB in AO and AT routing rules.

For information about configuring service centres, refer to the MGR Operator Manual.

Up to 250 SC (IP) entities can be defined in the RTR.

3.6.3 SMSC Groups

SMSC groups provide an enhanced distribution scheme for load balancing toward SMSCs. The RTR sends all messages to the highest-priority SMSC in the group; if that SMSC is overloaded, the RTR begins to distribute messages to the other SMSCs in the group, in priority order.

For information about configuring SMSC groups, refer to the MGR Operator Manual. Up to 500 SMSC group entities can be defined in the RTR.

AO Message Distribution

If AO messages must be distributed over SMSCs with the same priority, the RTR takes the specification of how to retrieve a distribution key from the recipient address into account. The load balancing algorithm attempts to relay AO messages for the same recipient to the same SMSC.

After selecting the SMSC, the distribution scheme selects one session from those that have been established between the HUB and the SMSC, based on the following criteria:

- The session has the lowest number of pending AO messages
- If multiple sessions have an equal lowest number of pending AO messages, the selected session is the one that was the least recently used

3.6.4 Service Centre Node

Service centre nodes are used with the HUB in AO and AT routing rules.

For information about configuring service centre nodes, refer to the MGR Operator Manual.

Up to 500 node entities can be defined in the RTR.

3.6.5 Termination Points

Service centre node termination points (TCP/IP ports) are used with the HUB in AO and AT routing rules.

For information about configuring termination points, refer to the MGR Operator Manual.

Up to 1000 termination point entities can be defined in the RTR.

3.6.6 SMSC Selection

This section discusses SMSC selection.

3.6.6.1 SMSC (SS7) Selection

The RTR selects the SS7-SMSC using priorities and weights.

3.6.6.2 Session Selection for SC (IP) without an SMSC Group

The RTR selects the HUB-SMSC session without an SMSC group round-robin.

3.6.6.3 Session Selection in an SMSC Group

If an SMSC group is used, the RTR selects the HUB-SMSC session on the basis of a key. By default, the key is derived from:

- The recipient address, if it is an MSISDN
- The originator address, if the recipient address is a short number

To change the default key generation method, use the following parameters in the semi-static (XML) configuration file:

- `messagekeyweightsformsisdndestination`—Specifies the weights for computing a key when the destination is an MSISDN.
- `messagekeyweightsforshortnumberdestination`—Specifies the weights for computing a key when the destination is a short number.

Each parameter value consists of two weight lists that are separated by a colon:

- The weight list before the colon specifies the weights for the originator address.
- The weight list after the colon specifies the weights for the recipient address

Each list is a comma-separated list of unsigned integer weights. Each list may be empty.

Note: Only decimal digits and the comma character are allowed in the parameter value.

The RTR supports up to 20 weights per number. If a number has more digits than the number of weights that are specified for it, the remaining digits have a weight of 0 (that is, they have no effect).

The key is calculated as the weighted sum of the originator and recipient digits.

The following example illustrates the key generation for an AO message with an MSISDN recipient, when `messagekeyweightsformsisdndestination` is set to its default value.

```
For recipient 31653769834, the key is equal to:
 key = 1000*recip(0) + 100*recip(1) + 100*recip(2) + 1*recip(3)
 = 1000*4 + 100*3 + 10*8 + 1*9
 = 4389
```

3.6.6.4 Preferred SMSC

If an SMSC group is used, the RTR uses a concept of a preferred SMSC for HUB-SMSC session selection. To determine the preferred SMSC, the RTR considers the SMSCs that have at least one sessions with the HUB. Internally, the RTR places these SMSCs in a list that is ordered on SNMP index and gives each SMSC an ID, starting with ID 0.

The preferred SMSC is the one with an ID that equals:

```
<key> mod N
```

Where N is the number of SMSCs in the internal RTR list.

Normally, the RTR uses the preferred SMSC. However, the RTR may use a different SMSC if:

- The preferred SMSC is not available because of throughput control.
- The session that the RTR selected was disconnected before the AO message could be sent.

If the HUB maintains multiple sessions with an SMSC, the RTR uses these sessions in a round-robin fashion.

The following example illustrates session selection.

```
A configuration has two SMSCs: SMSC X and SMSC Y. The HUB maintains two
sessions with each SMSC: X1 and X2 with SMSC X, and Y1 and Y2 with SMSC
Y.

The RTR receives AO messages for the following recipient:

1. 31627091234
2. 31627092234
3. 31627093234
4. 31627093234
5. 31627095234
6. 31627091234

The keys for these messages are: 4321, 4322, 4323, 4323, 4325, 4321.

The preferred SMSCs are: SMSC Y, SMSC X, SMSC Y, SMSC Y, SMSC Y,
SMSC Y.

The sessions used are: Y1, X1, Y2, Y1, Y2, Y1.
```

3.6.6.5 Session Model Usage

A session model is a type of connection that determines how the RTR and HUB handle incoming connections. The following session models are supported:

Session Model	Description
Inside only	Inbound application sessions are not allowed
Outside only	The HUB will only set up inside sessions to the RTR (no service centres will be addressable)
Replicate	Inbound application sessions are replicated to each service centre (if capacity is not sufficient, more inside sessions are set up)
Duplicate	Inbound application sessions are distributed to each service centre (if capacity it not sufficient, more inside sessions are not set up)

For applications and/or service classes, a session model that replicates a session from the application to all SMSCs is recommended. In this model, the HUB establishes sessions to all SMSCs, regardless of the number of sessions between the HUB and the application.

3.7 Country Entity

The country entity is the RTR's definition of a country. Before routing rules can route messages based on country, all countries to which traffic will be routed must be defined. Country information is used as follows:

- RTR uses country information to route messages based on country (for example, routing all traffic from a certain country to one SMSC)
- Firewall (FWL) uses country information for MT spoofing checks
- Statistics Viewer (STV) uses country information to collect detailed statistics

Note: Many country entities are predefined in the MGR.

For more information about configuring countries, refer to the MGR Operator Manual.

Up to 500 country entities can be defined in the RTR.

3.8 Network Entity

The network entity is the RTR's definition of a network. Before routing rules can route messages based on network, all networks to which traffic will be routed must be defined. Network information is used as follows:

- RTR uses network information to route messages based on network (for example, routing all traffic from a certain network to one SMSC)
- STV uses network information to collect detailed statistics
- The Firewall (FWL) uses network information for MO and MT spoofing checks

For information about configuring network entities, refer to the MGR Operator Manual.

Up to 1000 network entities can be defined in the RTR.

3.8.1 Mobile Network Code Limitations

The RTR cannot discern if a mobile network code (MNC) has a length of 2 or 3 digits. Therefore:

- You cannot enter a 2-digit MNC for a country if a 3-digit MNC that starts with those digits is already defined for that country.

  For example, if a country already has an MNC of 987, you cannot enter an MNC of 98 for that country.
- You cannot enter a 3-digit MNC for a country if its first two digits are equal to a 2-digit MNC that has already been defined for that country.

  For example, if a country already has an MNC of 65, you cannot enter an MNC of 654 for that country.

Attempts to do either will be rejected with a masking detected error.

3.8.2 Own IMSI Table

The own IMSI table enables you to specify IMSI prefixes. If an IMSI matches a provisioned prefix, it is considered an "own IMSI". This table is used to:

- Prevent the forwarding service (XS-FWD) from being provided to non-HPLMN subscribers (both the B and C number). If the semi-static parameter `rtrskipsrismforunconditionalforwarding` is set to TRUE, then the semi static parameter `restrictforwardingtoownsubscriberbase` will restrict only the C number (forward recipient) for own subscriber, and there will be no restriction for the B number (original recipient) for Unconditional forward service (XS-FWD).
- Prevent the copy service (XS-CPY) from being provided to non-HPLMN subscribers (both the B and C number)
- Ensure that, when processing inbound, Home-Routed MT messages from a suspect SMSC to an IMSI that is not whitelisted, the RTR only accepts messages for non-HPLMN subscribers (that is, for inbound roamers). Messages for HPLMN subscribers should not be accepted because they should have been Home Routed. In this case, it is possible to prevent certain IMSI prefixes of the

own IMSI table from being considered "own IMSIs" by clearing the **Prefix applicable to suspect inbound MT traffic** option.

3.9 External Condition Application Entity

The external condition (EC) application entity is an application that can be associated with a rule condition. The EC application's result can determine if a rule evaluates to true. EC applications allow for advanced message management, such as prepaid charging or advanced message screening.

3.9.1 External Condition Attributes

For EC attribute entities, the following fields must be completed in the MGR:

Field	M/O	Description
Name	M	Name of this external condition attribute.
Description	O	Description of this external condition attribute.
Position	M	Identifies the bit position of the external condition attribute (bit 1 - 32).

Up to 32 EC attributes entities can be defined in the RTR.

3.9.2 External Condition Applications

For EC application entities, the following fields must be completed in the MGR:

Field	M/O	Description
Name	M	Unique name of the EC application.
Description	O	Description of the EC application.
User Identity	M	Identifier of the EC application for authentication, used during the application log in.
ECI Password	M	Password of the EC application, used for authentication during the application log in.
Client IP White List	O	List of allowed IP addresses of accepted EC clients for this EC application. If no IP addresses are provisioned for an EC application, all addresses are allowed.
Distribution Key Originator	O	Indicator that determines if the originator address should be used as key parameter to calculate the key-based load distribution. The key can only be selected if at least one IP address is provisioned in the client IP white list.
Distribution Key Recipient	O	Indicator that determines if the recipient address should be used as key parameter to calculate the key-based load distribution. The key can only be selected if at least one IP address is provisioned in the client IP white list.

Field	M/O	Description
Distribution Key Calling Party	O	Indicator that determines if the calling party SCCP address should be used as key parameter to calculate the key-based load distribution. The calling party SCCP address can contain any combination of the originator point code (PC) or the originator global title (GT). The key can only be selected if at least one IP address is provisioned in the client IP white list.
Modification Allowed	M	Indicator that determines if the EC application is allowed to modify any fields that are passed between the RTR and the EC application.
Max. Inactivity Time	M	The maximum time span in seconds that a session can be Idle before the RTR disconnects it.
Max. Response Time	M	The maximum time span in seconds, that the RTR waits for a response from a EC application before it considers the relating request as timed out.
Max. Sessions	M	The maximum number of sessions that the EC application can establish.
Throughput	M	Maximum throughput in SMS per second that can be sent to the EC application.
Originator Format	M	Transparent, national, international, or system-wide setting.
Recipient Format	M	Transparent, national, international, or system-wide setting.
MSC Format	M	Transparent, national, international, or system-wide setting.
SMSC Format	M	Transparent, national, international, or system-wide setting.
<list of defaults>	O	Default settings.
<list of fields>	O	All selected SMS Messages fields that should be passed to the EC application.

Before the EC application entity can be used, it must be activated. To activate an entity, select the tick box on the overview screen and click **Activate** on the **Action** menu.

When the entity's activation status has changed, the **Status** indicated will show the activated icon.

Before being able to modify an EC application, it needs to be deactivated first. To modify an EC application entity, click the entity entry on the overview screen, edit the corresponding fields (ID is unchangeable), and click **Save**.

Before removing an EC application entity, ensure that no active rules are associated with the entity. Verify this by sorting by entity on the **Rules versus EC Application** overview screen.

To remove an EC application entity, select the tick box on the overview screen and click **Delete** on the **Action** menu.

Up to 100 EC application entities can be defined in the RTR.

3.9.3 External Condition Messages

The RTR is able to generate messages based on the evaluation response from an EC application. These messages are called External Condition Messages (ECM).

The ECM will be generated when an ECI evaluation response is received from the EC application and when the following configurable conditions match:

- When enabled, the **Condition** field and the **Result Code** pair
- The **External Condition Result**
- The specific EC Application sending the response
- The original message type as specified in the **Enabled For** field

For any ECI evaluation response, the RTR generates at most one ECM.

When the RTR generates an ECM, the following parameters of the ECM can be configured:

- The message text template (supporting variable substitution)
- The message recipient
- The message originator (as shown to the recipient)

Currently, ECM cannot be sent to recipients whose number is a short code; therefore, ECM can be sent to mobile recipients (MT) only and not to applications (AT).

It is configurable whether the sending of an ECM suppresses the sending of the status report for the original SM. For example, if the ECM is sent because the original SM cannot be delivered, the status report of the original message should not be sent.

3.9.3.1 ECM MGR Configuration

For the EC messages entities, the following fields must be completed in the MGR:

Field	M/O	Description
Message Name	M	Unique name for the external condition message.
Match On	M	Specifies whether or not the Condition Field and Result Code fields should be checked. If the fields are not checked, the message is generated irrespective of the Field and Code constraint. Possible values: • Specific Field and Code (default) • All Results ECM entries that match on 'All Results' are evaluated after the evaluation of entries that match on a specific Field/Code pair.
Condition Field	M	Field against which the Result Code is checked to see whether or not a message shall be generated. Possible values: • Message Key (default)

Field	M/O	Description
		• Diameter Status
Result Code	M	Code that is checked to see whether or not a message shall be generated. Default is 0.
Specific EC Application	O	If this field refers to an EC application (external condition), the message is only generated if the ECI response comes from that EC application. By default, this field is set to All, which means that any EC application can trigger the generation of this message.
External Condition Result	O	A filter on the Boolean ECI evaluation result. Possible values: • Any (default) • True Only • False Only By default, this field is set to Any, which means that the message can be generated irrespective of the evaluation result.
Enabled For	O	A filter on the type of the original message. An external condition message can only be generated if this is enabled for the type of the original message. Check which message types shall be filtered. • 0 - MO Message • 2 - AO Message By default, no message type is enabled.
Message Template	O	This is a template for the message to be generated. A maximum length of 480 bytes or 160 Unicode characters is supported. The message template supports the use of the following variables: • `$(SCTS)`: Service center timestamp, indicating when the RTR accepted the message • `$(DESTINATION)`: The message's destination address. • `$(SOURCE)`: The message's originator address. • `$(CODE)`: Numeric value of the code input parameter. Example of a message template: `Your message to $(DESTINATION) was not sent, because your handset might be infected by a virus. Please report code $(CODE) to our Customer Care Center.` By default, no template is specified.

Field	M/O	Description
Message Originator	O	Specifies the originator address to be used for the generated message. The originator can be numeric (up to 20 digits), or alphanumeric (up to 11 GSM default alphabet characters). If the field is left empty, the RTR will use its common global title.
Message Recipient	O	Specifies the recipient of the generated message. Possible values: • Original Originator (default) • Original Recipient • Charged Party By default, this is the originator of the original message.
Suppress Status Report	O	Specifies whether or not an MT status report (or AT notification) is to be suppressed when an external condition message has been generated for the original message based on this table entry and prior to the generation of the status report or notification. By default this is not enabled, so suppression does not take place.

Note: Please note that the provisioned ECM entries with a smaller index have a higher priority.

Before the EC messages entity can be used, it must be activated. To activate an entity, select the tick box on the overview screen and click **Activate** on the **Action** menu.

When the entity's activation status has changed, the Status indicated will show the activated icon.

Before being able to modify an EC application message, it needs to be deactivated first. To modify an EC application message, click the entity entry on the overview screen, edit the corresponding fields (ID is unchangeable), and click **Save**.

Before removing an EC messages message, ensure that no active rules are associated with the entity. Verify this by sorting by entity on the Rules versus EC Application overview screen.

To remove an EC application entity, select the tick box on the overview screen and click **Delete** on the **Action** menu.

Up to 1000 EC message entities can be defined in the RTR.

3.9.3.2 ECM XML Configuration

The following parameters in the semi-static (XML) configuration file apply to ECM:

- `actionforexternalconditionfailuremessages`: Possible values can be:
  - route: route the ECM to the provisioned recipient. Retries are applied if the FDA fails.
  - store: store the ECM in the provisioned AMS queue.
  - routeFallbackToStorage (default): route the ECM to the recipient first. If the FDA fails, the ECM is stored in AMS.

- `externalconditionfailuremessagesamsqueue`: The AMS queue to store the ECM. The AMS is used if the `actionforexternalconditionfailuremessages` is set to store or routeFallbackToStorage.
- `maxretriesforexternalconditionmessages`: The maximum number of times that the Router retries delivery of the ECM.
- `retryintervalforexternalconditionmessages`: The interval between two consecutive retries for an ECM.
- `externalconditionmessagessentasflashsms`: If true, the ECM is sent as a flash SMS.

3.9.4 ECI Service Port

The external condition interface (ECI) uses a single TCP service port with number 9500, on which the Router listens. External applications must connect to this port. This port number is not configurable.

RTRs running from non-textpass user use ECI ports configured for them, to which applications can connect.

To view the current ECI port used by target NMM user, execute the following command at the command prompt on server (traffic element server or logging element):

```
/usr/TextPass/bin/tp_manage_user --info
```

For detailed information about `tp_manage_user` script, refer NMM Tools Operator Manual document.

3.9.5 ECI Application Load Balancing

The RTR load balances traffic to ECI applications using one of the following algorithms:

- Adaptive round-robin
- Key-based load distribution.

3.9.5.1 Adaptive Round-Robin

By default the RTR distributes messages in an adaptive round-robin fashion to the ECI application clients. Any ECI application client that connects to the RTR using the correct ECI login credentials is accepted by the RTR and added to the round-robin list of ECI evaluation request targets.

3.9.5.2 Key-Based Load Distribution

Key-based ECI load distribution directs ECI evaluation requests to specific ECI application clients based on the value of a user-defined key. The ‘key’ is derived from a configurable set of message parameters. The goal of key-based ECI load distribution is to send evaluation requests for messages with the same key to the same EC application client.

For example, an EC application that profits from key-based load distribution is the FAF. The FAF can detect flooding earlier if messages with a specific originator address are directed towards a specific FAF.

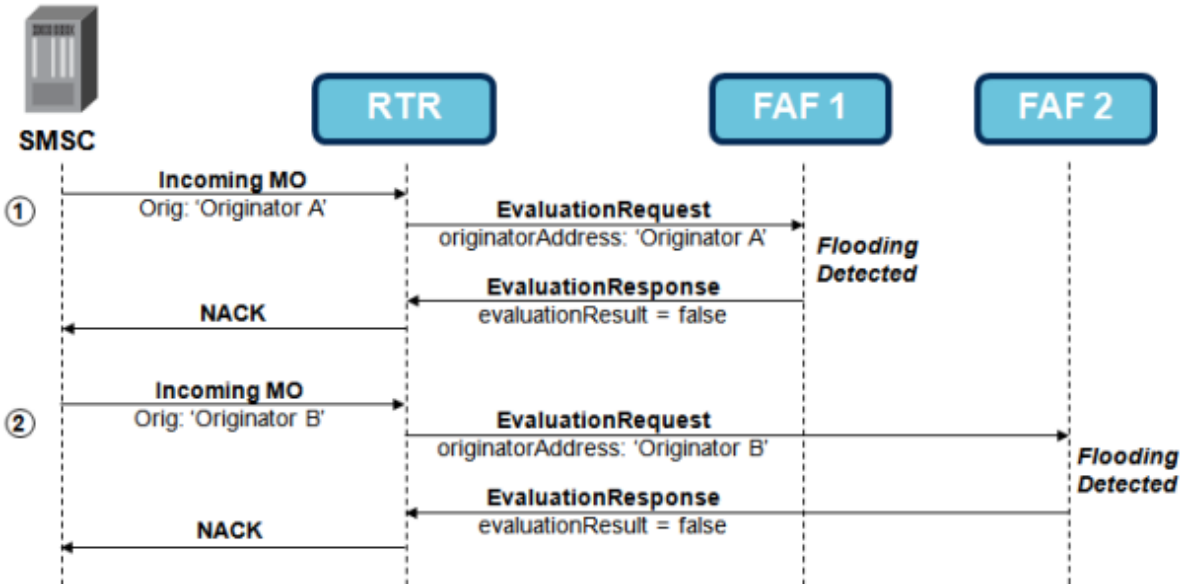


Figure 6: Key-based load distribution example

In this example, the RTR and two FAF clients are configured such that for flooding detection:

1. All SMs with originator address 'Originator A' are forwarded to FAF 1;
2. All SMs with originator address 'Originator B' are forwarded to FAF 2.

To use key-based ECI load balancing, the RTR EC Application must be provisioned with two sets of information:

- A list of ECI client IP addresses
- Message key parameters used to calculate the load balancing key

For key-based load distribution, the RTR maintains a *client IP address white list* for each EC application. An ECI client is identified by the EC application "user identity" and its IP address. Only the listed IP addresses in the client IP address white list are accepted and only ECI clients that connect from any of the white listed IP addresses can successfully log in to the RTR. The provisioned message key parameters are then used to direct the ECI request to one of those ECI clients.

If the client IP address white list is empty (default), all IP addresses are accepted and ECI clients are allowed to log in to the RTR from any IP address and normal round robin distribution is used.

The following key parameters can be used to calculate the load distribution key:

- *Originator address*: The RTR uses the whole originator address as the key.
- *Recipient address*: The RTR uses the whole recipient address as the key.
- *Calling party SCCP address*: The RTR uses the whole calling party SCCP address as the key. The calling party SCCP address can contain any combination of the originator Point Code (PC) or the originator Global Title (GT).
- *Dynamic*:
  - For MO and AO : ECI Load Balancing will be done using Originator as key;
  - For all other messages : ECI Load Balancing will be done using Recipient as key.

The key-based ECI load distribution is symmetric, which means that a combination of originator A and recipient B produces same key as originator B and recipient A.

The message key parameters and client IP address white list must be provisioned in the MGR. Refer to section 'Creating EC Applications' in the MGR Operator Manual for configuration details.

3.9.5.3 Round-Robin versus Key-Based Load Distribution

Round-Robin

For example, the RTR has an EC application configured with three ECI clients logging in to the EC application. The messages towards the ECI clients are round-robin distributed as follows:

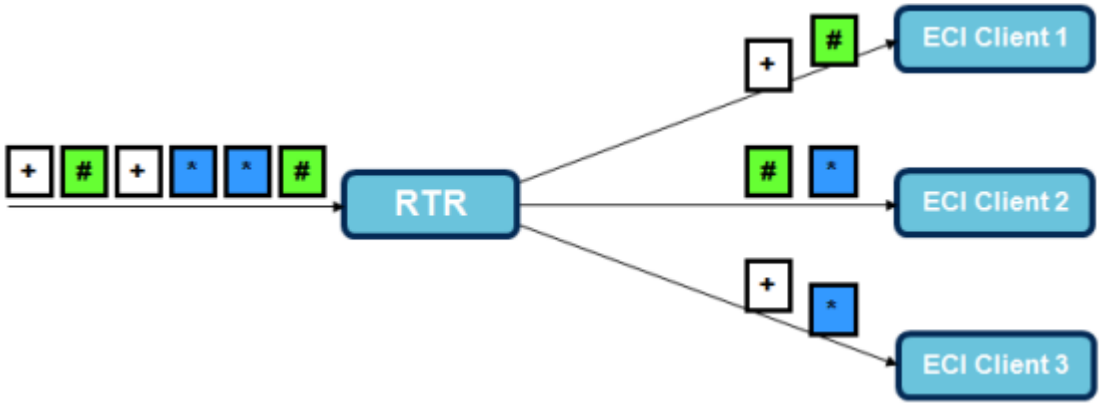


Figure 7: Round-robin load distribution

Now ECI client 1 fails. When round-robin load distribution is used, all the messages will be round-robin redistributed to the remaining two ECI clients.

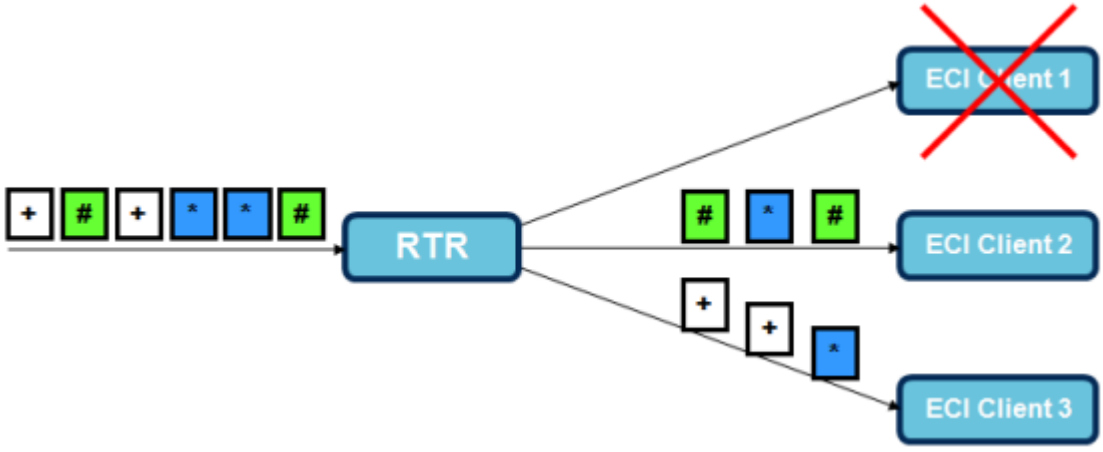


Figure 8: Round-robin load distribution with failed client

Key-Based

The messages towards the ECI clients are key-based distributed as follows. The messages with key '#' are distributed to ECI client 1, messages with key '*' are distributed to ECI client 2, and messages with key '+' are distributed to ECI client 3.

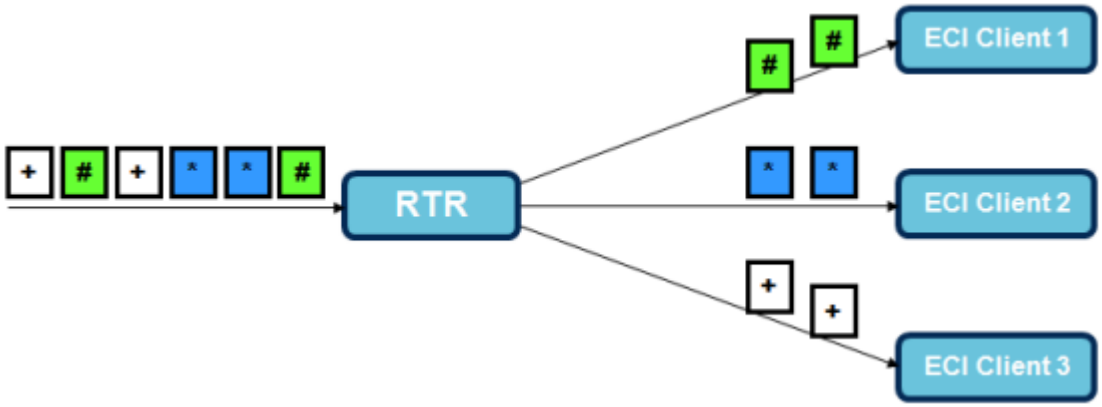


Figure 9: Key-based load distribution

Now ECI client 1 fails. When key-based load distribution is used, only the keys associated with ECI client 1 will be redistributed. In this example, only messages with key '#' are redistributed. Messages '*' and '+' remain distributed to the same ECI client as before.

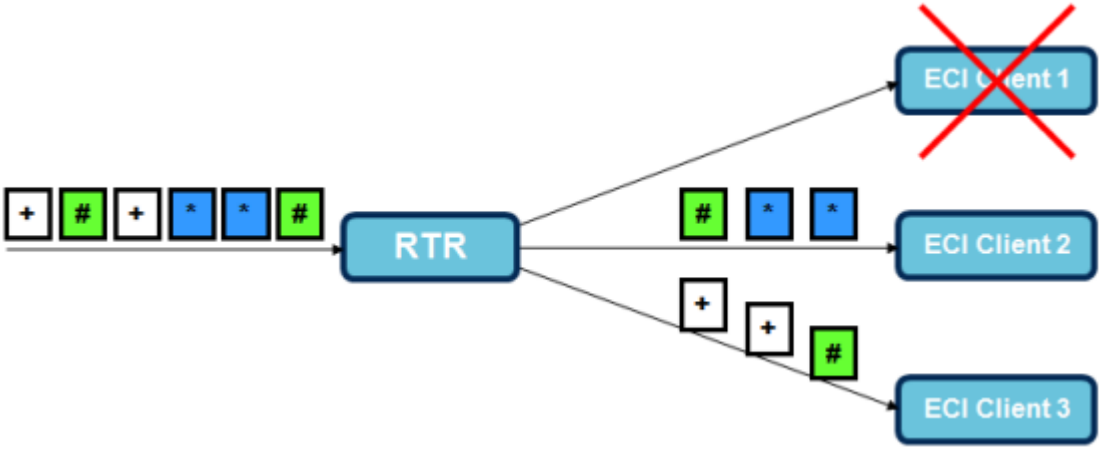


Figure 10: Key-based load distribution with failed client

Note: This simplified example assumes that messages '#' are redistributed to ECI client 2 and 3. When the keys of messages '#' are exactly the same they would both be redistributed to or client 2 or client 3.

When ECI client 1 reconnects again, the same messages ('#') get redistributed to ECI client 1 again.

Adaptive round-robin is used over all sessions of the ECI client.

3.9.5.4 ECI Client running in multi-instance mode

When multiple instances of an ECI Client are running on same server, then RTR does load-distribution in the same manner as ECI Client instances are running on separate server.

RTR maintains a list of ECI clients based on `hostid` and `uid` (operating system user identifier) and does load-distribution considering `hostid` and `uid`.

3.9.6 ECI Troubleshooting

The following syslog message:

```
proc_evaluation_rsp: no transaction pending for trn <number>
```

Indicates that the RTR received an ECI evaluation response with a sequence number (serverSequenceNumber) that is not related to any pending request toward an ECI application.

In this case, it is possible that an ECI application specified an invalid sequence number. However, it is more likely that the ECI application sent an evaluation response on a request that has already timed out.

3.10 Portable Applications

The RTR supports assigning of alias-MSISDNs to provisioned SMS applications, such that SMs addressed to such an alias-MSISDN can be routed to the corresponding application (as AT). This functionality supports UCP, SMPP, and CIMD connected applications.

An application referred to by an alias-MSISDN is referred to as *Portable Application*. Multiple alias-MSISDNs may be used for the same application.

An MT delivery (initiated by definition by an SMSC) is preceded by an SRI-SM operation towards the HLR. The HLR would not know the recipient MSISDN, as it refers to an application rather than to a mobile subscriber. For the MSISDNs provisioned as portable application, the RTR handles SRI-SM messages without forwarding the SRI-SM message to a HLR. This means that an IMSI range needs to be allocated for portable application MSISDNs similar to the SMS Firewall and SMS home routing functionality.

This functionality applies to the MO-AT and MT-AT routing paths.

Up to 10,000 portable application entities can be defined in the RTR.

Note: The total amount of portable applications and 'normal' applications cannot exceed 10,000.

Configuration

To configure the RTR:

- Alias-MSISDN routing to portable applications can be enabled/disabled globally per MGR domain for the MO-AT (and Store-variations) and the MT-AT path in the MGR using the **Enable Portable Application For MO** and **Enable Portable Application For MT** check boxes in **Routing ➤ Properties**.
- Portable applications are provisioned in the MGR (**SMS Applications ➤ Portable Applications**).

Refer to the MGR Operator Manual for more details.

Statistics

The RTR maintains the following portable application statistics:

Counter	Description
smsCntPortableApplicationSriSmSuccess	Counter specifying the number of times that an SRI-SM is successfully sent to a portable application.
smsCntPortableApplicationSriSmError	Counter specifying the number of times that an SRI-SM fails to be sent to a portable application.
smsCntPortableApplicationMtAtSuccess	Counter specifying the number of times that an MT-AT is successfully sent to a portable application.
smsCntPortableApplicationMtAtError	Counter specifying the number of times that an MT-AT fails to be sent to a portable application.
countryPortableApplicationSrismSuccessCounter	Per country counter, specifying the number of times an SRI-SM is successful for a portable application of this country.
countryPortableApplicationSrismErrorCounter	Per country counter, specifying the number of times an SRI-SM fails for a portable application of this country.
countryPortableApplicationMtAtSuccessCounter	Per country counter, specifying the number of times an MT-AT is successful for a portable application of this country.
countryPortableApplicationMtAtErrorCounter	Per country counter, specifying the number of times an MT-AT fails for a portable application of this country.
mobNetworkPortableApplicationSrismSuccessCounter	Per mobile network counter, specifying the number of times an SRI-SM is successful for a portable application of this mobile network.
mobNetworkPortableApplicationSrismErrorCounter	Per mobile network counter, specifying the number of times an SRI-SM fails for a portable application of this mobile network.
mobNetworkPortableApplicationMtAtSuccessCounter	Per mobile network counter, specifying the number of times an MT-AT is successful for a portable application of this mobile network.
mobNetworkPortableApplicationMtAtErrorCounter	Per mobile network counter, specifying the number of times an MT-AT fails for a portable application of this mobile network.
portableApplicationNumberMoMatchedCounter	Per a portable application entry counter, specifying the total number of times an alias-MSISDN in an MO/SM matches this a portable application entry.
portableApplicationNumberSrismMatchedCounter	Per a portable application entry counter, specifying the total number of times an alias-MSISDN in an SRI-SM request matches this a portable application entry.

Chapter 4

Personalized and Value Added Services

Topics:

4.1 Introduction

In the SMS network, personalized and also value added services are implemented using eXternal Service (XS) applications, which apply the services onto SMS sent or received by subscribers. The RTR allows the coupling of the XS applications into the message stream via a trigger interface.

Personalized services are services that enhance the subscribers SMS experience. Common reasons for operators to offer these services can be summarized as follows:

- Operators want to enhance customer loyalty by offering personalized services like copy of SMS, forwarding of SMS, blocking of unwanted SMS (black/white list) or to distribute an SMS to a group (distribution list).
- Operators are legally obliged to offer protection to subscribers from unwanted SMS (black/white lists)
- Operators might also want to earn extra money by charging for personalized services.
- Operators are able to offer reduced tariffs to subscribers that receive mobile advertisement, which targets the market segment of young mobile users.

A key feature of Personalized Services is the ability of subscribers to manage their personal service settings themselves, using their mobile or Internet access or with the assistance of the operator's customer service personnel.

The illustration shows the XS applications in combination with the RTR component, which contains the rule based logic to interface with the XS applications.

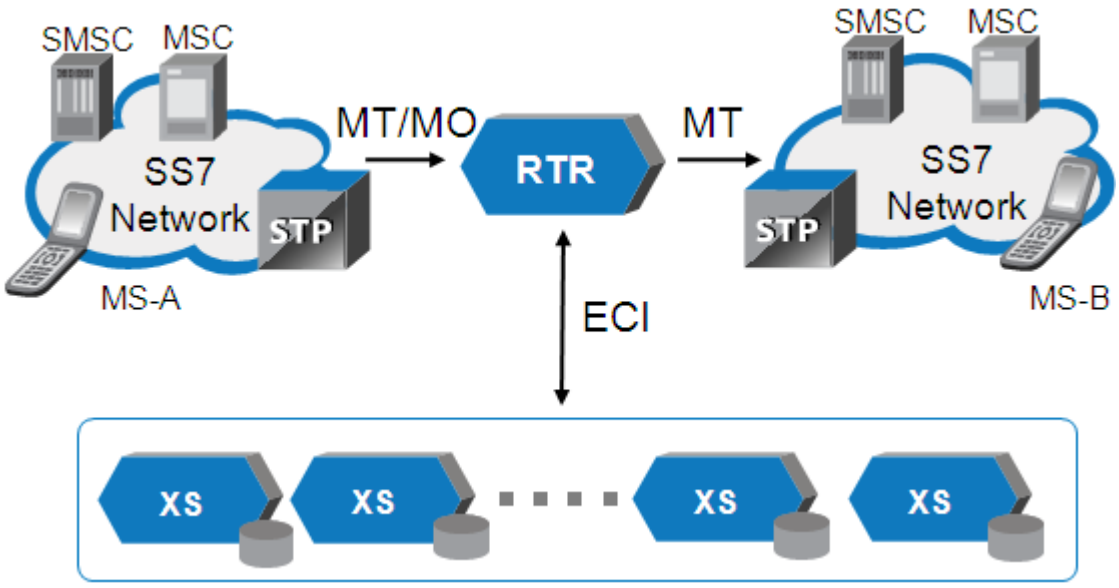


Figure 11: System Context

The interface between the RTR that handles the messages and the XS applications that host the various personalized and value added services is the ASN.1-based external condition interface (ECI). Based on rule logic (MOX/MTOX external condition rules), controlled by rule conditions on various message parameters, the RTR triggers the XS applications over the ECI for service execution on inbound or outbound messages.

The RTR has also access to the Service Subscription Information (SSI) which contains information about which services are active for the originator and the recipient of a message. SSI information can be used as a condition in any rule. For example, it can be used to decide whether an MT message should be home routed or not, or whether an XS application should be invoked to execute a personalized service.

The XS applications have locally stored subscriber service settings. The subscriber specific service settings are provided to the XS applications by the Service Provisioning Framework (SPF). Depending on the type of XS application, the service is executed by the application itself, or the instructions are passed back to the RTR for service execution.

Generally, all XS services work for single and concatenated SMS while preserving standard SMS features such as status report handling. Prepaid billing is supported for distribution list messages, copies and forwarding events using Diameter. Post-paid FCDR to charge for the use of personalized services are provided as well.

Note that an operator-controlled regulatory service like Auto Blacklist (ABL) does not have any XS-type application associated with it. Instead, the necessary service functionality is implemented through appropriately configured EC rules and Routing rules, which rely on the SSI information to determine whether any ABL service is active for an originator or recipient subscriber.

4.2 RTR Functionality

The RTR is needed for applying personalized services to SMS sent or received by a subscriber for the following reasons:

- The RTR is needed to tap into the message stream and make it available to the XS applications for service data lookup.
- The RTR is needed to execute services using the subscriber specific information provided by an XS application.

To provide *originator services*, the RTR needs to receive all MO messages submitted by the operator's subscribers. The RTR is connected to the operator's MSC possibly via an STP. In case the RTR receives an MO message, it might first do its Firewall (FWL) checks (if implemented as FWL with MO spoof check), it eventually does a prepaid check via the PBC before triggering the message details to the XS applications.

To provide *recipient services*, the RTR needs to get access to all MT messages directed to subscribers of the operator. If the RTR is combined with the FWL function, the RTR will first perform MT spoof checks and possibly use the Firewall Advanced Filter (FAF) before applying any personalized service to the MT message. The RTR always needs to home route messages coming from any foreign SMSC or from the operator's own SMSC. This is independent whether the receiving party roams in another network or not, since the RTR always needs to receive the MT message and correlate it with the corresponding preceding SRI-SM that contains the B-MSISDN for recipient service lookup.

4.3 Originator and Recipient Services

The RTR differentiates between *Originator services* and *Recipient services*:

- *Originator service* describes a service that is applied on behalf of the sender of a message, in other words, from the subscribers perspective, the service is applied to an SMS he/she sends. Typically, an originator service is applied to a successfully submitted (positively acknowledged) MO message.
- *Recipient service* describes a service that is applied on behalf of the receiver of a message, in other words, from the subscribers perspective, the service is applied to an SMS that somebody sends towards him or her. Typically, a recipient service is applied to an MT message.

The following table categorizes the personalized and value added services as originator and/or recipient service:

Service	Originator Service	Recipient Service
Copy to Phone (CPY)	Create a copy on behalf of the message originator (A-number). The message is only copied upon successful submission (originator received positive acknowledgment).	Create a copy on behalf of the message recipient (B-number). The message is only copied upon successful delivery.
Copy to Email (CTE)	Not applicable.	Create a copy on behalf of the message recipient (B-number) and send it towards e-mail addresses pre-provisioned by the concerned recipient subscriber. The message is copied only if it is successfully delivered.
Forward to Email (FTE)	Not applicable.	Forward an MT message on behalf of the recipient (B-number) to e-mail addresses pre-provisioned by the concerned recipient subscriber.
Copy to Application (CTA)	Create a copy on behalf of the message originator (A-number) and send it to an application, for example, the SMS archive that stores it in "Sent Items".	Create a copy on behalf of the message recipient (B-number) and send it to an application, for example, the SMS archive that stores it in "Inbox".
Forward (FWD)	Not applicable.	Forward the message to a third party (MSISDN), on behalf of the message recipient (B-number).
Black- and Whitelist (BWL)	Not applicable.	Reject the delivery of a message due to the combination of message originator (A-number) and recipient (B-number). On behalf of the B-party.
Distribution List (DIL)	Create a copy of the original message, which is addressed to a "list", to every member of that list, on behalf of the message originator (A-number). The original message is discarded.	Not applicable.
Text Insertion	Not applicable.	Insert a prologue and/or epilogue in the message text, on behalf of the message recipient (B-number).

Service	Originator Service	Recipient Service
Auto Reply (ARP)	Not applicable.	Send a personalized auto reply SMS, on behalf of the message recipient (B-number).
Signature (SIG)	Insert a personalized signature in the message text, on behalf of the message originator (A-number).	Not applicable.
Auto Blacklist (ABL)	Automatically blacklist the originator (A-number) of a spam/fraudulent /objectionable message and block all subsequent messages sent by that originating subscriber.	Automatically blacklist the intended recipient (B-number) of a spam/fraudulent /objectionable message and block all subsequent messages destined to that recipient subscriber.

4.4 License Dependency for Mobile-Terminating Traffic

When the XS application is applied to mobile-terminating (MT) traffic and is based on the recipient MSISDN, one of the following licensed features must be enabled:

- Home Routing;
- Anti-MT Spoofing.

When there are multiple MSISDNs per IMSI for the recipient, you must use the anti-MT spoofing feature to ensure that the RTR provides the correct recipient MSISDN to the XS application. When anti-MT spoofing is used, the traffic should be marked as *suspected*.

4.5 Service Subscription Information

The Service Subscription Information (SSI) functionality enables the RTR to query the SSI server to determine the applicable personalized subscriber services of the originator and recipient of the message. Based on those, the routing can be determined (for example, Home Routing) and the personalized subscriber services that need to be invoked. The information about the applicable services originates from the Service Provisioning Framework (SPF).

The main purpose is to restrict the number of external service triggers to those needed. When personalized subscriber services are only applicable to a small subset of the total traffic (which is typically the case), a large reduction in external service capacity required can be achieved. Another purpose is to make it possible to reduce Home Routing to only those messages for which there are recipient personalized subscriber services active.

The RTR functions as the SSI client and the SSI functions as the SSI server. Refer to the SSI Operator Manual for more information on the SSI server.

The following diagram illustrates the SSI and the SPF in the context of other Mobile Messaging components.

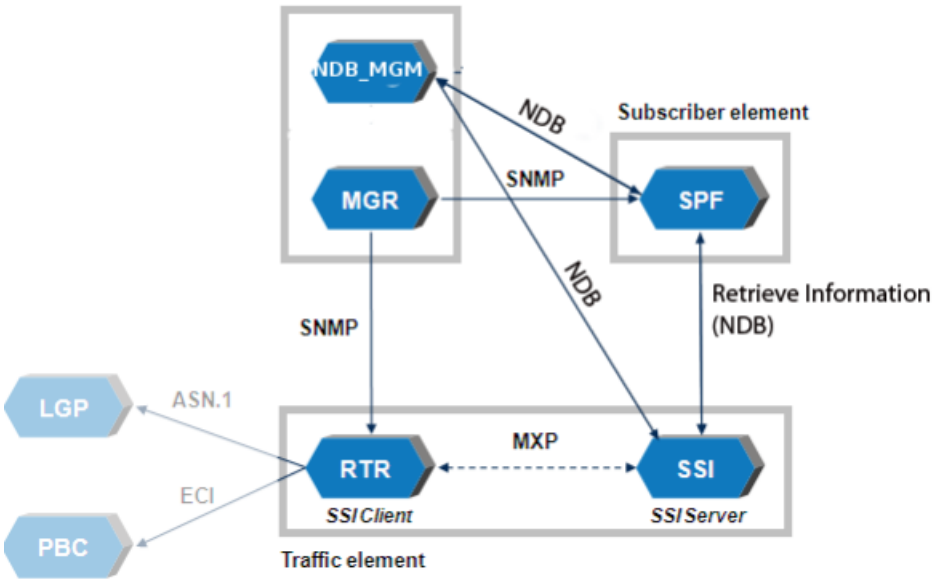


Figure 12: SSI System Context

The RTR communicates with the SSI server to retrieve the list of services for the originator and recipient of an SMS message.

The pool of available SSI servers is tracked using NewNet Mobile Messaging Network Layer (TNL). Each RTR uses its local SSI server, if available, and a remote SSI server otherwise. When there are multiple remote SSI servers, the RTR load balances using the one with the fewest outstanding requests.

If multiple instances of RTR and SSI are running on the same node, then each RTR (SSI client) first tries to select the local SSI server instance which is running under the context of the same user id as that of the RTR. If the local SSI server corresponding to the same user id is not available or is overloaded, then the RTR iterates through all SSI server instances running on other nodes and applies the same load-balancing procedure as described above for selecting a suitable SSI server.

Important: The data required by the SSI to respond to the RTR queries (i.e. active services information for a given subscriber) is actually stored on the reliable MySQL cluster of the SPF and is retrieved by the SSI through the efficient NDB API. Hence if a user chooses to alter or manipulate the relevant parts of the SPF database (which are accessed by the SSI) manually, it may lead to incorrect or invalid data being retrieved and effects of such an error may get propagated to the RTR and other components of the system.

Please take this into account when doing anything out of the ordinary.

4.5.1 Configuration

The SSI functionality is enabled through the *Subscriber Subscription Info* license entry of the RTR. When the SSI license is enabled (and one or more SSI servers are available), the RTR will perform SSI queries.

The `ssiqueriesenabled` parameter can be used to (temporarily) disable SSI queries. This can be done on a per-node basis (in the host-specific configuration file) or on a system-wide basis (in the common configuration file).

In case the retrieval of the SSI service information fails (e.g. disabled, no server, or error from server), it is configurable whether the requested service is available for any subscriber or not. This can be configured using the **Available When SSI is Unknown** checkbox on the MGR when defining an SPF service (refer to the MGR operator manual for more information). By default, the RTR assumes that no services are applicable.

CAUTION: Use this option with care. For example, when normally 2% of the traffic is effectively copied (subscriber has CPY service switched on) and send to the XS-CPY (using SSI in the EC rule), setting the CPY service to available when SSI information is unknown, 100% of the traffic will now go to XS-CPY. This is a 50x increase for which the XS-CPY might not be dimensioned.

The following EC application parameters control whether the list of *active* services should be sent to that EC application in the evaluation requests:

- **Inc. Originator SSI Services**
- **Inc. Recipient SSI Services**

A list of *requested* service IDs is generated by examining the SSI service condition (**Originator SSI** / **Recipient SSI**) in the external condition rule and the list of SSI services active for the subscriber who originated/receives the SM. The SSI service conditions work like a logical `AND` operation and perform a positive or negative test on one or more individual subscriber services.

An SSI service which is selected in the rule as a condition (by means of ☑) and is active for the SM is considered a *requested* service and is added to the list of requested service IDs:

- If the SSI rule condition itself is not inverted (by means of =,) only service IDs that are present in the SSI and have a positive match (by means of T) in the rule condition are put on the list.
- If the rule condition itself is inverted (by means of ≠,) only service IDs that are present in the SSI and have a negative match (by means of F) in the rule condition are put on the list.

The following EC application parameters control whether the generated list of *requested* service IDs (services that should be applied) should be sent to that EC application in the evaluation requests:

- **Inc. Masked Originator SSI Services**
- **Inc. Masked Recipient SSI Services**

These parameters are set on the MGR when defining the **EC Applications** for the service.

The routing rule conditions **Originator SSI** and **Recipient SSI** allow to configure positive or negative tests against a service. The conditions apply to MO, MTI, MTO, AO, ATI and ATO routing, counting, and external condition rules.

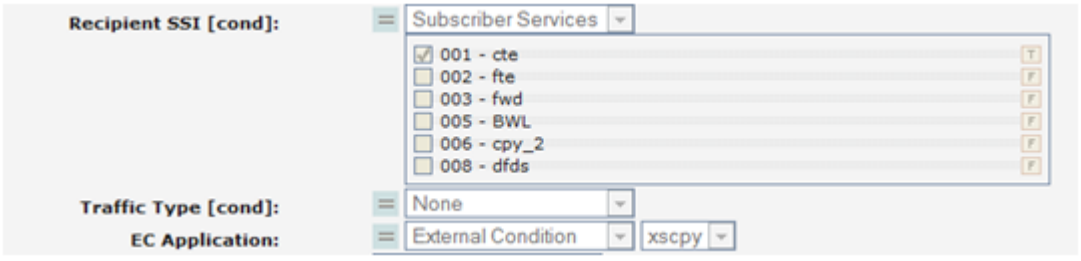
Refer to the MGR Operator Manual for more details.

4.5.1.1 SSI Condition Example

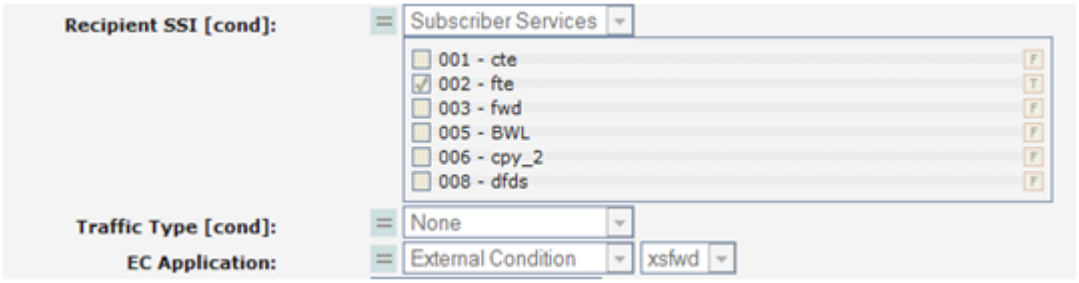
The following example shows how to invoke only recipient CPY irrespective of whether CTA is active or not using one MTOX rule (this in case different conditions should apply to invoke CPY or CTA services).

The following example shows how to invoke both recipient CPY and recipient CTA using one MTOX rule, in case both or either one of the two is active. This optimizes load on XS-CPY when most subscribers are using both CPY and CTA services.

The following example shows how to invoke recipient CTE using one MTOX rule:



The following example shows how to invoke recipient FTE using one MTOX rule:



4.5.2 Statistics and Logging

The RTR records the following statistics information about the number of SSI requests and how many were successful or not:

- `smsSsiCntTotal`
- `smsSsiCntSuccess`
- `smsSsiCntFailure`
- `smsSsiCntTimeout`

These statistics can be viewed on the Statistics Viewer (STV). Refer to the STV Operator Manual for more details.

The logging fields `originatorServices` and `recipientServices` will contain the service names in CSV format at the time of processing the SMS.

4.5.3 Billing

With respect to billing, the following fields can be included in the FCDR `CallDetailRecord` (for 'normal' messages), `OutboundMtMtRecord`, and `InboundMtMtRecord`:

- `originatorSsi`
- `recipientSsi`

These billing fields will contain the service names that are applicable to the SMS, in CSV format. These billing fields can be included in the FCDR by checking the **Inc. Originator SSI** and **Inc. Recipient SSI** fields in the billing profile.

4.6 Copy to Application Service

A given subscriber can have multiple services active upon his account. One of these services can be Copy to Application (CTA). When an SM from/to a subscriber enters the RTR, the RTR will obtain the list of services active for that subscriber (SSI query). The SM will then pass through the external condition rule stage in the RTR. External condition rules have a condition upon the SSI services active for the subscriber who originated/received the SM. If the external condition rule matches, the RTR sends the SM to the XS-CPY application for processing. The RTR also sends along with the SM a requested services list, generated by the RTR, that the XS-CPY application should apply to this SM.

The XS-CPY application then performs the appropriate processing on the SM. If it is that one or more of the requested services is CTA, then the XS-CPY application will in its `EvaluationResponse` to the RTR provide one copy request per copy that is to be made. The copy request specifies the short number to which a copy of the SM is to be sent, the requesting service ID and the copy service type.

The RTR notes in the state information it maintains for an SM whether or not that SM is internally generated (copies, forwards). If it is internally generated, then the RTR will not make any more copies of that SM *except* for CTA.

Example

For example, an external condition creates a copy to phone. If this copy hits an external condition rule which causes a copy to application to be generated, this will be permitted. But if it hits a rule which causes another personalized copy to be generated, this would not be permitted.

Related Semi-Static Configuration Attributes

The following related `tpconfig` configuration attributes apply:

- `outboundextcondrulesenabledforigsm`—Indicator specifying whether MTOX rules are applied to internally generated messages (for example, copy and forward).
- `copytoapplicationbinarydatasupportenabled`—Indicator specifying whether the CTA service will operate upon binary data short messages.

4.7 Copy Service

4.7.1 Copy Restrictions and Loop Prevention

The following copy restrictions are applied by the RTR:

- Copy to phone is only possible from mobile stations:
  - It is not possible to copy to phone on submitting/terminating application. It is possible to use an application as copy destination.
  - It is not possible to copy to phone Status Reports and SIM Data Download short messages. *
- To prevent loops, the following restrictions apply:
  - Copy to phone and forwarding cannot be combined. Forwarded messages cannot be copied to phone and copied to phone messages cannot be forwarded. **
  - Copied to phone message cannot be copied to phone again. When a short message of "X" has been copied to "Y", the short message will not be copied any further (even if "Y" has setup copy to phone). **
  - MSISDN being copied from (recipient-triggered copy) should be a HPLMN subscriber. **
  - MSISDN being copied to should be a HPLMN subscriber (or a Short Number assigned to an application). ***

Notes:

* AT-AT copy allows copying of SIM data download messages. For Copy to Application (CTA) it is configurable (`copytoapplicationbinarydatasupportenabled`).

** An exception applies to the Copy to Application (CTA) service. CTA can be applied to Copy to Phone (CPY) or Forwarded (FWD) messages if the receiving party has the CTA service activated.

*** The last two restrictions are controlled by the `restrictforwardingtoownsubscriberbase` attribute on the RTR. To prevent loops, it is strongly recommended to keep the default value for this attribute (`"true"`).

4.7.2 Billing Impact

Foreign SMSC (and local SMSC if not a NewNet Mobile Messaging SMSC):

- The recipient IMSI contains:
  - The B-IMSI in case the RTR/FWL acts in Home Routing mode
  - The scrambled IMSI in case the RTR/FWL acts in Anti-MT-Spoofing mode.
- The recipient MSC contains the RTR Global Title (GT).

NewNet Mobile Messaging billing:

- There is an additional delivery CDR generated for every copied message:
  - For recipient copy (to phone or to application), the recipient of the original message is indicated as the originator in the CDR and the copy destination as recipient.
  - For recipient copy to email, the recipient of the original message is indicated as the originator in the CDR and the E-mail Gateway application as recipient.
  - For originator copy, the originator of the original message is indicated as the originator in the CDR and the copy destination as recipient.
- The RTR may have setup some external attributes for copying. These are reflected in the FCDR `externalAttributes` field.

For more information about CDRs and configuring pre-paid billing for copied messages, refer to the NewNet Mobile Messaging RTR Billing Manual.

4.8 Forward Service

4.8.1 Forward Restrictions and Loop Prevention

The following forwarding restrictions are applied by the RTR:

- Forwarding is only possible to/from mobile stations.
  - It is not possible to forward MT messages to an application.
  - It is not possible to forward AT messages to a mobile station.
- To prevent loops, the following restrictions apply:
  - Forwarded message cannot be forwarded again. When “B” forwards to “C”, the short message will always be delivered to “C” (even if “C” has setup forwarding himself).
  - Copy to phone and forwarding cannot be combined. Forwarded messages cannot be copied and copied messages cannot be forwarded. *
  - MSISDN being forwarded from (“B”) should be a HPLMN subscriber. **
  - MSISDN being forwarded to (“C”) should be a HPLMN subscriber. **

  Notes:

  * An exception applies to the Copy to Application (CTA) service. CTA can be applied to Copy to Phone (CPY) or Forwarded (FWD) messages if the receiving party has the CTA service activated.

** The last two restrictions are controlled by the `restrictforwardingtoownsubscriberbase` attribute on the RTR. To prevent loops, it is strongly recommended to keep the default value for this attribute (`"true"`).

4.8.2 Unconditional Forward Services Handing for Forward to Phone (FWD)

`<recip MSISDN>` is the address of the message recipient.

`<fwd-to MSISDN>` is the address to which the message should be forwarded.

For Unconditional forwarding mode, the router does not attempt to deliver the message to `<recip MSISDN>` but it forwards the message immediately to `<fwd-to MSISDN>` instead.

Case: MO-Store-MT with unconditional XS-FWD service and 'rtrskipsrismforunconditionalforwarding' is false

In this case the RTR sends the SRI-SM request to `<recip MSISDN>` and after receiving the SRI-SM response, the RTR initiates the forwarding service.

The following points need to be considered for this scenario:

- If early SRI-SM is enabled Router applies the MTOX rule and then apply the MTOR rule over the SRI-SM message (if provisioned). After that Router sends the early SRI-SM request message.
- When the delivery of the message triggers from store, Router applies the MTOX rule and then apply the MTOR rule over the SRI-SM message (if provisioned) for `<recip MSISDN>` address.
- Router sends the SRI-SM message for `<recip MSISDN>` address.
- Router applies the MTOX and then MTOR rule over the MT FSM request message for `<recip MSISDN>` address.
- After that only RTR checks for the forwarding mode and if it's found to be Unconditional forwarding mode then Router sends the SRI-SM request message for `<fwd-to MSISDN>` address.

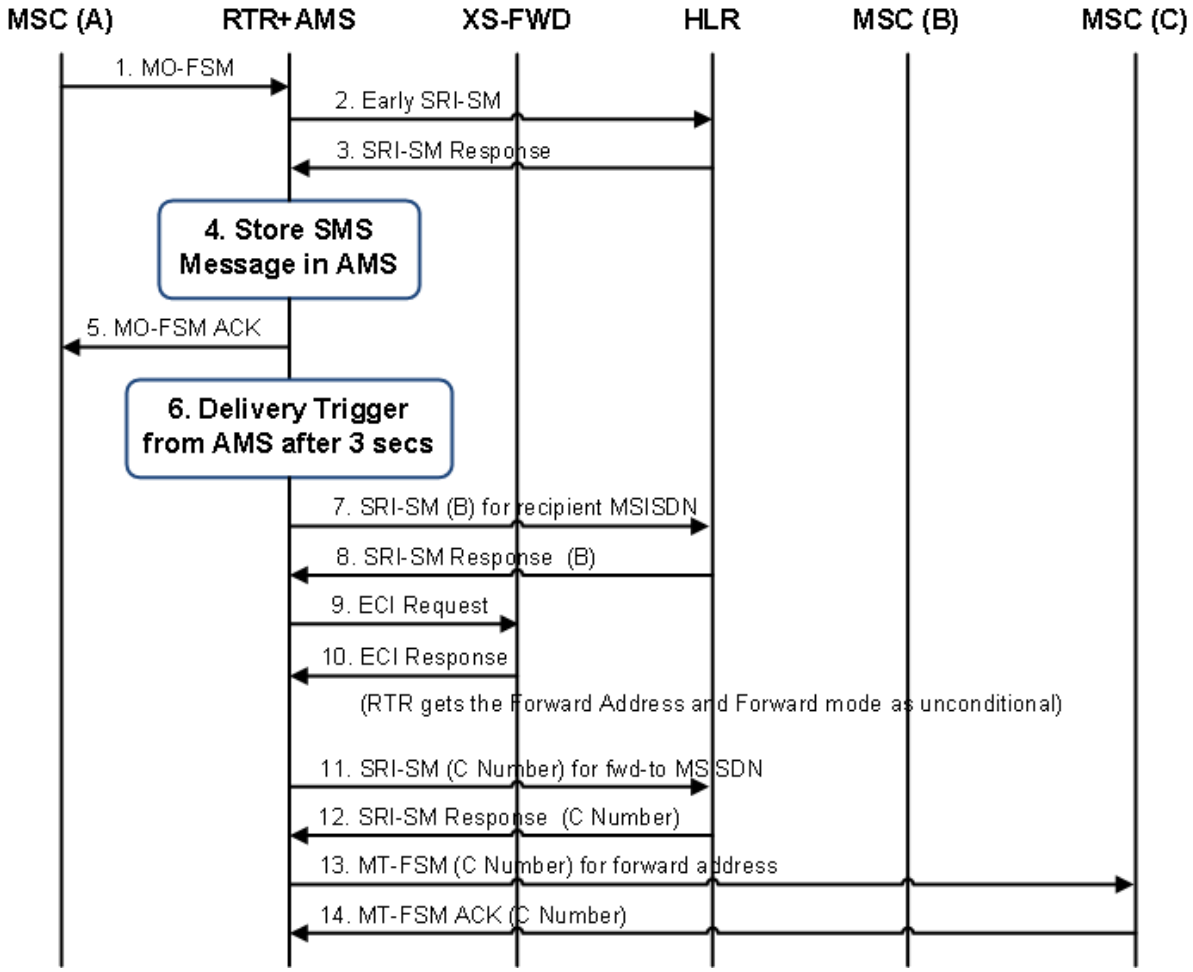


Figure 13: MO-Store-MT Scenario for unconditional XS-FWD service when rtrskipsrismforunconditionalforwarding is false

Case: MO-Store-MT with unconditional XS-FWD service and 'rtrskipsrismforunconditionalforwarding' is true

In this case RTR will not send the SRI-SM request to `<recip MSISDN>`.

The following points need to be considered for this scenario:

- If early SRI-SM is enabled, the router applies the MTOX rule and then applies the MTOR rule over the SRI-SM message (if provisioned). After that, the router sends the early SRI-SM request message.
- When the delivery of the message triggers from store, the router applies the MTOX rule and then applies the MTOR rule over the SRI-SM message (if provisioned) for `<recip MSISDN>` address.
- The RTR checks for the forwarding mode and if it's found to be Unconditional forwarding mode then the router sends the SRI-SM request message for `<fwd-to MSISDN>` address.

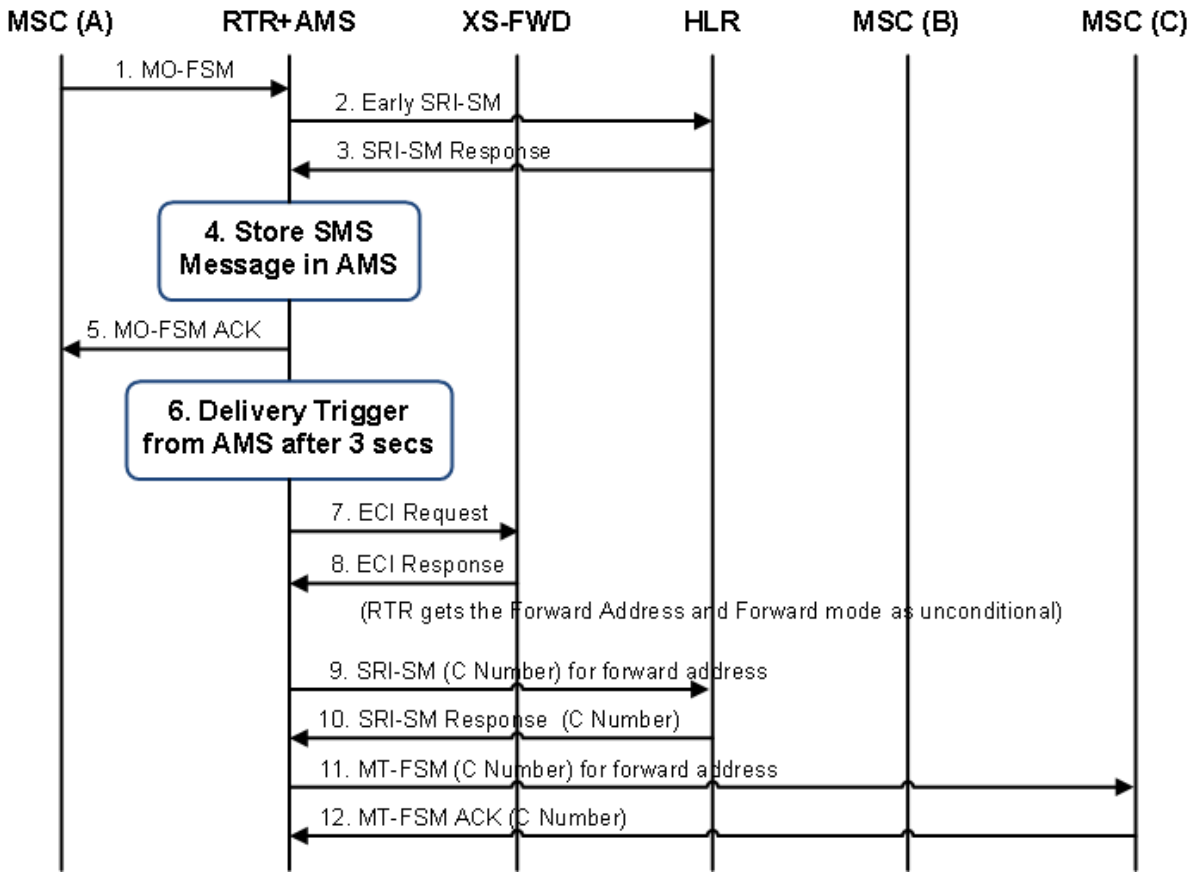


Figure 14: MO-Store-MT Scenario for unconditional XS-FWD service when 'rtrskipsrismforunconditionalforwarding' is true

Case: MO-Store-MT with unconditional XS-FWD service and 'rtrskipsrismforunconditionalforwarding' is true and Forwarded MT Message Failure with temporary error

In this case the RTR will not send the SRI-SM request to `<recip MSISDN>` and also as the MT-FSM for `<fwd-to MSISDN>` address fails with temporary error, the RTR will send the `destinationTempError` to the AMS and the AMS retries the message.

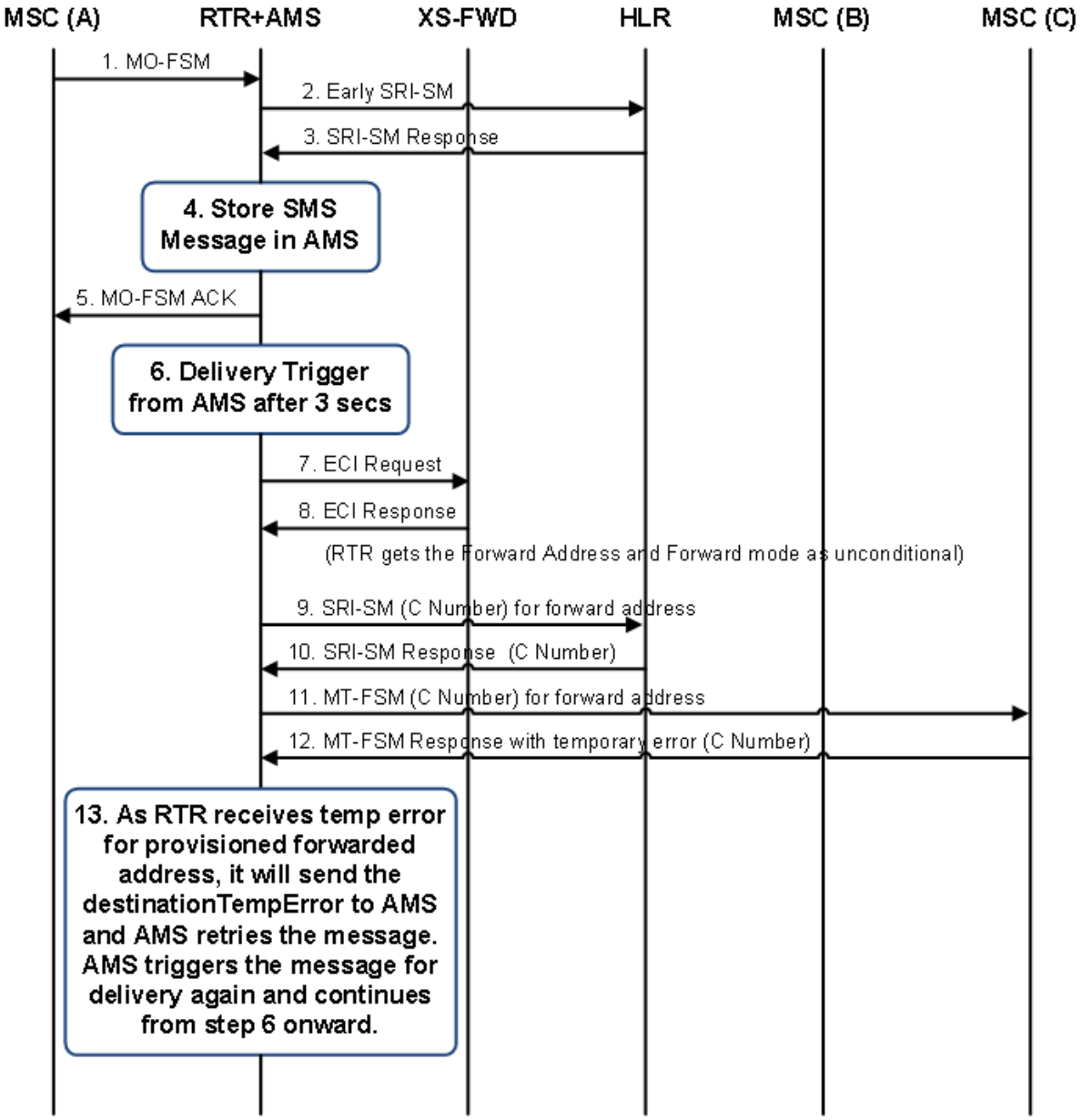


Figure 15: MO-Store-MT Scenario for unconditional XS-FWD service when rtrskipsrismforunconditionalforwarding is true and Forwarded MT message Failure with temporary error

Case: MO-Store-MT with unconditional XS-FWD service and 'rtrskipsrismforunconditionalforwarding' is true and Forwarded MT message Failure with permanent error

In this case the RTR will not send the SRI-SM request to `<recip MSISDN>` and also as the MT-FSM for `<fwd-to MSISDN>` address fails with permanent error, the RTR will send the `destinationPermError` to the AMS and the AMS will delete the message.

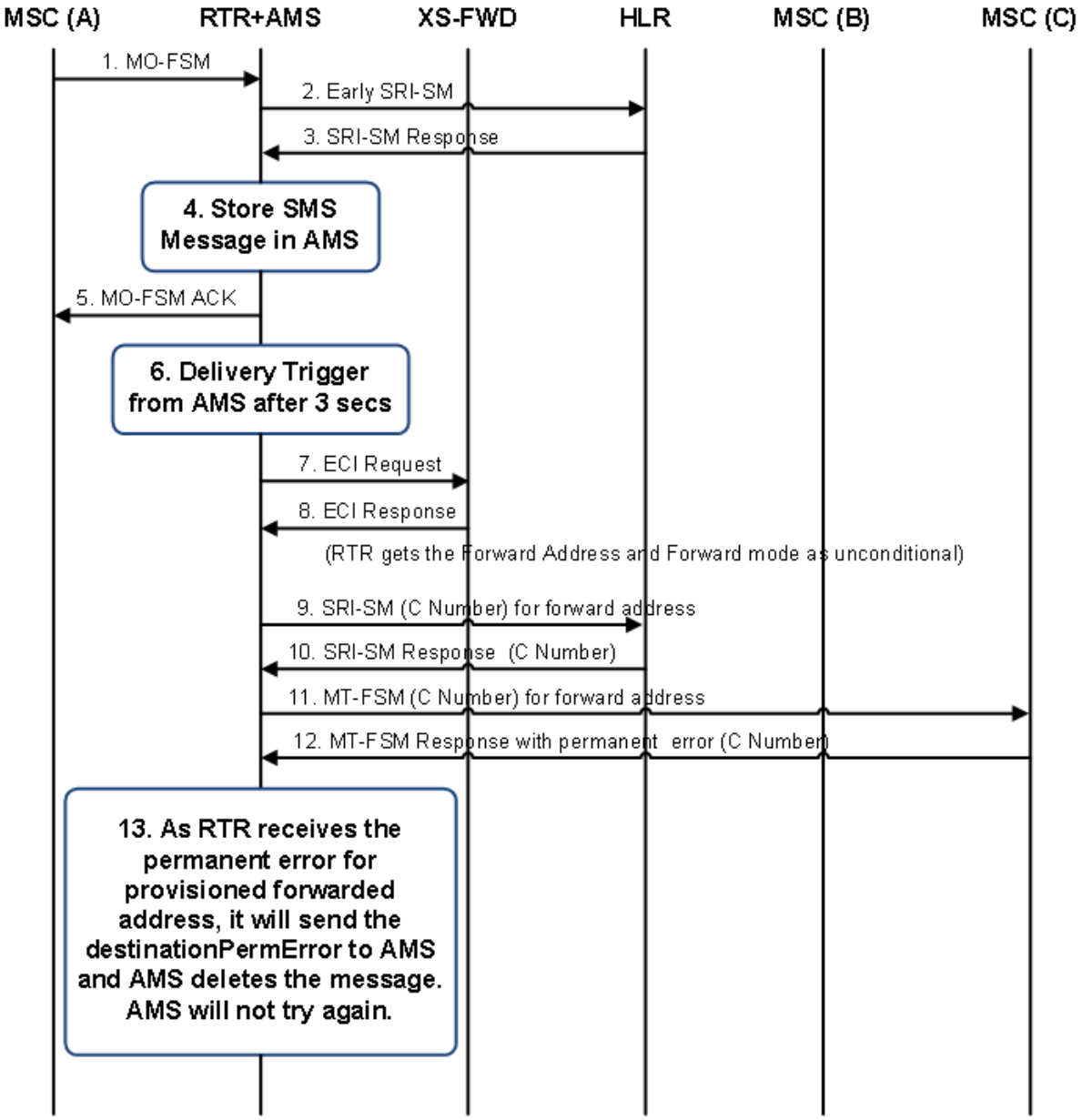


Figure 16: MO-Store-MT Scenario for unconditional XS-FWD service when rtrskipsrismforunconditionalforwarding is true and Forwarded MT message Failure with permanent error

Note: The behavior will be same in case of SRI-SM failure with temporary error or permanent error as in the case of MT failure as explained above (when the semi-static parameter `rtrskipsrismforunconditionalforwarding` is set to true).

Case: AO-Store-MT with unconditional XS-FWD service and 'rtrskipsrismforunconditionalforwarding' is true

In this case the RTR will not send the SRI-SM request to `<recip MSISDN>`.

The following points need to be considered for this scenario:

- If early SRI-SM for AO is enabled, then the router applies the MTOX rule and then applies the MTOR rule over the SRI-SM message (if provisioned). After that, the router sends the early SRI-SM request message.
- When the delivery of the message triggers from store, the router applies the MTOX rule and then applies the MTOR rule over the SRI-SM message (if provisioned) for `<recip MSISDN>` address.
- The RTR checks for the forwarding mode and if it's found to be Unconditional forwarding mode then the router sends the SRI-SM request message for `<fwd-to MSISDN>` address.

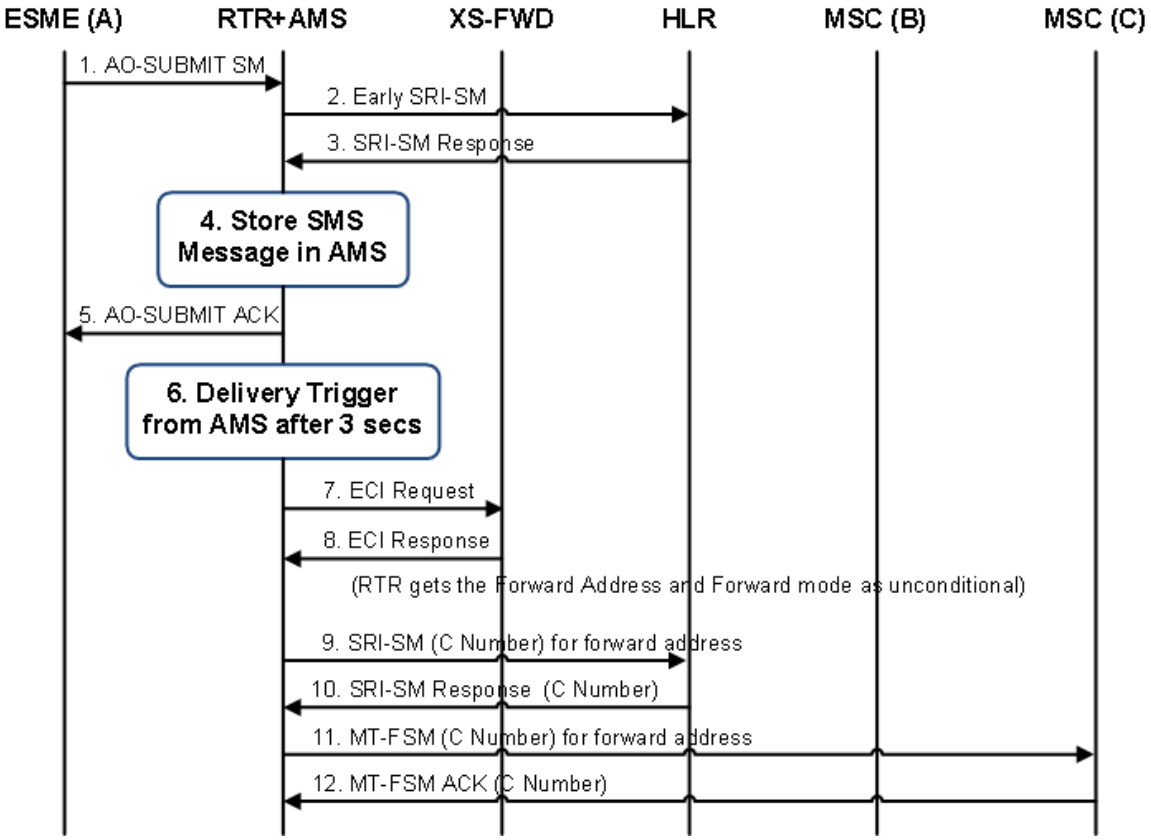


Figure 17: AO-Store-MT Scenario for unconditional XS-FWD service when rtrskipsrismforunconditionalforwarding is true

4.8.3 Billing Impact

Foreign SMSC (and local SMSC if not a NewNet Mobile Messaging SMSC):

- The recipient IMSI contains:
  - The B-IMSI in case the RTR/FWL acts in Home Routing mode
  - The scrambled IMSI in case the RTR/FWL acts in Anti-MT-Spoofing mode.
- The recipient MSC contains the RTR Global Title (GT).

NewNet Mobile Messaging billing:

- There is an additional delivery CDR generated for forwarded messages with the original recipient as originator. In the case of FWD the forward destination is used as recipient, whereas in the case of FTE the EMG application is considered as recipient.
- When the SM has been forwarded from "B" to "C" (FWD service):
  - The recipient MSC contains the C-MSC
  - The recipient IMSI contains the B-IMSI.
- The FCDR `nser` field's `fwad` and `fwad-cond` flags are supported.
- The RTR may have setup some external attributes for forwarding. These are reflected in the FCDR `externalAttributes` field.
- The semi-static parameter `rtrdefaultrecipimsiforfcdr` will be used to configure a Default B-IMSI (i.e. Dummy recipient IMSI)
  - If the actual B-IMSI is available, it is filled in for `intlMobileSubId` in the FCDR.
  - Else if not available due to Early SRI-SM being skipped or failing and default recipient IMSI configured in `rtrdefaultrecipimsiforfcdr`, then the default IMSI will be inserted in intlMobileSubId in the FCDR
  - Else intlMobileSubId is not included in the FCDR at all.

For more information about CDRs and configuring pre-paid billing for forwarded messages, refer to the NewNet Mobile Messaging RTR Billing Manual.

4.9 Auto Reply Service

The Auto Reply (ARP) service supports automatic generation of short messages on behalf of the recipient of the *original* SM, informing the originator of the original SM about a certain status of the recipient. For example, the recipient may be unreachable for a while. He can then use the ARP service to inform people trying to send him an SM about his inability to respond to an SMS or even receive it.

The ARP service is supported for Phone-to-Phone (P2P) traffic only.

To provide a working ARP service to subscribers, multiple Mobile Messaging components need to successfully interact. Basically, the RTR handles the original SM. It contacts the XS-ARP component to see if an ARP message should be generated. The XS-ARP component relies on the SPF component to indicate if for this original SM, at the present time, an ARP message should be requested. If so, it requests the RTR to generate an ARP message with a certain text and validity period.

4.9.1 ARP Message Generation

This section describes how to configure the RTR component to support the ARP service. ARP messages are generated upon request from an EC application, specifically, the XS-ARP application. How and when to generate an ARP message depends on the routing path taken by the original SM through the RTR.

XS-ARP applications must be configured using key-based ECI load distribution in order to let the caching function of XS-ARP work correctly (refer to *Key-Based Load Distribution*).

4.9.1.1 Inbound MO Traffic

To generate ARP messages for inbound MO messages, an MOX rule needs to be setup, triggering an ECI evaluation request towards the XS-ARP EC application. In its ECI evaluation response, XS-ARP may request the RTR to generate an ARP message. The RTR will only generate the ARP message when the inbound MO message is accepted, in other words, when a successful response is sent back to the MSC or SGSN.

An MO message may be segmented. To prevent that an ARP message is received by the MS sending the original SM before all segments have been submitted, the MOX rule for contacting XS-ARP should have the **Message Segments** condition specified such that it only matches for non-segmented messages or last segments. This can be achieved by selecting the fields for first and middle segments, and inverting the condition.

4.9.1.2 Inbound AO Traffic

To generate ARP messages for inbound AO messages (for example, P2P SMS sent by subscriber's of another operator via inter-carrier connect (SMPP)), an AOX rule needs to be setup, triggering an ECI evaluation request towards the XS-ARP EC application. In its ECI evaluation response, XS-ARP may request the RTR to generate an ARP message. The RTR will only generate the ARP message when the inbound AO message is accepted, in other words, when a successful response is sent back to the originating application.

4.9.1.3 Inbound MT Traffic

To generate ARP messages for inbound MT messages (for example, P2P messages from foreign subscribers), the MT messages need to be intercepted (Home Routed) (refer to *MT Routing*). In addition, an MTIX rule needs to be setup, triggering the ECI evaluation request towards the XS-ARP EC application. In its ECI evaluation response, XS-ARP may request the RTR to generate an ARP message. If it does so, the RTR will generate the ARP message independent of the delivery outcome of the original SM.

For concatenated inbound MT messages, optionally, ARP can be triggered on the first segment only. This is in case there are multiple sites and message segments can end up at different sites. The same applies to concatenated AO messages coming from an inter-carrier SMPP gateway.

To avoid delivery collisions between a Status Report associated with the original SM and the ARP message, it is possible to delay the processing and delivery of the ARP messages for MT messages by a few seconds. This can be achieved by setting the semi-static configuration attribute *delayforautoreplytomtmessage* to the desired number of milliseconds. By default, no delay is applied.

To *force* the original message to be Home-Routed, it may be desirable to ensure that the Priority flag of the SRI-SM request forwarded to the HLR is set to 1. This can be achieved with the following configuration:

1. Create and activate an MTO Modifier, but don't set any fields for modification.
2. Create an MTOR rule with an action of *pass*, a message type condition to only match for SRI-SM requests and optionally additional conditions if the set of to-be-home-routed messages should be limited in any way. Refer to the MTO Modifier from this MTOR rule.

This configuration has the effect that the SRI-SM request towards the HLR gets re-build, thereby setting the Priority field to 1.

4.9.2 ARP Message Regulation

The RTR supports a few configuration parameters to control the rate at which ARP messages are generated. The semi-static configuration attribute *maxnumarpspersecond* can be used to limit the number of ARP messages a single RTR instance is allowed to generate per second. By default, this limit is set to 100. This setting makes sure that consecutive ARP are not generated faster than one per 10 milliseconds (1 second/100).

If ARP messages are requested faster than the RTR is allowed to generate them, the requests are queued temporarily. There is an upper limit on the number of temporarily queued messages, which can be controlled through the semi-static configuration attribute *maxnumpendingarps*. By default, this limit is set to 1000. If the number of temporarily queued ARP messages surpasses 80% of that limit, the RTR generates an `arpConcurrentTransactionsHighWaterTrap` SNMP trap. Subsequently, if the number of temporarily queued ARP messages drops below 60% of that limit, a corresponding `arpConcurrentTransactionsLowWaterTrap` SNMP trap is issued. The high water traps are generated no more frequently than once per 60 seconds. If the upper limit for temporarily queued messages is exceeded, excess ARP requests are dropped. Refer to the NewNet Mobile Messaging SNMP Trap Reference Guide for more information on these traps.

4.9.3 ARP Message Processing

Generated ARP messages are processed by the RTR's logic for processing *internally generated SMs*. Refer to *IGM Routing* for more information.

4.9.4 Billing

Most of the RTR's mechanisms for billing ARP messages are described in the chapter on internally generated SMs.

Specifically for ARP messages, and on top of the mechanisms provided by the processing of internally generated SMs, the generation of CDRs can be enabled or disabled through the semi-static configuration attribute *billingforautoreplymessages*. By default, the generation of CDRs for ARP messages is disabled.

4.9.5 Logging

The RTR writes an event record for each generated ARP message. The ARP event record can be correlated to the event record of the original message that initiated the ARP message. The ARP event record contains the name of the XS-ARP application that requested the ARP generation:

Event	Description
smAutoReplied	An auto reply (ARP) message has been issued for this short message.
autoReplyCreated	An ARP message has been created.

4.9.6 Statistics

Internally generated message counting (IGMC) rules can be used for counting the delivery result of ARP messages.

Available ARP service counters in the RTR:

Counter Name	Description
arpCntRequestsReceived	Counter specifying how many ARP requests have been received.
arpCntRequestsGranted	Counter specifying how many ARP requests have been granted.
arpCntRequestsWithCookieReceived	Counter specifying how many ARP requests have been received, which included an ECI Service Notification Request Cookie.
arpCntRequestsDiscarded	Counter specifying how many ARP requests have been discarded as the RTR never converted the ARP request into an ARP message. For example, this can happen if the original message got rejected.
arpCntInvalidRequests	Counter specifying how many ARP requests have been received, that did not comply with the ECI ASN.1 definition.
arpCntRequestsDroppedDueToUnsupportedText	Counter specifying how many ARP requests have been received, that were dropped because they contained text that could not be processed successfully.
arpCntRequestsDroppedDueToThroughputLimitation	Counter specifying how many ARP requests have been received, that were dropped due to throughput limitations, as determined by *maxnumpendingarps*.
arpCntRequestsDroppedDueToMemoryShortage	Counter specifying how many ARP requests have been received, that were dropped due to memory shortage.

4.10 Signature Service

The personalized SMS Signature (SIG) service allows a subscriber to configure a personal signature and have it automatically added at the end of SMS he or she sends to other mobile subscribers.

The RTR queries the XS-SIG application for every segment in order to be able to calculate the correct amount of extra segments that have to be added to insert the signature at the end of the last segment. The UDH has to be adjusted for each of the segments to account for the extra segments that will be appended.

Note: If during the processing of a segmented message, the signature related provisioning data changes such that XS-SIG provides different results for different message segments, correct reassembly of the message cannot be guaranteed.

Signature insertion is supported for ECI evaluation requests triggered by MOX and AOX rules, and for all possible routing paths for those messages.

Note: The RTR does not insert a signature into messages with binary content (DCS value).

When a signature is provided for a message and the signature encoding varies from the message encoding, the RTR must choose whether to drop the signature or to try to convert the encoding. This behavior can be configured by the semi-static configuration attribute *sigencodingmismatchbehavior*. By default the signature will be converted.

Also the behavior when a signature is provided for a message for which the recipient is a short number can be configured by the semi-static configuration attribute *sigshortrecipientbehavior*. By default the signature will be omitted.

When the RTR inserts a signature it immediately becomes part of the message content. Therefore later operations on the message text will also encounter the signature text, for example, when processed by the FAF. This also applies to evaluation requests for lower-priority external condition rules than the rule that triggered the signature request and insertion. The inserted signature will be inherited by copied and forwarded messages.

4.10.1 Billing

Post-paid Billing

The RTR includes an indication that a signature has been inserted in the proprietary `signaturePresent` FCDR field in the CDR that pertains to the original SM and the service CDR that pertains to the SIG service. For segmented messages, this indication will be set only in the CDRs for the last segment.

The following parameters specify which billing profiles will be used for generating service CDRs for when the SIG service has been applied to a message. These parameter are configurable on the MGR (**Billing Post-paid Billing Properties**):

- **Profile For Successful Signature**—refers to the billing profile to use if the message with the inserted signature was delivered successfully
- **Profile For Failed Signature**—refers to the billing profile to use if the message with the inserted signature could not be delivered.

The service CDRs also apply to messages temporarily stored in the AMS, or tracked by means of the Icache. No service CDR will be generated if the signature was requested, but could not be inserted into the original message.

Prepaid Billing

Signature insertion must happen before online charging by the PBC (by means of the external condition rule priority). The evaluation request to the PBC indicates that signature insertion has been requested. In the case of a segmented message, this indication will only be included for the last segment of the message. If prepaid charging fails, the original message/segment is supposed to be rejected, inherently preventing the SIG service from being provided.

Note: Actual (extra) charging for the SIG service depends on the capabilities of the actual protocol used for online charging. There is no support for CAMEL charging of the SIG service.

4.10.2 Logging

The event of inserting a signature into a message is accompanied with an event record:

Event	Description
signatureInserted	A signature (SIG) has been inserted to an (inbound) SM.

4.10.3 Statistics

Available SIG service counters in the RTR:

Counter Name	Description
sigCntSignatureInsertion	Counter specifying the number of signatures inserted.

4.10.4 Processing of Multi-part MT Messages after Text/Signature Insertion

If text/signature insertion is applied on a MT message, the resulting size of the user data may become too long to fit within a single GSM message. Below steps describe how such a message is handled by the RTR.

- Once the relevant text/signature is inserted, the RTR determines the new user data size of the original message.
- Note that the original message in this scenario could be either a non-segmented MO/AO message or a single segment of a concatenated MO/AO message. In the latter case, the 'prologue' part of the text (if configured in XS-TIE service) would be inserted only if it is the first message segment and the 'epilogue' part of the text (if configured) would be inserted only if it is the last message segment.

  The signature would be inserted only in the last message segment.
- If the size of the user data is increased such that the message can no longer be delivered as a single MT message, it is split up into multiple parts.
- The RTR performs segmentation of the original user data of the long message and creates a concatenated MT message as per the GSM standard.
- The RTR then delivers the multiple parts of the concatenated MT message in succession.
- If **Transactional Logging** is configured in the matched MTOR, a single log record is created for the entire multi-part MT message. However, the boolean field "`isMultiPartMtMessage`" is set to '1' ('true') in the 'OutboundMt' log record, indicating that the MT message actually has multiple parts.

4.11 Automatic Blacklisting

Overview

The Automatic Blacklisting functionality is implemented by enhancing the NMM anti-fraud system. As part of this enhanced functionality, if a MO or MT message is detected as "spam" or "fraudulent" by appropriately configured FAF filters, the subscriber who had sent the message or/and for whom it was destined would get automatically blacklisted in the subscriber provisioning database of the SPF. Once a subscriber is blacklisted, all subsequent messages sent by or destined for this subscriber would be rejected by the RTR, either for a configurable time period or permanently. If the subscriber is blacklisted for a specific time period, then upon expiry of that period the subscriber will be removed

from the blacklist in the subscriber provisioning DB and he or she would be able to send messages to or receive messages from the SMS network again.

Important: A small time-interval is likely to elapse after the expiry of a subscriber's blacklist period before that subscriber is actually removed from the blacklist and his/her messages are allowed to pass by the RTR. This small time-interval is not expected to exceed 5 minutes under normal operational conditions, provided only one Auto Blacklist Service (see below) is provisioned in the system.

Note: Apart from automatic addition and removal of subscribers to/from the blacklist in the SPF database, the operator can also use manual procedure for the same purpose by issuing appropriate commands through the Customer Care Interface (CCI) GUI or the SPF Command-line Interface. A blacklisted subscriber can be removed from the blacklist through a manual procedure at any time, irrespective of the blacklist period of that subscriber or even if the subscriber is blacklisted permanently.

Refer to FAF Operator Manual and SPF Operator Manual for more details.

Auto Blacklist Service

A new service type 'Auto Blacklist' has been introduced in order to allow the operator to provision ABL-specific services from the MGR for automatic blacklisting of originator and recipient subscribers. It is a special service category which is neither a Personalized service nor a Value-added Non Provisionable Service (NPS), but the operator will still have full control regarding service activation and service parameter configuration (e.g. the blacklist period) for each subscriber to be blacklisted.

- *Originator ABL service*refers to a service type that is used to automatically blacklist subscribers who send messages that are detected as spam or fraudulent by FAF filters
- *Recipient ABL service*refers to a service type that is used to automatically blacklist subscribers who are the intended recipients of messages detected as spam or fraudulent by FAF filters.

Refer to MGR Operator Manual for details regarding the creation and activation of Auto Blacklist services.

4.11.1 Originator Blacklisting

Automatic blacklisting of an originating subscriber can take place either in the MO path (in case the originator is a home network subscriber) or in the MT path (in case the originator is a foreign network subscriber).

In both the scenarios the Router will first query the SSI to verify if an ABL service is already active for the originator; the subsequent behavior of the Router will depend on how the relevant MO/MT External Condition Rule(s) and MO/MT Routing Rule(s) are configured.

As an example of a *typical*configuration, the Router may be configured with a MOX/MTOX rule such that if the SSI response indicates that no ABL service is active for the originator, then the MO/MT message should be forwarded to the FAF as an EC application. On the other hand, if the SSI response indicates that an ABL service is already active for the originating subscriber, then the Router may be configured to discard the MO/MT message with a NACK through a suitable MOR/MTOR rule, instead of forwarding the message to the FAF again. However, the operator may also choose to send the message to the FAF again, e.g. in order to allow for the possibility of the message being matched by a different filter than the one that had originally caused the blacklisting of the message originator; if that happens, then depending upon how the new filter 'action' is configured, the blacklist period of the concerned subscriber may actually get increased or decreased, or it may also remain unchanged.

If the originator is not already blacklisted and the MO/MT message sent by him/her matches a FAF filter that is configured for auto blacklisting action, then also the behavior of the Router may vary depending upon how the 'failure action' of the corresponding MOX/MTOX rule is configured. The

operator may choose to discard the message straightaway with a NACK, or may decide to evaluate other EC rules (e.g. to check for the applicability of other Personalized or Value-added services which the originating subscriber might be having) and eventually pass on the message for MOR/MTOR rule evaluation, whereupon the message may finally get rejected.

Important: It is strongly recommended that the EC rule responsible for sending a MO/MT message to the FAF is assigned the highest priority among all provisioned EC rules. This is mainly to ensure that a message is not subjected to unnecessary ECI requests and XS application processing, without the Router having even determined as to whether the message was actually supposed to be rejected in the first place**.**

4.11.2 Recipient Blacklisting

Similar to originator blacklisting, automatic blacklisting of a recipient subscriber can also take place either in the MO path or in the MT path; however, unlike in the case of originator blacklisting, the recipient subscriber must be a home network subscriber in both the scenarios. Also, for a recipient subscriber to get auto blacklisted on the MT path, Home Routing needs to be enabled on the Router.

The Router processing logic for the SSI query/response, various MOX/MTOX and MOR/MTOR rule configurations etc. are mostly similar to what has been described above w.r.t. originator blacklisting.

One significant difference with the originator blacklisting is that the Router may even block a message for a recipient subscriber directly on the basis of an incoming SRI-SM, without waiting for the corresponding MT-FSM, if the SSI response for the SRI-SM indicates that the recipient subscriber is already blacklisted.

Note that the same subscriber could get auto blacklisted concurrently as an originator as well as a recipient through two separate messages, but never in the same message flow.

Important: It is strongly recommended that the EC rule responsible for sending a MO/MT message to the FAF is assigned the highest priority among all provisioned EC rules. This is mainly to ensure that a message is not subjected to unnecessary ECI requests and XS application processing, without the Router having even determined as to whether the message was actually supposed to be rejected in the first place.

4.12 Copy to Email

Copy to E-mail (CTE) service supports copies of MT messages on behalf of their recipients towards e-mail addresses provisioned by the recipient subscribers. This service allows copying to email only upon successful delivery of the corresponding MT messages.

4.12.1 CTE Message Processing

This section describes the RTR processing logic for supporting the CTE service. When and how to generate an CTE message depends on the routing path taken by the original SM through the RTR.

The recipient subscribers would subscribe to the “Copy to E-mail” service and provision their respective contact e-mail addresses in the SPF database through the existing interfaces, i.e. either by sending specific SMS requests, or by contacting the Customer Care Centre. Up to 10 e-mail addresses are allowed to be provisioned per subscriber for the Copy to Email service.

While processing a message destined for a subscriber who has the CTE service activated, SSI indicates this to RTR and RTR then sends an ECI Request to the XS-CPY component using an appropriate MTOX rule, for retrieving the e-mail contact(s) provisioned by the recipient subscriber.

Once the original MT message is delivered successfully, RTR sends the relevant e-mail addresses and other message fields to HUB as an AT delivery request and HUB in turn forwards the same to EMG as a SMPP 'Deliver_SM' message. EMG then generates the email message based on the information provided in SMPP Deliver_SM message and delivers it to the mail server.

In the case of a successful delivery to the mail server, RTR generates the appropriate delivery CDR and log records upon receiving the response from EMG. However, if the delivery attempt to the mail server fails, or any other error occurs on the EMG side, then RTR always considers any such error response as a permanent error and discards the CTE message (after generating the relevant CDR and log records).

The figure below shows the system context for the Copy to E-mail service:

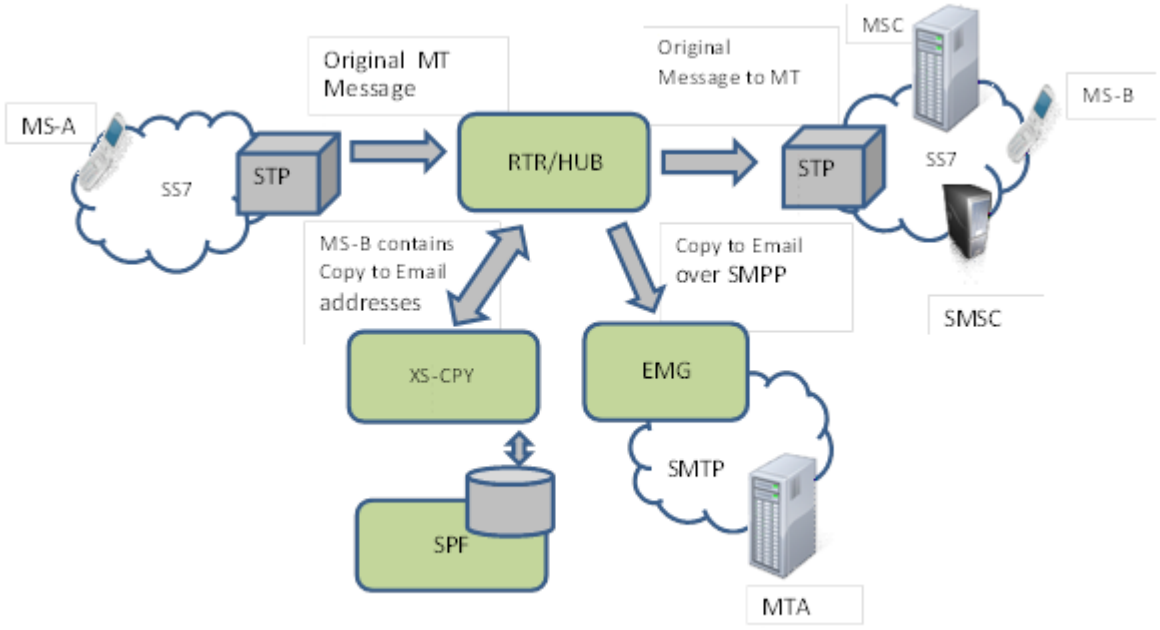


Figure 18: Copy to E-mail

4.12.2 CTE Restriction and Loop Prevention

The following restrictions are applied by the RTR for CTE service:

- Copy to Email service is only supported for MT recipients.
- Similar to the Copy to Phone (CPY) service, the Copy to Email service also cannot be applied on messages containing binary data (e.g. SIM data download messages), Status Reports, Auto-Reply messages etc.
- To prevent loops, the following restrictions apply:
  - CTE cannot be applied on a message that has already been copied or forwarded once (i.e. as a result of applying the CPY or FWD service).

- MSISDN being copied from (i.e. recipient address of the original message) should belong to a HPLMN subscriber.

Interactions of CTE with other personalized services are as follows:

- Both CPY and CTE services can be applied on the same message.
- Both CTA (i.e. Copy To Application) and CTE services can be applied on the same message.
- If either unconditional forwarding to phone or forwarding to email is applied, then CTE is not applied on the same message.
- If a recipient subscriber has both conditional forwarding to phone (FWD) and CTE services activated, then RTR first performs a delivery attempt for the MT message; depending on the outcome of the delivery attempt, either the CTE service would be applied (i.e. in case of successful delivery) or conditional forwarding to phone would be applied (i.e. in case of unsuccessful delivery).
- A message which is copied to email inherits all text added earlier to the original message, including signature and advertisement texts associated with the personalised Signature service and the TIE (Text Insertion Engine) service, respectively.

Note: For Copy to Email service, RTR ignores the semi-static parameter 'restrictcopyingtoownsubscriberbase '. This parameter is not relevant for CTE since the message is copied to one or more e-mail addresses rather than to another subscriber's mobile number.

4.12.3 Billing

Post-paid Billing

A single FCDR record is generated for applying the CTE service on a message, irrespective of the number of destination e-mail addresses the message is copied to. For non-segmented messages, this FCDR is actually the delivery record that is generated upon receiving a successful response from the EMG; no separate submission CDR record is generated in this case. However, if the original message is a segment of a concatenated message then a submission CDR record is generated upon receiving a successful response from the EMG.

There is an additional final delivery CDR generated for concatenated messages upon a successful delivery to the SMTP server by the EMG.

In the event of receiving a failure response from the EMG (e.g. if the delivery attempt to the mail servers fails, or any other error occurs on the EMG side), a single FCDR record is generated with the "delivery status" being indicated as "failed", irrespective of whether it is a non-segmented message or a concatenated message.

Each FCDR record generated for CTE includes the original MT recipient as the 'originator' and the configured address (e.g. short number) of EMG application as the 'recipient'. No e-mail address is included in the generated FCDR records.

An appropriate ATOR rule as well as an AOR rule needs to be pre-configured with the desired billing profile for the post-paid billing of CTE service. While the ATOR rule is used for generating submission CDR records for concatenated message segments and the delivery CDR record for non-segmented messages, the AOR rule is required for generating the final delivery CDR record for a concatenated message.

Also, the configuration parameter 'billingforcopiedmessages' should be set to "true".

Prepaid Billing

For online billing of CTE service, RTR sends a single ECI request to PBC for every incoming message (including each segment of a concatenated message), irrespective of the number of e-mail addresses it is going to be copied to. However, an appropriate EC Application needs to be pre-configured for this purpose, as identified by the MGR configuration setting "Recipient Copy to Email Billing Application".

For recipient copy to email, the recipient of the original message is indicated as the 'originator' in the request sent to PBC, and is typically charged for utilizing the CTE service. The configured address (short number) of the EMG application is indicated as the 'recipient'. Both single-phase (i.e. "direct-debit") and two-phase (i.e. "debit-refund" or "reserve-deduct") modes of online charging are supported, depending on how the PBC is configured.

For more information about generating CDRs and configuring pre-paid billing for copied messages, refer to the NewNet Mobile Messaging RTR Billing Manual.

4.12.4 Logging

Transaction log records

RTR generates transaction log records of type 'copyForwardEventWithCountryAndNetworkInfo' (see *Appendix A*) for applying Copy to Email service on each incoming message or segment.

Only a single log record is generated per message/segment irrespective of the number of destination e-mail addresses, but it includes a comma-separated list of all the e-mail addresses.

Event records

The RTR writes an event record for each generated CTE message. The CTE event record can be correlated to the event record of the original message that was copied

Records	Description
smCopied	This record is generated every time a CTE request has been issued for a short message. The destination field in 'smCopied' contains the configured address (short number) of the EMG application.
copyRejection	This record is written in the event of an error response returned from EMG.

Note: Note that the necessary logging profile would need to be associated with an appropriate ATOR rule for generating the transaction log records. An appropriate AOR rule also needs to be pre-configured with the desired log profile in order to generate the final delivery log record for a concatenated short message.

4.12.5 Statistics

Available CTE counters in the RTR:

Counter Name	Description
cpyCntCteReqReceived	Counter specifying the number of requests that the RTR received to copy a short message to email.
cpyCntCteReqApproved	Counter specifying the number of copy to email requests that the RTR has approved and executed.

Counter Name	Description
cpyCntCteReqDiscardedAs OriginalSmNotInCopyableState	Counter specifying the number of copy to email requests that the RTR has discarded because the original short message did not reach a state in which it can be copied (i.e. a MT message can be copied when the RTR has successfully delivered the short message).
cpyCntCteReqDiscardedAs SimDataDownloadNotCopyable	Counter specifying the number of copy to email requests that the RTR has discarded because the request related to a short message with data to be loaded on the SIM.
cpyCntCteReqDiscardedAs CopyOfCopiedSmNotSupported	Counter specifying the number of copy to email requests that the RTR has discarded because the original short message is already a copy of a short message.
cpyCntCteReqNotProcessedAs TooManyCopiesInProgress	Counter specifying the number of times that the RTR did not process a copy to email request because too many copies were already in progress.

4.13 Forward to Email

Forward To E-mail (FTE) service forwards MT messages on behalf of their recipients towards e-mail addresses provisioned by the recipient subscribers.

This service supports only unconditional forwarding of MT messages, i.e. immediate forwarding without attempting delivery of the original MT message to the recipient subscriber.

4.13.1 FTE Message Processing

This section describes the RTR processing logic for supporting the FTE service. When and how to generate an FTE message depends on the routing path taken by the original SM through the RTR.

The recipient subscribers would subscribe to the “Forward to E-mail” service and provision their respective contact e-mail addresses in the SPF database through the existing interfaces, i.e. either by sending specific SMS requests, or by contacting the Customer Care Centre. Up to 10 e-mail addresses are allowed to be provisioned per subscriber for the Forward to Email service.

While processing a message destined for a subscriber who has the FTE service activated, SSI indicates this to RTR and RTR then sends an ECI Request to the XS-FWD component using an appropriate MTOX rule, for retrieving the e-mail contact(s) provisioned by the recipient subscriber.

RTR sends the relevant e-mail addresses and other message fields to HUB as an AT delivery request and HUB in turn forwards the same to EMG as a SMPP Deliver_SM message. EMG then generates the email message based on the information provided in SMPP Deliver_SM message and delivers it to the mail server.

In the case of a successful delivery to the mail server, RTR generates the appropriate delivery CDR and log records upon receiving the response from EMG. However, if the delivery attempt to the mail server fails, or any other error occurs on the EMG side, then RTR always considers any such error response as a permanent error and discards both the FTE message and the original message (after generating the relevant CDR and log records).

The figure below shows the system context for the Forward to E-mail service:

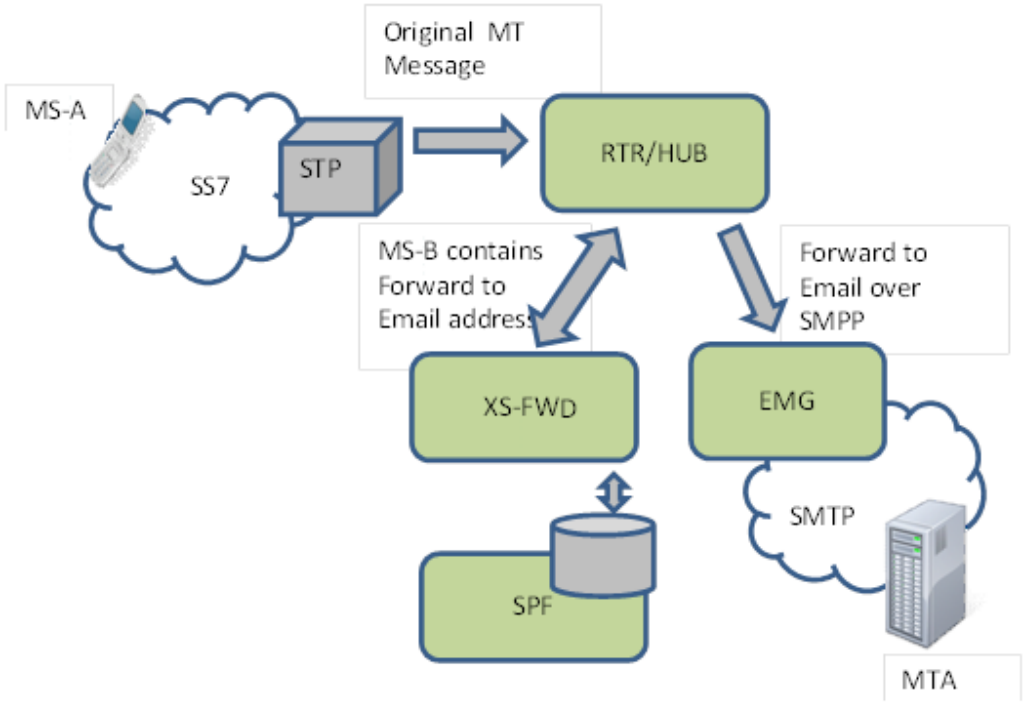


Figure 19: Un-Conditional Forward To E-mail

4.13.2 FTE Restriction and Loop Prevention

The following restrictions are applied by the RTR for FTE service:

- Forward to Email service is only supported for MT recipients.
- Similar to the Forward to Phone (FWD) service, the Forward to Email service also cannot be applied on Auto-Reply messages. FTE support for Status Reports and for messages containing binary data (e.g. SIM data download messages) is likewise controlled by the semi-static parameters 'statusreportprocessingforunconditionalforwarding' and 'simdownloadprocessingforunconditionalforwarding', respectively.
- To prevent loops, the following restrictions apply:
  - FTE cannot be applied on a message that has already been copied or forwarded once (i.e. as a result of applying the CPY or FWD service).
  - MSISDN being forwarded from (i.e. recipient address of the original message) should belong to a HPLMN subscriber.

Interactions of FTE with other personalized services are as follows:

- In case a subscriber actually subscribes to both CTE and FTE services, then the Forward To Email service is applied at the expense of the Copy To Email functionality.
- If a recipient subscriber has both CPY (i.e. Copy to Phone) and FTE services activated, RTR performs FTE-related processing only and no delivery attempt is made for the original MT message.

- Unconditional FWD (Forward to Phone) and FTE services cannot be applied together on the same message.
- A message which is forwarded to email inherits all text added to the message prior to the actual forwarding, including signature and advertisement texts associated with the personalised Signature service and the TIE (Text Insertion Engine) service, respectively.

Note: For Forward to Email service, RTR ignores the semi-static parameter 'restrictforwardingtoownsubscriberbase'. This parameter is not relevant for FTE since the message is forwarded to one or more e-mail addresses rather than to another subscriber's mobile number.

4.13.3 Billing

Post-paid Billing

A single FCDR record is generated for applying the FTE service on a message, irrespective of the number of destination e-mail addresses the message is forwarded to. For non-segmented messages, this FCDR is actually the delivery record that is generated upon receiving a successful response from the EMG; no separate submission CDR record is generated in this case. However, if the original message is a segment of a concatenated message then a submission CDR record is generated upon receiving a successful response from the EMG.

There is an additional final delivery CDR generated for concatenated messages upon a successful delivery to the SMTP server by the EMG.

In the event of receiving a failure response from the EMG (e.g. if the delivery attempt to the mail servers fails, or any other error occurs on the EMG side), a single FCDR record is generated with the "delivery status" being indicated as "failed", irrespective of whether it is a non-segmented message or a concatenated message.

Each FCDR record generated for FTE includes the original MT recipient as the 'originator' and the configured address (e.g. short number) of the EMG application as the 'recipient'. No e-mail address is included in the generated FCDR records.

An appropriate ATOR rule as well as an AOR rule needs to be pre-configured with the desired billing profile for the post-paid billing of FTE service. While the ATOR rule is used for generating submission CDR records for concatenated message segments and the delivery CDR record for non-segmented messages, the AOR rule is required for generating the final delivery CDR record for a concatenated message.

Also, the configuration parameter 'billingforforwardedmessages' should be set to "true".

Prepaid Billing

For online billing of the FTE service, RTR sends a single ECI request to PBC for every incoming message (including each segment of a concatenated message), irrespective of the number of e-mail addresses it is going to be forwarded to. However, an appropriate EC Application needs to be pre-configured for this purpose, as identified by the MGR configuration setting "Unc. Forward to Email Billing Application".

For FTE, the recipient of the original message is indicated as the 'originator' in the request sent to PBC, and is typically charged for utilizing the service. The configured address (short number) of the EMG application is indicated as the 'recipient'. Both single-phase (i.e. "direct-debit") and two-phase (i.e. "debit-refund" or "reserve-deduct") modes of online charging are supported, depending on how the PBC is configured.

For more information about generating CDRs and configuring pre-paid billing for forwarded messages, refer to the NewNet Mobile Messaging RTR Billing Manual.

4.13.4 Logging

Transaction log records

RTR generates transaction log records of type 'copyForwardEventWithCountryAndNetworkInfo' (see *Appendix A*) for applying Forward to Email service on each incoming message/segment.

Only a single log record is generated per message/segment irrespective of the number of destination e-mail addresses, but it includes a comma-separated list of all the e-mail addresses.

Event Records

The RTR writes an event record for each generated FTE message. The FTE event record can be correlated to the event record of the original message that was forwarded.

Records	Description
forwardAttempt	This record is generated every time a FTE message is generated and forwarded for a short message. The destination field in 'forwardAttempt' contains the configured address (short number) of the EMG application
forwardRejection	This record is written in the event of an error response returned from EMG.

Note: Note that the necessary logging profile would need to be associated with an appropriate ATOR rule for generating the transaction log records. An appropriate AOR rule also needs to be pre-configured with the desired log profile in order to generate the final delivery log record for a concatenated short message.

4.13.5 Statistics

Available FTE counters in the RTR:

Counter Name	Description
fwdCntUnCndFteReqApprovedAndFwdSucceeded	Counter specifying the number of unconditional forward to email requests that the RTR has approved and for which forwarding has succeeded.
fwdCntUnCndFteReqApprovedAndFwdFailedWithPermanentError	Counter specifying the number of unconditional forward to email requests that the RTR has approved and for which forwarding has failed with a permanent error.
fwdCntUnCndFteReqDiscardedAsSimDataDownload	Counter specifying the number of unconditional forward to email requests that the RTR has discarded because the request pertained to a SM with data to be loaded on the SIM, whilst the RTR has been configured not to forward such an SM

Counter Name	Description
fwdCntUnCndFteReqDiscarded AsIsCopiedSm	Counter specifying the number of unconditional forward to email requests that the RTR has discarded because the original SM is a copy of an SM.

Note: Whenever the RTR determines that an MT message is to be Unconditionally Forwarded towards the short number corresponding to the EMG Application, the original message is from that point onwards considered as an AT message rather than an MT message, and this is also reflected in any counters or statistics associated with the original message. For example, the smsCntMoAtSuccess counter is incremented (instead of the smsCntMoMtSuccess counter) in case of successful delivery of the forwarded message to the mail server by the EMG.

Chapter 5

Lists

Topics:

5.1 Introduction

Lists can be used to group multiple condition entries in one condition. Lists can reduce the number of rules that are required and increase the flexibility of the conditions in which lists are used. If a list is used in a condition, any message that matches an entry in the list will cause the condition to evaluate to true.

Some examples of lists are:

- All MSC point codes in the home PLMN
- All premium SMS short numbers
- A physical and virtual SMSC addresses

Lists can be referenced in the following routing and counting rule condition fields:

- Originator
- Recipient
- SMSC
- MSC/SGSN
- IPAddress-Port

The type of list that can be selected depends on the condition formats that are allowed for the condition field.

Up to 1000 lists can be defined in the RTR, with up to 10,000 entries in each list.

Overlapping lists are allowed. List entries can be modified without disabling the list or the associated rule.

Note: The number of defined lists and their lengths will impact the RTR's restart time.

For information about configuring lists, refer to the MGR Operator Manual.

5.2 Application Originator Restriction

You can use an application originator whitelist or blacklist to restrict the originator address of configured applications. Each application can have one associated whitelist or one associated blacklist. A whitelist or blacklist can contain entries with the following originator address formats:

- MSISDN
- Short number
- Alphanumeric

If an application-originated (AO) message does not match a whitelist entry or does match a blacklist entry, the RTR will return the appropriate permanent message error to the application and will block corresponding messages.

Application originator restriction only works for an application if application originator replacement is disabled. If application originator replacement is enabled, the RTR uses the whitelist or blacklist that is defined for the application to determine if the application originator address should be replaced.

Note: To enter an SC(/MSISDN) in a list, enter it in both the SC(/MSISDN) and alphanumeric fields. If you omit it from the alphanumeric field, the SC(/MSISDN) will be included in the list for all TONs but will not be included for TON 5 (alphanumeric).

Up to 10,000 application originator lists can be defined in the RTR, with up to 10,000 entries in each list.

5.3 Application Originator Replacement

The RTR can replace an application-originator (AO) message's originator address with a configurable:

- MSISDN
- Short number (default)
- Alphanumeric

When this functionality is enabled, the RTR compares the originator address to a whitelist and a blacklist. The RTR replaces the originator address when:

- The originator address does not match an address in the whitelist, or
- The originator address matches an address in the blacklist

If the functionality is enabled but no whitelist or blacklist is defined for the application, the RTR replaces the originator address with the replacement address.

Note: If the prepaid or post-paid billing settings include the originator address as a billing field and the RTR replaced the originator address, the billing field will contain the replacement address.

Originator replacement is configured for each application in the MGR. In **SMS Applications ➤ Applications**, set **Enable Originator Replacement** and **Originator Replacement Address**.

Note: Application originator replacement is not supported for query/cancel/replace operations.

Chapter 6

Modifiers

Topics:

6.1 Introduction

Modifiers change certain message fields before the RTR routes a message to its destination. The RTR supports modifiers for the following types of messages:

- Mobile-originated (MO)
- Incoming mobile-terminated (MTI)
- Outgoing mobile-terminated (MTO)
- Application-originated (AO)
- Incoming application-terminated (ATI)

6.2 Modifier Priority

Message fields can be modified by both routing rule modifiers and external condition (EC) applications. If both modify the same field, the EC application value takes priority.

6.3 Creating MO Modifiers

To create a mobile-originating (MO) modifier:

1. In the left navigation bar, select **Routing ➤ Modifiers ➤ MO**.
   The MO Modifiers tab appears.
2. Click **Add New**.
   A new MO Modifiers tab appears.
3. Enter a unique name for the modifier in the **Name** box (up to 31 characters).
4. Optionally enter a description of the modifier in the **Description** box.
5. If you want to modify the message originator, enter an E.164 number in the **Originator** box.
   The E.164 number must be:
   - A full number in international format, without international prefix, or
   - A short number
6. If you want to modify the message recipient, enter an E.164 number in the **Recipient** box.
   The E.164 number must be:
   - A full number in international format, without international prefix, or
   - A short number
7. If you want to modify the IMSI in the message, enter a value in the **IMSI** box.
8. If you want to remove characters from the beginning of the user data (content) of the message, enter a number in the **User Data chars to strip** box (defaults to 0).

If the user data contains less characters than this number, the user data becomes empty. This functionality is useful for stripping keywords from a message (such as `*LONG#`). Only the standard GSM character set is supported.

9. If you want to modify the reply path bit, enter a value between -1 and 1 in the **Reply Path** box.

   A value of -1 means that the bit should not be modified (this is the default).

10. If you want to modify the status report request bit, enter a value between -1 and 1 in the **Status Report request** box.

    A value of -1 means that the bit should not be modified (this is the default).

11. If you want to modify the protocol ID (PID), enter a value between 00 and FF in the **Protocol ID (PID)** box.

    A value of -1 means that the PID should not be modified (this is the default).

12. If you want to modify the data coding scheme (DCS), enter a value between 00 and FF in the **Data Coding Scheme (DCS)** box.

    A value of -1 means that the DCS should not be modified (this is the default).

    Note: It is not recommended to use the MO Modifier if the DCS conversion feature set to `japan` (i.e. '`hubdcscharcodingconversion`' and '`rtrdcscharcodingconversion`' set to '`japan`'). However, if one uses the MO Modifier and the DCS conversion feature with `japan` together, the behavior (i.e. user data conversion and character set conversion) is not as per the expectation.

13. If you want to modify the SMSC address at the MAP layer (SM-RP-OA) of the incoming MO message, enter an E.164 number (in international format, without international prefix) in the **SMSC Address** box.

    The RTR applies the SMSC modifier after applying the routing and external condition rules. Therefore, the RTR will compare an 'SMSC Address' condition in the rules to the SCA field's original value in the incoming message, not the modified value from the modifier. The SMSC modifier affects the MAP layer's SMS-RP-OA field.

    Note: See RTR Billing Manual section "5.1.3 Virtual SMSC Fields" when "SMSC Address" modifier affects the FCDRs.

14. If you want to delay the first delivery attempt of a MO message, then modify the **Delivery Delay** field with a value between 0 and 8035200 (93 days).

    - The default value of this parameter is 0, meaning there is no delay in the FDA of a MO message.
    - When the parameter **Delivery Delay** is set to a non-zero value, the following table describes the RTR behavior on a MO message according to the MO routing action:

Routing action	Behavior	Remarks
Route to SMSC	The **Delivery Delay** value will be ignored and the MO will be forwarded to the SMSC.	NA
Route to Application	The **Delivery Delay** value will be ignored and FDA will be attempted.	NA
Route to MS	The MO routing rule will not match	NA

Routing action	Behavior	Remarks
Route to MS fallback to SMSC	Go for fallback option. The **Delivery Delay** value will be ignored and the MO will be forwarded to the SMSC. **Note:** MTFSM will not be attempted by the RTR.	If at the time of rule matching fallback option is not available then MO routing rule will not match.
Route to MS fallback to application	Go for fallback option. The **Delivery Delay** value will be ignored and FDA will be attempted. **Note:** MTFSM will not be attempted by the RTR.	If at the time of rule matching fallback option is not available then MO routing rule will not match.
Store for Delivery to MS	Message stored in AMS. Delivery from AMS will be attempted based on the **Delivery Delay** value.	NA
Route to MS fallback to storage	Go for fallback option. Message stored in AMS. Delivery from AMS will be attempted based on the **Delivery Delay** value.	If at the time of rule matching fallback option is not available then MO routing rule will not match.
Store for delivery to Application	Message stored in AMS. Delivery from AMS will be attempted based on the **Delivery Delay** value.	NA
Route to application fallback to storage	Go for fallback option. Message stored in AMS. Delivery from AMS will be attempted based on the **Delivery Delay** value.	If at the time of rule matching fallback option is not available then MO routing rule will not match.
Route to SMSC group	The **Delivery Delay** value will be updated in the AO and sent to the SMSC group.	NA
Route to MS fallback to SMSC group	Go for fallback option. The **Delivery Delay** value will be updated in the AO and sent to the SMSC group. **Note:** MTFSM will not be attempted by the RTR.	If at the time of rule matching fallback option is not available then MO routing rule will not match.

Routing action	Behavior	Remarks
Route to SMSC application as AO	The **Delivery Delay** value will be updated in the AO and sent to application.	NA
Route to MS fallback to SMSC application as AO	Go for fallback option. The **Delivery Delay** value will be updated in the AO and sent to application. **Note:** MTFSM will not be attempted by the RTR.	If at the time of rule matching fallback option is not available then MO routing rule will not match.

- If both the `deferreddeliveryrelativehours` for the MO scan tag and the MO modifier's **Delivery Delay** are applied on a message, then the MO scan tag value will be used as it is specifically requested for this message.
- If the field **Delivery Delay** is disabled in the MO modifier, then `deferreddeliveryrelativehours` for the MO scan tag works as per the existing behavior. Please refer to the section *Configurable MO Deferred Delivery Relative Hours*.
- If the field **Delivery Delay** is set, then submit and delivery CDR will be populated with the **Delivery Delay** value for those scenarios in which **Delivery Delay** has been applied.
- If this parameter is set, then RTR delay the first delivery attempt (FDA) of MO message with the configurable amount of time in the following path:

  1. MO-ST-MT
  2. MO-MT-ST
  3. MO-ST-AT
  4. MO-AT-ST
  5. MO-AO
  6. MO-MT-AO

  Note: For MO-AO or MO-MT-AO path , when the RTR forwards the MO messages as AO to SMSC/SMSC group then the **Delivery Delay** value are updated in the AO message field as per below:

  1. deferred-delivery-time field for UCP
  2. schedule-delivery-time field for SMPP
  3. first-delivery-time field for CIMD

- If the MO message sent to store (i.e. AMS) and the delivery delay value is greater than the MO message's validity period, then the store will reject the MO message by considering it as an invalid MO message.
- If the field **Delivery Delay** is set, then submit and delivery CDR will be populated with the **Delivery Delay** value in the CDR, which will capture the defer period either in hours, or minutes. Seconds will be round up by 1 minute in the CDR.
- Submit FCDR will have the Delivery period even though MO modifiers Delivery delay parameter is ignored for the below scenario.

  - MO-MO
  - MO-MT-MO
  - MO-AT

  - MO-MT-AT
- Delivery FCDR will have the defer period included even though MO modifiers **Delivery Delay** parameter is ignored with below scenario.
  - MO-AT
  - MO-MT-AT
- If the field **Delivery Delay** is set, the counter specifying the number of times an inbound MO/SM was routed using the MO actions, where the RTR skipped the first delivery attempt due to the delivery delay in the MO modifier and go to fallback option, is incremented by the RTR, as in the following table:

Routing Action	Counters
Route to MS fallback to SMSC	smsCntMoMtMoPrimaryFailure
Route to MS fallback to SMSC Application as AO	smsCntMoMtAoPrimaryFailure
Route to MS fallback to storage	smsCntMoMtAmsPrimaryFailure
Route to MS fallback to SMSC Group	smsCntMoMtAoPrimaryFailure
Route to MS fallback to Application	smsCntMoMtAtPrimaryFailure

15. Click **Save**.
    The MGR creates the MO modifier and closes the tab.
16. Activate the modifier.

6.4 Creating MTI Modifiers

To create an incoming mobile-terminating (MTI) modifier:

1. In the left navigation bar, select **Routing ➤ Modifiers ➤ MTI**.
   The MTI Modifiers tab appears.
2. Click **Add New**.
   A new MTI Modifiers tab appears.
3. Enter a unique name for the modifier in the **Name** box (up to 31 characters).
4. Optionally enter a description of the modifier in the **Description** box.
5. In the Defer Period box, enter the number of seconds to defer the delivery of an MT message.
   The modification is applied to the inbound message after MTIR rule evaluation, and only has an effect if the routing action is "store for delivery to MS" or "route to SMSC as AO".
6. Click **Save**.
   The MGR creates the modifier and closes the tab.
7. Activate the modifier.

6.5 Creating MTO Modifiers

To create an outgoing mobile-terminating (MTO) modifier:

1. In the left navigation bar, select **Routing ➤ Modifiers ➤ MTO**.
   The MTO Modifiers tab appears.
2. Click **Add New**.
   A new MTO Modifiers tab appears.
3. Enter a unique name for the modifier in the **Name** box (up to 31 characters).
4. Optionally enter a description of the modifier in the **Description** box.
5. If you want to modify the time zone, select a new time zone from the **Timezone** list.
   This modifier applies to the:
   - TP-SCTS (service center timestamp) field of the SMS-DELIVER PDU
   - TP-SCTS (service center timestamp) field of the STATUS-REPORT PDU
   - TP-DT (discharge time) field of the STATUS-REPORT PDU

   The limitations on this modifier are:
   - It can only be used on the MO-MT-MO, MO-MT-AT, AO-MT, and MT-MT routing paths
   - It cannot be used on MtForwardSm operations that are issued by an SMSC that the RTR/FWL considers to be suspect
6. If you want to modify the reply path bit, enter a value between -1 and 1 in the **Reply Path** box.
   A value of -1 means that the bit should not be modified (this is the default).
7. If you want to modify the SMSC address, enter an E.164 number (in international format, without international prefix) in the **SMSC Address** box.
   The RTR applies the SMSC modifier after applying the routing and external condition rules. Therefore, the RTR will compare an SMSC condition in the rules to the SMSC field's original value. The SMSC modifier affects the MAP layer's SMS-RP-OA field.
8. If you want to modify the message originator format, select a format from the **Originator Format** list:
   - **Transparent**—Do not modify the originator address (default)
   - **National**—Change the originator address to national format
   - **International**—Encode the originator address as international

   This modifier overrides the format specified in the `mtoriginatorformatfordomestictraffic` and `mtoriginatorformatformtmtdomestictraffic` parameters in the semi-static configuration file. These parameters take effect only when the modifier is set to **Transparent**.
9. If you want to modify the originator TON, select the value from the **Originator TON** drop-down list.

   Note: For newly created MTO Modifiers, any time the **Originator Format** is changed, the **Originator TON** value will be reset to the default value of the selected **Originator Format** in the MGR GUI.

Example: If the **Originator Format** is **National** and the user changes it to **International**, the **Originator TON** will automatically be reset to 1 (default value for the **International** format).

Default values for the Originator TON

Originator Format	Originator TON
Transparent	-1
International	1
National	0

10. If you want to modify the originator NPI, select the value from the **Originator NPI** drop-down list.

    Note: For newly created MTO Modifiers, any time the **Originator Format** is changed, the **Originator NPI** value will be reset to the default value of the selected **Originator Format** in the MGR GUI.

    Example: If the **Originator Format** is **National** and the user changes it to **International**, the **Originator NPI** will automatically be reset to 1 (default value for the **International** format).

    Default values for the Originator NPI

Originator Format	Originator NPI
Transparent	-1
International	1
National	1

11. If you want to modify the message's SMSC address during SendRoutingInfoForSM (SRI-SM) operations, enter an E.164 number (in international format, without international prefix) in the **SMSC Address for SRI SM Ops** box.

    This modifier overrides the `smscaddressforhlroperations` parameter in the semi-static configuration file.

12. If you want to modify the message's SMSC address during ReportSMDeliveryStatus operations, enter an E.164 number (in international format, without international prefix) in the **SMSC Address for Report SM Ops** box.

    This modifier overrides the `smscaddressforhlroperations` parameter in the semi-static configuration file.

13. If you want to remove digits from the beginning of the message's SCCP called party address (CdPA) during the SendRoutingInfoForSM operation, enter a number of digits in the **Strip SCCP CdPA of SRISM** box.
14. If you want to add digits to the beginning of the message's SCCP called party address (CdPA) during the SendRoutingInfoForSM operation, enter the digits in the **Prefix SCCP CdPA of SRISM** box.

    Note:

    1. If the strip and prefix functionalities are used together, stripping occurs before prefixing.
    2. The maximum configurable length of the **Prefix SCCP CdPA of SRISM** is 15 digits. The number of configured prefix digits used to modify the SCCP called party address is decided such that

the modified SCCP called party address after adding the prefix to the SCCP called party address is not more than 20 digits. For example, if the configured **Prefix SCCP CdPA of SRISM** is of 10 digits and received SCCP called party address is of 12 digits then only first 8 digits of the configured prefix value will only be used to modify the SCCP called party address.

15. If you want to replace the message's SCCP called party address (CdPA) with a different global title (GT) during the SendRoutingInfoForSM operation, enter the GT in the **Replace SCCP CdPA of SRISM** box.

    The **Replace SCCP CdPA of SRISM** also supports special character 'Z'. This special character is replaced with the 3-digits Country Code of the Recipient MSISDN. After the replacement of 'Z', the configured address will be used as E164 address.

    - If Country code consists of 1 digit, then 2 zeros are prepended to it.
    - If Country code consists of 2 digits, then 1 zero is prepended to it.
    - If Country code consists of 3 digits, then it is replaced directly.

    For example:

    - If **Replace SCCP CdPA of SRISM** is set as `99999Z`
    - If the recipient is `+1 2345 678 9012` (USA number), the CDPA of SRI SM will be `99999001`
    - If the recipient is `+86 13916316470` (China number), the CDPA of SRI SM will be `99999086`
    - If the recipient is `+389 73420405` (Macedonia number), the CDPA of SRI SM will be `99999389`
    - Multiple special character 'Z' can be configured in address.
    - If the country is not known, then country code will not be appended.

    Below are a couple SRI-SM scenarios where **Replace SCCP CdPA of SRISM** will be applicable:

    - Applicable for early SRI-SM scenarios
    - Applicable for regular SRI-SM scenarios

    Below are a couple SRI-SM scenarios where **Replace SCCP CdPA of SRISM** will NOT be applicable:

    - NOT applicable for AO early SRI-SM scenarios
    - NOT applicable for SRI-SM for originators

    In case of MT-MT scenarios, the Recipient's country and scramble IMSI range must belong to the domestic country (i.e. RTR's own country), otherwise the behavior of the special character 'Z' replacement will be changed. In this case special character 'Z' will be replaced with the 3-digits Country Code of the scrambled IMSI instead of the recipient MSISDN.

    Note: The replace functionality is mutually exclusive with the strip and prefix functionalities. The strip and prefix functionalities can be used together, but neither should be used with the replace functionality.

16. If you want to modify the message's SCCP called party address (CDPA) during ReportSMDeliveryStatus operation with the modifiers that were applied during the SendRoutingInfoForSM operation, set the **Apply SCCP CdPA Modifier for Report SM operation** parameter.

    Note: This field can be enabled in the MGR GUI when at least one of the following fields contains a valid value:

    - **Strip SCCP CdPA of SRISM**
    - **Prefix SCCP CdPA of SRISM**

- **Replace SCCP CdPA of SRISM**

  If this field is configured with the special character 'Z', then the special character is replaced with the 3-digits Country Code of the Recipient MSISDN. For more detail refer to the previous step.

17. Click **Save**.

    The MGR creates the modifier and closes the tab.

18. Activate the modifier.

    Note:

    1. The MTO modifier is not applied to intercepted MT traffic (unsolicited TCAP CONTINUE messages) from non-trusted external SMSC. One such scenario for intercepted MT traffic from non-trusted SMSC is when the recipient of the intercepted MT traffic belongs to a different operator. In such scenario the RTR will forward the message to MCS/SGSN without any modification.

       The originating external SMSC of an inbound MT message is categorized as trusted if the SMSC address at the SCCP layer (and at the MAP layer, if present) matches the list of trusted SMSCs in the semi-static configuration attribute `firewalltrustedsmsclist`.
    2. The MT modifiers are not applied on the message's SCCP called party address (CdPA) during early SRISM operation triggered for incoming AO message. But if the parameter **Apply SCCP CdPA Modifier for Report SM operation** is set, then message's SCCP called party address (CDPA) during ReportSMDeliveryStatus operation will be modified as per the applied MTO modifier configuration.
    3. In case early SRISM operation is enabled for incoming AO message, then, on activating a MTO modifier with the configuration to modify the CdPA address of the SRISM request, the RTR will log a warning message in the syslog. The same will be true if early SRISM is enabled for the incoming AO message when at least one active MTO modifier rule exists on the RTR with the configuration to modify the CdPA address of the SRISM request.
    4. If Japanese MNP is enabled on the RTR, the MTO modifiers are applied on outgoing SRISM request. In case, early SRISM operation is also enabled for incoming MO message then RTR will apply MTO modifier on the early SRISM request as well.
    5. If Japanese MNP is enabled on the RTR, the MTO modifiers are applied on the message's SCCP called party address (CdPA) when the message delivery is triggered through AMS.
    6. If Japanese MNP is enabled on the RTR, the CdPA for ReportSMDeliveryStatus operation will be modified based on the configured MTO modifier as per below:

       - If MTO modifier's field "Apply SCCP CdPA Modifier for Report SM operation" is checked and Recipient country belongs to international, the MTO modifiers will be applied on the SCCP called party address (CdPA) of Report SM Delivery Status Message.

         CdPA for Report SM Delivery Status will be prepared as below:

         - CdPA GT address = <MTO modifier provisioned SCCP CdPA>;
         - Subsystem Number = 6;
         - Nature of Address Indicator = 0x04;
         - TT = <Fallback SRI-SM TT retrieved from Network Table entry, default 0x0 if not found>;
         - CgPA GT address = <RTR's own GT>;
         - Subsystem Number = 8;
         - Nature of Address Indicator = 0x04;

- If MTO modifier's field "Apply SCCP CdPA Modifier for Report SM operation" is checked and Recipient country belongs to national (i.e. own country), the MTO modifiers will not be applied on the SCCP called party address (CdPA) for Report SM Delivery Status Message.

  CdPA for Report SM Delivery Status will be prepared as below:

  - CdPA GT address = <MNP Prefix retrieved from Network Table entry><MSIN>;
  - Subsystem Number = 6;
  - Nature of Address Indicator = 0x03;
  - TT = <Fallback SRI-SM TT retrieved from Network Table entry, default 0x0 if not found>;
  - CgPA GT address = <RTR's own GT>;
  - Subsystem Number = 8;
  - Nature of Address Indicator = 0x04;

The message's SCCP called party address (CDPA) during ReportSMDeliveryStatus operation is described in section *Japanese MNP Processing While Sending a Report SM Delivery Status*.

7. If multiple routing rules are configured with different modifiers and on conditions other than the recipient, then on receiving multiple messages for the same recipient, only some of the SRISM requests will be triggered by the RTR based on the MTQ functionality. Since different rules are configured with different modifiers, it is possible that the messages' SCCP called party address(CdPA) during SRISM operation is different from messages' SCCP called party address(CdPA) during the ReportSMDeliveryStatus operation.

6.6 Creating AO Modifiers

To create an application-originating (AO) modifier:

1. In the left navigation bar, select **Routing ➤ Modifiers ➤ AO**.
   The AO Modifiers tab appears.
2. Click **Add New**.
   A new AO Modifiers tab appears.
3. Enter a unique name for the modifier in the **Name** box (up to 31 characters).
4. Optionally enter a description of the modifier in the **Description** box.
5. If you want to modify the message's validity period, enter a value in the **Validity Period** box:
   - -1—Do not modify (default)
   - 0—Remove the validity period field (if present)
   - Any other value (up to 16,000,000)—Number of seconds in the future

   Note: The AMS treatment of the **Validity Period** takes precedence for messages that pass through the AMS in the course of their routing. Specifically, the AMS will reset a zero, missing, or too-large **Validity Period** to the default value specified in the AMS configuration.
6. If you want to modify the delivery delay, enter a value in the **Delivery Delay** box:
   - -1—Do not modify (default)
   - 0—Remove the delivery delay field (if present)

- Any other value—Number of seconds in the future

This value affects the:

- `deferred-delivery-time` field for UCP
- `schedule-delivery-time` field for SMPP
- `first-delivery-time` field for CIMD

Note: AO-MT messages that have a delivery delay that is a positive value are normally dropped. Set this property to 0 to remove the field and allow these messages to be routed rather than dropped.

7. If you want to modify the `replace-if-present` bit for SMPP messages, enter a value between -1 and 1 in the **Replace If Present** box.

   A value of -1 means that the bit should not be modified (this is the default).

8. If you want to modify the delivery notification request bit, enter a value between -1 and 1 in the **Delivery Notification** box.

   A value of -1 means that the bit should not be modified (this is the default).

9. If you want to modify the non-delivery notification request bit, enter a value between -1 and 1 in the **Non Delivery Notification** box.

   A value of -1 means that the bit should not be modified (this is the default).

10. If you want to modify the buffered notification request bit, enter a value between -1 and 1 in the **Buffered Notification** box.

    A value of -1 means that the bit should not be modified (this is the default).

    The delivery notification request bit, non-delivery notification request bit, and buffered notification request bit modifiers are similar to the semi-static configuration attributes `overridedeliverynotificationrequestforaoaomessages`, `overridenondeliverynotificationrequestforaoaomessages`, and `overridebufferednotificationrequestforaoaomessages`, respectively. For each bit, you may set the parameter to a non-default value in the MGR or in the semi-static configuration file, but not in both. Changing both items to a non-default value will result in unexpected behaviour. For example, if `Delivery Notification` is set to 1, `overridedeliverynotificationrequestforaoaomessages` must be set to -1 (its default).

11. If you want to modify the notification address for UCP messages, enter a value in the **Notification Address** box (up to 38 characters in length).

    If the specified value is IGNORE (default), the RTR will not modify the notification address. If no value is specified, the RTR will remove the notification address field.

12. If you want to modify the protocol ID, enter a value between -1 and 255 in the **Protocol Id** box.

    A value of -1 means that the protocol ID should not be modified (this is the default).

13. If you want to modify the notification protocol ID for UCP messages, select a value from the **Notification Protocol Id** list:

    - No change (default)
    - None
    - Mobile station
    - Fax group 3
    - X400
    - Menu over PSTN

- PC application over PSTN
- PC application over X25
- PC application over ISDN
- PC application over TCP/IP

14. If you want to modify the priority flag, select a value from the **Priority** list:

    - No change (default)
    - Background
    - Bulk
    - Low
    - Normal
    - Interactive
    - Medium
    - Urgent
    - High
    - Emergency

    Note: UCP messages have Boolean priority values representing priority and non-priority delivery. These values correspond to modifier settings Emergency and Normal, respectively. Using other modifier settings on UCP messages may cause inconsistent priority values to appear in CDRs and log files.

15. If you want to modify the message's single-shot indicator bit, enter a value between -1 and 1 in in the **Single Shot Indicator** box:

    This field affects the single-shot indicator bit in the FCDR's ASER field in submit and deliver CDRs. A value of -1 means that the bit should not be modified (this is the default).

16. Click **Save**.

    The MGR creates the AO modifier and closes the tab.

17. Activate the modifier.

Note: You can change the properties of an active AO modifier; deactivating it is not required.

6.7 Creating AT Modifiers

Application-terminating (AT) modifiers can be used with incoming AT routing (ATIR) rules.

To create an AT modifier:

1. In the left navigation bar, select **Routing ➤ Modifiers ➤ AT**.

   The AT Modifiers tab appears.

2. Click **Add New**.

   A new AT Modifiers tab appears.

3. Enter a unique name for the modifier in the **Name** box (up to 31 characters).
4. Optionally enter a description of the modifier in the **Description** box.
5. If you want to modify the priority flag, select a value from the **Priority** list:

- No change (default)
- Background
- Bulk
- Low
- Normal
- Interactive
- Medium
- Urgent
- High
- Emergency

6. Click **Save**.
   The MGR creates the AT modifier and closes the tab.
7. Activate the modifier.

Note: You can change the properties of an active AT modifier; deactivating it is not required.

6.8 Priority Values for AO and AT Modifiers

The values that are available for the AO and AT message priority modifiers correspond to:

Priority	SMPP	UCP	CIMD
Background	4	0	9
Bulk	0	0	8
Low	0	0	7
Normal	1	0	6
Interactive	1	1	5
Medium	2	1	4
Urgent	2	1	3
High	3	1	2
Emergency	3	1	1

Chapter 7

Routing Numbers

Topics:

7.1 Introduction

A routing number (RN) is a hexadecimal address prefix of up to eight digits (0-9 and a-f; only lowercase characters are supported). If RN functionality is enabled, the RTR attempts to match a received address against a set of known RNs. The RTR supports RN matching for:

- The recipient MSISDN in MO messages
- The recipient IMSI in SendRoutingInfoForSm (SRI-SM) responses

RN matching functionality can be enabled or disabled independently for each type.

When the RTR detects an RN, it removes the matching digits from the beginning of the MSISDN or IMSI.

7.2 Routing Number Groups

Routing numbers (RNs) are organized in RN groups, which you create in the MGR (under **Routing ➤ Routing Numbers ➤ RN Groups**).

An RN matches an RN group if:

- The prefix matches, and
- The TON and NPI values match, if they are specified in the RN group configuration

By default, the TON and NPI are not specified. When the RTR detects an RN, it removes the matching digits from the beginning of the MSISDN or IMSI.

MO and AO routing rules can contain a recipient RN group condition, which enables routing based on the matched RN. If an address does not match any group, it can be assigned to a default RN group. MO and AO rules can use this default group in the recipient RN group condition (although the condition will effectively only contain addresses without RNs). You can configure different default groups for recipient MSISDNs and IMSIs.

The RTR provides total and per-address counters for individual RN or RN group matches. You can retrieve these counters via SNMP for monitoring purposes.

7.3 Recipient Routing Number Billing

Matched RNs are stored in MO and AO log records and can be included in the proprietary `RecipientRoutingNumber` field in LogicaCMG billing records. This field can be enabled in the Manager if the FCDR file format has been selected.

Up to 100 RN groups can be defined in the RTR, with up to 100 RNs in each group.

7.4 Including Recipient IMSI in AO Rules

To use routing numbers when routing AO messages, set the **Early SRI-SM for AO/SM** parameter in the MGR GUI (**Routing ➤ Properties**). This instructs the RTR to perform an HLR query to retrieve the recipient IMSI before evaluating the AO rules.

If the HLR query for the IMSI results in a permanent error, the RTR will ignore the error and will not return a NACK for the AO message.

Retrieving IMSI for a Subset of Recipients

This functionality may only be required for a subset of recipients. In the MGR, you can define a list of recipient numbers for which the RTR should send an HLR query. Then, use the **Early SRI-SM for AO/SM Whitelist** parameter in the MGR GUI (**Routing ➤ Properties**) to refer to the list.

Note: If the RTR cannot find the list that is specified in the configuration file, it will send HLR queries for all numbers. Therefore, it is important that the list is not removed from the MGR. The MGR does not read the configuration file and therefore does not provide a warning if you attempt to remove the list. It is recommended to include a reminder in the list name (for example, `AOWhiteList_DO_NOT_REMOVE`).

Chapter 8

Address Conversions

Topics:

8.1 Introduction

Address conversion applies to **all** inbound messages (MO, MT, AO, AT). Address conversion affects the addresses in the CDR if the chosen format in the billing profile is not "transparent".

8.2 Number Normalization

The normalized form of an MSISDN is equal to a internationally significant number, in other words, starting with the country code.

When no GSM address conversion rules are defined, the RTR uses a scheme for number normalization that is based on the TON, NPI, the number of digits, and any national or international prefix digits.

The rule processor bases its actions on normalized numbers. This does not imply that the RTR modifies numbers, the pre-normalized value will still be used within outgoing messages.

The primary addresses used in rule matching are the:

- Recipient address
- Originator address
- SMSC (MAP level) address
- MSC address.

Because the rule processor matches against the normalized numbers, it is important to understand the normalization algorithm.

8.2.1 Normalization Algorithm

The normalization algorithm employs the global parameter `maxlengthforshortnumber`. This value is configurable between 3 and 6 (default is 5).

For the normalization algorithm to work the following parameters must be correctly configured:

- `nationalprefix` (default is 0)
- `internationalprefix` (default is 00)
- `countrycode`

```
IF TON = Alphanumeric THEN
    (Number is alphanumeric.)
    DONE
ELSE IF no conversion rules are present THEN
    IF number of digits <= maxlengthforshortnumber THEN
        (Number is a short number.)
        DONE
    ELSE IF  NPI is ISDN/Telephony  AND  TON is national or unknown  THEN
        IF number starts with international prefix  THEN
            Strip international prefix.
            (Number is an MSISDN.)
            DONE
        ELSE IF number starts with national prefix  THEN
            Strip national prefix.
            Add country code.
            (Number is an MSISDN.)
```

```
            DONE
        ELSE
            Add country code.
            (Number is an MSISDN.)
            DONE
        END IF
    ELSE
        (Number is an MSISDN.)
        DONE
    END IF
ELSE IF matching conversion rule can be found THEN
    Perform Advanced Number Normalization.
    DONE
ELSE IF number of digits <= maxlengthforshortnumber THEN
    (Number is a short number.)
    DONE
ELSE
    (Number is an MSISDN.)
    DONE
END IF
```

An error is generated if the normalization results in a number longer than 38 digits.

8.2.2 Originator Short Number Address

In an AO message, an originator short number address with TON=6 (`abbreviated`) and NPI=1 (`isdnTelephony`) will be converted to have TON=0 (`unknown`) and NPI=1 (`isdnTelephony`).

8.3 Advanced Number Normalization

Advanced number normalization can be applied by using GSM address conversion rules. These GSM address conversion rules can be provisioned using the MGR.

The addresses that result from a conversion are used by the rule processor to match conditions in any kind of rules, including external condition rules. Furthermore, the addresses are used when the RTR requires a conversion to international format for a specific purpose (for example, doing an HLR query or an HLR update).

For AT messages, the converted originator address is used if the `atoriginatorformat` parameter is set to `national` or `international` and the converted recipient address is used if the `atrecipientformat` parameter is set to `national` or `international`.

The converted addresses are used in some but not all billing formats.

8.3.1 GSM Address Conversion Rules

The GSM address conversion rules have the ability to recognize and insert area codes into MSISDNs. These area codes pertain to the operator's own/home country (as identified by the globally configured `countrycode`). These area codes are not intended for use in combination with different countries.

To be able to recognize the home country area codes, they must be specified as follows:

- For countries with *fixed-length* area codes, use the parameter **Fixed Area Code Length**, accessible via **Routing ➤ Address Conversion ➤ Properties** in the MGR, to set the fixed area code length (valid values are 0-6, default is 0).

- For countries with *variable-length* area codes, specify the area codes in the area code table in the MGR via **Routing ➤ Address Conversion ➤ Area Codes**. The area codes can be 1 up to 6 digits.

Note: Either a fixed-length area code or variable-length area codes can be provisioned. It is not possible to provision both.

GSM address conversion rules are specified in the MGR via **Routing ➤ Address Conversion ➤ Conversion Rules**. A maximum of 1000 GSM address conversion rules configuration is supported. Each address conversion rule consists of the following parameters:

Parameter	Description
Description	A unique description for this conversion rule.
Input TON	The value for Type of Number (TON) that should match the TON of an address-to-be-converted in order for the GSM address conversion rule to apply. Possible values are: • any (wildcard) • unknown (default value) • international • national • networkActual • subscriber • abbreviated All other values are reserved. For details (standard values) refer to 3GPP TS 23.040.
Input NPI	The value for Numbering Plan Identification (NPI) that should match the NPI of an address-to-be-converted in order for the GSM address conversion rule to apply. Possible values are: • any (wildcard) • unknown (default value) • isdnTelephony • data • telex • national • private • ermes All other values are reserved. For details (standard values) refer to 3GPP TS 23.040.
Input Address Prefix	Specifies the input pattern for the prefixing digits of the GSM address. The pattern is a string (up to 38 characters) and may contain only digits and, optionally, one or more `N` wild card character(s) and/or one `A` wild card character, where:

Parameter	Description
	• A matches the longest area code defined in the area code list provisioned in **Routing ➤ Address Conversion ➤ Area Codes**. **Note:** The longest area code match takes priority for multiple applicable matches. • N matches a single digit.
Input Minimum Address Length	Minimum value for length (0 up to 38) of an address-to-be-converted in order for the GSM address conversion rule to apply.
Input Maximum Address Length	Maximum value for length (0 up to 38) of an address-to-be-converted in order for the GSM address conversion rule to apply.
Output Address Prefix	Specifies the GSM address output pattern. This field specifies the output replacement pattern (up to 38 characters) for the prefixing digits of the GSM address. The pattern may contain only digits and, optionally, one or more N character(s) and, optionally, one A and/or @ character, where: • A is replaced by the area code matched by the respective A in the input pattern **Input Address Prefix**. • N is replaced by the digit matched by the respective N in the input pattern **Input Address Prefix**. • @ is replaced by the area code for local number support.
Output Type	Specifies how an address is classified. Possible values are: • `determinedByLength` (default), implies that the address type is determined based on the address length. If the length exceeds the threshold that has been configured for the `maxlengthforshortnumber` parameter in the common configuration file, the rule processor will treat the address as an MSISDN. Otherwise, it will be treated as a short number. • `msisdn`, indicates that the rule processor should treat the address as an MSISDN • `shortNumber`, indicates that the rule processor should treat the address as a short number.

Note: Address conversion rules may not overlap each other within the conversion "space". Meaning, a particular **Input TON**, **Input NPI**, and **Input Address Prefix** combination may only be covered by one conversion rule. Trying to activate a second conversion rule that exactly matches another active rule's **Input TON**, **Input NPI**, and **Input Address Prefix**, will result in an error. However, two rules with the same input TON, NPI, and Prefix are allowed, provided that their input address length ranges do not overlap.

Refer to the MGR Operator Manual for more details.

When none of the configured GSM Address Conversion rule matches for a message, RTR treats the number as normalized without any further processing. This implies RTR will not strip any prefix or add any prefix to the received number and treat it as normalized MSISDN or short number (as per the normalization algorithm described in section *Normalization Algorithm*).

8.3.2 Default GSM Address Conversion

This section describes the RTR's default GSM address conversion rules. These rules are used if you do not create any address conversion rules. If you create at least one address conversion rule, the default rules are disabled.

Input TON	Input NPI	Input Address Prefix	Input Minimum Address Length	Input Maximum Address Length	Output Address Prefix	Output Type
national	isdntelephony	[national prefix]	7	15	[local country code]	msisdn
unknown	isdntelephony	[national prefix]	7	15	[local country code]	msisdn
national	isdntelephony	[international prefix]	7	15	(blank)	msisdn
unknown	isdntelephony	[international prefix]	7	15	(blank)	msisdn
national	isdntelephony	(blank)	7	13	[local country code]	msisdn
unknown	isdntelephony	(blank)	7	13	[local country code]	msisdn

Note: If you create address conversion rules, ensure that you set the length conditions to match the address lengths that you expect to see in actual traffic.

8.3.3 GSM Address Conversion Examples

This section provides some address prefix conversion examples using wildcard characters.

Example 1

Sample values:

- **Input Address Prefix** = 12A34
- **Output Address Prefix** = 567A8

If the area code table contains two area codes, 09 and 111, then the following example numbers will be transformed as follows:

- 12**09**3477777 into 567**09**877777
- 12**111**3499999 into 567**111**899999

Example 2

Sample values:

- **Input Address Prefix** = 12N34
- **Output Address Prefix** = 567N8

The following example numbers will be transformed as follows:

- 12**9**3477777 into 567**9**877777
- 12**5**3499999 into 567**5**899999

Example 3

Sample values:

- **Input Address Prefix** = 12AN34
- **Output Address Prefix** = 9A0N

The following example numbers will be transformed as follows, provided that 87 appears in the area code list:

- 12**87**634 into 9**87**0**6**

8.3.4 Local Number Support for MO-MT

The GSM address conversion rules are also used for local number support, where the area code can be skipped when submitting an MO-MT message within the same area.

For local number support, the **Output Address Prefix** parameter in the conversion rule can contain an at sign (@), which will be replaced with the area code as present in the originator of the message.

Local Number Support for MO-MT Example

This example illustrates a fixed-length area code configuration when the originator address is 551234567890 and the recipient address is 99887766:

- Country code = 55 (specified by `countrycode` in the common configuration file)
- **Fixed Area Code Length** = 2
- **Input TON** = unknown
- **Input NPI** = ISDN Telephony
- **Input Address Prefix** = ' '
- **Input Minimum Address Length** = 8
- **Input Maximum Address Length** =8
- **Output Address Prefix** = 55@

The fact that **Input Address Prefix** is not set to a value indicates that the value of the digits received for the destination can be anything, as long as the address consists of exactly eight digits.

To determine the area code to use in the destination address, the country code (55) is removed from the originator address, resulting in the area code of 12. The address

conversion rule then prefixes the destination address with 55 and the area code of the sender (represented by @). Because the area code is 12, the resulting recipient address is 551299887766.

Note: When the Intermediate Cache (Icache) is in use, the recipient address used when a message state is stored in the Icache must match the recipient address used when a message state is looked up in the Icache. Therefore, if your configuration requires local number support for MO messages, the inside-only application must be configured with an address format of "international" for both the originator and the recipient address. Otherwise, the recipient addresses will not match as is required for the Icache.

8.3.5 GSM Address Conversion Rules for Originator Address

The GSM address conversion rules are also used for Originator address translation. The translated address is used in:

- CDRs (if Originator format is International in FCDR billing profile)
- Rules Evaluation
- Diameter Charging Request/ECI Requests (if Originator format is International in ECI Application)
- IN Server Charging
- Originator address sent in MTFSM/Deliver SM is not impacted. Translated address is not used in outgoing messages.

The RTR converts 6-digit source address to 4-digits address for CAMEL Charging, Diameter Charging and FCDR. However, in outgoing MTFSM/Delivery SM the original 6-digit short code will be sent.

GSM address conversion rule for AO-ST-MT Example with IN Server charging

This example illustrates the originator address conversion for AO-ST-MT case with IN server as charging with the originator address as 446677 (source address in Submit SM request message):

- **Input TON** = Any
- **Input NPI** = Any
- **Input Address Prefix** = 4466NN
- **Input Minimum Address Length** = 6
- **Input Maximum Address Length** = 6
- **Output Address Prefix** = 4466
- **Output Type** = Short Number

These GSM AC rules convert the originator address value from 446677 to 4466 in the ECI request, IDP Request (to IN server). For MT-FSM request, 446677 will be used.

The following diagram explains the above example in case of CAMEL as IN server charging:

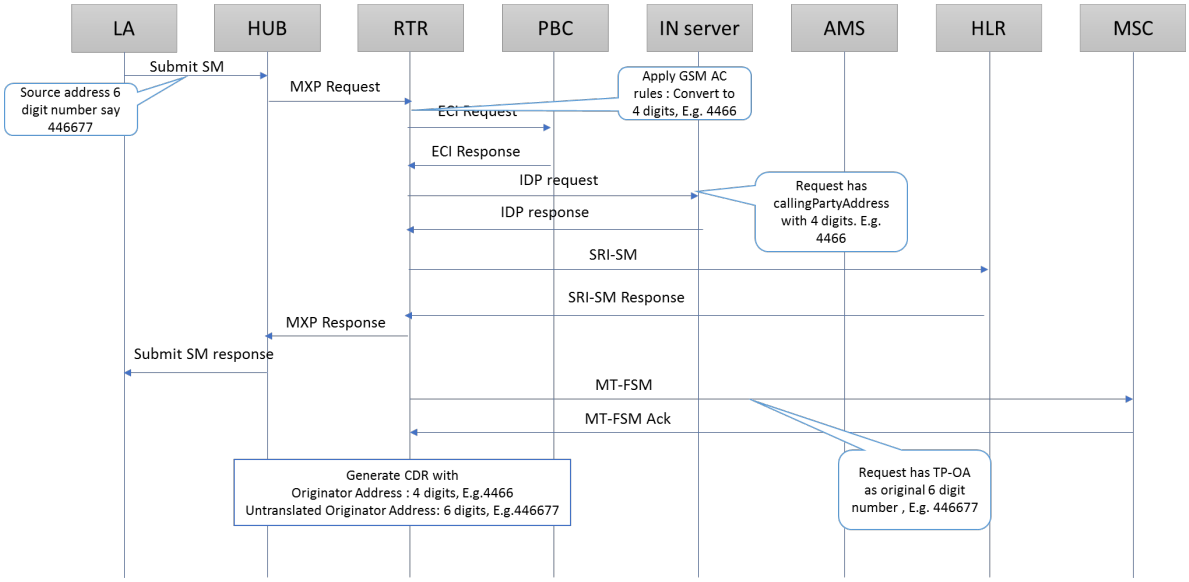


Figure 20: Flow Diagram where an IN server is used for charging

GSM address conversion rule for AO-ST-MT Example with Diameter server as charging

This example illustrates the originator address conversion for AO-ST-MT case with diameter server as charging with the originator address as 446677 (source address in Submit SM request message):

- **Input TON** = Any
- **Input NPI** = Any
- **Input Address Prefix** = 4466NN
- **Input Minimum Address Length** = 6
- **Input Maximum Address Length** = 6
- **Output Address Prefix** = 4466
- **Output Type** = Short Number

These GSM AC rules convert the originator address value from 446677 to 4466 in the ECI request, Diameter Messages. For MT-FSM request, 446677 will be used.

The following diagram explains the above example in case of diameter server used for charging:

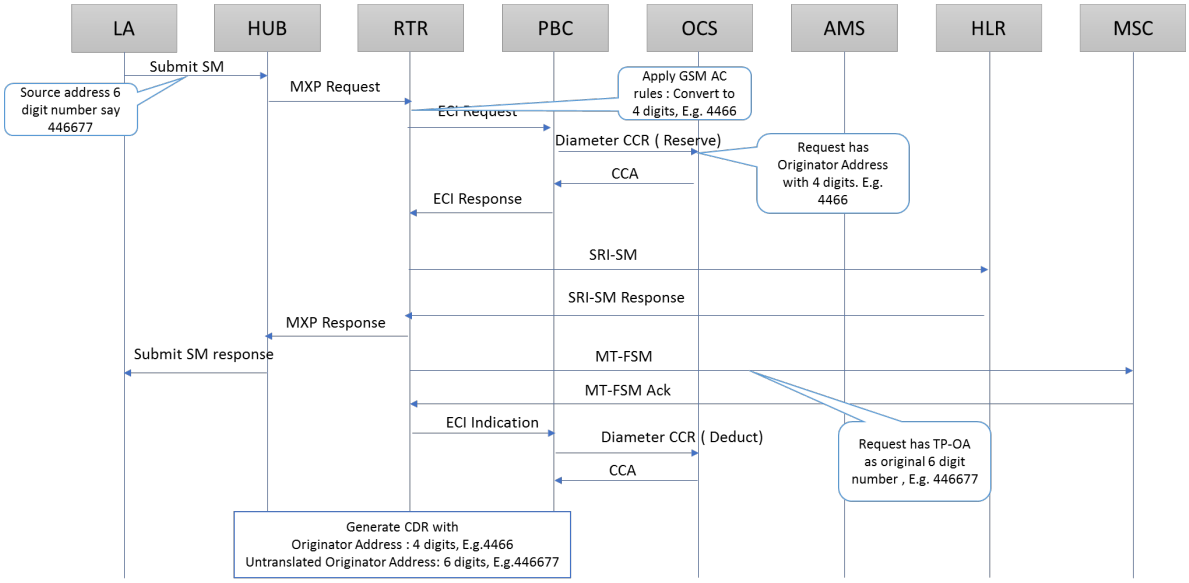


Figure 21: Flow Diagram where a Diameter server is used for charging

Note:

The semi-static parameter *rtrusetransaddrforabbreviatednumberforfcdr* will allow the use of translated address in case of Abbreviated numbers in FCDR. The default value is false for this parameter.

If set to true, the RTR will use the translated address for an abbreviated originating number. The impacted FCDR fields are origAddress and origAddressGSM and they will contain the translated address (GSM AC rule applied).

The FCDR fields untranslOrigAddress and untranslOrigAddressGSM will contain the untranslated addresses.

For Notification FCDR, orglOrigAddress and orglOrigAddressGSM will contain the translated value (GSM AC rule applied).

This parameter does not affect other values of Originator TON (besides abbreviated) and will display the translated address in the FCDR as long as the Originator format is set to international in the FCDR billing profile.

8.4 Numbering Plan Change Support

The RTR supports numbering plan changes by allowing the normalized address (the output of the number normalization process described in the previous chapters) to be modified according to some numbering plan change. When in use, the output of the numbering plan change processing logic replaces the output of the number normalization process for all subsequent message processing and storage within the RTR SPF.

The numbering plan change feature allows changing the prefix of normalized addresses, which (prior to the numbering plan change processing) match against a provisioned set of address prefixes. The feature first selects which normalized addresses should be changed, and then changes them by replacing the first *N* digits with a configurable new prefix.

The behavior of the numbering plan change processing is provisioned through the semi-static common configuration file. Selection of the to-be-modified addresses is done based on the *planchangeprefix* entities, and the address modification is controlled by the *planchangeaction* entities. Typically, multiple *prefix* entities refer to one *action* entity. The *prefix* entity with the longest matching prefix will determine the action to be applied. The *action* entity may impose additional conditions on the normalized address in order to apply the prefix replacement, such as a maximum and/or minimum length. However, if these conditions are not met, no other action will be attempted to be applied, and the normalized address is left unchanged.

Up to 10000 prefixes and up to 100 actions can be provisioned. Refer to *Configuration* for more information on syntax and semantics of these two entities.

For troubleshooting, both the prefix and the action MIB tables contain a counter indicating how often a prefix matched or an action was applied:

```
tp_walk numberingPlanChangePrefixTable

tp_walk numberingPlanChangeActionTable
```

Example

The following example shows an excerpt of the common configuration file, which has the effect that all normalized addresses that start with "3161" will have the "316" prefix replaced by "3151", except for numbers that start with "31616". The example also shows that numbering plan change processing can change the length of a normalized address.

```
<planchangeaction name="xyz" strip="3" prefix="3151" minlength="11" />

<planchangeprefix digits="3161" action="xyz" />

<planchangeprefix digits="31616" />
```

If the normalized address, input to the numbering plan change processing, is "31612345678", then the first of the two provisioned prefixes will match, the "xyz" action is selected, and the first three digits ("316") will be replaced by "3151", producing a changed address of "315112345678".

If the normalized address is "31616987654", then the second of the two provisioned prefixes will match, no action is selected, and the number remains unchanged.

If the normalized address is "31625556666", no prefix matches and the number remains unchanged.

If the normalized address is "3161234567", the first of the two provisioned prefixes will match and the "xyz" action is selected, but since the length of the normalized address is only 10 digits, which is less than the required minimum length of 11 digits, no prefix replacement takes place and the number remains unchanged.

8.5 Outgoing Address Conversion

The Outgoing Address Conversion functionality is supported by multiple sets of Outgoing Address Conversion Rules. Like the GSM address conversion rules, the sets of outgoing address conversion rules also can be provisioned from the MGR GUI; however, these rules can be applied only on various address fields of outbound MT or AT messages. Also, unlike the GSM address conversion rules no default set of outgoing address conversion rules is supported.

The outgoing address conversion rule set can be selected for each MT or AT routing rule. Refer to *MT Outgoing Address Conversion* or *AT Outgoing Address Conversion* for more details.

The outgoing address conversion functionality can perform various customized manipulation of the digit string in an outgoing Originator address field. For example, these rules can be used to insert a Carrier Specific Prefix (CSP) in the outgoing Originator address such that the CSP is placed immediately after an initial long-distance prefix or international prefix of the address string.

8.5.1 Outgoing Address Conversion Rule Sets

Outgoing Address Conversion rule sets are specified in the MGR via **Routing ➤ Address Conversion ➤ Out. Rule Sets** with the following parameter:

Parameter	Description
Name	Outgoing address conversion rule set name

A maximum of 500 Outgoing Address Conversion Rule set configuration is supported.

8.5.1.1 Outgoing Address Conversion Rules

To create an outgoing address conversion rule select the rule set and click **Add New**. A maximum of 1000 Outgoing Address Conversion Rule configuration is supported. Each outgoing address conversion rule consists of the following parameters:

Parameter	Description
Name	Outgoing address conversion rule name (optional)
Input TON	The value for Type of Number (TON) that should match the TON of an address-to-be-converted in order for the Outgoing address conversion rule to apply. Possible values are: • any (wildcard) • unknown (default value) • international • national • networkActual • subscriber • abbreviated All other values are reserved. For details (standard values) refer to 3GPP TS 23.040.
Input NPI	The value for Numbering Plan Identification (NPI) that should match the NPI of an address-to-be-converted in order for the Outgoing address conversion rule to apply. Possible values are: • any (wildcard) • unknown (default value) • isdnTelephony • data

Parameter	Description
	• telex • national • private • ermes All other values are reserved. For details (standard values) refer to 3GPP TS 23.040.
Input Address Prefix	Specifies the input pattern for the prefixing digits of the Outgoing GSM address. The pattern is a string (up to 38 characters) and may contain only digits and, optionally, one or more `N` wild card character(s) and/or one `A` wild character, where: • `A` matches the longest area code defined in the area code list provisioned in **Routing ➤ Address Conversion ➤ Area Codes**. **Note:** The longest area code match takes priority for multiple applicable matches. • `N` matches a single digit.
Input Minimum Address Length	Minimum value for length (0 up to 38) of an address-to-be-converted in order for the Outgoing address conversion rule to apply.
Input Maximum Address Length	Maximum value for length (0 up to 38) of an address-to-be-converted in order for the Outgoing address conversion rule to apply.
Output TON	May specify an exact Type of Number (TON) value to be used in the output address. Possible values are: • default • unknown • international • national • networkActual • subscriber • abbreviated All other values are reserved. For details (standard values) refer to 3GPP TS 23.040.
Output NPI	May specify an exact NPI value to be used in the output address. Possible values are: • default • unknown • isdnTelephony • data

Parameter	Description
	• telex • national • private • ermes All other values are reserved. For details (standard values) refer to 3GPP TS 23.040.
Output Address Prefix	Specifies the GSM address output pattern. This field specifies the output replacement pattern (up to 38 characters) for the prefixing digits of the Outgoing GSM address. The pattern may contain only digits and, optionally, one or more `N` character(s) and, optionally, one `A` and/or `@` character and/or one `C` character, where: • `A` is replaced by the area code matched by the respective `A` in the input pattern **Input Address Prefix**. • `N` is replaced by the digit matched by the respective `N` in the input pattern **Input Address Prefix**. • `@` is replaced by the area code for local number support. • `C` is replaced by the Carrier Specific Prefix of the operator.
Output Address	Specifies the exact output address with a maximum of 38 digits or 11 alphanumeric characters. **Note:** It is not possible to specify both an output address prefix and an exact output address.

Notes:

- Outgoing address conversion rules may not overlap each other within the "conversion space". Meaning, a particular Input TON, Input NPI, and Input Address Prefix combination may only be covered by one outgoing conversion rule. Trying to activate a second outgoing conversion rule that exactly matches another active rule's Input TON, Input NPI, and Input Address Prefix, will result in an error.

  However, two outgoing rules with the same input TON, NPI, and Prefix are allowed, provided that their input address length ranges do not overlap.
- In case both output TON and output NPI are set to `default` for MT originator address the RTR will follow some older conversion semantics in order to avoid a possible upgrade issue. Refer to *MT Outgoing Address Conversion* for more details.
- As specified in *MT Outgoing Address Conversion*, Outgoing address conversion is not applied in case of delivery to IMS domain (SIP-MT).
- Some other limitations for MT messages are described in *MT Outgoing Address Conversion*.

Refer to the MGR Operator Manual for more details.

8.5.2 Outgoing Address Conversion Examples

This section provides some outgoing address conversion examples.

1. CSP insertion when recipient subscriber is in home network and Originator address is own country number.

If for an operator say, its MSC address starts with 3161 and IMSI range is of the form 26202*

- The MTOR rule should be provisioned with appropriate Terminating MSC Address and Recipient IMSI conditions and the 'Outgoing Address Conversion' option should be selected as 'Originator'.
- 'Outgoing Address conversion' rules should be provisioned to strip the country code and add the following: <long-distance dialing prefix> (e.g. '0')<CSP>.

> **Example 1**
>
> Sample values:
>
> - **Input Address Prefix** = 31
> - **Output Address Prefix** = 0C
>
> If the CSP is configured as "41", the numbers will be transformed as follows:
>
> - 31617778888 into 041617778888

2. CSP insertion when recipient subscriber is in home network and Originator address is another country number.

If for an operator say, its MSC address starts with 3161 and IMSI range is of the form 26202*,

- The MTOR rule should be provisioned with appropriate Terminating MSC Address (i.e. not equal to 3161*) and Recipient IMSI conditions and the 'Outgoing Address Conversion' option should be selected as 'Originator'.
- 'Outgoing Address conversion' rules should be provisioned to add the following: <international dialing prefix> (e.g. '00')<CSP>.

> **Example 2**
>
> Sample values:
>
> - **Input Address Prefix** = ' '
> - **Output Address Prefix** = 00C
>
> If the CSP is configured as "41", the numbers will be transformed as follows:
>
> - 49617778888 into 004149617778888

8.6 Address Format Configuration

8.6.1 AT Address Format Conversion

To convert address formats in application-terminated (AT) messages, you can configure the following attributes in the semi-static configuration file, depending on the `useaddressformattingforatnotifications` attribute:

- `atoriginatorformat` (originator address)
- `atrecipientformat` (recipient address)
- `atmscformat` (MSC address)
- `atsmscformat` (SMSC address)

Each attribute can be set to:

- transparent (default)
- national
- international

Each attribute can be overridden per application in the MGR.

8.6.2 ECI Address Format Conversion

To convert address formats in external condition interface (ECI) messages, you can configure the following attributes in the semi-static configuration file:

- `ecioriginatorformat` (originator address)
- `ecirecipientformat` (recipient address)
- `ecimscformat` (MSC address)
- `ecismscformat` (SMSC address)

Each attribute can be set to:

- transparent (default)
- national
- international

Each attribute can be overridden per EC application in the MGR.

8.6.3 National Originator Address Format for FDA

For first delivery attempts (FDAs), the originator address format can be configured to represent a national originator address. The `mtoriginatorformatfordomestictraffic` (only applies when the recipient and the originator are in the same country) attribute in the semi-static configuration file controls the format. The attribute can be set to:

- transparent (default)
- national
- international

For example, this functionality can cause the recipient to see an originator address as `017234567890` instead of `+4917234567890`.

Note: To forward the message to the SMSC if the FDA does not succeed, the originator address must be in international format (`+4917234567890`).

8.6.4 Address Format Configuration in Billing Profile

The address format to be used in the billing records can be chosen in the billing profile. When the address format is set to "national" or "international", the billing record will contain the converted address. In case "transparent" is chosen, the unformatted and unconverted address will appear in the

billing records. For example, if someone submitted an SMS with "0612345678" as destination number, the recipient address will appear as "0612345678" in the billing record.

Chapter 9

MO Routing

Topics:

9.1 Introduction

Mobile-originating (MO) routing is the generic name for the processing of incoming MO messages. To deliver MO messages to their destinations, the RTR works in conjunction with the HUB for routing to applications and in conjunction with the AMS for routing that involves storage.

MO routing (MOR), external condition (MOX), and counting (MOC) rules operate on MO messages. The following diagram illustrates the entities that are involved in MOR rules.

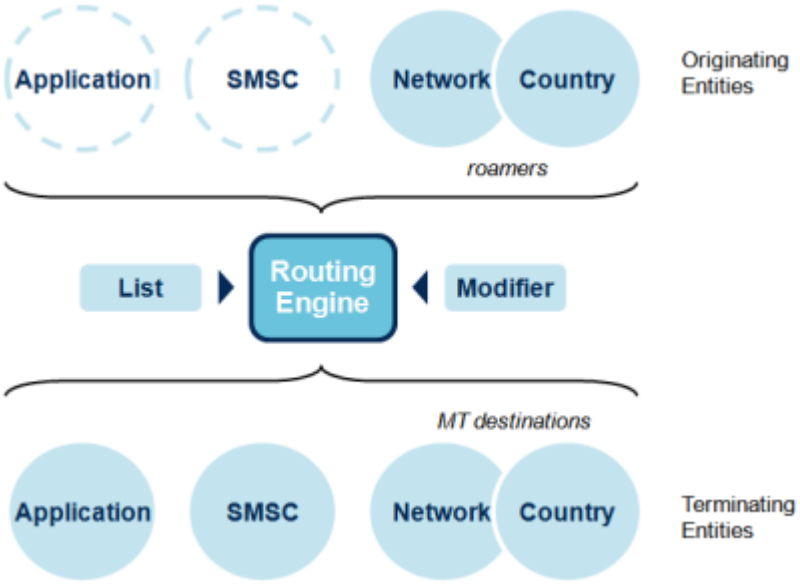


Figure 22: MOR entities

The following diagram illustrates how the RTR handles the parameters that influence MO messages are routed.

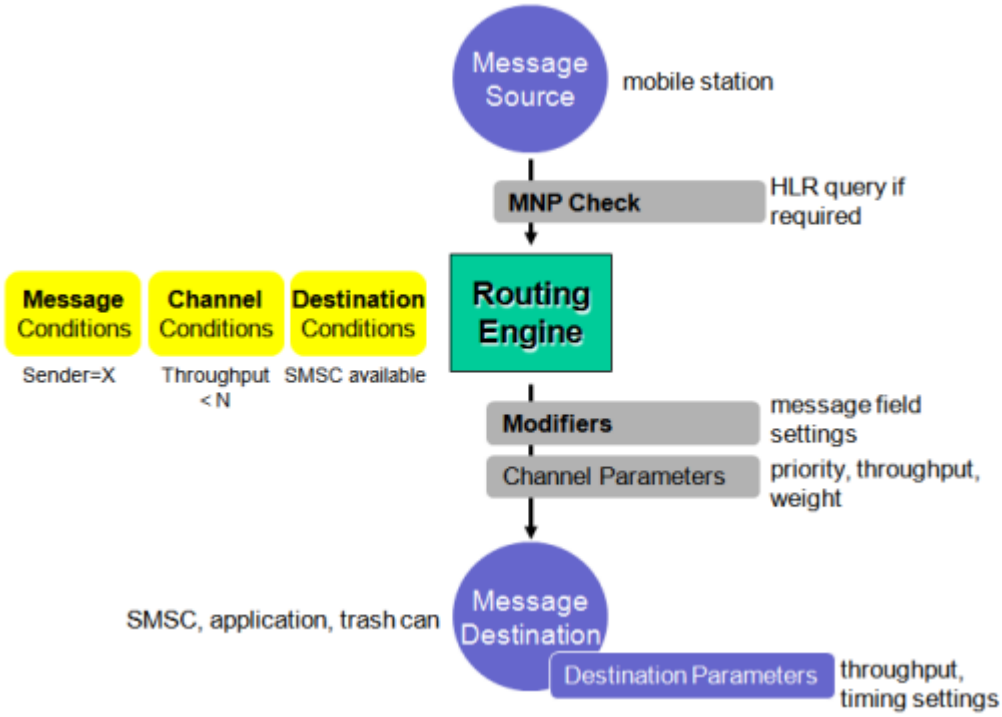


Figure 23: MOR parameters

For an MO message, the message source is always a mobile station. The message destination is another mobile station or an SMSC, an application, or the trash can (if the message is discarded). The mobile number portability (MNP) check for originator performs an HLR query only if it is required.

An MO rule contains the following types of conditions:

Condition Type	Description	Example
Message	Message conditions can evaluate virtually any message field. You set these conditions when defining the MO rule.	• Recipient = 31652463380 • Data coding scheme = 12
Channel	Channel conditions evaluate the properties of the route to the destination.	Throughput resulting from this rule to SMSC1 ≤ 100 messages per second
Destination	Destination conditions evaluate the condition of the destination.	• Application 2200 is available • Total throughput toward SMSC3 for all rules ≤ 750 messages per second

You can define up to:

- 500 MOR rules
- 500 MOX rules
- 500 MOC rules

9.2 MO Routing Paths

This section discusses MO routing paths in detail.

9.2.1 MO-MO Routing

In the MO-MO routing path (also called route to SMSC), incoming MO traffic is routed toward an SMSC. MO-MO routing provides the following features:

- Monitoring
- Message control based on message processing or redirection
- Mobile number portability (MNP) verification for originator (if enabled)
- Advanced load balancing using prioritized and weighted schemes

The following diagram depicts the MO-MO routing path:

Figure 24: MO-MO routing

An MO-MO routing rule can be applied as a primary routing rule or as a fall-through rule, depending on the priority and conditions in MO routing.

The primary objective of message control is to protect the SMS infrastructure from overload, congestion, and misuse. Throughput control, load balancing, and optimised MNP checks support this objective.

9.2.2 MO-MT Routing

In the MO-MT routing path incoming MO traffic is processed and delivered using optimized MT delivery. MO-MT routing provides the following features:

- Route incoming MO traffic
- Directly delivery MT messages to mobile recipients
- Discard MO messages on failure
- Generate CDRs (if configured)

MO-MT routing can provide SMSC offloading and offers differentiated SMS service. MO-MT routing can optionally be combined with a phase 1 status report that is returned to the originator if the first delivery attempt (FDA) was unsuccessful and the message was discarded. Also, MO-MT routing can be configured with direct MT delivery, called optimized MT routing (see *Optimized MT Routing*).

The following diagram depicts the MO-MT routing path:

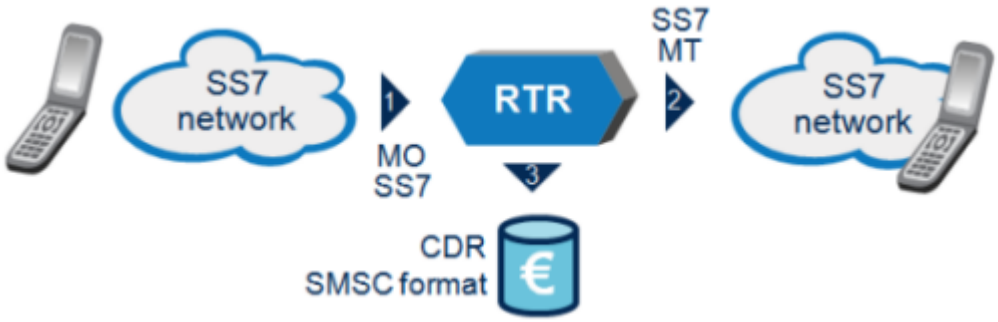


Figure 25: MO-MT routing

MO-MT routing flows as follows:

1. The sender sends a message, which arrives in the RTR (flow 1).
2. Immediately, the RTR performs a first delivery attempt (FDA) to the recipient, which in the above diagram is a mobile phone (flow 2).
3. If the delivery attempt is successful, a billing record can optionally be generated (flow 3).
4. If the delivery attempt is not successful, the message is dropped and the originator can receive a message not sent message, depending on the configuration.

9.2.3 MO-MT-MO Routing

MO-MT-MO routing can provide SMSC offloading and SMSC overload protection.

MO-MT-MO routing enables:

- Processing of incoming MO messages
- Performing an optimized MT delivery (Try-and-Forward MO)
- Routing MO messages toward an SMSC (if required)
- Generating CDRs (if configured)

The following diagram depicts the MO-MT-MO routing path:

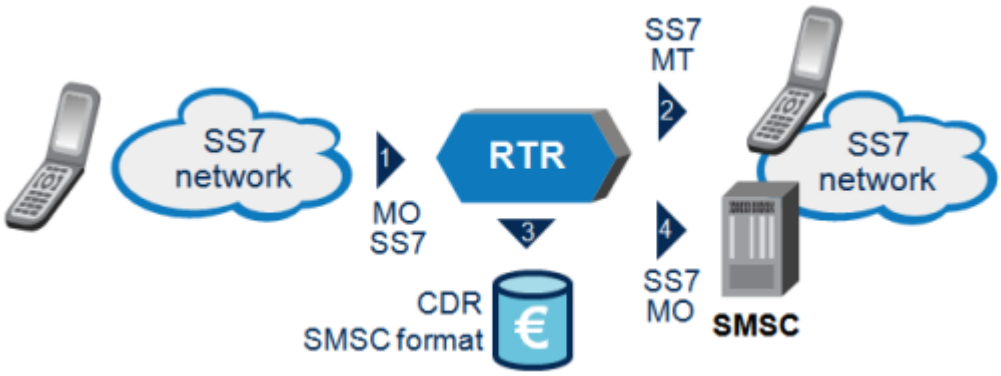


Figure 26: MO-MT-MO routing

MO-MT-MO routing flows as follows:

1. The sender sends an SMS message, which arrives in the RTR (flow 1).

2. Immediately, the RTR performs one delivery attempt to the recipient (flow 2), which in the above diagram is a mobile phone.
3. If the delivery attempt succeeds, a billing record is optionally generated (flow 3).
4. If the delivery attempt does not succeed, the message is forwarded to the appropriate SMSC (flow 4) for further delivery.

   Now, the SMSC will perform delivery retries of the message and generate a billing record when the message is delivered.

MO-MT-MO routing's direct MT delivery functionality can use optimized MT routing, as described in *Optimized MT Routing*.

When MO-MT routing is applied, the RTR only does a single attempt to deliver a message. If that attempt fails, the message is immediately dropped and not stored.

9.2.4 MO-MT-AO Routing

The HUB, in conjunction with the RTR, can support MO-MT-AO routing (*route to* MS *fallback to SMSC Group as AO* or *route to MS fallback to SMSC Application as AO* option in the Manager). In this routing path, the SMS RTR executes the first delivery attempt (FDA).

If this delivery attempt fails, the HUB enables routing the message to the SMSC as an application-originated (AO) message.

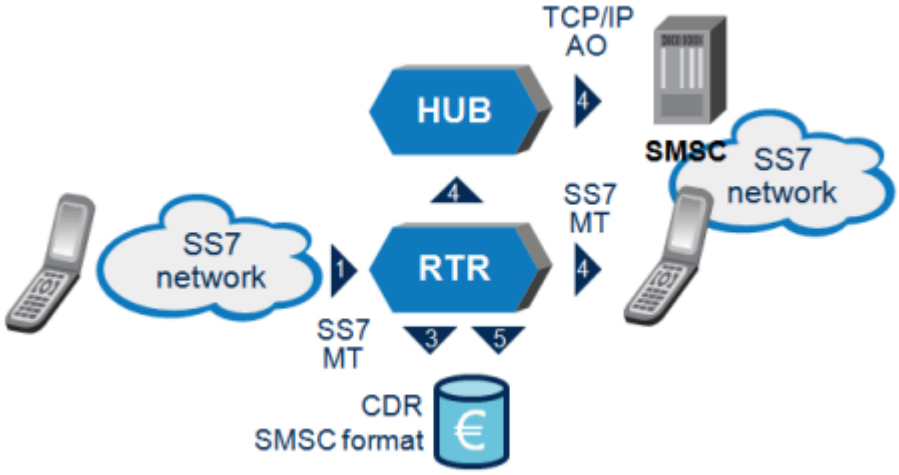


Figure 27: MO-MT-AO routing

The sender sends an SMS message, which arrives in the RTR (flow 1). Immediately, the RTR performs one delivery attempt to the recipient (flow 2), which in this example is a mobile phone. When this delivery attempt is successful, optionally a billing record is generated (flow 3). If the attempt fails, the HUB forwards the message as an AO message to the SMSC over TCP/IP (flow 4). Optionally, a billing record can be generated when the message is delivered to the SMSC (flow 5).

9.2.5 MO-MT-AT Routing

The MO-MT-AT routing path (also called route to MS, fallback to application) enables:

- First delivery attempt (FDA) with AT fallback to an SMS application
- Direct delivery of MO messages to a mobile

- Routing MO messages to an application upon failure
- Generating CDRs (if configured)

The following diagram illustrates the MO-MT-AT routing path:

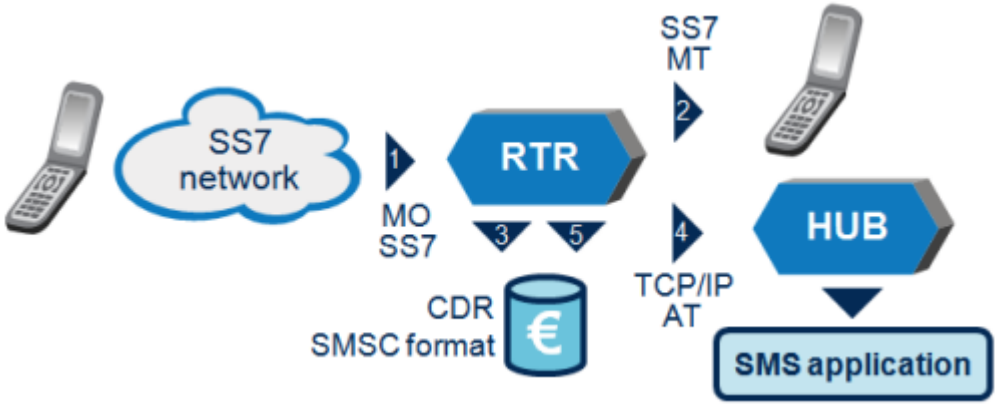


Figure 28: MO-MT-AT routing

MO-MT-AT routing flows as follows:

1. The originator sends an SMS message, which arrives in the RTR (flow 1).
2. Immediately, the RTR performs one delivery attempt to the recipient (flow 2), which in the above diagram is a mobile phone.
3. If this delivery attempt succeeds, a billing record is optionally generated (flow 3).
4. If it does not succeed, the message is forwarded as an application-terminated (AT) message via TCP/IP (using SMPP or UCP) to the appropriate application for further processing (flow 4).

   Optionally, a billing record can be generated (flow 5) when the message is delivered to the application.

   Note: During the AT delivery via store, the configured value of the "outside transmit window size" is used as the `maxtransactions` in the store request. For the AT delivery "outside transmit window size" of the configured application is used for load balancing the traffic towards the HUB.

The application that is used in the MO-MT-AT routing path should be an SMS gateway that offers protocol conversion.

MO-MT-AT routing's direct MT delivery functionality can use optimized MT routing, as described in *Optimized MT Routing*.

Note: To avoid MO timeouts, the RTR sends the ACK to the MO message originator after the MNP check (if applicable) and after evaluating the selected rule.

9.2.6 MO-AT Routing

MO-AT routing processes incoming MO messages and routes them toward SMS applications, using a Deliver SM operation. MO-AT routing provides:

1. Direct delivery of MO messages to an SMS application
2. Decimation (if required)
3. CDR generation (if configured)

Note: The RTR forwards MO messages that are not configured for direct delivery toward an application, to the SMSC only if an MOR rule exists for that.

Note: During the AT delivery via store, the configured value of the "outside transmit window size" is used as the `maxtransactions` in the store request. For the AT delivery "outside transmit window size" of the configured application is used for load balancing the traffic towards the HUB.

The following diagram illustrates the MO-AT routing path:

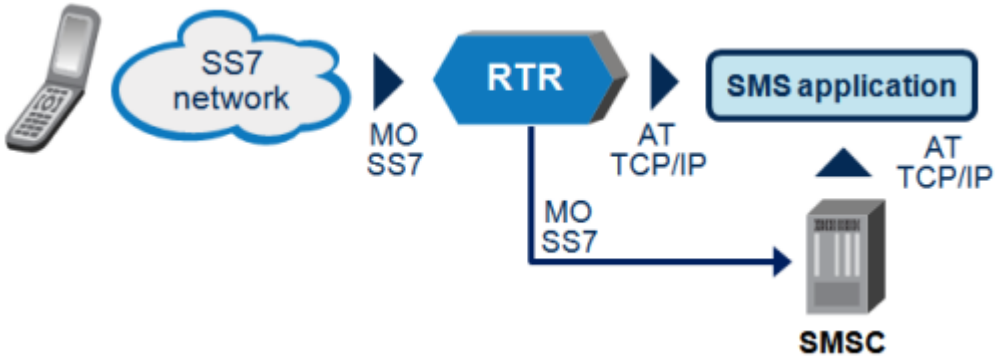


Figure 29: MO-AT routing

Note: The RTR can derive the application destination from the short code specified in the recipient address. This is the default MO-AT routing.

9.2.6.1 SMS Voting Example

The following sample message flow illustrates MO routing for an SMS voting application:

1. An MO message that is destined for a voting application short number is originated in the PLMN.
2. In the PLMN, the message is routed to a RTR.
3. The RTR identifies the message as voting traffic and evaluates the first applicable rule, route to application:
   a) The RTR evaluates the message condition (the destination equals the short number that is associated with the voting application).
   b) The RTR evaluates the destination condition (the application is connected and available).
   c) The RTR evaluates the channel condition (the throughput limit has not yet been reached and the current transmission window is not yet full).
4. If all of the above conditions are true, the RTR performs the specified action for the rule (forwards the message to the voting application).

   If any of the conditions had been false, the RTR could apply subsequent fall-though rules.
5. The voting application responds with the result status of the message delivery (ACK or NACK).
6. The RTR creates a CDR that reflects the result in the status field.
7. The RTR initiates a status report toward the originator (if it was requested), reflecting the success of the message delivery.

9.2.6.2 SMS Voting Example: First Fall-Through Rule

The following sample message flow illustrates a typical first fall-through rule for an SMS voting application:

1. Evaluate the first applicable fall-through rule, route to SMSC.
   a) The RTR does not have to evaluate the message condition, as it was evaluated in the initial rule.
   b) The RTR evaluates the destination condition (SMSC is available).
   c) The RTR evaluates the channel condition (the throughput limit for this route and the total SMSC throughput have not yet been reached).
2. If all of the above conditions are true, the RTR performs the specified action for the rule (forwards the message to the SMSC).

   If any of the conditions had been false, the RTR could apply subsequent fall-though rules.
3. The SMSC responds with the result status of the message delivery (ACK or NACK).
4. The SMSC creates a CDR that reflects the result in the status field.
5. The SMSC initiates a status report toward the originator (if it was requested), reflecting the success of the message delivery.

9.2.6.3 SMS Voting Example: Second Fall-Through Rule

The typical second fall-through rule for an SMS voting application might have one of the following actions:

1. Discard the message with ACK and create a CDR that reflects this result in the status field
2. Discard the message with NACK and do not create a CDR.

9.2.6.4 SMS Voting Example: Message Flow

The following diagram illustrates the MO routing message flow.

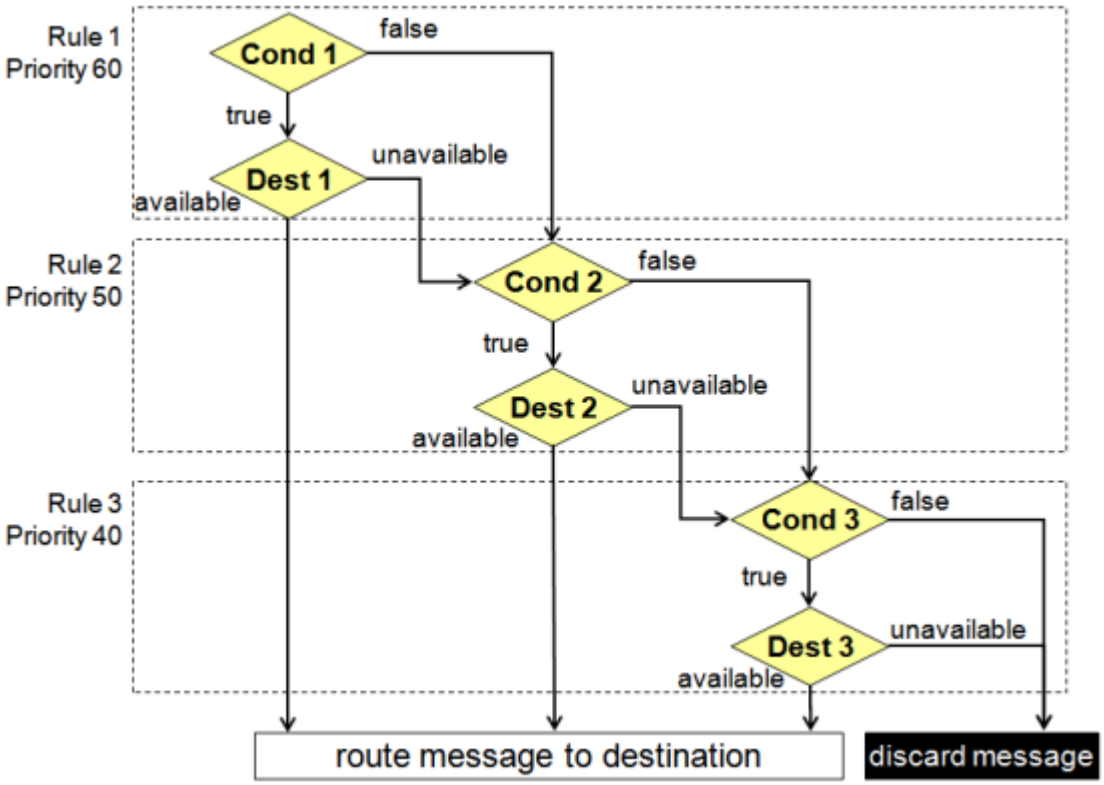


Figure 30: SMS voting message flow

9.2.6.5 Mobile Number Portability Verification for Originator

For mobile number portability (MNP) verification for originator, the following additional conditions should be included in the MO routing rules:

- The originating global title is an MSC or SGSN in the range used within the HPLMN (for example, 49172000000-49172999999), and
- The MSISDN in the originator address begins with the HLPMN country code (for example, +49)

If these conditions are false, the message is routed to a configured SMSC, which performs an MNP verification (via an HLR query) and obtains the originator's IMSI.

Therefore, for an application to receive messages from subscribers who are roaming in foreign networks, it should have a session with the available SMSCs.

9.2.6.6 Application Selection

For MO routing to application, the RTR supports provisioning of the destination application in the MOR rule with the **Application Selection** and **Application** parameters in the MGR:

Parameter	Description
Application Selection	Specifies how the destination application is to be determined. Valid values are: • `Specify Application`—The destination application is an application specified by the routing rule itself, by means of the **Application** parameter. • `Based on Recipient Address`—The destination application is determined by analyzing the recipient address. If it is a short number, alphanumeric application alias or alias-MSISDN of an application, the corresponding application will be selected as the destination application. If no application can be determined, the rule will not match. • `Based on SMSC Address`—The destination application is determined by matching the SMSC address (at the MAP layer) against the set of provisioned per-application private VSMSC addresses. Upon finding a (exact) match, the application related to the VSMSC addresses is selected as the destination application. If the SMSC address does not match any of the provisioned private VSMSC addresses, the rule does not match. Refer to *Virtual SMSC Support*.
Application	Select the application to which to route the message. Only applies when **Application Selection** is set to `Specify Application`.

These parameters are applicable to the MO-AT related routing actions (MO-AT, MO-AT-Store or MO-Store-AT).

9.2.6.7 MO-AT Routing Rule Set Example

The following diagram illustrates a typical set of rules representing the fall-through mechanism.

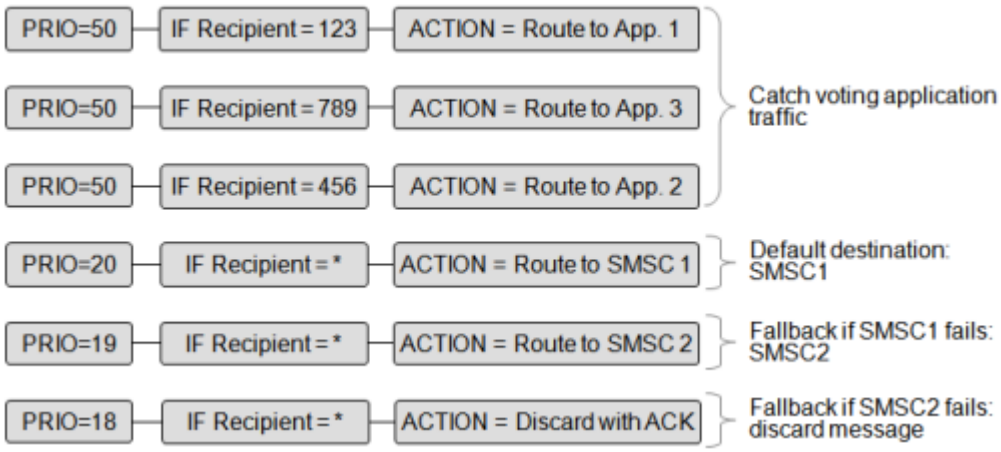


Figure 31: MO-AT routing rule set

A typical message flow for regular MO routing (route to SMSC) is:

1. Evaluate the first applicable routing rule (route to SMSC).
   a) The RTR does not have to evaluate the message condition, assuming it was already checked.

b) The RTR evaluates the destination condition (SMSC is available).
c) The RTR evaluates the channel condition (the throughput limit for this route and the total SMSC throughput have not yet been reached).

2. If all of the above conditions are true, the RTR forwards the message to the SMSC.
3. The RTR optimises the message routing and allows the SMSC to respond directly to the MSC with the result status of the message delivery (ACK or NACK).
4. The RTR does not generate a CDR for an MO message that is routed to an SMSC.

Note: The scenarios and message flow that are described above are examples and contain simplifications.

9.2.7 MO-AO Routing

In the MO-AO routing path (*route to SMSC Group as AO* or *route to SMSC Application as AO* option in the Manager), the RTR forwards MO messages to a service centre or message gateway as AO messages. This functionality can be used to relieve traffic on the SS7 connection to the SMSC or in cases where there is no SS7 connection to the SMSC or message gateway.

The following diagram illustrates the MO-AO routing path:

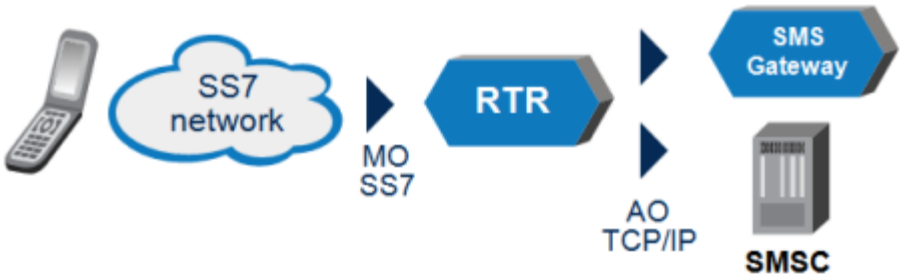


Figure 32: MO-AO routing

For MO-AO routing, the RTR and HUB mimic the behaviour of an application toward the AO message's receiver. The service centre sees the NewNet system as an application that issues short messages. On the NewNet system:

- A dedicated application must be configured for this purpose
- The MO-AO routing rule must refer to the application
- The session model of the application must be inside only - all SCs or inside only - SC list

The NewNet system sends acknowledgement to the MO message originator only after the result of the AO submission is known. Therefore, if the service centre or the message gateway rejects the message, the originator will receive an message not sent error and the RTR will not generate a CDR. If the AO message is accepted, CDRs for the submission to the RTR and for the successful delivery to the service centre or message gateway may be generated, depending on the configuration of the rule.

When configuring the application to which an MO-AO message should be routed, you must select the session model (inside only - all SCs or inside only - SC list) directly in the application. You cannot create a service class with a certain session model and then set the application to use service class model.

For more information about session models and service classes, refer to the HUB Operator Manual. For more information about configuring applications, refer to the Manager Operator Manual.

9.2.7.1 AT Notification

If you use the NewNet system to combine MO-AO routing with charging responsibilities (generation of CDRs and/or prepaid triggers), the RTR always requests an AT notification when submitting an MO message as AO, by default. This functionality ensures that the final delivery result of an AO-forwarded message is communicated back to the NewNet system.

However, you can use the `overridenotificationtypeformoaomessages` parameter in the semi-static configuration file to override this functionality.

Note: The MO-AO routing path can be used together with the Icache functionality. The Icache final delivery status notification is received from external Service Centre (SC) as an individual message. The information in this final delivery status notification may not correspond to the original AO message sent from the RTR to the external SC. For example, the TON/NPI of the same number in the two messages can be different. If the TON/NPI do not match, there is a possibility that the Final Deliver FCDR will not be generated, since the condition in the MOR rule does not match.

To match the two messages, the GSM Address Conversion (AC) rule can be used to change the TON/NPI of the addresses in the delivery notification according to the original AO message.

Whenever RTR receives an AT delivery notification from an external SMSC and the Icache is enabled, RTR internally discards the received notification if the original message is found to be Mobile Originated (MO). In such a case RTR also sends back a positive acknowledgement to the SMSC because no further processing or routing is required for the AT notification. If the originator of the MO message requested a status report, then RTR generates the same and sends it to the originator.

9.2.7.2 MO-AO Routing with the Prepaid Billing Controller

Because many message parameters that are required to generate delivery CDRs and/or prepaid triggers are not part of the AT notification message, the NewNet system uses the Prepaid Billing Controller (PBC) to temporarily store the required data in a transaction database. The PBC is a required component to enable delivery CDRs and/or prepaid triggers.

To correlate the AT notification with the original MO message's parameters, the SMPP protocol's message ID field must be available.

To retrieve the parameters from the PBC's transaction database when an AT notification is received, an ATX rule must be provisioned for the MO-AOapplication toward the PBC. To generate the final delivery CDR, the RTR uses the billing profile that is specified for notifications in the original MO-AO rule. The PBC's transaction database is also required if the originator requests a status report.

Note: A configuration involving the PBC transaction database can be complex, depending on the existing infrastructure. In all cases, use of the SMPP protocol for AO/AT message exchange is required. It is strongly recommended to look for alternatives to the PBC transaction database for MO-AO routing.

9.2.7.3 Configuration

To ensure that MO-AO messages can be routed and billed, the following `tpconfig` attributes in the semi-static configuration file should be set to true:

- `adjustprepaidindicatorondeductfailure`
- `delivercdrforsuccessfulmoaoforwarding`

Also, the index for a number of PBC external attributes must be configured:

- `externalattributeforpostpaidoriginator`
- `externalattributeforprepaidonlineoriginator`
- `externalattributeforprepaidhotbillingoriginator`
- `externalattributeforpostpaidrecipient`
- `externalattributeforprepaidonlinerecipient`
- `externalattributeforprepaidhotbillingrecipient`

Refer to *Configuration* for detailed information about these attributes.

9.2.8 MO-Discard

MO-Discard routing processes incoming MO messages and discards messages based on specified conditions. MO-Discard routing provides:

- Discard with acknowledgement
- Discard with negative acknowledgement
- Discard without response
- CDR generation (if configured)

Note:

1. CDR will be generated using the billing profile (if configured) for Successful Delivery when the action is set to `Discard with ACK`.
2. CDR will be generated using the billing profile (if configured) for Discarded Messages when the action is set as `Discard with negative acknowledgement` or `Discard without response`.
3. Only the FCDR format will be supported for generating CDRs for messages discarded by the RTR.

9.2.9 MO External Condition Routing

MO external condition (MOX) routing processes incoming MO messages and forwards selected message fields to a configured external condition (EC) application. MO external condition routing provides one of the following responses:

Response	Description
True	The rule condition evaluates to true and the message processing continues normally.
False	The rule condition evaluates to false and the failure action is applied.
EC attributes	A returned matrix of result flags that the EC application sets and upon which the RTR can base its routing decision. **Note:** To use EC attributes in a rule condition, all used EC attributes must be configured in the EC attribute entry.

MOX rules get evaluated using the logic common to all external condition rule sets (refer to Rule Evaluation).

The possible failure actions are:

Action	Effect
None	Ignore the false result and continue to process the list of matching MOX rules, or assume that the message "passed" the MOX rule evaluation if there are no more matching rules in the list.
Discard with negative acknowledgment	Return an error to originator and discard the message.
Discard with acknowledgment	Return an acknowledge to originator and discard the message.
Discard with no response	Do not set any response to originator and discard the message.

Note: CDRs will be generated using the billing profile (if configured) for `Discarded Messages` when the message is discarded due to the application of any of the following failure action:

1. Discard with negative acknowledgment
2. Discard with no response

Only the FCDR format will be supported for generating CDRs for messages discarded by the RTR.

Note: A return message will be generated and send back to the originator when a configured message template is associated with one of the following failure action:

1. Discard with acknowledgment
2. Discard with negative acknowledgement

For more details refer to section *Return Error Message for MO Originate Message*.

9.2.9.1 Including Recipient IMSI in MOX Rules

The RTR can retrieve the recipient IMSI from the HLR before it evaluates the MOX rules, allowing the recipient IMSI to be used on the external condition interface (ECI). This functionality enables systems that include the Prepaid Billing Controller (PBC) to implement differentiated prepaid charging that depends on the recipient network, even in the case of mobile number portability (MNP) for originator.

To enable this functionality, set the **Early SRI-SM for MO/SM** parameter in the MGR GUI (**Routing ➤ Properties**). When it is set:

- The submission CDR will contain the recipient IMSI.
- The RTR might retrieve the recipient IMSI at times that are different from the behavior when the recipient IMSI is not included; for example, when an MOR rule that does not result in a delivery attempt toward a mobile applies (such as when the rule's action is discard with ACK).

You can use the `tpconfig` attribute *ignorepermanentfailureofhlrqueryforrecipient* to customize the RTR's behavior if the HLR query for the IMSI results in a permanent error:

- If it is set to "false" (default), the RTR will NACK the MO message.
- If it is set to "true", the RTR will ignore the permanent error. To prevent MT delivery retries for a message with a permanent HLR query error, you should configure the MO rules such that no message with a permanent HLR query error is routed to a fallback to MT. Typically, such messages should be routed to an application or be rejected.

If the routing of the MO message results in a delivery attempt toward a mobile, the RTR will not retrieve the recipient IMSI again. The RTR will use the information from the recipient IMSI that was retrieved in the HLR query prior to the evaluation of the MOX rule.

Invalid Recipient MSISDNs

The RTR does not retrieve the recipient IMSI if the RTR regards the MO message recipient MSISDN as invalid. The RTR considers an MSISDN to be valid when all of the following are true:

- The recipient address is 15 digits or shorter after conversion to international format
- The recipient NPI is equal to ISDN/telephony
- The recipient is not classified as a short number

Retrieving IMSI for a Subset of Recipients

This functionality may only be required for a subset of recipients. In the MGR, you can define a list of recipient numbers for which the RTR should send an HLR query. Then, use the **Early SRI-SM for MO/SM Whitelist** parameter in the MGR GUI (**Routing ➤ Properties**) to refer to the list.

Note: If the RTR cannot find the list that is specified in the configuration file, it will send HLR queries for all numbers. Therefore, it is important that the list is not removed from the MGR. The MGR does not read the configuration file and therefore does not provide a warning if you attempt to remove the list. It is recommended to include a reminder in the list name (for example, `MOWhiteList_DO_NOT_REMOVE`).

9.3 Defining an MO Routing Rule

All MO traffic that is routed through the RTR is subject to MO routing (MOR) rules, which you configure using the Manager (MGR).

To configure the RTR to always retrieve the originator's IMSI (with an SRI-SM request) before evaluating the MOR rules, set the `tpconfig` parameter `alwaysretrieveoriginatorimsi` to "true" in the semi-static configuration file. If an MOR rule contains a condition that requires the message originator's IMSI, the RTR will always attempt to retrieve the IMSI when evaluating the rule, even if `alwaysretrieveoriginatorimsi` is set to "false".

9.3.1 MO Rule Conditions

The following table details the conditions that are available for MO rules.

Condition	Values	Description
Time Schedule	• Always • Schedule	Condition on the evaluation time of the message: • Always: The condition is always true. • Schedule: The condition is true if the current time falls within the schedule as specified by the selected routing schedule, defined in **Routing ➤ Schedules**.

Condition	Values	Description

Recipient TON	• None
	• Bit string
	  • 0: Unknown
	  • 1: International number
	  • 2: National number
	  • 3: Network specific number
	  • 4: Subscriber number
	  • 5: Alphanumeric
	  • 6: Abbreviated number
	  • 7: Reserved
		Type of number (TON) specified in the recipient address of the message.

Originator	• MSISDN • MSISDN range • MSISDN prefix • Country • IMSI Prefix • IMSI range • IMSI • List	Originator specified in the message. **Note:** When an IMSI-related condition is used but the originator IMSI is not known at the moment of rule evaluation, the condition will evaluate to FALSE if not negated or TRUE if negated. To ensure that the originator IMSI is always retrieved before the rule evaluation, set the `alwaysretrieveoriginatorimsi` attribute in the common configuration file to true.
Recipient	• MSISDN • MSISDN range • MSISDN prefix • Country • IMSI prefix • IMSI range • IMSI • List • Short number • Short number range • Short number prefix • Application • Network • Alphanumeric	Recipient specified in the message. **Note:** When an IMSI-related condition is used but the recipient IMSI is not known at the moment of rule evaluation, the condition will evaluate to FALSE if not negated or TRUE if negated. For MOR and MOX rules, this condition requires the recipient number to be an MSISDN and the HLR query to be performed before the rule evaluation (to obtain the recipient IMSI). The **Early SRI-SM for MO/SM** attribute in the (**MGR Routing** > **Properties**) controls when the HLR query is performed. **Note:** The Network configuration may include provisioned network number ranges and/or network prefixes.
SMSC Address	• MSISDN • MSISDN range	SMSC address specified in the message.

Condition	Values	Description
	• MSISDN prefix • List	
Orig. MSC/SGSN	• MSISDN • MSISDN range • MSISDN prefix • List • Point code • Point code range • Country • Network	Originating MSC and/or SGSN specified in the message. **Note:** **1.** If global title (GT) routing is used and this condition is specified in terms of Point code or Point code range, then a non-inverted condition always evaluates to false and an inverted condition always evaluates to true. **2.** If PC/SSN routing is used instead of GT routing and this condition is specified in terms of Country or Network, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer. **3.** The Network configuration may include provisioned network number ranges and/or network prefixes.
Orig. MSC/SGSN Translation Type	• None • Byte value (value between 00 and FF, hexadecimal)	Translation Type specified in Originating MSC/SGSN Address.
Terminating MSC/SGSN	• MSISDN • MSISDN Range • MSISDN Prefix • Country • Network • List	Destination MSC and/or SGSN. This condition requires the recipient number to be an MSISDN, and requires the HLR query to be performed before MO rule evaluation (to obtain the MSC and/or SGSN). The **Early SRI-SM for MO/SM** attribute in the MGR (**Routing ➤ Properties**) controls when the HLR query is performed. If both the MSC and SGSN are present, the `preferredmtdestination` attribute determines which will be used for rules evaluation. If the HLR query fails, the condition will evaluate to "false", whether it is a negative or positive condition. **Note:** The Network configuration may include provisioned network number ranges and/or network prefixes. **Note:** If the Network configuration is available according to the MSC and/or SGSN (i.e. received in the HLR query), The '**Preferred MT Destination**' in the Network configuration overrides the semi-static

Condition	Values	Description
		attribute '`preferredmtdestination`' for the rules evaluation.
SCCP Called Party Address	• MSISDN • MSISDN range • MSISDN prefix • List • Point code • Point code range • Country • Network	SCCP Called Party Address specified in the message. **Note:** **1.** If global title (GT) routing is used and this condition is specified in terms of Point code or Point code range, then a non-inverted condition always evaluates to false and an inverted condition always evaluates to true. **2.** If PC/SSN routing is used instead of GT routing and this condition is specified in terms of Country or Network, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer. **3.** The Network configuration may include provisioned network number ranges and/or network prefixes.
Called Party Translation Type	• None • Byte value (value between 00 and FF, hexadecimal)	Translation Type specified in SCCP Called Party Address.
Orig. HLR	• MSISDN • MSISDN range • MSISDN prefix • List • Point code • Point code range • Country • Network	HLR that serves the message originator. This condition requires the recipient number to be an MSISDN, and requires the HLR query to be performed before MO rule evaluation (to obtain the HLR). The **Early SRI-SM for MO/SM** attribute in the MGR (**Routing ➤ Properties**) controls when the HLR query is performed. **Note:** The Network configuration may include provisioned network number ranges and/or network prefixes.
User Data	• None • Full text • Text tag • Subtext (contains) • Text length	Content of the message: • Full text: Compares the entire message content with a defined string. Only evaluates positively if there is an exact match with the user data (message content). • Text tag: Compares the first part of the message content with a defined tag-string. Only evaluates positively if the message starts exactly with the defined tag-string. Useful to define a rule on keywords (e.g. `*LONG#` for CMG SMSCs).

Condition	Values	Description
		• Subtext (contains): Compares if the message content contains a defined tag-string. To optimise the search, a start position (default 1) and an end position (default 160) must be specified in which the string is to be found. **Note:** All message content scanning is case-insensitive.
User Data Header	• None • Byte value	Value specified in one of the information element identifiers (IEIs) of the user data header (UDH) of the message. Only evaluates positively if there is an exact match with the information element identifier (00-FF, hexadecimal) of the UDH. Refer to technical specification 3GPP 23.040 for more information. Most common IEI values: • 00: Concatenated short message • 01: Special SMS message indication • 04: Application port addressing scheme, 8-bit address • 05: Application port addressing scheme, 16-bit address • 06: SMSC control parameters • 07: UDH Source Indicator

Reply Path	• None
	• Bit value
	  • 0: Off
	  • 1: On
		Reply path bit in the message.

Status Report Request	• None
	• Bit value
	  • 0: Off
	  • 1: On
		Status report request bit in the message.

Protocol Identifier (PID)	• None • Byte value (value between 00 and FF, hexadecimal)	Protocol ID specified in the message.
Data Coding Scheme (DCS)	• None	Data coding scheme (DCS) specified in the message.

Condition	Values	Description
	• Byte value (value between 00 and FF, hexadecimal)	

Recipient NPI	• None
	• Bit string
	  • 0: Unknown
	  • 1: ISDN/telephone numbering plan
	  • 2: Reserved
	  • 3: Data numbering plan (X.121)
	  • 4: Telex numbering plan
	  • 5: Service centre-specific plan
	  • 6: Service centre-specific plan
	  • 7: Reserved
	  • 8: National numbering plan
	  • 9: Private numbering plan
	  • 10: ERMES numbering plan
	  • 11: Reserved
	  • 12: Reserved
	  • 13: Reserved
	  • 14: Reserved
	  • 15: Reserved
		Number plan identifier (NPI) specified in the recipient address of the message.

Ext Att	• None • External attributes	A set of 32 attributes (defined in **Routing ➤ EC Applications ➤ Attributes**), the value of which can be controlled by external condition (EC) applications.
Recipient RN Group	• None • SNMP index	Routing number (RN) group to which the RN in the recipient address belongs.
Recipient Query Result	• None • Bit string • Any permanent error	Result of the HLR query for the recipient. This condition requires the recipient number to be an MSISDN, and requires the HLR query to be performed before MO rule evaluation (to obtain the HLR query result). The **Early SRI-SM for MO/SM Whitelist**and **Early SRI-SM for MO/SM** attributes in the MGR

Condition	Values	Description
	• Any temporary error • Timeout • System failure • Data missing • Unexpected data value • Facility not supported • Unknown subscriber • Absent subscriber • Call barred • Teleservice not provisioned • TCAP aborted • SCCP aborted • MS deregistered • MS purged • Other errors	(**Routing ➤ Properties**) control when the HLR query is performed.
Originator SSI	• None • Subscriber Services	Perform a positive or negative test on one or more individual originator subscriber services (defined in **SPF Services ➤ SPF Services**). The condition test works like a logical `AND` operation (similar to the external attributes). For example, if positive tests are selected for originator copy and distribution list, the condition would only be satisfied if both of these tests are true.
Recipient SSI	• None • Subscriber Services)	Perform a positive or negative test on one or more individual recipient subscriber services. The condition test works like a logical AND operation (similar to the external attributes). For example, if positive tests are selected for originator copy and distribution list, the condition would only be satisfied if both of these tests are true.

Message Segments	• None
	• Bit String
	  • First Segment
	  • Last Segment
	  • Not First Nor Last
		Segment sequence number of a concatenated message.

Condition	Values	Description
SIP Header	• None • SIP Header	If set as "SIP Header", the sub-conditions will be matched against the SIP header received in the incoming SIP Originated message. Four sub-conditions can be provisioned. Please refer the section *MO Rule Conditions for SIP Originated Message* for configuring the sub-conditions.

9.3.2 MO Routing Action Parameters

This section describes the parameters for MO routing actions.

Multiple MO Routing Actions

Parameter	Description	Default
Submission	Billing profile to use for submission; applies to all MO routing actions.	None
Successful Delivery	Billing profile to use when the routing action succeeds. Applies to: • Route to SMSC • Route to application • Route to MS fallback to SMSC • Discard with acknowledgment • Route to MS fallback to application • Route to MS fallback to storage • Route to application fallback to storage • Route to SMSC Group as AO • Route to MS fallback to SMSC Group as AO • Route to SMSC Application as AO • Route to MS fallback to SMSC Application as AO	None
Failed Delivery	Billing profile to use when the routing action fails. Applies to: • Route to SMSC • Route to application • Route to MS fallback to SMSC • Discard with acknowledgment • Route to MS fallback to application • Route to MS fallback to storage • Route to application fallback to storage	None

Parameter	Description	Default
	• Route to SMSC Group as AO • Route to MS fallback to SMSC Group as AO • Route to SMSC Application as AO • Route to MS fallback to SMSC Application as AO	
Delivery Notification	Billing profile to use for delivery notification. Applies to: • Route to SMSC • Route to application • Route to MS fallback to SMSC • Discard with acknowledgment • Route to MS fallback to application • Route to MS fallback to storage • Route to application fallback to storage • Route to SMSC Group as AO • Route to MS fallback to SMSC Group as AO • Route to SMSC Application as AO • Route to MS fallback to SMSC Application as AO	None
Discarded Messages	Billing profile to use when routing action discard the message. Applies to: • Discard with negative acknowledgment • Discard without response	None
Return Message Template	Return message template to use when routing action. Applies to: • Discard with negative acknowledgment • Discard with acknowledgment	None

Route to SMSC and Route to MS, Fallback to SMSC

Parameter	Description	Default
SMSC Assignments	SMSC(s) to which this rule applies.	None
Priority	Priority of the SMSC (between 1 and 100).	50
Weight	Relative weight of messages to send to the SMSC (for example, an SMSC with a weight of 2 will receive twice as many messages as an SMSC with a weight of 1).	1

Parameter	Description	Default
Throughput	Throughput for the SMSC (messages per second); if set to 0, throughput will be unlimited.	10,000
CdPA Based Forwarding	Enables forwarding based on the SCCP called party address (CdPA) of received messages; if enabled, the MOR rule not be associated with any provisioned SMSC.	False
Keep MSC/SGSN SCCP CdPA	Enables transparent routing: • False: The RTR will start a new TCAP dialogue when forwarding messages to the external SMSC. • True: The RTR will reuse the existing TCAP dialogue when forwarding messages to the external SMSC. • Use global setting: The RTR will use the value of the `optimisedmorouting` parameter in its semi-static configuration file (which defaults to "false").	Use global setting
Modifier	Modifier to apply to the message.	None

Route to Application

Parameter	Description	Default
Always Respond with ACK	Controls if the message should always be positively acknowledged, regardless of the delivery result.	Cleared
Modifier	Modifier to apply to the message.	None
Application Selection	Controls how the destination application is to be determined: • Specify Application: The destination application is an application specified by the routing rule itself, by means of the **Application** parameter. • Based on Recipient Address: The destination application is determined by analyzing the recipient address. If it is a short number, alphanumeric application alias or alias-MSISDN of an application, the corresponding application will be selected as the destination application. If no application can be determined, the rule will not match. • Based on SMSC Address: The destination application is determined by matching the SMSC address (at the MAP layer) against the set of provisioned per-application private Virtual SMSC addresses. Upon finding a (exact) match, the application related to the Virtual SMSC addresses	Specify Application

Parameter	Description	Default
	is selected as the destination application. If the SMSC address does not match any of the provisioned private VSMSC addresses, the rule does not match.	
Application	Select the application to route the message to (only applies when **Application Selection** is set to "Specify Application").	First application on the list
Application Load Balancing Group	Application load balancing group to use (only applies to AT traffic).	None
Decimation	Controls how many messages must be delivered to the application.	1/1

Store for Delivery to MS

Parameter	Description	Default
Modifier	Modifier to apply to the message.	None
AMS Queue	AMS queue to use for storage.	First defined AMS queue

Route to MS

Parameter	Description	Default
Always Respond with ACK	Controls if the message should always be positively acknowledged, regardless of the delivery result.	Cleared
Modifier	Modifier to apply to the message.	None

Route to MS, Fallback to Application

Parameter	Description	Default
Application Selection	Controls how the destination application is to be determined: • Specify Application: The destination application is an application specified by the routing rule itself, by means of the **Application** parameter. • Based on Recipient Address: The destination application is determined by analyzing the recipient address. If it is a short number, alphanumeric application alias or alias-MSISDN of an application, the corresponding application will be selected as the destination application. If no application can be determined, the rule will not match.	Specify Application

Parameter	Description	Default
	• Based on SMSC Address: The destination application is determined by matching the SMSC address (at the MAP layer) against the set of provisioned per-application private Virtual SMSC addresses. Upon finding a (exact) match, the application related to the Virtual SMSC addresses is selected as the destination application. If the SMSC address does not match any of the provisioned private VSMSC addresses, the rule does not match.	
Application	Select the application to route the message to (only applies when **Application Selection** is set to "Specify Application").	First application on the list
Application Load Balancing Group	Application load balancing group to use (only applies to AT traffic).	None
Successful Delivery on Fallback	Billing profile to use when the fallback leg of the routing action succeeds.	None
Failed Delivery on Fallback	Billing profile to use when the fallback leg of the routing action fails.	None

Route to MS, Fallback to Storage

Parameter	Description	Default
Modifier	Modifier to apply to the message	None
AMS Queue	AMS queue to use for storage.	First defined AMS queue
Failed Delivery on Fallback	Billing profile to use when the fallback leg of the routing action fails.	None

Store for Delivery to Application

Parameter	Description	Default
Modifier	Modifier to apply to the message.	None
Application Selection	Controls how the destination application is to be determined: • Specify Application: The destination application is an application specified by the routing rule itself, by means of the **Application** parameter. • Based on Recipient Address: The destination application is determined by analyzing the recipient address. If it is a short number, alphanumeric application alias or alias-MSISDN	Specify Application

Parameter	Description	Default
	of an application, the corresponding application will be selected as the destination application. If no application can be determined, the rule will not match. • Based on SMSC Address: The destination application is determined by matching the SMSC address (at the MAP layer) against the set of provisioned per-application private Virtual SMSC addresses. Upon finding a (exact) match, the application related to the Virtual SMSC addresses is selected as the destination application. If the SMSC address does not match any of the provisioned private VSMSC addresses, the rule does not match.	
Application	Select the application to route the message to (only applies when **Application Selection** is set to "Specify Application").	First application on the list
Application Load Balancing Group	Application load balancing group to use (only applies to AT traffic).	None
AMS Queue	AMS queue to use for storage.	First defined AMS queue

Route to Application, Fallback to Storage

Parameter	Description	Default
Always Respond with ACK	Controls if the message should always be positively acknowledged, regardless of the delivery result.	Cleared
Modifier	Modifier to apply to the message.	None
Application Selection	Controls how the destination application is to be determined: • Specify Application: The destination application is an application specified by the routing rule itself, by means of the **Application** parameter. • Based on Recipient Address: The destination application is determined by analyzing the recipient address. If it is a short number, alphanumeric application alias or alias-MSISDN of an application, the corresponding application will be selected as the destination application. If no application can be determined, the rule will not match. • Based on SMSC Address: The destination application is determined by matching the SMSC address (at the MAP layer) against the set of	Specify Application

Parameter	Description	Default
	provisioned per-application private Virtual SMSC addresses. Upon finding a (exact) match, the application related to the Virtual SMSC addresses is selected as the destination application. If the SMSC address does not match any of the provisioned private VSMSC addresses, the rule does not match.	
Application	Select the application to route the message to (only applies when **Application Selection** is set to "Specify Application").	First application on the list
Application Load Balancing Group	Application load balancing group to use (only applies to AT traffic).	None
AMS Queue	AMS queue to use for storage.	First defined AMS queue
Decimation	Controls how many messages must be delivered to the application.	1/1
Failed Delivery on Fallback	Billing profile to use when the fallback leg of the routing action fails.	None

Route to SMSC Group as AO

Parameter	Description	Default
Always Respond with ACK	Controls if the message should always be positively acknowledged, regardless of the delivery result.	Cleared
Modifier	Modifier to apply to the message.	None
Application	Select the application to route the message to (only applies when **Application Selection** is set to "Specify Application"). The application must have a session model of **Inside only - All SCs** or **Inside only - SC List**.	None
SMSC Load Balancing Group	SMSC group to which to route the MO message.	None

Route to MS, Fallback to SMSC Group as AO

Parameter	Description	Default
Modifier	Modifier to apply to the message.	None
Application	Select the application to route the message to (only applies when **Application Selection** is set to "Specify Application"). The application must have a session	None

Parameter	Description	Default
	model of **Inside only - All SCs** or **Inside only - SC List**.	
Successful Delivery on Fallback	Billing profile to use when the fallback leg of the routing action succeeds.	None
Failed Delivery on Fallback	Billing profile to use when the fallback leg of the routing action fails.	None
SMSC Load Balancing Group	SMSC group to which to route the MO message.	None

Route to SMSC Application as AO

Parameter	Description	Default
Always Respond with ACK	Controls if the message should always be positively acknowledged, regardless of the delivery result.	Cleared
Modifier	Modifier to apply to the message.	None
Application	Select the application to route the message to (only applies when **Application Selection** is set to "Specify Application"). The application must have a session model of **Inside only - All SCs** or **Inside only - SC List**.	None

Route to MS, Fallback to SMSC Application as AO

Parameter	Description	Default
Modifier	Modifier to apply to the message.	None
Application	Select the application to route the message to (only applies when **Application Selection** is set to "Specify Application"). The application must have a session model of **Inside only - All SCs** or **Inside only - SC List**.	None
Successful Delivery on Fallback	Billing profile to use when the fallback leg of the routing action succeeds.	None
Failed Delivery on Fallback	Billing profile to use when the fallback leg of the routing action fails.	None

9.3.3 Condition Logic

The logic of MO rule conditions is:

```
([NOT] Condition1) AND ([NOT] Condition2) AND ([NOT] Condition3) AND...
```

When you add a condition to an MO rule in the MGR, it defaults to "equals." To change the logic to "does not equal" (inverting it), click

.

The icon changes to

.

To change the logic back to "equals," click

.

9.3.4 Rule Logic

9.3.4.1 Routing to SMSC

The following rule logic describes how messages are routed to an SMSC.

```
IF any of message conditions do not match THEN
   Evaluate next rule;
END IF

Select SMSC from set of SMSCs defined for rule to route SM to.
Only SMSCs for which all of the following conditions satisfy should be
considered:
   > Rule-specific throughput for SMSC should not be exceeded
   > SMSC-specific throughput for SMSC should not be exceeded
   > SMSC should be reachable

If multiple SMSCs:
   > When multiple SMSCs apply, select the one with highest priority.
   > When multiple SMSCs of the highest priority are available, select the one based

     on their assigned weight and the load that they have received during the current
       second.

IF no SMSC selected THEN
   Evaluate next rule;
ELSE
   Route SM to selected SMSC.
   SMSC will send ACK/NACK directly to originator or through RTR.
   In the latter case, the RTR will just forward ACK/NACK to originator.
END IF
```

9.3.4.2 Routing Messages to Application

The following rule logic describes how messages are routed to an application.

```
IF any of message conditions do not match THEN
   Evaluate next rule;
END IF
IF application not connected THEN
   Evaluate next rule;
END IF
IF application throughput regulation does not allow more MO/SMs to be routed to
   application THEN
   Evaluate next rule;
END IF
IF no capacity available on sessions with application (due to windowing) THEN
   Evaluate next rule;
END IF
IF decimation function does instruct to drop MO/SM THEN
```

```
   IF billing enabled THEN
      Generate billing record
   END IF
   send ACK to originator
ELSE
   send SM to application. use session with least number of unacknowledged SMs.
   IF "always ACK" is true THEN
      send ACK to originator
      IF billing enabled THEN
         Generate billing record
      END IF
   ELSE
      Wait for ACK/NACK from application
      IF ACK THEN
         IF billing enabled THEN
            Generate billing record
         END IF
         Send ACK to originator
      ELSE
         Send NACK to originator
      END IF
   END IF
END IF
```

9.3.4.3 Discarding Messages with ACK

The following rule logic describes how messages are discarded with ACK.

```
IF any of message conditions do not match THEN
   Evaluate next rule;
END IF
send ACK to originator
IF billing enabled THEN
   Generate billing record
END IF
```

9.3.4.4 Discarding Messages with NACK

The following rule logic describes how messages are discarded with NACK.

```
IF any of message conditions do not match THEN
   Evaluate next rule;
END IF
send NACK to originator
```

9.4 Configurable ACK Functionality

This section discusses the configurable ACK functionality for MO messages.

9.4.1 FDA with Fallback

When the RTR is configured to perform a first delivery attempt (FDA) with a fallback action (store, MO, AO, or AT) and `moresponseafterhlrquery` is set to "false", the RTR sends the MO ACK immediately, before doing the HLR query (SRI-SM) for the recipient.

The `moresponseafterhlrquery` flag indicates whether TextPass should send a response to an MO/SM after it has completed the HLR query to obtain the details of the recipient. The response

depends on the HLR query result. If the HLR query resulted in an error of permanent nature, the response to the MO/SM is a NAK. When the HLR query is successful or the HLR query failed due to a temporary error, the MO/SM response is an ACK. A typical case in which this setting is activated is for operators requiring that MO/SM's to unknown recipients are rejected. Default of this setting is "false".

9.4.2 FDA without Fallback

When the RTR is configured to perform a first delivery attempt (FDA) without a fallback action (known as route to MS) and **Always Respond With ACK** is not enabled, the RTR will generate the MO response only after the final result is known (which may occur after the MT delivery).

When **Always Respond With ACK** is enabled and the `moresponseafterhlrquery` parameter in the semi-static configuration file is set to:

- False: The RTR generates the MO ACK immediately.
- True: The RTR delays the MO response until after the HLR query. The HLR response will determine whether the RTR will return an ACK (successful HLR query) or a NACK (unsuccessful HLR query).

The following table illustrates the scenarios for route to MS that determine whether the RTR acknowledges the message:

1. Before issuing the HLR query for the recipient
2. Between the HLR query and the MT message delivery
3. Only after the delivery result is fully known (which may occur after the MT message delivery)

Always Respond with ACK	MO Response After HLR Query	HLR Query Result	MT Delivery Result	MO Response (Position)
False	Any setting	Negative	N/A	Negative (B)
False	Any setting	Positive	Negative	Negative (C)
False	Any setting	Positive	Positive	Positive (C)
True	False	Any result	Any result	Positive (A)
True	True	Negative	Not applicable	Negative (B)
True	True	Positive	Any result	Positive (B)

WARNING: When the ACK is configured to be sent after the FDA, there is a risk of MO time-outs due to the difference in the MT time-out as compared to the MO time-out (as per the 3GPP 29.002 specification).

9.4.3 Store

When the RTR is configured to store messages immediately (without a first delivery attempt) and `moresponseafterhlrquery` is set to false, the MO message is stored in the AMS without an issued HLR query. The result of the storage request to the AMS determines whether the RTR returns an ACK or a NACK.

When `moresponseafterhlrquery` is set to true, the RTR generates an extra HLR query before it requests that the AMS store the MO message (typically for the purpose of validating the message). When this HLR query:

- Results in a permanent error, the message is rejected.
- Results in a success or a temporary (recoverable) error, the RTR requests that the AMS store the message. The MO response depends on whether the AMS accepts the message.

9.5 Configurable Status Report Functionality

The `forcestatusreportfordroppedmomessage` parameter in the semi-static configuration file is available to instruct the RTR to always send a phase 1 status report to the originator, indicating that the delivery failed and will not be attempted again (this functionality only applies when **Always Respond With ACK** is selected).

If the originator requested a phase 2 status report, the value of the `phase1statusreportoverrules` parameter determines whether the status report that the RTR sends will be phase 1 or phase 2 (which is the default).

Refer to *Phase 1 Status Reports* for more information about phase 1 status reports.

9.6 Configurable MO Deferred Delivery Relative Hours

When the parameter `deferreddeliveryrelativehours` is configured in the semi-static configuration file, it instructs the RTR to delay the MO message for a particular amount of time (i.e. in hours).

This functionality only applies when the semi static parameter `enableadvancedmotagmode` is set to true.

The SMSC delays the MO message for a particular amount of time when it scans the received MO message with a tag at the beginning of the message (usually starting with `*<TAG>#`). The tag must be in GSM 7-bit format.

The syntax of a MO message with a tag is:

```
*<tag string><single space><relative hours>#<message content>
```

For example:

```
*defer 2#This is a message.
```

The exact value of `<TAG>` is configured in the `string` attribute of the `motag` entity in the semi-static configuration file. The following example defines the value of `<TAG>` as `defer`:

```
<motag string="defer" function="deferreddeliveryrelativehours"/>
```

9.7 Configurable CDR Generation

The RTR can generate:

- A submission CDR when it acknowledges an MO message, containing destination information (such as DGTI, DPC, and termination date).
- A notification CDR for status and delivery reports.

- A rejected CDR for discarded message, when the MO routing rule action is configured as `Discard with negative acknowledgement` or `Discard without response`.

CDRs contain the fields identified by the billing profile that is selected for the applicable routing action, in the applicable MO routing rule. In the MGR interface, you can create billing profiles, set a default billing profile for MO traffic, and select a billing profile for each routing action in the MO routing rules.

Refer to the Billing Manual for more information about CDR creation, the CDR formats that the RTR supports, and the fields that can be included in CDRs.

9.8 Load Balancing over Multiple SMSCs

The RTR load balances MO messages over multiple SMSCs over SS7 or IP. The RTR's load balancing mechanism is based on a combination of:

- Dynamic variables:
  - Availability of SMSCs
  - Throughput threshold state per SMSC
  - Total number of messages to distribute over the SMSCs
- Semi-static variables:
  - Maximum throughput
  - Priority
  - Weight

The load balancing mechanism is recalculated every second. If any quasi-static variable is changed, the mechanism takes the new value into account in the next second. Every second, the status of the variables is refreshed and used as a basis for calculating the load balancing ratio. This dynamic load balancing mechanism enables allocation of certain SMS traffic to particular SMSCs that are selected based on priority and weight.

9.8.1 SMSC Availability

You must define each SMSC that interfaces with a RTR as an SMSC entity in the Manager. The SMSC entity configuration includes:

- Throughput regulation—Controls whether the RTR regulates throughput toward the SMSC. If throughput regulation is enabled, you define a threshold for the maximum number of messages per second that the SMSC receives from each RTR.
- SMSC status tracking—Controls whether the RTR tracks the status of the SMSC. If SMSC status tracking is enabled, the RTR verifies the SMSC status at regular intervals by opening a dialogue with the SMSC at the application level. If the SMSC responds, the RTR considers it to be up. If the dialogue opening times out or if the SMSC aborts the dialogue at a lower level, the RTR considers the SMSC to be down.

Throughput regulation and SMSC status tracking can both cause the SMSC to not be available for routing. The SMSC entity's operational state reflects the SMSC's availability. The following table describes the possible operational states:

State	Description
adminDisabled	The SMSC entity is currently deactivated in the administration
unreachable	The SMSC status tracking function reports the SMSC as being down
throughputExceeded	The throughput regulation function has determined that the threshold has been reached **Note:** This state applies only to SS7 SMSC.
available	The SMSC is available for routing

9.8.2 Load Balancing Scheme

When you define an MO routing rule that will route traffic toward an SMSC, you must specify a load balancing scheme that specifies how traffic should be distributed over the set of available SMSCs. For each SMSC, you must specify the following parameters:

Parameter	Description
Maximum throughput	Maximum number of messages that an RTR will send toward an SMSC (0 disables throughput regulation)
Priority	SMSC priority between 0 (least urgent) and 99 (most urgent); significant when multiple SMSCs are defined
Weight	SMSC weight; significant when multiple SMSCs have the same priority
Modifier	Modifier to apply when a message is routed to the SMSC. **Note:** This parameter applies only to SS7 SMSCs.

The RTR only considers SMSCs that satisfy the following conditions:

- SMSC operational status is available
- The number of messages that the RTR has sent to the SMSC (for the MO routing rule) during the current second does not exceed the threshold that the maximum throughput parameter specifies

The RTR will always route messages to the SMSC with the highest priority. Any other SMSC will not receive any messages unless the highest-priority SMSC becomes unavailable for routing because:

- It is unreachable
- As a result of the SMSC-specific throughput regulation
- As a result of the rule-specific throughput regulation (only for SS7 SMSCs).

When multiple SMSCs have the same priority, the RTR will distribute traffic toward the SMSCs in the rates defined by the weight parameter.

The RTR recalculates the load balancing scheme when the weight or priority of the SMSCs changes or when SMSCs are added to or removed from the scheme.

9.8.3 Load Balancing Example: Equal Weights

Given the following:

- 20 SMSCs
- All SMSCs have a weight of 1
- Load of 600 messages per second over two RTRs (300 messages per second per RTR)
- Interval is 60 seconds (total of 36,000 messages)

Load balancing is calculated per RTR; therefore, every RTR must divide 300 messages over 20 SMSCs, every second.

Because all SMSCs have an equal weight of 1, each SMSC in the load balancing scheme will receive:

```
300 * 1 / 20 = 900 messages from each RTR in the 60-second interval
```

9.8.4 Load Balancing Example: Mixed Weights

Given the following:

- 20 SMSCs
- 7 SMSCs with a weight of 4
- 13 SMSCs with weight 1
- Total sum of the weights is 41
- Load of 600 messages per second over two RTRs (300 messages per second per RTR)
- Interval is 60 seconds (total of 36,000 messages)

Load balancing is calculated per RTR; therefore, every RTR must divide 300 messages over 20 SMSCs, every second.

Because the SMSCs have different weights, they will receive an unequal number of messages. The SMSCs with a weight of 4 will receive:

```
60 * 300 * 4 / 41 = 1756 messages from each RTR in the 60-second interval
```

The SMSCs with a weight of 1 will receive:

```
60 * 300 * 1 / 41 = 439 messages from each RTR in the 60-second interval
```

Note: Actual amounts may differ due to the rounding used in this example.

9.8.5 Load Balancing Use Case

Load balancing over multiple SMSCs can be used when person-to-person MO traffic with an originating global title in the range of yyy to zzz should be routed to SMSC X because the SMSC is located in the same area (thus limiting the signalling traffic).

When SMSC X reaches its defined throughput threshold, traffic should be routed to SMSC Y. To achieve this overload mechanism, apply a higher priority to SMSC X than to SMSC Y.

9.9 Mobile Number Portability Support

The RTR can perform a configurable, efficient mobile number portability (MNP) check for incoming MO messages. The RTR's MNP check reduces signalling load and efficiently uses HLR capacity.

Note: Using the MNP check functionality will impact the RTR's performance.

9.9.1 MNP Configuration

The MNP support of the RTR is based on the following attributes in the common configuration file:

Attribute	Description
allowmofromfriendlysubscribersonly	Indicates if the RTR should perform an MNP check. If set to: • "false" (disabled, default), all MO messages are accepted, irrespective of the `numberportabilityenabled` and `nationalroamingenabled` settings. • "true" (enabled), MO messages with an originator MSISDN of a different country are rejected independently of the `numberportabilityenabled` and `nationalroamingenabled` settings.
smschavenumberportabilitycheck	Indicates if the SMSCs should perform an MNP check. If set to: • "false" (disabled, default), the RTR performs the MNP check (if `allowmofromfriendlysubscribersonly` is "true"). • "true" (enabled), the RTR does not check the originator when incoming MO traffic is routed to an SMSC.
numberportabilityenabled	Indicates if MNP is implemented in the HPLMN country. If set to: • "false" (disabled, default), the RTR does not care about the `nationalroamingenabled` setting, but only looks at the originator MSISDN (accept own MSISDN and reject foreign MSISDN). • "true" (enabled), the RTR looks at the `nationalroamingenabled` setting.
nationalroamingenabled	Indicates if network is shared on national basis. If set to: • "false" (disabled, default), MO messages from own network MSCs are passed, MO messages from other operators of the same country are blocked.

Attribute	Description

	• "true" (enabled) **or** if the MO message comes from a different country, the RTR starts considering the originator IMSI:
	  • If the IMSI is known, the RTR rejects messages with invalid IMSIs or IMSIs that are not from own network. Only own ("friendly") IMSIs are passed.
	  • If the IMSI is not known, the RTR tries to retrieve it by means of an SRI-SM. If the SRI-SM fails, the MO will be rejected, except for the two errors "call barred" and "teleservice not provisioned", for which the message can be accepted if so configured, refer to:
	  • `actionformnpcheckfailureduetocallbarred`
	  • `actionformnpcheckfailureduetotsvcnotprov`

9.9.2 Advanced MNP Configuration

The RTR can perform an advanced MNP check using the configurable behaviour described below.

9.9.2.1 Configurable MO Access Control

You can specify the TT value for SRI-SM operations that the RTR issues to perform MO access control (by default, the TT is 0). The `ttusedfororiginatorimsiretrieval` attribute in the semi-static configuration file controls the TT value.

If you need to address the HLRs using PC/SSN, you must define a GTT rule for each HLR. Each GTT rule should impose the following conditions on the SCCP CDPA:

- TT is equal to the value specified for the `ttusedfororiginatorimsiretrieval` attribute
- GTAI masks the MSISDN range that is served by the HLR

You can implement MO access control using MO routing (MOR) rules. When the RTR evaluates an MOR rule that includes an originator condition that pertains to an IMSI, the RTR first evaluates whether or not all other conditions in the rule are satisfied. If this is the case, the RTR then retrieves the originator IMSI.

The originator IMSI could already be available. If this is the case, the RTR will use that IMSI (instead of retrieving it again).

If an SRI-SM query returns "teleservice not provisioned" or "call barred", the sender IMSI may not be available, which will result in an MNP check error. Configure the RTR's behaviour in this case with the following `tpconfig` attributes in the semi-static configuration file:

- `actionformnpcheckfailureduetotsvcnotprov`
- `actionformnpcheckfailureduetocallbarred`

If these attributes are not set, the RTR will treat the error as if it is an MNP violation.

Mobile-originated counting (MOC) rules never trigger IMSI retrieval. If an MOC rule has an originator condition that pertains to the IMSI, the rule will also match when the:

- Originator IMSI was part of the MO-ForwardSM operation, or
- The RTR retrieved the originator IMSI from the HLR

9.9.2.2 Configurable SRI-SM Routing

The configuration supports a per number range basis implemented on a per network basis. The configuration for the mobile network entity has the following items:

- TT value to be used for first SRI-SM.
- Indication whether a second SRI-SM is to be issued when the first
- SRI-SM fails with an indication that the concerning MSISDN has been ported.
- TT value to be used for second SRI-SM (only applicable if second SRI-SM is enabled).

9.9.2.3 Accessing HLR when IMSI is Known

An optimized way to access the HLR once the IMSI is known. This specific way of addressing saves resources on the MNP/SRF and the STP. The MNP is basically bypassed as the HLR is accessed directly.

For this addressing method, the IMSI is used to determine the network that has the concerning MSISDN as a subscriber. In the GTAI of the CDPA, the country code should replaced by a prefix that identifies the network.

9.10 TON/NPI Support

The RTR supports a configurable combination of recipient TON/NPI values in MO rule conditions, which enables routing or discarding of MO messages using a TON/NPI filter.

For originator MSISDN, the following standard validation applies:

- TON is equal to international or unknown
- NPI is equal to ISDN/telephony or private numbering plan - TCP/IP (value 5)

By default, the RTR will use the pre-normalized TON for the routing conditions. A new parameter, `rtruseprenormalizedtypeofnumberforroutingcondition` has been introduced. If it is set to false, the RTR will use the normalized TON value.

9.11 MO Routing to Unknown SMSCs

The RTR/FWL supports a type of MO-MO routing in which it routes MO messages to external SMSCs that are not provisioned in the Mobile Messaging network ("unknown" SMSCs). This functionality enables an operator to pass MO traffic from inbound roamers through their FWL, without requiring the operator to provision the SMSC address of every roaming partner.

The RTR/FWL also supports routing MO messages to unknown SMSCs transparently. Transparent routing means that:

- There is only a single TCAP dialogue between the originating MSC and the external SMSC.

- The Mobile Messaging network preserves the protocol layers up to and including TCAP, with the exception of global title translation (the network may modify protocol layers above TCAP).
- The external SMSC to which messages are forwarded is not aware that the messages have passed through the Mobile Messaging network.
- When a message arrives at the external SMSC, the SCCP Calling Party Address (CgPA) contains the global title (GT) of the originating MSC, not the global title of the RTR.
- By default, the RTR makes use of SCCP Called Party Translation Type 0 for ITU-T/Japanese SS7 or 10 for ANSI in the outbound MO message. A new parameter, `rtrusedefaulttranslationtypeformoforwarding`, has been introduced. If it is set to false, the RTR will forward the exact same Translation Type received to the SMSC.

9.11.1 Sample Inbound Roaming Message Flow

The following is an example of the message flow when an MO message from an inbound roamer is routed to an external SMSC that is not provisioned:

1. The MSC sends a TCAP Begin message and the Mobile Messaging network intercepts it.
2. The CdPA in the Begin message matches an address in a provisioned list.
3. The RTR transparently forwards the Begin message toward the external SMSC.
4. The SMSC responds to the Begin message by sending a Continue message toward the MSC (the Mobile Messaging network does not intercept this message).
5. The MSC responds with a Continue message with components.
6. The Mobile Messaging network intercepts the message and the RTR processes it. Standard mobile number portability (MNP) for originator and anti-spoofing checks can be performed.
7. The MOX rules are evaluated and any resulting EC application actions (such as evaluation by the FAF and/or PBC).
8. If the evaluation is positive, the MOR rules are evaluated.
9. If the message matches the MOR rule, and the selected action is route to SMSC, and CdPA-based forwarding is enabled:
    - If transparent routing is enabled (the **Keep MSC/SGSN SCCP of CdPA** parameter is "true"), the RTR will reuse the existing TCAP dialogue to forward the message to the external SMSC
    - If transparent routing is disabled (the **Keep MSC/SGSN SCCP of CdPA** parameter is "false"), the RTR will start a new TCAP dialogue to forward the message to the external SMSC
    - If transparent routing is set to use the global setting, the RTR checks the `optimisedmorouting` parameter in the semi-static configuration file:
        - If it is "true", the RTR will reuse the existing TCAP dialogue to forward the message to the external SMSC
        - If it is "false", the RTR will start a new TCAP dialogue to forward the message to the external SMSC
10. If transparent routing was used, the SMSC sends the End message directly to the MSC (the Mobile Messaging network does not intercept this message). If transparent routing was not used, the SMSC sends the End message to the Mobile Messaging network.

9.11.2 Restrictions on Firewalling MO Traffic from Inbound Roamers

There are some restrictions on routing MO traffic from inbound roamers to unknown SMSCs:

- The RTR cannot send the messages to an SMSC other than the one identified by the CdPA of the TCAP Begin message.
- The RTR cannot load balance the messages over multiple SMSCs.
- The MAP phase cannot be changed between the incoming MO message and the outgoing MO message (except when required by the RTR's MAP phase negotiation functionality).
- If transparent routing is used, the message length cannot be increased such that it transforms from a TCAP non-segmented message to a TCAP-segmented message. Therefore:
  - The RTR's global title translation (GTT) functionality should not increase the address length
  - Text insertion (via the XS-TIE component) should not be used
  - The FAF should not be used in a way that increases the length of the user data (such as by masking or replacing text)

  If the message would require more than a single MTP PDU (because the address or the user data is too long), the RTR will refuse the message and return a "system failure" message to the originating MSC. The `smsCntMoRejectedDueToLengthChangeOnTransparentForwarding` counter indicates how many messages the RTR rejected for this reason.

Note: If transparent routing is used, the RTR will not know the result of the message submission nor the result of the message delivery. Online billing can be applied to this type of routing; however, for cases in which online billing depends on the delivery result, the RTR will assume that the message was submitted and delivered successfully. This could result in over-charging of the subscriber, so it is therefore not recommended.

9.11.3 Route MO Traffic from Inbound Roamers

To enable the FWL to intercept MO traffic from inbound roamers, in the MGR:

1. In **Routing ➤ Lists**, create an MSISDN list. The addresses in this list will be matched against the CdPA of all empty Begin messages received for MO messages. You can use the list as a blacklist or as a whitelist.

   If the CdPA matches an entry in a whitelist or does not match an entry in a blacklist, the RTR/FWL will transparently forward the Begin message to the external SMSC.

   If the CdPA does not match an entry in a whitelist or does match an entry in a blacklist, the RTR/FWL will send a Continue back to the MSC (this makes transparent routing impossible because it makes the MSC aware of the RTR). Once the RTR/FWL has a Begin and a Continue with components, it will evaluate the MOR rules. If the RTR/FWL sees that the MOR rule is configured for transparent routing, the RTR/FWL will return a "system failure" error to the MSC and increment the `smsCntTransparentForwardingOverriddenForSegmentedMo` counter.
2. In **Firewall ➤ MO ➤ Properties**, select the list that you created and set whether it will be a blacklist or a whitelist.
3. In **Routing ➤ Routing Rules ➤ MOR**, create an MOR rule that will handle MO traffic from inbound roamers. For the rule's action, select **Route to SMSC**. Set the **CdPA Based Forwarding** parameter to "true".

   If you want the RTR/FWL to route MO messages transparently, for the **Keep MSC/SGSN SCCP CdPA** parameter, select:

   - False—Start a new TCAP dialogue to forward the message to the external SMSC
   - True—Reuse the existing TCAP dialogue to forward the message to the external SMSC

- Use global setting—Use the value of the `optimisedmorouting` parameter in its semi-static configuration file (which defaults to "false")

9.12 Using Alternative Global Titles for MO Routing

The RTR supports alternative identities for global title (GT) routing through the use of configurable alternative GTs. Each RTR instance can have up to 10 alternative identities. The alternative GTs are used on the same physical network connection; additional physical network connections are not added.

Note: This feature is not supported for point code (PC) routing.

The RTR receives an SCCP message at its virtual point code (VPC); any SCCP called party address (CDPA) is accepted. It applies a best-matching algorithm to the CDPA to determine which identity to use within the scope of the TCAP dialogue. This algorithm compares GTs digit-by-digit, starting with the country code. If the same number of digits matches for two or more candidate GTs, then the best-matching GT is unpredictable; however, if one of them is the RTR's own GT, then that is considered to be the best match.

Subsequent SCCP messages that the RTR receives for the same TCAP dialogue will address the chosen identity, which the RTR instance will accept as the CDPA GT.

The billing records (CDRs) and log records that the RTR writes will contain the GT that it receives.

Note: The RTR will not apply this feature in a configuration where transparent routing or interception of TCAP CONTINUE dialogues is done.

9.12.1 MO Use Case for Alternative GTs

The RTR can use multiple alternative GTs to support an operator that uses dual IMSI SIM cards to facilitate roaming agreements.

For example, there are three operators:

- Operators A and B have a roaming agreement and SS7 interconnect
- Operators B and C have a roaming agreement and SS7 interconnect
- Operators A and C do not have a roaming agreement and do not have SS7 interconnect

This figure illustrates the scenario.

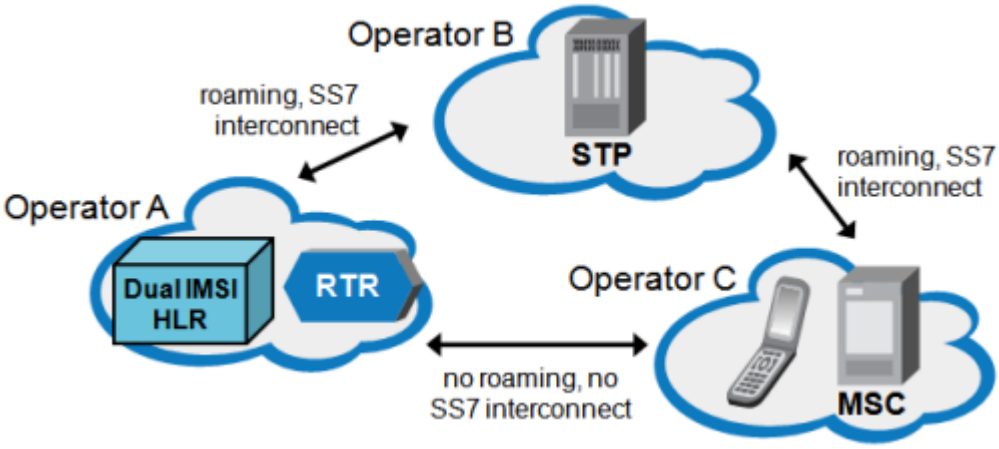


Figure 33: Operators with roaming agreements

Operator A does not have many roaming agreements, but Operator B does. Therefore, they agree that A's subscribers can roam into networks with which B has a roaming agreement (including the network of Operator C). To ensure that A's subscribers can register with C's network, A uses SIM cards that contain two IMSIs:

- One of A's own IMSIs, which the phone uses whenever possible
- An alternative IMSI that belongs to a range that B has set aside for A's subscribers, which the phone uses when attempting to register with the networks of B's roaming partners

When an A subscriber roams in C's network, C recognizes the alternative IMSI as belonging to B and allows the subscriber to register with the network. Also, B's STPs recognize the SMSC address that is associated with the IMSI and route messages to A.

To ensure that the lack of SS7 interconnect between A and C does not block MO responses and MtForwardSm requests, the RTR manipulates the GT in the SCCP CGPA.

When an MO message arrives at the RTR, it will:

- Address the RTR's virtual point code (VPC) at the MTP/M3UA level, and
- Have a B GT at the SCCP level (CDPA)

The RTR will accept the message. However, if the RTR's response contains its own GT in the CGPA (which is a GT belonging to A), C might drop or reject the response. Therefore, the RTR should use an B GT instead.

This figure illustrates a TCAP dialogue with an alternative GT (RTRx).

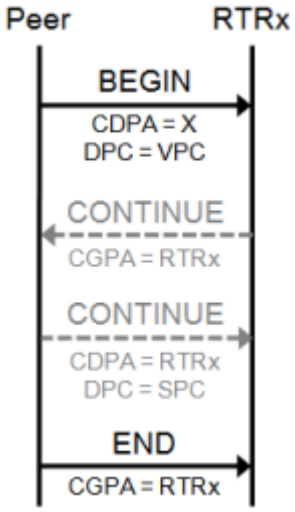


Figure 34: MO TCAP dialogue with alternative GT

9.12.2 Configuring Alternative GTs

Configure the alternative GTs by adding the `alternativeidentity` tag to the **host-specific** configuration file as a sub-tag of `tpconfig`. Set the `gt` attribute to a string of 1 to 20 digits representing an alternative GT.

The RTR supports up to 10 `alternativeidentity` tags in the configuration file.

Sample Alternative GT Configuration

This excerpt of a host-specific configuration file shows the RTR's main identity in the `gtaddressinfo` attribute and its alternative identities in the `alternativeidentity` tag.

```
<tpconfig
     gtaddressinfo="491720499014"
     [other attributes]
 >

     <alternativeidentity gt="31600001003"/>
     <alternativeidentity gt="33890022276"/>

     [other tags]
</tpconfig>
```

9.13 Virtual SMSC Support

A Virtual SMSC (VSMSC) is a logical SMSC node, identified primarily by a dedicated global title (VSMSC address), that resides on a physical SMSC node. The physical SMSC node (the RTR) only performs a relay service for VSMSCs.

All MO traffic sent to the global title of the VSMSC (as indicated by the MO/SM's MAP layer service center address field) can be provisioned to be routed/relayed to a dedicated SMS application (MO-AT).

All AO traffic from that SMS application can be provisioned to be AO-MT routed/relayed using the SMSC address of the VSMSC in the MT/SM's MAP layer service center address field.

Virtual SMSC Provisioning

There is a tight coupling between the VSMSC's address and an SMS Application. The VSMSC address for an SMS application can be provisioned through the application provisioning in the MGR (**SMS Applications ➤ Application**). The related parameters are:

Parameter	Description
Virtual SMSC type	Specifies the VSMSC type of an application. This type relates to the FCDR format. Valid values are: • `public` (default) • `private`—The VSMSC address of this application (see **Virtual SMSC Address**) is required to be unique among all private VSMSC addresses, assisting in the correct routing of MO-AT traffic. The value of this parameter influences the `vsmscType` field of FCDRs for AO and AT messages (refer to the RTR Billing Manual for additional information). When the RTR tries to MT-deliver an AO message from an application that has a VSMSC address provisioned (irrespective of the VSMSC type), the SMSC address at the MAP layer of the MT-FSM will be set to that address, unless it is overruled by an explicit MTO modifier.
Virtual SMSC Address	Specifies the VSMSC address associated with this application. The address must be specified in E.164 format, i.e. as internationally significant numbers, starting with the country code. When specified, this value can be used for routing MO traffic for this VSMSC address to this application (as AT/SM), and for delivering AO messages from this application (as MT/SM) using the VSMSC address as the SMSC address. The value of this parameter influences the `vsmscId` field of FCDRs for AO and AT messages (refer to the RTR Billing Manual for additional information).

For MO routing to an application, the RTR supports determining the destination application by matching the received SMSC address against the set of provisioned, private Virtual SMSC (VSMSC) addresses (refer to *Application Selection*).

For AO-MT routing, where the **Virtual SMSC Address** is specified, the service center in the MT-FSM will be based on the specified **Virtual SMSC Address**, unless it is modified by an MTO modifier. The SRI-SM and Report-SM delivery service center addresses will **not** be changed by the **Virtual SMSC Address**.

9.14 Portable Application Support for MO-AT

The MO-AT routing path for portable applications is applied when:

- MO-AT, MO-AT-Store or MO-Store-AT routing path is licensed
- Portable application for MO is enabled (**Routing ➤ Properties ➤ Enable Portable Application For MO**)
- The recipient address of the received MO-SM is recognized as an alias-MSISDN for a portable application.

MO-AT routing takes place by an MOR rule with the MO-AT, MO-AT-Store or MO-Store-AT action in use, and the **Application** field not referring to a specific application. An MO-AT rule only matches if during the rule evaluation, the destination application is 'available' (i.e. is logged into at least one HUB and has room for receiving additional AT messages), in the same way as the RTR currently treats 'regular' MO-AT messages.

It is possible to use the condition **Recipient [cond]** of type **Application** in all MO rule types, to have the rule match if the recipient is an alias-MSISDN for that application.

Note: This condition does not support matching of multiple applications through a single rule, there would need to be a rule for each application.

When an MOX rule triggers an evaluation request to an EC application, if the recipient is an alias-MSISDN, the RTR will populate `terminatingApplication` message field with the short code of the application associated with the alias-MSISDN.

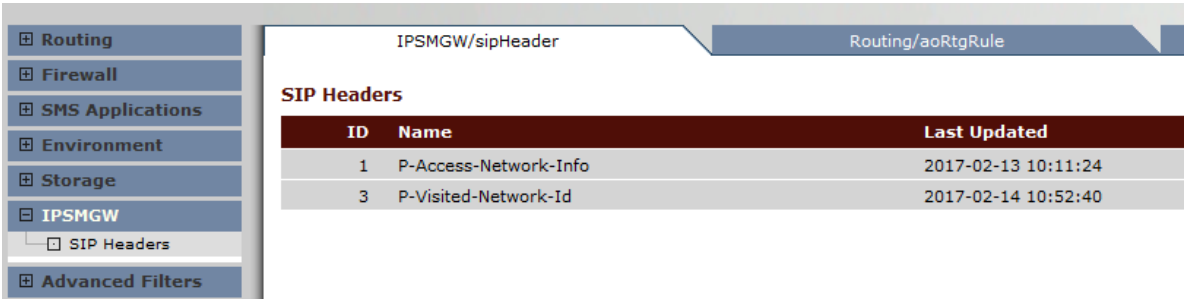
Since an alias-MSISDN is used for the recipient, any early SRI-SM will be skipped, as the HLR would not know the MSISDN.

9.15 MO Rule Conditions for SIP Originated Message

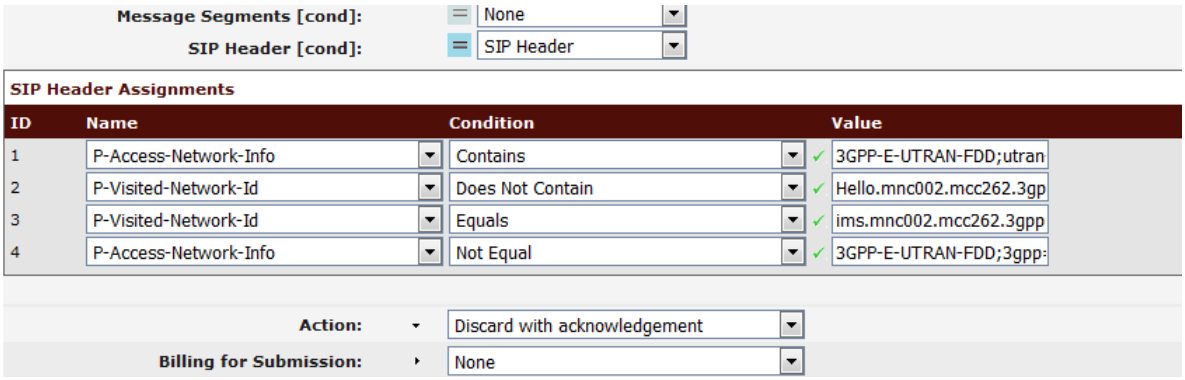
MO Routing rules support SIP Headers conditions which can be used to determine Routing Action based on SIP Header values received in incoming SIP messages.

If set as "SIP Header", sub-conditions will be matched against SIP header received in incoming SIP Originated message. Four sub-conditions can be provisioned.

Note: SIP Header to be used in Rule Evaluation must be provisioned in SIP Header Screen under IPSM-GW tab. For example, if user wants to apply condition on SIP header "P-Access-Network-Info"& "P-Visited-Network-Id" then, it should be configured Under the IPSM-GW tab.



Four SIP Header conditions can be provisioned in MO Rules as in the following image:



Each SIP Header condition consists of three parts:

1. Name:

   Index to the SIP Header Table. It indicates the SIP Header on which this condition must be applied.

2. Condition type:

   This parameter indicates the Condition Type: contains, does not contain, equals, not equal. Default value is `none`. Below table describe for the condition type.

Condition type	Description
`contains`	If the condition type is **Contains**, then the condition will match only if the configured **Value** string is contained in the corresponding SIP Header of the incoming message.
`doesNotContain`	If the condition type is **Does not Contain**, then the condition will match only if the configured **Value** string is not contained in the corresponding SIP Header of the incoming message.
`equals`	If the condition type is **Equals**, then the condition will match only if the configured **Value** string is exactly contained in the corresponding SIP Header of the incoming message.
`notEqual`	If the condition type is **Not Equal**, then the condition will match only if the configured **Value** string is not exactly contained in the corresponding SIP Header of the incoming message.

3. Value:

   This parameter indicates the SIP header value to be searched in corresponding SIP Header in the incoming message. The value can be 255 characters long.

Note: If non-basic ASCII characters are configured in the SIP Header condition, the SNMP commands like "`tp_walk`" on a terminal may not display the characters properly. This does not means the configuration is wrong. Please check the SNMP trace to confirm the configuration. The terminal display of the characters depends on the Operating System, Locale setting and language support of the machine where the terminal runs.

9.15.1 Processing Logic

On receiving a SIP Originated Message, the IIW parses the message and captures the SIP Header provisioned in the SIP Header table. The IIW forwards the captured headers to the RTR using the internal interface. The RTR further uses the headers in rule evaluation.

Some important points to observe:

1. If the SIP Header provisioned in the condition wass not received in the incoming SIP message, then the condition fails and the rule is not matched.
2. Only first 255 bytes of SIP header are captured. The rest are ignored and will not be part of the rule evaluation.
3. The header can be a multi-header in comma separated format or multiple instances of the same header. In both cases the header will be shared in comma separated format.
4. For a SIP multi-header string, the search will be performed on the complete string (including the comma as well) and not just on the last header.
5. Up to 10 SIP headers can be provisioned.
6. Up to 4 SIP header sub-conditions are allowed.
7. Evaluation is performed on the sub-conditions one by one and the combined result is the logical AND of all the sub-conditions.
8. If negation is specified for a SIP condition, then the combined result of all SIP sub-conditions will be reverted.
9. Search will be performed case-insensitive.
10. Leading spaces in the SIP header name are not recommended due to the default behavior in IIW which will truncate the leading spaces (if any) present in a SIP Originated Message.
11. When an incoming SIPO message with more than 255 characters is received by the IIW, the IIW truncates the SIP header and captures only first 255 characters. In case if the 255th character is a space (" "), the IIW & RTR consider it as a character, which further impacts the rule matching as in MGR GUI only 254 characters with condition type as "equal" & SIP header length in the capture is 255 character, then rule will not match.
12. When the IIW receives incoming SIP message with short form of the header name and the SIP header provisioned in the condition with original header name in MGR GUI then condition fails and rule will not matched.

The following are examples of valid `To` header fields.

The compact form of the `To` header field is `t`.

```
t: sip:+12125551212@server.phone2net.com
```

If the SIP header is configured as `To`, the condition fails and the rules will not match.

The rule evaluation logic based on the **Condition type**, assuming A, B, C are strings without comma:

Header Value	**Condition Value**	**Condition: contains**	**Condition: does not contains**	**Condition: equals**	**Condition: not equal**
A	A	Match	Fail	Match	Fail
AB	A	Match	Fail	Fail	Match

Header Value	Condition Value	Condition: contains	Condition: does not contains	Condition: equals	Condition: not equal
(A is a substring of AB)					
A;B	A	Match	Fail	Fail	Match
A	A;B	Fail	Match	Fail	Match
A;B	A;B	Match	Fail	Match	Fail
B;A	A;B	Fail	Match	Fail	Match
A;B;C	A;B	Match	Fail	Fail	Match

9.15.2 Examples of MO Rule Conditions for SIP Originated Message

Example 1:

If the operator wants to discard a SIP message, using the headers `P-Access-Network-Info` and `P-Visited-Network-Id` with condition types "`contains`" and "`equal`", respectively, where:

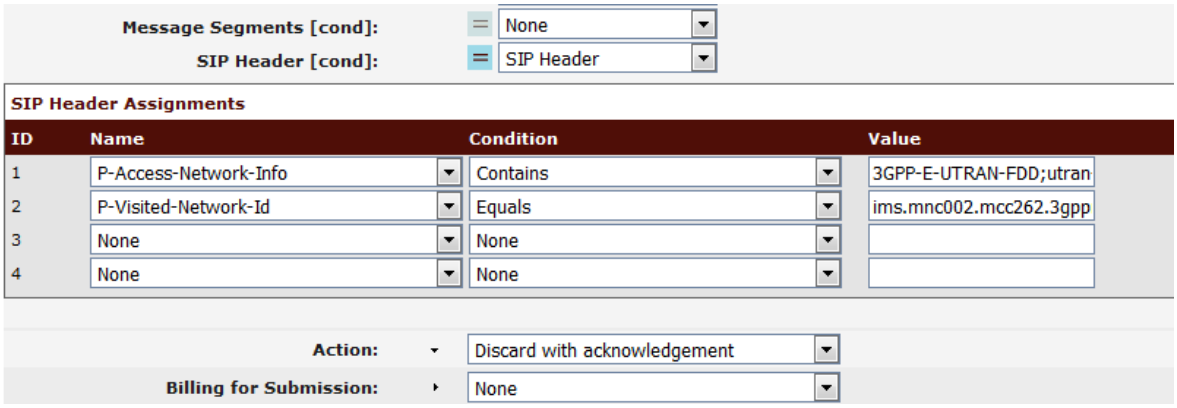
- The `P-Access-Network-Info` header contains the value "`3GPP-E-UTRAN-FDD; utran-cell-id-3gpp=262096ea10014104`"
- The `P-Visited-Network-Id` header contains the value "`ims.mnc002.mcc262.3gppnetwork.org`"

and SIP Header conditions are configured as given in the below example. Here,

```
P-Access-Network-Info: Contains = 3GPP-E-UTRAN-FDD; utran
P-Visited-Network-Info: Equals = ims.mnc002.mcc262.3gppnetwork.org
```

Note: The **Value** box in the GUI displays a limited amount of text, as shown in this example.

If the content of **Value** exists as a substring in the `P-Access-Network-Info` header and a complete string in the `P-Visited-Network-Info header`, then the condition matches and the MO rule will be applied as per the routing action.



Example 2:

If the operator wants to route the SIP message using headers `P-Access-Network-Info` and `P-Visited-Network-Id`, with condition types "`does not contain`" and "`not equal`", respectively, where :

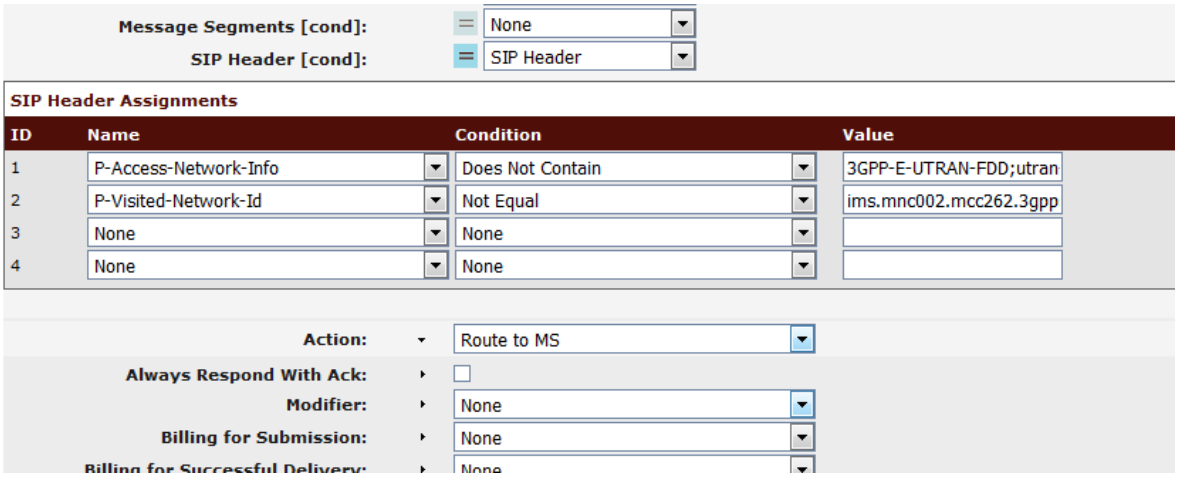
- The `P-Access-Network-Info` header contains the value "`3GPP-E-UTRANS-FDDS; utran-cell-id-3gpp=262096ea10014104`"
- The `P-Visited-Network-Id` header contains the value "`ims.mnc002.123mcc262.3gppnetwork.org`"

and SIP Header conditions are configured as given in the below example. Here,

```
P-Access-Network-Info: Does Not Contain = 3GPP-E-UTRAN-FDD; utran
P-Visited-Network-Info: Not Equal = ims.mnc002.mcc262.3gppnetwork.org
```

Note: The **Value** box in the GUI displays a limited amount of text, as shown in this example.

If the sub-string search for the `P-Access-Network-Info` header and complete string search for the `P-Visited-Network-Info` header, as per the configured **Value** (example), is not successful, the condition will be successful and the MO rule will be applied as per the routing action.

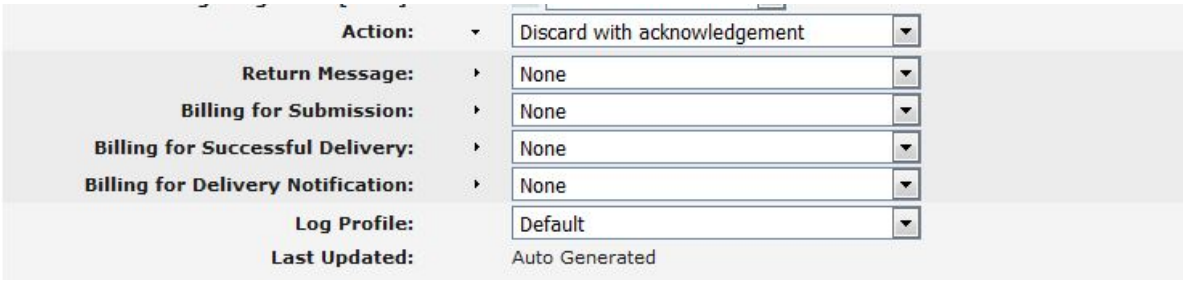


Note: The SIP header conditions are applicable in the MOR/MOX/MOC rule.

9.16 Return Error Message for MO Originate Message

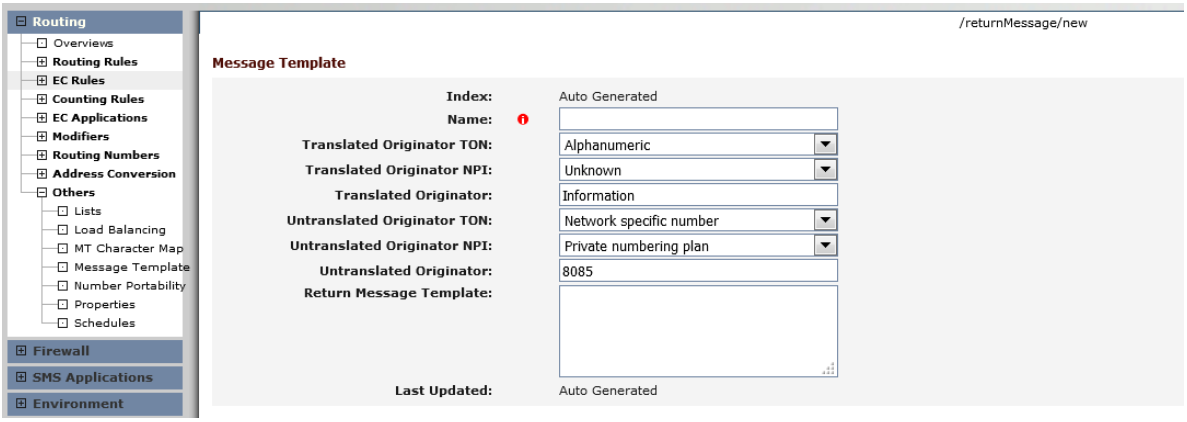
When the RTR receives an incoming MO message, if the applied MO rule rejecting the message (MOR/MOX rule failure action: discard with Ack/Nack) is associated with a configured message template, then the RTR will send the custom return message back to the originator. For this feature, the RTR supports sending an SMS back to the originator, specifically also in Japanese (i.e. UCS-2) .

The MOR/MOX Rules allow the selection of Message template when the action is set to **Discard with Ack** or **Discard with Nack**. This functionality is controlled by the license "Enable Message Template".



Note: Select Return message template for the MOR/MOX Rule when the action is set to **Discard with ACK** or **Discard with NACK**.

The return message template can be configured in the section **Others ➤ Message Template**:



The below placeholders can be used in the return message template:

- `$(USER_DATA)` - the user data of the original message, received by the RTR
- `$(SCTS_2)` - the service center timestamp, indicating the local time
- `$(RCP)` - the address of the recipient of the original MO message

Example of a template with proper order of placeholders:

```
Message from $(RCP) at $(SCTS_2) "$(USER_DATA)" is not sent.
```

Note:

- If Translated or Untranslated Address are configured as Alphanumeric Address then TON/NPI should be 5/0 respectively, otherwise, it cannot be sent via AMS. For more information about the TON/NPI in CCDRG, refer to the Billing Manual.
- For configured return messages, the first 160 characters (for ASCII) or first 140 bytes (for UCS2) are sent to the final return message. The remaining characters will be truncated.
- If the user executes `tp_walkall` for the return message template, only the template having the state `active` will be displayed.

9.17 Point code (PC) Routing for MO Messages

The PC routing functionality is applicable to MO-FSM and MO-FSM Response traffic, where the RTR acts as a SMSCs and retains the Global Title Address of the incoming MO-FSM, even when the Routing

Indicator is 1 (i.e. Route on SSN), and creates a response with a GTI of 0x04 and the RTR's own Actual Global Title address.

Following are the functionalities in details related to PC routing:

The details related to this functionality are presented below:

- If the semi-static parameter *rtrsetownnetandownctyforpcroutedmofsm* is set to false, the RTR determines the MSC country and network using the received SCCP CGPA GTA (i.e. MSC GT Address) and will be used for rule matching transactional log and Comverse 3g CDR.

  Note: In case of The Comverse 3g CDR, the field `Service Type` contains the abbreviated network of the incoming MSC address. The `Service Type` will be updated as per the description given in the section *defaultoperatorabbreviation* and *operatorabbrevationforunknownnetworks*.

- If the semi-static parameter *rtrsetownnetandownctyforpcroutedmofsm* is set to true, the RTR will use its own country and network as Originator MSC country and network for the Rule matching and transactional log, while it will match the originating MSC GT to determine the network and will use the defined 'Operator Abbreviation' (for the determined network) against the field "Service Type" in 3g CDR.
- If the parameter *sccppointcoderoutingfunctionsformofsm* is set to true and the RTR receives MO-FSM in TCAP begin with SCCP CGPA GTA with RI=PC/SSN and close using TCAP-End/TCAP-Abort, the RTR will perform the following steps (*Figure 35: MO-FSM closed using TCAP-End or Abort*):

  1. The RTR receives MO-FSM request on virtual PC and GT address and send MO-FSM response back to SGP. In MO-FSM response:

     a. The MTP OPC is set to the RTR's actual point code.
     b. The SCCP CgPA RI is GT, GTA is set as the RTR's actual GT.
     c. The SCCP CdPA is the same as the SCCP CgPA of the incoming MOFSM.
     d. The MTP DPC is set to either the MTP OPC or SCCP PC of the incoming MO-FSM based on the below condition:

        - MTP OPC if CgPA RI is SSN and SCCP PC is not available in incoming MOFSM.
        - SCCP PC if CgPA RI is SSN and SCCP PC is different from MTP OPC in incoming MOFSM. If it is same, then either of the PC's will be used (it makes no difference).

  2. If the SCCP CgPA PC is available in the MO-FSM Request, the same PC will be used for the "Orig. MSC/SGSN" condition in the MOR/MOX/MOC rule. If not available, the MTP OPC will be used.

  Note: There is no impact on the SCCP UDTS due to this functionality.

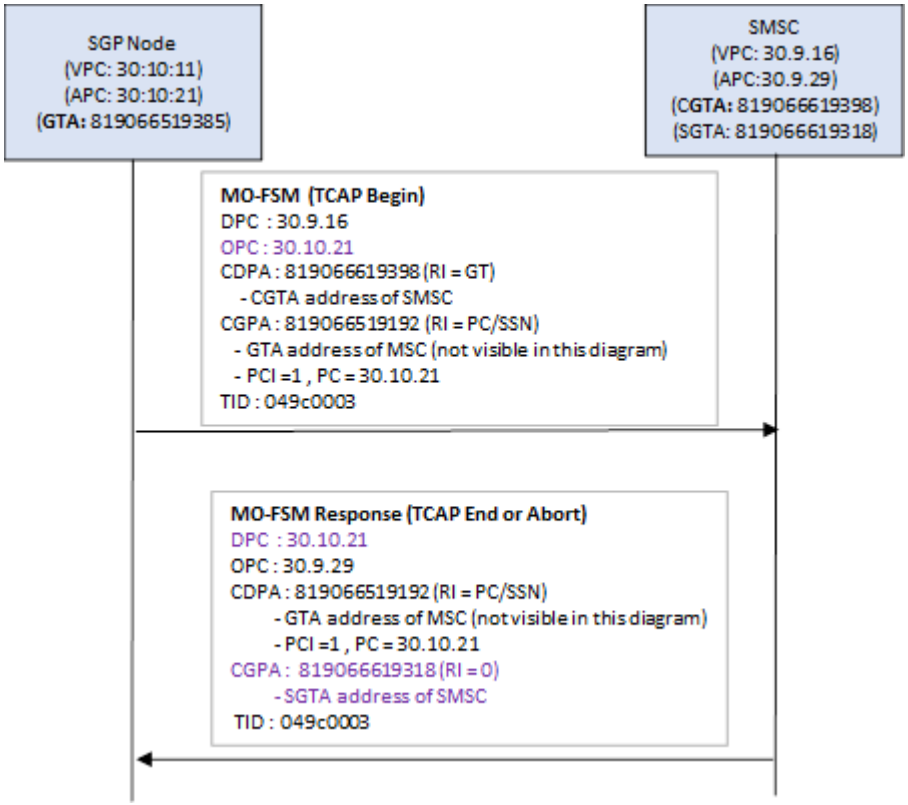


Figure 35: MO-FSM closed using TCAP-End or Abort

- If the parameter *sccppointcoderoutingfunctionsformofsm* is set to true and the RTR receives MO-FSM in TCAP continue with SCCP CGPA GTA with RI=PC/SSN and close using TCAP-End/TCAP-Abort, then RTR will perform the following steps (*Figure 36: MO-FSM continue using TC-continue and closed using TC-End or Abort*):

  1. The RTR receives TCAP begin without component to established a TCAP dialogue on virtual PC and GT address and send TCAP-continue back to SGP Node. In MO-FSM response:

     a. The MTP OPC is set to RTR actual point code.
     b. The SCCP CgPA RI is GT, GTA is set as RTR's actual GT address.

  2. In continuation of the above, the RTR will receive MO-FSM Request in TCAP-Continue on the actual PC and GT address of the RTR and send the MO-FSM response back to the SGP. In the MO-FSM response:

     a. The MTP OPC is set to the RTR's actual point code.
     b. The SCCP CgPA RI is GT, GTA is set as the RTR's specific GT.
     c. The SCCP CdPA is same as the SCCP CgPA of the incoming MOFSM.
     d. The MTP DPC is set to either the MTP OPC or SCCP PC of the incoming MO-FSM based on the below condition:

        - The MTP OPC if CgPA RI is SSN and the SCCP PC is not available in the incoming MOFSM.

- The SCCP PC if CgPA RI is SSN and the SCCP PC is different from the MTP OPC in the incoming MOFSM. If it is the same, then either of the PC's will be used (it makes no difference).

3. If the SCCP CgPA PC is available in the MO-FSM Request, then the same PC will be used for the "Orig. MSC/SGSN" condition in the MOR/MOX/MOC rule. If not available, the MTP OPC will be used.

Note: There is no impact on the SCCP UDTS due to this functionality.

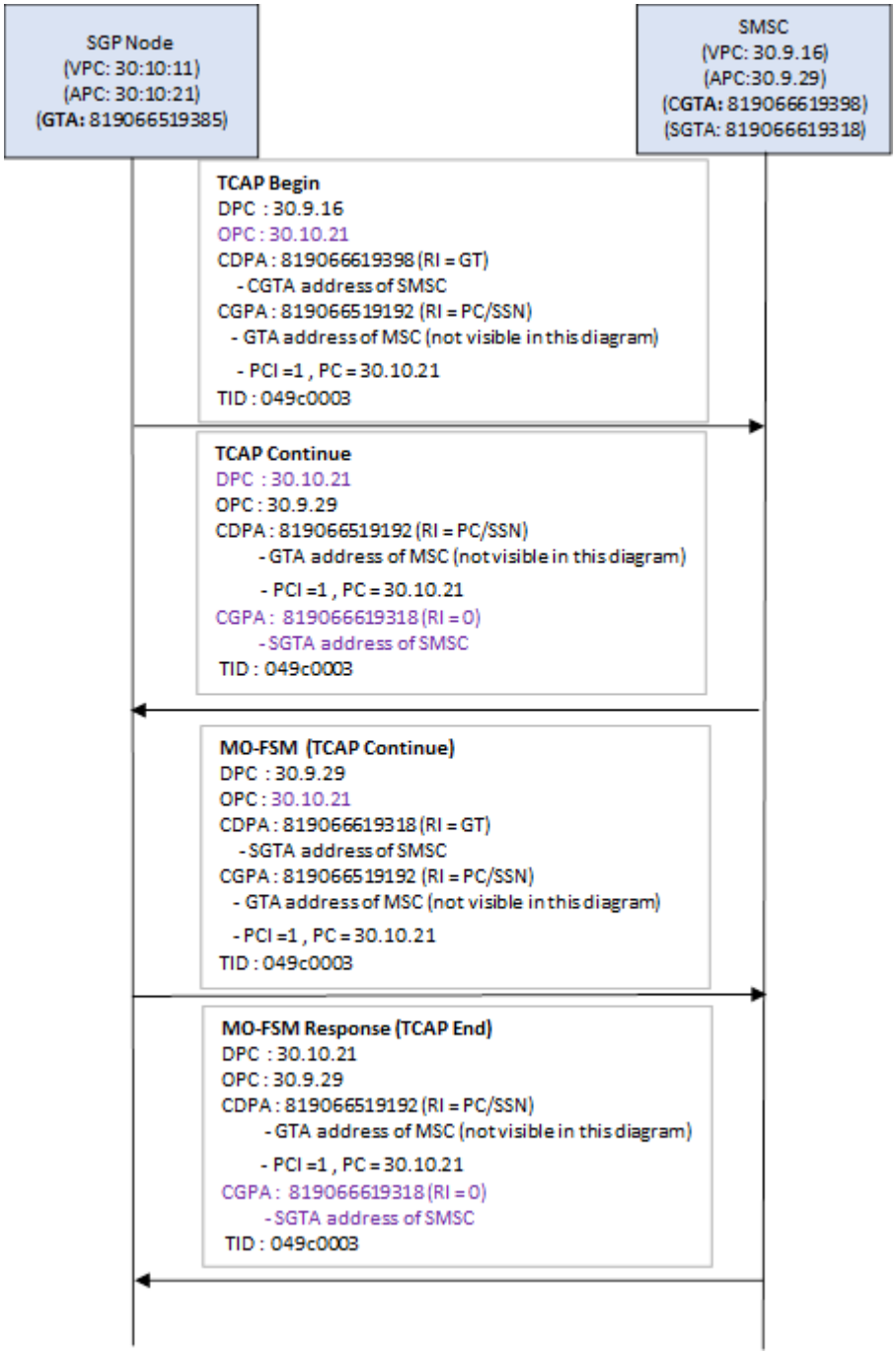


Figure 36: MO-FSM continue using TC-continue and closed using TC-End or Abort

- If the RTR acts as a SMSC and the SGP Node will be configured as an MTP destination from the RTR, the following configuration is required:
  - If MTP destination configured as 'msc' then it will be used for the functionality as described in this feature to work.

- If MTP destination configured as 'stp' then it will be used to route the message on GTT and this is not the desired behavior of functionality of this feature.
- Set the semi-static parameter *rtrsetownnetandownctyforpcroutedmofsm* to false.
- Set the semi-static parameter *sccppointcoderoutingfunctionsformofsm* to true.

- If the RTR acts as a SGP towards the SMSC, the following configuration is required:
  - Set the below semi-static parameters to false:
    - *rtrincludepcinmofwdsmtosmsc*
    - *optimisedmorouting*
    - *sccpoptimisedaddressing*
  - Set the semi-static parameter *includemscaddrinmofwdsmtosmsc* to `always`.
  - Set the semi-static parameter *pcssnroutingwhenincludingmscaddrinmofwdsmtosmsc* to true.

9.18 Opcode and SMS-SUBMIT-REPORT in MO-FSM_ack and MO-FSM_nack Messages

- When the value of value of semi-static parameter *rtrinsertsubmitreportinmofsmresponse* is set to 'false' then, Opcode & SMS-SUBMIT-REPORT will not be included in MO-FSM_ack/MO-FSM_nack; this follows the current behavior.
- When the value of semi-static parameter *rtrinsertsubmitreportinmofsmresponse* is set to 'true' and incoming MO-FSM request MAP Phase version is 3, then Opcode and SMS-SUBMIT-REPORT will be included in MO-FSM_ack and MO-FSM_nack. The SMS-SUBMIT-REPORT will have fields as per the format specified below.

1. For MO-FSM_ack following fields will be added to SMS-SUBMIT-REPORT:

```
TP-UDHI = 0
TP MTI = 1
TP-Parameter-Indicator = 0x00
TP-Service-Centre-Time-Stamp:
    <Year, Month, Day
     Hour, Minutes, Seconds
     Timezone: GMT +  hour minutes>
```

2. For MO-FSM_nack following fields will be added to SMS-SUBMIT-REPORT:

```
TP-UDHI = 0
TP MTI = 1
TP-FCS =0xc2
TP-Parameter-Indicator = 0x00
TP-Service-Centre-Time-Stamp:
   <Year, Month, Day
     Hour, Minutes, Seconds
     Timezone: GMT +  hour minutes>
```

Note: In case of MOMO, the RTR will transparently forward the MO-FSM_ack/nack response received from the external SMSC.

Note: This functionality supports only MAP Phase 3.

9.19 Conversion of NAI/NP of SCCP CgPA in Incoming MOFSM to GSM TON/NPI

While storing SCCP CgPA of an incoming MOFSM as Originated MSC Address, the NAI/NP is converted to GSM TON/NPI. The conversion of SCCP NAI/NP to GSM TON/NPI takes place differently for different SS7 flavor. The converted Originated MSC Address type is used in transactional logs and the CDRs except 3G Comverse CDR.

1. For Japanese SS7 flavor, conversion takes place as per below tables:

Table 1: Conversion table for NAI to TON for Japanese SS7

NAI	TON
0 (unknown)	0 (unknown)
1 (subscriber number)	4 (subscriber number)
2 (reserved for national use)	3 (network specific)
3 (national significant number)	2 (national)
4 (international number)	1 (international)
all others	7 (reserved)

Table 2: Conversion table for NP to NPI for Japanese SS7

NP	NPI
0 (unknown)	0 (unknown)
1 (ISDN/telephony numbering plan)	1 (ISDN/telephony numbering plan)
6 (land mobile E.212)	6 (land mobile E.212)
7 (ISDN/mobile E.214)	7 (undefined in 23.040)
all others	1 (ISDN/telephony numbering plan)

If **GTI is 1** (only NAI present)	
TON	As per Conversion table for NAI to TON for Japanese SS7 (make reference to table above)
NPI	Default value of 1 (ISDN)

If **GTI is 2** (the translation type also implies the encoding scheme, used to encode the address information, and the numbering plan), set TON/NPI with value as present in current code of ITU-T SCCP flavor for this condition.	
TON	0 (unknown)
NPI	Default value of 1 (ISDN)

If **GTI is 3** (only NP present)	
TON	Default value of 7 (reserved)
NPI	As per Conversion table for NP to NPI for Japanese SS7 (make reference to table above)

If **GTI is 4** (NAI and NP present)	
TON	As per Conversion table for NAI to TON for Japanese SS7 (make reference to table above)
NPI	As per Conversion table for NP to NPI for Japanese SS7 (make reference to table above)

2. If the CgPA in an incoming MOFSM request has any GTI for ITU-T SS7 flavor, then the conversion takes place as per below tables:

Table 3: Conversion table for NAI to TON for ITU-T SS7

NAI	TON
0 (unknown)	0 (unknown)
3 (national significant number)	2 (national)
4 (international number)	1 (international)
all others or NAI not present	0 (unknown)

Table 4: Conversion table for NP to NPI for ITU-T SS7

NP	NPI
Any value or NP not present	1 (ISDN/telephony numbering plan)

3. For ANSI SS7 flavor, the NAI/NP of SCCP CgPA in incoming MOFSM is always converted to TON/NPI 1 (International)/1 (ISDN).

9.20 Early SRI-SM Behavior for Store Cases

The following table describes the behavior of **Early SRI-SM** for MO-Store-MT and MO-MT-Store Flow:

moresponseafterhlrquery	Early SRISM	Early SRI-SM Behavior against Paths
Disable	Disable	MO-ST-MT • Early SRI-SM **will not be** performed MO-MT-ST

moresponseafterhlrquery	Early SRISM	Early SRI-SM Behavior against Paths
		• Early SRI-SM **will not be** performed
Disable	Enable	MO-ST-MT • Early SRI-SM **will be** performed MO-MT-ST • Early SRI-SM **will be** performed
Enable	Disable	MO-ST-MT • Early SRI-SM **will be** performed MO-MT-ST • Early SRI-SM **will be** performed
Enable	Enable	MO-ST-MT • Early SRI-SM **will be** performed MO-MT-ST • Early SRI-SM **will be** performed

The parameter *moresponseafterhlrquery* is a flag that indicates whether RTR should send a response to an MO/SM after it has completed the HLR query in order to obtain details of the recipient.

If it is false, the MO response is sent immediately. If it is true, the MO response is sent after the completion of the HLR query.

There are two ways by which the RTR evaluates if the early SRI-SM is enabled or not:

1. There is a white list including the recipient
2. The parameter *hlrqueryforrecipientbeforeapproval* is enabled

If the white list is configured, the parameter *hlrqueryforrecipientbeforeapproval* will not be used. The white list overrides the configuration of parameter *hlrqueryforrecipientbeforeapproval*.

Chapter 10

MT Routing

Topics:

10.1 Introduction

This chapter describes how the RTR handles mobile-terminated (MT) messages.

The process of delivering an MtForwardSm request (which can carry a "normal" Deliver-SM or a Status Report) has two phases:

1. The node that plays the role of an SMSC issues a SendRoutingInfoForSm (SRI-SM) request for the MT message's recipient, which is routed to the Home Location Register (HLR). The HLR typically returns the recipient's International Mobile Subscriber ID (IMSI) and the address of the Mobile Switching Center (MSC) where the mobile phone is currently registered.
2. The SMSC uses the routing data that the HLR returned to send the MT message to the MSC where the recipient is registered.

For a more detailed description of the MT delivery process, refer to the documentation of the SS7 protocols, especially the MAP protocol's SMS-related operations.

Inbound and Outbound MT Routing

When processing MT messages:

- The RTR can play the role of the SMSC, in which case SendRoutingInfoForSm and MT messages are always **outbound** messages. For example, this is the case when applying MO-MT or AO-MT routing.
- The RTR can play the role of an MT firewall that is logically located between the SMSC and the HLR and/or between the SMSC and the terminating MSC. In this case, SendRoutingInfoForSm and MT messages are always **inbound** messages.

  If the provisioned logic results in forwarding a SendRoutingInfoForSm to the HLR or forwarding an MT message to the MSC, they are also **outbound** messages. In the case of forwarding an MT message to the MSC, the processing of the inbound message occurs before the processing of the outbound message.

Home Routing

"Home Routing" refers to a scenario in which an external SMSC intends to deliver an MT message and the associated SendRoutingInfoForSm request is received by the RTR. In this case, the RTR returns a SendRoutingInfoForSm response that includes its own address as the address of the MSC where the recipient is currently registered. This causes the external SMSC to send the subsequent MT message(s) to the RTR instead of to the real MSC. Home Routing is described in more detail with the SRI-SM response rule set.

10.2 MT Rule Sets

The RTR supports several rule sets that are relevant to MT routing. The following table provides an overview of the rule sets and the types of messages they apply to:

Rule Set	Inbound SRI-SM Request	Outbound SRI-SM Request	Response to Outbound SRI-SM Request	Response to Inbound SRI-SM Request	Inbound MT Message	Outbound MT Message
SRI-SM Request Rule Set	X					
SRI-SM Response Rule Set				X		
MTIR Rule Set					X	
MTIX Rule Set					X	
MTIC Rule Set					X	
MTOR Rule Set		X	X[1]			X
MTOX Rule Set		X	X			X
MTOC Rule Set		X				X

This image illustrates the order in which MT rule sets are evaluated.

[1] The MTOR rule set is only evaluated in the firewalling case, where the SRI-SM arrived at the RTR as an inbound SRI-SM request that the RTR relayed to the HLR. This must be explicitly enabled. This is a deprecated way of controlling Home Routing. It is recommended to use the SRI-SM response rule set instead.

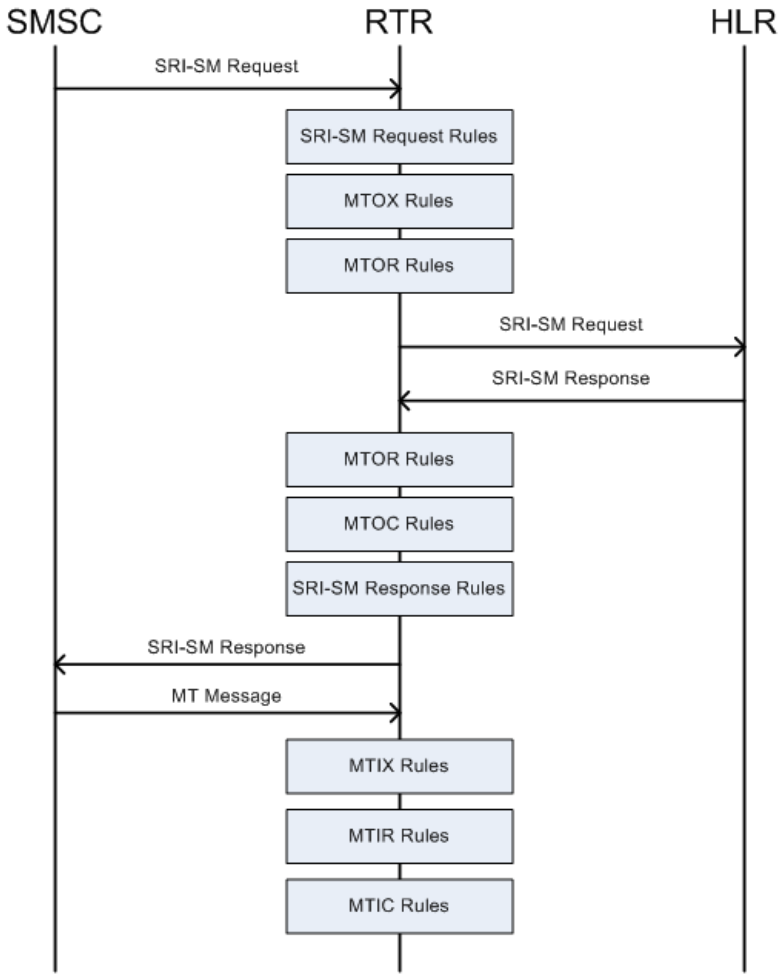


Figure 37: MT rule set evaluation order

10.3 MT Rule Set Evaluation Examples

This section describes the order of MT rule set evaluation for common routing scenarios.

MO-MT Routing Example

In a simple MO-MT routing scenario, the RTR plays the role of the SMSC. The RTR received a message as MO, and is attempting the message as MT.

1. Evaluate the MTOX rule set for the outbound SRI-SM request. Result: pass.
2. Evaluate the MTOR rule set for the outbound SRI-SM request. Result: pass.
3. Send the SRI-SM request to the HLR.
4. Receive the SRI-SM response from the HLR (assuming success).
5. Evaluate the MTOC rule set for the SRI-SM operation.
6. Evaluate the MTOX rule set for the inbound SRI-SM response. Result: pass.

7. Evaluate the MTOX rule set for the outbound MT message. Result: pass.
8. Evaluate the MTOR rule set for the outbound MT message. Result: pass.
9. Send the MT message to the MSC.
10. Receive the MT response from the MSC (assuming success).
11. Evaluate the MTOC rule set for the MT message.

This image illustrates the process described in this example.

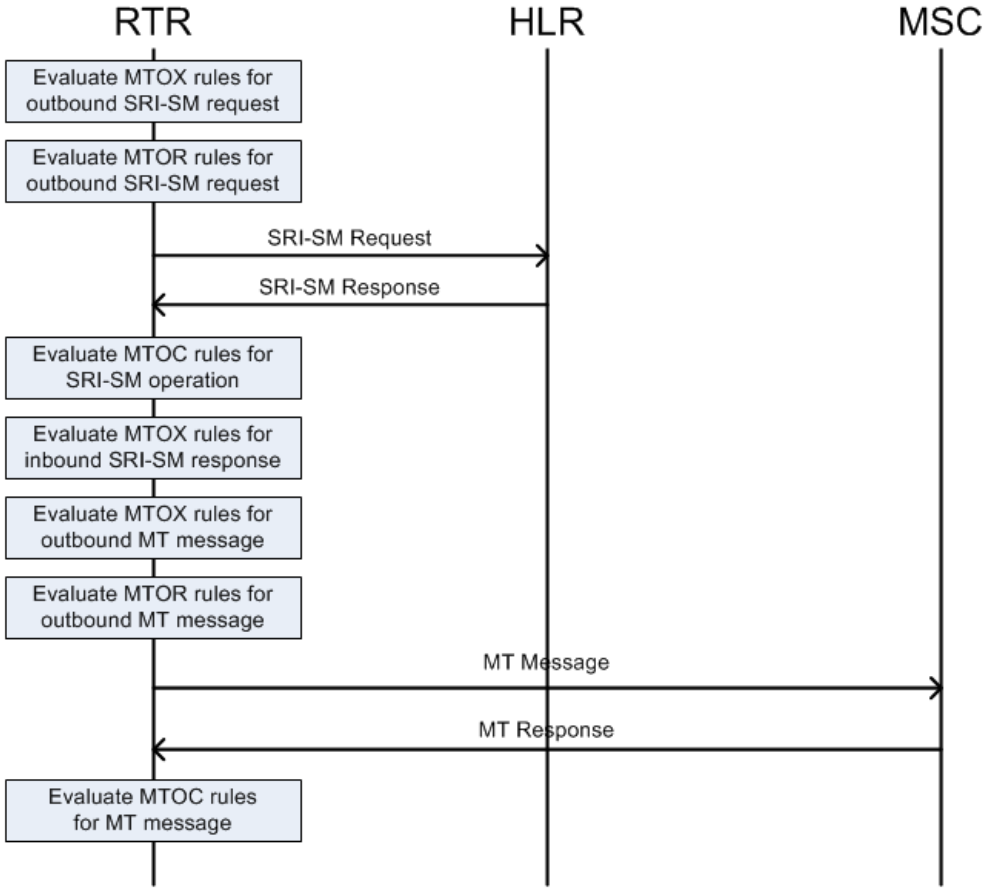


Figure 38: MO-MT routing example

MT-MT Routing Example

In a simple MT-MT routing scenario, the RTR plays the role of a firewall. The RTR contacts the HLR during the SRI-SM processing phase and Home Routes the MT message to relay it to the MSC.

1. Receive the inbound SRI-SM request.
2. Execute MT anti-spoofing checks. Result: success
3. Evaluate the SRI-SM request rule set. Result: query HLR.
4. Evaluate the MTOX rule set for the outbound SRI-SM request. Result: pass.
5. Evaluate the MTOR rule set for the outbound SRI-SM request. Result: pass.
6. Send the SRI-SM request to the HLR.
7. Receive the SRI-SM response from the HLR (assuming success).
8. Evaluate the MTOC rule set for the SRI-SM operation.

9. Evaluate the MTOX rule set for the inbound SRI-SM response. Result: pass.
10. Optionally evaluate the MTOR rule set for the inbound SRI-SM response. Result: pass.
11. Evaluate the SRI-SM response rule set. Result: home route.
12. Send the SRI-SM response to the SMSC.
13. Receive the inbound MT message from the SMSC.
14. Execute MT anti-spoofing checks. Result: success
15. Evaluate the MTIX rule set for the inbound MT message. Result: pass.
16. Evaluate the MTIR rule set for the inbound MT message. Result: route to MS.
17. Evaluate the MTOX rule set for the outbound MT message. Result: pass.
18. Evaluate the MTOR rule set for the outbound MT message. Result: pass.
19. Send the MT message to the MSC.
20. Receive the MT response from the MSC (assuming success).
21. Evaluate the MTOC rule set for the MT message.
22. Send the MT response to the SMSC.
23. Evaluate the MTIC rule set for the MT message.

This image illustrates the process described in this example.

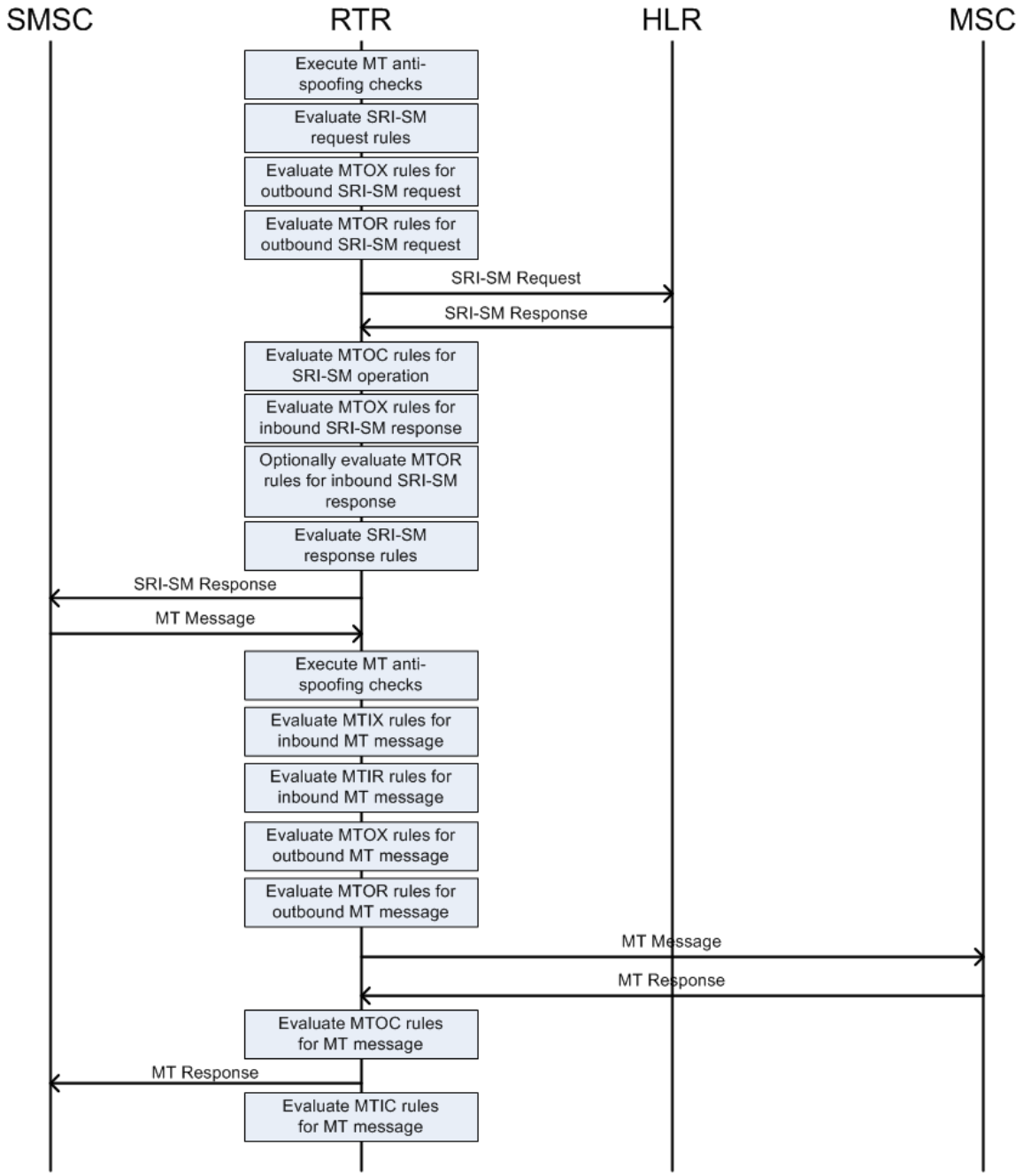


Figure 39: MT-MT routing example

10.4 SRI-SM Request Rule Set

The SRI-SM Request rule set determines how the RTR handles **inbound** SendRoutingInfoForSm requests, as emitted by an external SMSC. Use the SRI-SM request rule set to control the RTR's behavior regarding the following questions:

1. Should we process SRI-SM request, or reject it?
2. Should we immediately pass the SRI-SM request to the HLR, or not?

10.4.1 SRI-SM Request Rule Evaluation

When the RTR receives a SendRoutingInfoForSm request from an external SMSC, it first executes any applicable validation checks[2]. If the request successfully passes these tests, you may query the Subscriber Service Information (SSI) component for the recipient and the originator MSISDN, if it is present. Then, the RTR evaluates the SRI-SM Request rule set and applies the resulting routing action.

The SRI-SM Request rule set is **not** evaluated for outbound SRI-SM requests (that is, when the RTR plays the role of the SMSC).

The RTR evaluates the SRI-SM Request rule set in the same way that it evaluates the routing rule set; it evaluates individual rules in priority order, and the first matching rule is used, with any lower-priority rules being disregarded. If no rule matches the RTR behaves as if a rule with the routing action "query HLR" had matched.

10.4.2 SRI-SM Request Rule Conditions

The SRI-SM Request rule set supports conditions on the following parameters:

Condition	Format	Description
Time Schedule		This condition is independent of the received SRI-SM request, but is evaluated against the time at which the rule is evaluated.
Originator	General	This condition is evaluated against the address included in the SRI-SM request's optional RP-SMEA parameter. When the parameter is absent, but this condition is specified, the condition evaluates to false if not inverted and to true if inverted.
	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the normalised MSISDN, if the RP-SMEA address is categorized as MSISDN.
	Single short number, short number range, or short number prefix	This condition is evaluated against the RP-SMEA address, if the RP-SMEA address is categorized as a short number.

[2] Depending on the installed licenses, this may include MT anti-spoofing checks.

Condition	Format	Description
	Alphanumeric	This condition is evaluated against the RP-SMEA address, if the RP-SMEA address is specified as an alphanumeric address.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the normalized MSISDN, if the RP-SMEA address is categorized as MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges and/or network prefixes, if the RP-SMEA address is categorized as MSISDN.[3]
	List	This condition evaluates the normalized MSISDN against a list of MSISDNs, , if the RP-SMEA address is categorized as MSISDN. This enables logical OR operation.
Originator TON		This condition is evaluated against the type of number (TON) parameter of the SRI-SM request's optional RP-SMEA parameter. If that parameter is not present, the non-inverted condition evaluates to true if it requires a TON of "unknown"; otherwise, it evaluates to false.
Originator NPI		This condition is evaluated against the numbering plan indicator (NPI) parameter of the SRI-SM request's optional RP-SMEA parameter. If that parameter is not present, the non-inverted condition evaluates to true if it requires a NPI of "unknown"; otherwise, it evaluates to false.
Originator SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the SRI-SM Request rule set. It enables you to specify which services the originator must or must not have. If SSI is not used, this condition should not be specified. If the originator is not available, or if it is not categorized as MSISDN, the SSI will be empty (no services).
Recipient	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the MSISDN received at the MAP layer of the SRI-SM request. It refers to the recipient of the subsequent MT messages.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the received MSISDN. Successful extraction of the country code depends on the provisioned countries.

[3] In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
	Network	This condition is evaluated against the network, as derived from matching the MSISDN against the provisioned mobile network number ranges and/or network prefixes.[4]
	Application	This condition is evaluated against the application, which may be associated with the recipient MSISDN, based on the portable application configuration of the RTR.
	List	This condition evaluates the received MSISDN against a list of MSISDNs. This enables logical OR operation.
Recipient SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the SRI-SM Request rule set. It enables you to specify which services the recipient must or must not have. If SSI is not used, this condition should not be specified.
SMSC Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the SMSC address received at the MAP layer of the SRI-SM request.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SMSC address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the SMSC address against the provisioned mobile network number ranges and/or network prefixes.
	List	This condition evaluates the SMSC address received at the MAP layer of the SRI-SM request against a list of E.164 numbers. This enables logical OR operation.
SCCP Calling Party Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the Calling Party Address in E.164 format received at the SCCP layer of the SRI-SM request.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Calling Party Address. Successful extraction of the country code depends on the provisioned countries. **Note:** If PC/SSN routing is used instead of GT routing then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.

[4] In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
	Network	This condition is evaluated against the network, as derived from matching the Calling Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	List	This condition evaluates the Calling Party address received at the SCCP layer of the SRI-SM request against a list of E.164 numbers. This enables logical OR operation.
	PC or PC Range	This condition evaluates the PC included in Calling Party address received at the SCCP layer of the SRI-SM request against a Point Code or a Point Code Range. **Note:** **1.** If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. **2.** If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
Calling Party Translation Type	• None • Byte value (value between 00 and FF, hexadecimal)	Translation Type specified in SCCP Calling Party Address received in the SRI-SM request.
SCCP Called Party Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the Called Party Address in E.164 format received at the SCCP layer of the SRI-SM request.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Called Party Address. Successful extraction of the country code depends on the provisioned countries. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	Network	This condition is evaluated against the network, as derived from matching the Called Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes.

Condition	Format	Description
		Note: If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	List	This condition evaluates the Called Party address received at the SCCP layer of the SRI-SM request against a list of E.164 numbers. This enables logical OR operation.
	PC or PC Range	This condition evaluates the PC included in Called Party address received at the SCCP layer of the SRI-SM request against a Point Code or a Point Code Range. **Note:** **1.** If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. **2.** If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
Called Party Translation Type	• None • Byte value (value between 00 and FF, hexadecimal)	Translation Type specified in SCCP Called Party Address received in the SRI-SM request.
Traffic Type		This condition is evaluated against the trusted/suspect categorization of the external SMSC that issued the SRI-SM request. Refer to the Firewall Guide for information about how this categorization is done.
Portable Application		This condition is evaluated against the outcome of matching the recipient MSISDN against the provisioned portable application MSISDNs. If there is a match, the recipient is considered to be a portable application.

10.4.3 SRI-SM Request Rule Routing Action

The sole effect of the evaluation of the SRI-SM Request rule set is that the RTR applies the resulting routing action to the SendRoutingInfoForSm operation. The possible actions are:

Action	Effect
Send to HLR	Send the SRI-SM request to the RTR's outbound SRI-SM request processing, with the intent to forward the SRI-SM to the HLR in such a way that the response will be routed back to the RTR (using a new TCAP dialogue).
Discard with temporary error	Reject the SRI-SM request by sending a ReturnError response that contains the configurable error code for temporary errors of the HLR back to the

Action	Effect
	external SMSC. You can configure the error code using the semi-static configuration attribute `mttemporarydiscarderrorforhlr`. In this case, the SRI-SM Response rule set is not evaluated.
Discard with permanent error	Reject the SRI-SM request by sending a ReturnError response that contains the configurable error code for permanent errors of the HLR back to the external SMSC. You can configure the error code using the semi-static configuration attribute `mtpermanentdiscarderrorforhlr`. In this case, the SRI-SM Response rule set is not evaluated.
Discard with no response	Drop the SRI-SM request, without sending a response back to the external SMSC. In this case, the SRI-SM Response rule set is not evaluated.
Accept and respond to SMSC immediately	Do not send the SRI-SM request on to the RTR's outbound SRI-SM request processing, but proceed with the evaluation of the SRI-SM response rules.
Have HLR respond to SMSC directly	Send the SRI-SM request to the RTR's outbound SRI-SM request processing, with the intent to relay the SRI-SM to the HLR in such a way that the response will be routed directly back to the external SMSC (using the same TCAP dialogue). In this case, the SRI-SM Response rule set is not evaluated.

10.4.4 SRI-SM Request Rule Matching Ratio

The SRI-SM Request **Rule Matching Ratio** parameter enables you to provision a matching fraction. This is a fraction of two integers, M and N; N must be equal to or greater than M, and both integers must be between 1 and 9999. The matching fraction causes the rule to:

- Only match M out of N times
- Not match N minus M of N times

Non-matching due to the matching fraction only occurs if all other provisioned conditions evaluate to true.

10.5 SRI-SM Response Rule Set

The SRI-SM Response rule set determines how the RTR handles **inbound** SendRoutingInfoForSm requests, to be sent back to an external SMSC. Use the SRI-SM response rule set to control the RTR's behavior regarding the following questions:

1. Should we Home Route subsequent MT messages?
2. What IMSI should we return to the external SMSC?

Home Routing, as well as returning a real IMSI vs. a generated IMSI is described in more detail at the end of this section.

10.5.1 SRI-SM Response Rule Evaluation

If the SRI-SM Request rule set routed the inbound SendRoutingInfoForSm request such that the HLR was not contacted (routing action "accept and respond to SMSC immediately"), the RTR evaluates the SRI-SM Response rule set immediately after evaluating the SRI-SM Request rule set.

If the inbound SendRoutingInfoForSm request was forwarded to the HLR (routing action "send to HLR") and the outbound SendRoutingInfoForSm processing (MTO) resulted in the intent to neither reject nor release the SendRoutingInfoForSm request, the RTR also evaluates the SRI-SM Response rule set.

In all other situations, the SRI-SM Response rule set is ignored.

The RTR evaluates the SRI-SM Response rule set in the same way that it evaluates the routing rule set; it evaluates individual rules in priority order, and the first matching rule is used, with any lower-priority rules being disregarded. If no rule matches and the RTR successfully queried the HLR previously, the RTR behaves as if a rule with the routing action "no home routing" action had matched. If no rule matches and the RTR did not successfully query the HLR, the RTR behaves as if a rule with the routing action "discard with temporary error" action had matched.

10.5.2 SRI-SM Response Rule Conditions

The SRI-SM Response rule set supports conditions on the following parameters:

Condition	Format	Description
Time Schedule		This condition is independent of the received SRI-SM request or response, but is evaluated against the time at which the rule is evaluated.
Originator	General	This condition is evaluated against the address included in the SRI-SM request's optional RP-SMEA parameter. When the parameter is absent, but this condition is specified, the condition evaluates to false if not inverted and to true if inverted.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the normalized MSISDN, if the RP-SMEA address is categorized as MSISDN.
	Single short number, short number range or short number prefix	This condition is evaluated against the RP-SMEA address, if the RP-SMEA address is categorized as a short number.
	Alphanumeric	This condition is evaluated against the RP-SMEA address, if the RP-SMEA address is specified as an alphanumeric address.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the normalized MSISDN, if the RP-SMEA address is categorized as MSISDN. Successful extraction of the country code depends on the provisioned countries.

Condition	Format	Description
	Network	This condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges and/or network prefixes, if the RP-SMEA address is categorized as MSISDN[5].
	List	This condition evaluates the normalized MSISDN against a list of MSISDNs if the RP-SMEA address is categorized as MSISDN. This enables logical OR operation.
Originator TON		This condition is evaluated against the type of number (TON) parameter of the SRI-SM request's optional RP-SMEA parameter. If that parameter is not present, the non-inverted condition evaluates to true if it requires a TON of "unknown"; otherwise, it evaluates to false.
Originator NPI		This condition is evaluated against the numbering plan indicator (NPI) parameter of the SRI-SM request's optional RP-SMEA parameter. If that parameter is not present, the non-inverted condition evaluates to true if it requires a NPI of "unknown"; otherwise, it evaluates to false.
Originator SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the SRI-SM Request rule set. It enables you to specify which services the originator must or must not have. If SSI is not used, this condition should not be specified. If the originator is not available, or if it is not categorized as MSISDN, the SSI will be empty (no services).
Recipient	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the MSISDN received at the MAP layer of the SRI-SM request. It refers to the recipient of the subsequent MT messages.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the received MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the MSISDN against the provisioned mobile network number ranges and/or network prefixes[6].

[5] In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

[6] In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
	Single IMSI, IMSI range or IMSI prefix	This condition is evaluated against the "real" IMSI for the recipient of the subsequent MT messages, as returned by the HLR or retrieved from the portable application provisioning data. If no "real" IMSI is available, the condition evaluates to false if not inverted and to true if inverted.
	Application	This condition is evaluated against the application, which may be associated with the recipient MSISDN, based on the portable application configuration of the RTR.
	List	This condition evaluates the received MSISDN against a list of MSISDNs or the recipient IMSI against a list of IMSIs. This enables logical OR operation.
Recipient SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the SRI-SM Request rule set. It enables you to specify which services the recipient must or must not have. If SSI is not used, this condition should not be specified.
SMSC Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the SMSC address received at the MAP layer of the SRI-SM request.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SMSC address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the SMSC address against the provisioned mobile network number ranges and/or network prefixes.
	List	This condition evaluates the SMSC address received at the MAP layer of the SRI-SM request against a list of E.164 numbers. This enables logical OR operation.
Dest. MSC or SGSN	General	This condition is evaluated against the MSC or SGSN address as returned by the HLR. If the HLR returns both addresses, the rule set is evaluated against either the MSC or the SGSN address, as selected by the semi-static attribute `preferredmtdestination`. If neither an MSC nor SGSN address is available when the SRI-SM Response rule set is evaluated, a non-inverted condition evaluates to false and an inverted condition evaluates to true. **Note:** If the Network configuration is available according to the MSC and/or SGSN (i.e. received in the HLR query), The '**Preferred MT Destination**' in

Condition	Format	Description
		the Network configuration overrides the semi-static attribute '`preferredmtdestination`' for the rules evaluation.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the selected MSC or SGSN address received at the MAP layer of the SRI-SM response from the HLR.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the selected MSC or SGSN address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the selected MSC or SGSN address against the provisioned mobile network number ranges and/or network prefixes.
	List	This condition evaluates the selected MSC or SGSN address against a list of E.164 numbers. This enables logical OR operation.
SCCP Calling Party Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the Calling Party Address in E.164 format received at the SCCP layer of the SRI-SM request.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Calling Party Address. Successful extraction of the country code depends on the provisioned countries. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	Network	This condition is evaluated against the network, as derived from matching the Calling Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	List	This condition evaluates the Calling Party address received at the SCCP layer of the SRI-SM request

Condition	Format	Description
		against a list of E.164 numbers. This enables logical OR operation.
	PC or PC Range	This condition evaluates the PC included in Calling Party address received at the SCCP layer of the SRI-SM request against a Point Code or a Point Code Range. **Note:** **1.** If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. **2.** If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
Calling Party Translation Type	• None • Byte value (value between 00 and FF, hexadecimal)	Translation Type specified in SCCP Calling Party Address received in the SRI-SM request.
SCCP Called Party Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the Called Party Address in E.164 format received at the SCCP layer of the SRI-SM request.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Called Party Address. Successful extraction of the country code depends on the provisioned countries. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	Network	This condition is evaluated against the network, as derived from matching the Called Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will evaluate to true if no GT address is present at the SCCP layer.
	List	This condition evaluates the Called Party address received at the SCCP layer of the SRI-SM request

Condition	Format	Description
		against a list of E.164 numbers. This enables logical OR operation.
	PC or PC Range	This condition evaluates the PC included in Called Party address received at the SCCP layer of the SRI-SM request against a Point Code or a Point Code Range. **Note:** **1.** If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. **2.** If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
Called Party Translation Type	• None • Byte value (value between 00 and FF, hexadecimal)	Translation Type specified in SCCP Called Party Address received in the SRI-SM request.
Traffic Type		This condition is evaluated against the trusted/suspect categorization of the external SMSC that issued the SRI-SM request. Refer to the Firewall Guide for information about how this categorization is done.
Portable Application		This condition is evaluated against the outcome of matching the recipient MSISDN against the provisioned portable application MSISDNs. If there is a match, the recipient is considered to be a portable application.

10.5.3 SRI-SM Response Rule Routing Action

The primary effect of evaluating the SRI-SM Response rule set is that the RTR determines whether subsequent MT messages should be Home Routed or not, which is implemented through the matching SRI-SM rule's routing action. The possible actions are:

Action	Effect
Home Routing	Return a successful SRI-SM response to the external SMSC so that when the returned routing data is used, subsequent MT messages will be routed to the RTR. A rule with this action can only match if: • A real IMSI is available (from the HLR or the portable application provisioning data), or • The rule specifies a range of IMSIs from which an IMSI can be generated

Action	Effect
Discard with temporary error	Reject the SRI-SM request by sending a ReturnError response that contains the configurable error code for temporary errors of the HLR back to the external SMSC. You can configure the error code using the semi-static configuration attribute `mttemporarydiscarderrorforhlr`.
Discard with permanent error	Reject the SRI-SM request by sending a ReturnError response that contains the configurable error code for permanent errors of the HLR back to the external SMSC. You can configure the error code using the semi-static configuration attribute `mtpermanentdiscarderrorforhlr`.
Discard with no response	Drop the SRI-SM request, without sending a response back to the external SMSC.
No Home Routing	Return a successful SRI-SM response to the external SMSC that includes the IMSI and MSC and/or SGSN address as returned by the HLR. This causes the SMSC to direct subsequent MT delivery attempts for that recipient directly to the MSC or SGSN. A rule with this action can only match if the RTR successfully queried the HLR previously, so there is real routing data to return to the external SMSC.

10.5.4 SRI-SM Response Rule Matching Ratio

The SRI-SM Response **Rule Matching Ratio** parameter enables you to provision a matching fraction. This is a fraction of two integers, M and N; N must be equal to or greater than M, and both integers must be between 1 and 9999. The matching fraction causes the rule to:

- Only match M out of N times
- Not match N-M of N times

Non-matching due to the matching fraction only occurs if all other provisioned conditions evaluate to true.

For example, to Home-Route only 30% of the Home-Routable messages, all SRI-SM Response rules with the "Home Route" action should have a **Rule Matching Ratio** of 3/10.

10.5.5 IMSI Generation

If an SRI-SM Response rule has a routing action of "home route", you can associate it with a range of IMSIs between 5 and 15 digits. The range is used to generate an IMSI for use in the RTR's SendRoutingInfoForSm response to the external SMSC in two cases:

- No "real" IMSI (that is, no IMSI provided by the HLR or portable application provisioning data) is available, so a "fake" IMSI must be generated to make Home Routing possible.
- A "real" IMSI is available, but the MT anti-spoofing license is enabled, and generated[7] IMSIs are used to generate a one-to-one mapping between the SendRoutingInfoForSm request and the subsequent MT messages on a per-SMSC basis.

[7] Generated IMSIs have also been called "scrambled" IMSIs. However, this term implies that there is a reverse-engineerable algorithm that translates a real IMSI into a scrambled IMSI, which is not the case. When an IMSI is generated, the RTR selects a random IMSI out of the configured range.

Therefore, if the MT anti-spoofing license is disabled and a real IMSI is available, the RTR will return the real IMSI to the external SMSC. This is called "plain" Home Routing.

Note: When a generated IMSI is returned to the external SMSC instead of a real IMSI, you should be aware that the result is that all logging and billing done on the external SMSC will show the generated IMSI instead of the real IMSI.

IMSI Generation Range

The ranges for generating IMSIs must be large enough to supply sufficient IMSIs under high load conditions. If more IMSIs cannot be generated, the SRI-SM request is rejected with a temporary error. A guideline for calculating the appropriate size of an IMSI generation range is:

```
throughput * max_interval_between_srism_and_mt * 2.2 / number_of_rtr_nodes
```

Where:

- `throughput` is the expected number of MT messages that are supposed to be Home-Routed using this IMSI generation range under peak traffic load, in SMs per second.
- `max_interval_between_srism_and_mt` is the value of the semi-static configuration attribute `firewallmaxintervalbetweensrismandmtfwdsm`, which defaults to 60 seconds.
- `number_of_rtr_nodes` is the number of RTR nodes that perform the same task (that is, that share the message load as identified by (`throughput`)

For example, if a certain IMSI generation range is supposed to support a throughput of 1000 SM/s and four RTR nodes are deployed to share that load, the IMSI generation range should contain at least 33,000 IMSIs.

10.5.6 Home Routing

Home Routing is a RTR feature that causes an external SMSC to deliver MT messages to the RTR instead of to a real MSC or SGSN. You can use Home Routing to:

- Apply MT anti-spoofing checks
- Apply personalized services or services such as message forwarding, message copying, spam detection, or spam filtering to MT messages
- Take advantage of interconnect agreements that may exist between the foreign PLMN and the HPLMN or between the HPLMN and the visited PLMN

Home Routing requires the RTR to maintain a *correlation database* that contains *correlation records*. These records preserve message parameters that are available during SendRoutingInfoForSm processing, so they will be available during MT message processing. The database is stored in volatile memory[8], and the key for retrieving a record is the recipient IMSI[9] (as included in the Home Routed MT message issued by the external SMSC). A correlation record typically preserves the recipient MSISDN (as it is not available in an MT message) and the relevant routing data returned by the HLR. Each correlation

[8] This means that when the RTR is restarted, the database will be cleared. In this case, if the external SMSC attempts to delivery Home Routed MT messages, an "unsolicited MT message" event will occur on the RTR. By default, this event causes the RTR to drop the MT message with no response. The SMSC's delivery attempt will time out, and the next delivery attempt will begin with a SendRoutingInfoForSm operation again, re-installing the correlation record.

[9] If the HLR returned an LMSI, that LMSI is not returned to the SMSC when Home Routing, so that the recipient IMSI is always present in a Home-Routed MT message.

record exists only on a single RTR instance; the instance that processed the SendRoutingInfoForSm request.

Home Routing works because the MSC and/or SGSN address returned to the external SMSC in the SendRoutingInfoForSm response is populated with an E.164 address that is uniquely assigned to that RTR instance. By default, that is the RTR's global title (GT) or one of the E.164 addresses specified in the list that is provisioned in the semi-static configuration attribute `firewallmscsgsnaddressinsuspectsrismresponse`. If, during the processing of the SendRoutingInfoForSm request, the HLR was queried successfully and the HLR returned both an MSC and an SGSN address, the RTR's SendRoutingInfoForSm response will include the same E.164 address in the MSC and SGSN fields. Therefore, the external SMSC can choose whether to deliver the MT message to the SGSN or to the MSC. That decision is conveyed to the RTR by means of the subsystem number (SSN) in the called party address (CDPA) of the subsequent MT delivery attempt.

10.6 MTI Rule Set

There are three types of MTI rules:

- MTI routing rules (MTIR)
- MTI external condition rules (MTIX)
- MTI counting rules (MTIC)

All rules are evaluated for **Home-Routed**, **inbound** MT traffic only; that is, when the RTR plays the role of a firewall. They are not evaluated for outbound MT traffic, and they are not evaluated for MT traffic that is rerouted to the RTR through MAP screening functionality.

All MTI rule sets support the same conditions.

Note: An MT message can be either a GSM 03.40 Deliver-SM (a normal message) or a phase 2 Status-Report.

10.6.1 MTI Rule Evaluation

When the RTR processes inbound MT traffic from an external SMSC, it begins by categorizing the SMSC as trusted or suspect. The originating external SMSC of an inbound MT message is categorized as trusted if:

- The SMSC address at the SCCP layer (and at the MAP layer, if present) matches the list of trusted SMSCs in the semi-static configuration attribute `firewalltrustedsmsclist`, or
- If the MT message was received with an originating point code (OPC) that is different from the provisioned STP's[10] or
- If the SCCP CgPA GT address present in an incoming SendRoutingInfoForSm exists in the **Trusted SMSC SCCP CgPA List** configured in the MGR GUI (**Firewall ➤ MT ➤ Properties**), then the SMSC is considered trusted and the corresponding MT Forward SM received with the same IMSI as returned in SendRoutingInfoForSm response is also considered trusted.

[10] This way of categorizing originating SMSCs means that operators must instruct their own SMSCs to directly route SRI-SMs (and MT messages) to the RTR; that is, GT translation rules on the SMSC would address the RTR, and any intermediate STP would not need to apply GTT rules, and therefore not change the message's OPC. Therefore, any SRI-SM or MT message received on the RTR from an STP's OPC would not come from any of the operator's own SMSCs, but from a foreign, suspect SMSC.

MT messages from suspect sources undergo stricter MT anti-spoofing checks (when the MT anti-spoofing license is present).

After the SMSC is categorized as trusted or suspect, the RTR validates the categorized MT message, which includes normalization of address parameters and performing MT anti-spoofing checks. During validation, the RTR retrieves the correlation record from the correlation database. If retrieval fails, the RTR rejects the MT message as unsolicited. If the retrieval succeeds, the message parameters contained in the correlation record (such as the recipient MSISDN and, possibly, the recipient's real IMSI and serving MSC) become available to be used in rule conditions.

If the message passes the validation phase successfully, the RTR can optionally retrieve the SSI data. Then, the RTR evaluates the MTIX rule set. After the message passes MTIX rule evaluation, the RTR evaluates the MTIR rule set, primarily to determine the routing path for the inbound MT message. The RTR then routes the MT message and sends a response back to the external SMSC. The RTR evaluates the MTIC rule set during the post-processing phase for the message, and increments MTIC counters according to the response sent back to the SMSC.

Note: The external SMSC may use a single TCAP dialogue to request the delivery of multiple MT messages. For Home-Routed MT traffic, the TCAP dialogue is always established between the SMSC and the RTR; it is never established between the SMSC and the real MSC or SGSN. If the RTR needs to forward the MT message to the real MSC or SGSN, the RTR initiates a second TCAP dialogue to do so. For each MT message received over the same TCAP dialogue, the same evaluation process is executed. Therefore, every message can potentially take a different route (even if this would be desirable only for rare scenarios). When routing the MT message to an application (MT-AT), to storage (MT-Store), or to another SMSC as AO (MT-AO), the RTR uses the TP-MMS field of the inbound MT message to determine if the inbound TCAP dialogue should be continued. When the MT message is routed to the real MSC or SGSN, that node's dialogue continuation behavior will be mirrored on the inbound TCAP dialogue.

10.6.2 MTI Rule Conditions

The MTI rule sets support conditions on the following parameters:

Condition	Format	Description
Time Schedule		This condition is independent of the received MT message, but is evaluated against the time at which the rule is evaluated.
Originator	General	By originator, we generally refer to the TP-OA parameter of a Deliver-SM message or the TP-RA parameter of a Status-Report message.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the originator address, if the originator address is categorized as MSISDN.
	Single short number, short number range or short number prefix	This condition is evaluated against the originator address, if the originator address is categorized as a short number.
	Alphanumeric	This condition is evaluated against the originator address, if the originator address is specified as an alphanumeric address.

Condition	Format	Description
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the normalized originator address, if the originator address is categorized as MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges and/or network prefixes, if the originator address is categorized as MSISDN.
	List	This condition evaluates the normalized address against a list of MSISDNs or short numbers, enabling logical OR operation.
Originator TON		This condition is evaluated against the type of number (TON) parameter of the TP-OA or TP-RA parameter.
Originator NPI		This condition is evaluated against the numbering plan indicator (NPI) parameter of the TP-OA or TP-RA parameter.
Originator SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the MTI rule set. It enables you to specify which services the originator must or must not have. If SSI is not used, this condition should not be specified.
Recipient	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the recipient MSISDN retrieved from the correlation record.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the recipient MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the recipient MSISDN against the provisioned mobile network number ranges and network prefixes[11].
	Single IMSI, IMSI range or IMSI prefix	This condition is evaluated against the "real" IMSI for the recipient of the subsequent MT messages, as returned by the HLR or retrieved from the portable application provisioning data. If no "real" IMSI is available, the condition evaluates to false if not inverted, and to true if inverted.

[11] In general, deriving a mobile network from an MSISDN only works reliably if that network does not support mobile number portability (MNP).

Condition	Format	Description
	Application	This condition is evaluated against the application, which may be associated with the recipient MSISDN, based on the portable application configuration of the RTR.
	List	This condition evaluates the recipient MSISDN against a list of MSISDNs, or the "real" recipient IMSI against a list of IMSIs. This enables logical OR operation.
Recipient SSI		This condition is evaluated against the SSI information that is retrieved prior to evaluating the MTI rule set. It enables you to specify which services the recipient must or must not have. If SSI is not used, this condition should not be specified.
DCS		This condition is evaluated against the Deliver-SM's TP-DCS parameter. If the MT message is a Status Report, the condition evaluates as if the TP-DCS parameter were set to 0.
Message Type		This condition is evaluated against the MT message type, which is a Deliver-SM or a Status Report.
User Data		This condition is evaluated against the user data portion of the MT message. In the case of a Status Report, this condition behaves as if the user data portion were empty.
User Data Header		This condition is evaluated against the list of user data header information element identifiers that are present in the MT message.
Ext Att		This condition is evaluated against the external attributes as set and reset by the EC application consulted during the evaluation of the MTIX rules. This condition is not supported in the MTIX rule set.
SMSC Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the SMSC address received at the MAP layer of the MT message.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SMSC address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the SMSC address against the provisioned mobile network number ranges and/or network prefixes.
	List	This condition evaluates the SMSC address received at the MAP layer of the MT message against a list of E.164 numbers. This enables logical OR operation.

Condition	Format	Description
Originator - SMSC Addr. Match		This condition is evaluated by comparing the Originator address and the SMSC Address on the basis of their country and network parameters. The respective country is derived by extracting the E.164 country code from the Originator and the SMSC address and matching the same against the provisioned countries. Similarly, the respective network is derived by matching the Originator and the SMSC address against the provisioned mobile network number ranges/prefixes. In case no provisioned country or network number range/prefix is matched, then the corresponding country or network is considered as “unknown”. The comparison of the Originator and the SMSC address is based on the following criteria, which are configurable on the MGR: • 0 - Originator Country equals SMSC • 1 - Originator Country strictly equals SMSC • 2 - Originator Network equals SMSC • 3 - Originator Network strictly equals SMSC The 'strictly equals' criterion requires an exact match of the two values being compared, and it is a special case of the 'equals' criterion which can be satisfied even if one (or both) of the values being compared is (are) 'unknown'. Note that only one criterion can be configured at a time. In case none of the criteria is configured, the non-inverted condition always evaluates to FALSE and the inverted condition always evaluates to TRUE.
Dest. MSC or SGSN	General	This condition is evaluated against the real MSC or SGSN address as retrieved from the correlation record. If addresses are available, the rule set is evaluated against either the MSC or the SGSN address, as selected by the SSN included in the SCCP CDPA. If neither an MSC nor SGSN address is available in the correlation record, a non-inverted condition evaluates to FALSE, and an inverted condition evaluates to TRUE.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the selected MSC or SGSN address retrieved from the correlation record.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the selected MSC or SGSN address. Successful extraction of the country code depends on the provisioned countries.

Condition	Format	Description
	Network	This condition is evaluated against the network, as derived from matching the selected MSC or SGSN address against the provisioned mobile network number ranges and/or network prefixes.
	List	This condition evaluates the selected MSC or SGSN address against a list of E.164 numbers. This enables logical OR operation.
SCCP Calling Party Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the Calling Party Address in E.164 format received at the SCCP layer of the inbound MT message.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Calling Party Address. Successful extraction of the country code depends on the provisioned countries. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	Network	This condition is evaluated against the network, as derived from matching the Calling Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layers.
	List	This condition evaluates the Calling Party address received at the SCCP layer of the inbound MT message against a list of E.164 numbers. This enables logical OR operation.
	PC or PC Range	This condition evaluates the PC included in Calling Party address received at the SCCP layer of the inbound MT message against a Point Code or a Point Code Range. **Note:** **1.** If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. **2.** If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.

Condition	Format	Description
SCCP Called Party Address	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the Called Party Address in E.164 format received at the SCCP layer of the inbound MT message.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Called Party Address. Successful extraction of the country code depends on the provisioned countries. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	Network	This condition is evaluated against the network, as derived from matching the Called Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	List	This condition evaluates the Called Party address received at the SCCP layer of the inbound MT message against a list of E.164 numbers. This enables logical OR operation.
	PC or PC Range	This condition evaluates the PC included in Called Party address received at the SCCP layer of the inbound MT message against a Point Code or a Point Code Range. **Note:** **1.** If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. **2.** If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
Reply Path		This condition is evaluated against the MT message's TP-RP flag.
Status Report		This condition is evaluated against the MT message's TP-SRI flag.
PID		This condition is evaluated against the Deliver-SM's TP-PID parameter. If the MT message is a Status Report, the condition evaluates as if the TP-PID parameter were set to 0.

Condition	Format	Description
Traffic Type		This condition is evaluated against the trusted/suspect categorization of the external SMSC that which issued the MT message.
Message Segments		This condition is evaluated against the interpreted user data header information element, indicating that the message is segmented. **Note:** A condition with neither the first, nor the last, nor the intermediate segment flags turned on will evaluate to false if the MT message is not segmented. To match on unsegmented messages only, turn on all three flags and invert the condition.
Recipient RN Group		During the processing of the preceding SRI-SM request, the HLR may have returned an IMSI that was prefixed with a provisioned routing number. If a routing number was recognized, it was stripped off the real IMSI, associated with a routing number group, and added to the correlation record. This condition is evaluated against that routing number group.
Portable Application		This condition is evaluated against the outcome of matching the recipient MSISDN against the provisioned portable application MSISDNs during the processing of the SRI-SM request. If there was a match, the recipient is considered to be a portable application.

10.6.3 MTIR Rule Set

The RTR evaluates the MTIR rule set to determine how inbound, Home-Routed MT messages will be routed. An MT message can be Deliver-SM (a normal message) or a Status Report. For information about the circumstances in which the MTIR rule set is evaluated, refer to *MTI Rule Evaluation*.

10.6.3.1 MTIR Routing Action

The primary effect of the evaluation of the MTIR rule set is that the RTR determines where the MT message will be routed, which is implemented through the matching MTIR rule's routing action. The possible actions are:

Action	Effect
Discard with temporary error	Reject the MT message by sending a ReturnError response that contains the configurable error code for temporary errors of the MSC/SGSN back to the external SMSC. You can configure the error code using the semi-static configuration attribute `mttemporarydiscarderrorformscorsgsn`.
Discard with permanent error	Reject the MT message by sending a ReturnError response that contains the configurable error code for permanent errors of the MSC/SGSN back

Action	Effect
	to the external SMSC. You can configure the error code using the semi-static configuration attribute `mtpermanentdiscarderrorformscorsgsn`.
Discard with no response	Drop the MT message without sending a response back to the external SMSC.
Discard with acknowledgment	Discard the MT message after sending a response to the external SMSC that indicates delivery success. The external SMSC will proceed as if the MT messages was delivered successfully.
Store for delivery to MS	Store the MT message in the specified AMS queue and return a response depending only on the storage result. At a later point in time, the AMS will request that the RTR deliver the MT message, which may lead to multiple retries. You must specify the AMS queue in which to temporarily store the MT message in the MTIR rule. A rule with this routing action only matches if, at the time of the rule evaluation, at least one AMS is available, which indicates the capability for storing messages (as opposed to Icache functionality only).
Route to mobile	Directly send the inbound MT message on to the MSC or SGSN with which the recipient is currently registered. If no routing data is available from the correlation record (because the HLR was not queried during the preceding SRI-SM processing), the HLR query is executed before the MT message is sent to the MSC or SGSN. **Note:** In this case of a "late" HLR query, the transparent nature of MT-MT forwarding is lost, the RTR recreates the outbound MT message, and the RTR typically uses its own global title (GT) to identify the SMSC toward the terminating MSC or SGSN. Likewise, the transparent nature of the MT response forwarding toward the external SMSC is lost. Depending on the categorization of the MT response from the MSC or SGSN, the error code that is sent back to the SMSC is determined in the same way as for the "discard with temporary error" or "discard with permanent error" action. In the case of a late HLR query, the MTO rules are evaluated during the outbound SRI-SM processing in the same way as they are evaluated for an outbound SRI-SM during the inbound SRI-SM processing, with one exception: the MTOR rule set does not follow the `firewallenablemtrtgruleevaluationforsrismresponse` attribute, but rather is never evaluated for SRI-SM responses.
Route to application	Route the inbound MT message as an AT message to an application. The target application can be determined in three ways: • By the rule. The MTIR rule explicitly refers to a provisioned application. All MT messages matching this rule are delivered as AT messages to that application. Such MTIR rules only match if, at the time of the rule evaluation, the target application is available for receiving AT messages. • By recipient address. The recipient address can refer to a provisioned application by means of the provisioned portable applications. If that is the case of the inbound MT message, such an MTIR rule can only

Action	Effect
	match if at the time of the rule evaluation, the application associated with the recipient address is available for receiving AT messages. • By load balancing group. Refer to the description of AT load balancing groups. The MTIR rule explicitly refers to a provisioned load balancing group. All MT messages matching this rule are delivered as AT messages to one of the applications in that load balancing group. Such MTIR rules only match if at the time of the rule evaluation, at least one of the applications in the load balancing group is available for receiving AT messages. When an temporary/permanent error is returned, the error code can be configured using the semi-static configuration attributes: • `mttemporarydiscarderrorformscorsgsn` • `mtpermanentdiscarderrorformscorsgsn`
Route to SMSC as AO	Route the inbound MT message as an AO message to an external SMSC so that the SMSC will take care of the (further) delivery of the message. The rule explicitly specifies: • Which application should be used to submit the AO message to the SMSC • Which SMSC group the AO message should be forwarded to For such an MTIR rule to match, the following additional conditions must be met: • The MT message must be a Deliver-SM (it is not possible to route Status Report messages as AO) • At the time of the rule evaluation, at least one of the SMSCs in the SMSC group must be available to receive AO messages from the designated application When an temporary/permanent error is returned, the error code can be configured using the semi-static configuration attributes: • `mttemporarydiscarderrorformscorsgsn` • `mtpermanentdiscarderrorformscorsgsn`

Note:

CDRs will be generated using the billing profile (if configured) for `Discarded Messages` when the message is discarded due to the application of any of the following routing action:

1. Discard with permanent error
2. Discard with no response

Only the FCDR format will be supported for generating CDRs for messages discarded by the RTR.

Apart from the above stated condition, if the semi-static parameter `rtrcreatemtmtcdrforerrorscenarios` is configured as true, CDRs will also be generated using

the billing profile (if configured) for Discarded Messages when the configured billing profile is of 3G CDR format and the message is discarded due to the application of any of the following routing actions:

1. Discard with permanent error
2. Discard with no response
3. Discard with temporary error

If no MTIR rule matches, the RTR applies the following logic:

```
If the recipient MSISDN is associated with an application by means of the portable
application provisioning data, then
     If that application is available to receive AT messages
          Route the MT message as AT to that application
     Else
          Behave as if a MTIR rule with action "discard with temporary error" had
          matched
Else
     Behave as if a MTIR rule with action "route to MS" had matched
```

10.6.3.2 MTIR Rule Modifier

MTIR rules can refer to an MTI modifier. The MTI modifier only supports the **Defer Period** parameter, which enables you to defer the delivery of an MT message that matches an MTIR rule that refers to the modifier. The modification is applied to the inbound message after MTIR rule evaluation, along with any modifications requested by EC applications that were contacted during evaluation of the MTIX rules. The defer period only has an effect if the routing action is "store for delivery to MS" or "route to SMSC as AO".

10.6.3.3 MTIR Rule Billing

MTIR rules can refer to a billing profile that will trigger the generation of CDRs representing the processing of the inbound MT messages. When processing inbound MT traffic, the RTR creates CDRs that represent the fact that the inbound MT message was accepted (that is, a positive acknowledgment is sent back to the SMSC) or the MT message is rejected due to temporary/permanent error or blocked due routing action when the semi-static parameter *rtrcreatemtmtcdrforerrorscenarios* is set to "true" and the billing profile is for 3G CDR only. When generating CDRs for inbound MT traffic, the RTR also considers any billing profiles that were assigned to the message during the evaluation of the MTOR or ATOR rule sets.

For more information about the CDR formats that the RTR supports, refer to the Billing Manual.

10.6.4 MTIX Rule Set

The RTR evaluates the MTIX rule set so that EC applications can process the inbound MT message. EC processing may include providing extra personalized services, filtering messages, and/or performing real-time charging.

MTIX rules get evaluated using the logic common to all external condition rule sets (refer to *Rule Evaluation*).

For information about the circumstances in which the MTIX rule set is evaluated, refer to *MTI Rule Evaluation*.

10.6.4.1 MTIX Rule Failure Action

If the ECI evaluation produces a result of false (after the optional inversion of the corresponding MTIX rule's external condition), then the processing of the sorted list of matching MTIX rules stops and the failure action of the MTIX rule is applied.

The possible failure actions are:

Action	Effect
None	Ignore the false result and continue to process the list of matching MTIX rules, or assume that the message "passed" the MTIX rule evaluation if there are no more matching rules in the list.
Discard With Temporary Error	Leave the MTIX rule evaluation and behave as if an MTIR rule with action "discard with temporary error" had matched.
Discard With Permanent Error	Leave the MTIX rule evaluation and behave as if an MTIR rule with action "discard with permanent error" had matched.
Discard With No Response	Leave the MTIX rule evaluation and behave as if an MTIR rule with action "discard with no response" had matched.
Discard With Ack	Leave the MTIX rule evaluation and behave as if an MTIR rule with action "discard with ACK" had matched.

Note:

CDRs will be generated using the billing profile (if configured) for `Discarded Messages` when the message is discarded due to the application of any of the following routing action:

1. Discard with permanent error
2. Discard with no response

Only the FCDR format will be supported for generating CDRs for messages discarded by the RTR.

Apart from the above stated condition, if the semi-static parameter `rtrcreatemtmtcdrforerrorscenarios` is configured as true, CDRs will also be generated using the billing profile (if configured) for Discarded Messages when the configured billing profile is of 3G CDR format and the message is discarded due to the application of any of the following routing actions:

1. Discard with permanent error
2. Discard with no response
3. Discard with temporary error

10.6.5 MTIC Rule Set

The MTIC rule set is evaluated to generate statistics about the handling of inbound, Home-Routed MT messages. Each MTIC rule has a set of per-result counters in addition to the "total" counter. The result counters pertain to the result as the external SMSC would see it (coming from the RTR).

10.6.6 Portable Application Support for Inbound MT Traffic

The portable applications feature enables you to associate certain MSISDNs with an application. Messages addressing one of these MSISDNs can be routed as AT messages to the associated application.

To use the portable applications feature for home-routed inbound MT messages, you must have the MT-AT routing path license, and you must enable the feature for inbound MT traffic in **Routing ➤ Properties ➤ Enable Portable Application for MT**).

The RTR will match the recipient MSISDN of the inbound SendRoutingInfoForSm request against the portable application provisioning data. If there is a match, the RTR associates the recipient address with the corresponding application and flags the message as making use of the portable application feature. The flag and the association of the recipient address with an application can be used during the evaluation of the SRI-SM and MTI rule sets.

By default, the portable application feature works in the absence of SRI-SM Request and MTI rules. However, it is recommended to explicitly express the fact that the portable application feature is in use for inbound MT traffic by defining rules.

Sample Portable Application Configuration

This is a sample of a recommended configuration for the portable application feature:

1. Create an SRI-SM response rule that Home Routes all MT traffic that is destined for a portable application. Enable the portable application condition. Set the routing action of the rule to "home route". The specification of an IMSI range is not necessary.
2. Create an SRI-SM Request rule with the appropriate priority and the portable application condition enabled. Set the routing action to "Accept and Respond to SMSC immediately."
3. Create an MTIR rule of appropriate priority with the portable application condition enabled. Set the routing action to "route to application" and set the Application to "by recipient".

This configuration implements rule-based MT-AT routing for inbound MT traffic toward portable applications. The RTR will automatically select the appropriate destination application based on the portable application provisioning data.

10.7 MTO Rule Set

There are three types of MTO rules:

- MTO routing rules (MTOR)
- MTO external condition rules (MTOX)
- MTO counting rules (MTOC)

All rules are evaluated for **outbound** MT traffic only; this includes processing of the MT messages (Deliver-SMs and Status Reports) and the processing of SendRoutingInfoForSm (SRI-SM) requests and responses. Outbound MT traffic can originate from the RTR or from an external SMSC (in which case the traffic would have passed through inbound MT processing before arriving at outbound MT processing).

All MTO rules support the same conditions.

10.7.1 MTO Rule Evaluation

SRI-SM Evaluation

When the RTR processes outbound SendRoutingInfoForSm (SRI-SM) requests, it begins by evaluating the MTOX rule set. After the message passes MTOX rule evaluation, the RTR evaluates the MTOR rule set. The RTR then sends the SRI-SM request toward the HLR. After the RTR receives the HLR's response, it evaluates the MTOC rule set, and then re-evaluates the MTOX rule set for the outbound SRI-SM request. The RTR can then optionally re-evaluate the MTOR rule set, if the SRI-SM request originated from an external SMSC.

If, after evaluating the MTOR rule set, no rule matches, the RTR passes the SRI-SM request or response to the next stage of message processing.

MT Message Evaluation

The RTR processes outbound MT messages:

- Immediately after processing the preceding SRI-SM if the RTR initiated the SRI-SM, or
- After the inbound MT message processing if an external SMSC initiated the MT delivery attempt

For information about inbound MT message processing, refer to *MTI Rule Set*.

MT messages that pass through the RTR's outbound MT message processing fall into three groups:

- Delivery attempts initiated by the RTR
- Home-Routed MT messages issued by an external SMSC
- "Unsolicited" (not Home-Routed) MT messages issued by an external SMSC[12]

When the RTR processes outbound MT messages, it begins by evaluating the MTOX rule set. After the message passes MTOX rule evaluation, the RTR evaluates the MTOR rule set. The RTR then sends the MT message toward the terminating MSC or SGSN.

If the HLR returned both an MSC and SGSN address in the SRI-SM response, the RTR or the external SMSC may attempt to deliver the MT message to one of them first and, upon failure, attempt to deliver to the other. If such a second attempt is made, all outbound MT processing is executed twice, once for each delivery attempt.

If, after evaluating the MTOR rule set, no rule matches, the RTR passes the MT message to the MSC or SGSN.

10.7.2 MTO Rule Conditions

MTO rule sets are evaluated in many scenarios; therefore, the amount of message-related information that is available to the rule set evaluation varies significantly. Most conditions should be used with care. Additional conditions may be required to disambiguate among cases. The message type condition is the primary example of such an additional condition.

The MTO rule sets support conditions on the following parameters:

[12] The RTR receives these messages if an SS7 network node with MAP screening functionality re-routes them to the RTR.

Condition	Format	Description
Time Schedule		This condition is independent of the MT message, but is evaluated against the time at which the rule is evaluated.
SMSC Address	General	If the MT message was issued by an external SMSC, this condition is evaluated against the normalized SMSC address found at the MAP layer of the inbound MT message. If the message was issued by the RTR, this condition is evaluated against the RTR's common address or, if there is no common address, the RTR's specific global title (GT). The latter is not commonly used.
	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the E.164 address representing the SMSC.
	Country	This condition is evaluated against the country derived from the SMSC address by extracting the E.164 country code. Evaluation of this condition depends on the provisioned countries.
	Network	This condition is evaluated against the mobile network derived from the SMSC address by matching the E.164 number against the number ranges and/or network prefixes that are provisioned for each mobile network. Evaluation of this condition depends on the provisioned countries and mobile networks.
	List	This condition evaluates the SMSC address against a list of MSISDNs.
Originator	General	This condition is evaluated against a normalized version of the originator address of the MT message. In case of a Status Report, the condition is evaluated against the recipient of the original message that caused the generation of the status report. When the MTO rule set is evaluated for an SRI-SM request issued by an external SMSC or for the HLR's response to that request, the originator may not be available (the RP-SMEA field of the SRI-SM request is optional and typically not present). If the originator address is not present, a non-inverted condition evaluates to false and an inverted condition evaluates to true.
	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the originator address of the MT message, if it is categorized an MSISDN.
	Single short number, short number range, or short number prefix	This condition is evaluated against the originator address of the MT message, if it is categorized as a short number.
	Application	This condition is evaluated against the application associated with the originator address of the MT

Condition	Format	Description
		message, if a locally provisioned application matches the originator address by means of the short number or an alphanumeric alias. **Note:** MT messages originating from an external SMSC may have a different meaning/application assigned to a certain short number or alphanumeric alias. Therefore, this condition should be used with care.
	Country	This condition is evaluated against the country derived from the originator address by extracting the E.164 country code from the normalized MSISDN. Evaluation of this condition depends on the provisioned countries.
	List	This condition evaluates the normalized originator against a list of MSISDNs or short numbers (as determined by the list's type).
	Alphanumeric	This condition is evaluated against an alphanumeric originator address (as determined by the type of number of the originator address). Alphanumeric addresses can be no longer than 11 characters from the GSM default alphabet.
	Application category	The **Application Category** configured under the **Originator** condition is considered matched when at least one of the configured bit matches with the originating application. In case of MTOR rules, for incoming application originated message (e.g. AO-MT path), while evaluating the Originator condition, the source application is considered as the originating application.
Originator - SMSC Addr. Match		This condition is evaluated by comparing the Originator address and SMSC Address on the basis of their country and network parameters. The respective country is derived by extracting the E.164 country code from the Originator and the SMSC address and matching the same against the provisioned countries. Similarly, the respective network is derived by matching the Originator and the SMSC address against the provisioned mobile network number ranges/prefixes. In case no provisioned country or network number range/prefix is matched, then the corresponding country or network is considered as “unknown”. The comparison of the Originator and the SMSC address is based on the following criteria, which are configurable on the MGR:

Condition	Format	Description
		• 0 - Originator Country equals SMSC • 1 - Originator Country strictly equals SMSC • 2 - Originator Network equals SMSC • 3 - Originator Network strictly equals SMSC The 'strictly equals' criterion requires an exact match of the two values being compared, and it is a special case of the 'equals' criterion which can be satisfied even if one (or both) of the values being compared is (are) 'unknown'. Note that only one matching criterion can be configured at a time. In case none of the criteria is configured, the non-inverted condition always evaluates to FALSE and the inverted condition always evaluates to TRUE. The Originator address used for evaluating this condition is the same as the address used for evaluating the 'Originator' condition. The SMSC address is taken from the MAP layer service centre address (SM-RP-OA) in the case of an incoming MT message, and for other types of messages it is the same as the address used for evaluating the 'SMSC Address' condition. Note: This condition is not supported for outgoing MT Status Reports, SRI-SM Requests and SRI-SM Responses. If configured, the condition will always evaluate to false while matching a MTO rule against any of the above message types.
Dest. MSC or SGSN	General	This condition is evaluated against the terminating MSC or SGSN of the MT message. This information is not available when: • The MTO rule set is evaluated for an SRI-SM request (in such a case, a non-inverted condition evaluates to false and an inverted condition evaluates to true) • The MTOX rule set is evaluated for the response to an SRI-SM request • The MTOR rule set is evaluated for the response to an SRI-SM request issued by the RTR When the MTOR rule set is evaluated for the response to an SRI-SM request issued by an external SMSC and the MSC and SGSN address are both available, the rule set is evaluated twice: once for the MSC and once for the SGSN, as selected by the semi-static attribute `preferredmtdestination`. The RTR uses the matching rule with the higher priority.

Condition	Format	Description
		Note: If the Network configuration is available according to MSC and/or SGSN (i.e. received in the HLR query), the **Preferred MT Destination** in the Network configuration overrides the semi static attribute `preferredmtdestination` for the rules evaluation.
	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the E.164 address representing the terminating MSC or SGSN.
	Country	This condition is evaluated against the country derived from the MSC or SGSN address by extracting the E.164 country code. Evaluation of this condition depends on the provisioned countries.
	Network	This condition is evaluated against the mobile network derived from the MSC or SGSN address by matching the E.164 number against the number ranges and/or number prefixes that are provisioned for each mobile network. Evaluation of this condition depends on the provisioned countries and mobile networks.
	List	This condition evaluates the MSC or SGSN address against a list of MSISDNs.
	Single point code or point code range	When the MTO rule set is evaluated against an MT message issued by an external SMSC, the MSC/SGSN address is only available in the SCCP called party address (CDPA). If PC/SSN routing is used, rather than global title (GT) routing, the MSC/SGSN address may only be available in the form of a point code (PC). This condition is evaluated against that PC. If the PC is not available, a non-inverted condition evaluated to false and an inverted condition evaluates to true.
Recipient	General	This condition is evaluated against the MT message's recipient address. The recipient MSISDN is not part of an MT message; therefore, if the MT message was issued by an external SMSC and not Home Routed, the recipient MSISDN is not available to this condition. The recipient IMSI is not available when: • The MTO rule set is evaluated for an SRI-SM request • The MTOX rule set is evaluated for the response to an SRI-SM request issued by the RTR
	Single MSISDN, MSISDN range, or MSISDN prefix	This condition is evaluated against the recipient MSISDN. When not available, the non-inverted condition evaluates to false, and the inverted condition evaluates to true.

Condition	Format	Description
	Single IMSI, IMSI range or IMSI prefix	This condition is evaluated against the recipient IMSI.
	Country	This condition is evaluated against the country for which the recipient's IMSI has been issued. Evaluation of this condition depends on the provisioned countries.
	Network	This condition is evaluated against the mobile network for which the recipient IMSI has been issued. Evaluation of this condition depends on the provisioned countries and mobile networks.
	List	This condition evaluates the recipient MSISDN or IMSI against a list of MSISDNs or IMSIs.
SCCP Calling Party Address	General	This condition is evaluated against the Calling Party Address received at the SCCP layer of the MT message. This information is applicable only for MT-FSM requests originated from external SMSCs. For all other types of MT messages, a non-inverted condition evaluates to false and an inverted condition evaluates to true.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the E.164 address representing Calling Party at the SCCP layer.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Calling Party Address. Successful extraction of the country code depends on the provisioned countries. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is received at the SCCP layer.
	Network	This condition is evaluated against the network, as derived from matching the Calling Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	List	This condition evaluates the Calling Party address received at the SCCP layer of the MT message against a list of E.164 numbers. This enables logical OR operation.

Condition	Format	Description
	PC or PC Range	This condition evaluates the PC included in Calling Party address received at the SCCP layer of the MT message against a Point Code or a Point Code Range. **Note:** **1.** If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. **2.** If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
SCCP Called Party Address	General	This condition is evaluated against the Called Party Address received at the SCCP layer of the MT message. This information is applicable only for MT-FSM requests originated from external SMSCs. For all other types of MT messages, a non-inverted condition evaluates to false and an inverted condition evaluates to true.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the E.164 address representing the Called Party at the SCCP layer.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the SCCP Called Party Address. Successful extraction of the country code depends on the provisioned countries. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	Network	This condition is evaluated against the network, as derived from matching the Called Party Address received at the SCCP layer against the provisioned mobile network number ranges and/or network prefixes. **Note:** If PC/SSN routing is used instead of GT routing, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true if no GT address is present at the SCCP layer.
	List	This condition evaluates the Called Party address received at the SCCP layer of the MT message against a list of E.164 numbers. This enables logical OR operation.

Condition	Format	Description
	PC or PC Range	This condition evaluates the PC included in Called Party address received at the SCCP layer of the MT message against a Point Code or a Point Code Range. **Note:** **1.** If global title (GT) routing is used, then a non-inverted condition will always evaluate to false and an inverted condition will always evaluate to true. **2.** If PC/SSN routing is used but no SCCP PC is available, OPC at MTP3 layer will be used for rule matching.
User Data		This condition is evaluated against the user data of an MT message. If the message is a Status Report or if the MTO rule set is evaluated against a SRI-SM request (or its response) issued by an external SMSC, no user data is available.
User Data Hdr		This condition is evaluated against the list of user data header information element identifiers present in the MT message. If the message is a Status Report, if the MTO rule set is evaluated against a SRI-SM request issued by an external SMSC (or its response), or if the MT message does not contain a user data header, no user data header is available.
Reply Path		This condition is evaluated against the MT message's TP-RP flag. If the MTO rule set is evaluated against a SRI-SM request issued by an external SMSC (or its response), no reply path information is available.
Status Report		This condition is evaluated against the MT message's TP-SRI flag. If the MTO rule set is evaluated against a SRI-SM request issued by an external SMSC (or its response), no status report indication information is available.
PID		This condition is evaluated against the Deliver-SM's TP-PID parameter. If the MT message is a Status Report or if the MTO rule set is evaluated against a SRI-SM request issued by an external SMSC (or its response), the condition evaluates as if the TP-PID parameter were set to 0.
DCS		This condition is evaluated against the Deliver-SM's TP-DCS parameter. If the MT message is a Status Report or if the MTO rule set is evaluated against a SRI-SM request issued by an external SMSC (or its response), the condition evaluates as if the TP-DCS parameter were set to 0.

Condition	Format	Description
Originator TON		This condition is evaluated against the type of number (TON) parameter of the originator. Refer to the description of the originator condition for information about this parameter's availability.
Originator NPI		This condition is evaluated against the numbering plan indicator (NPI) parameter of the originator. Refer to the description of the originator condition for information about this parameter's availability.
Ext Att		This condition is evaluated against the external attributes as set and reset by the EC application consulted during the evaluation of EC rules.
XS Message		This condition is evaluated against the XS message type of an MT message. Only Deliver-SMs can have an XS message type other than "no XS message". Valid XS message types are: • Forwarded message • Message copied to a subscriber • Message copied to an application (not relevant to MTO rule sets) • Auto-reply message • Copy to Email (not relevant to MTO rule sets) • Forward to Email (not relevant to MTO rule sets) This condition is not supported in the MTIC and MTIX rule sets.
Message Type		This condition is evaluated against the type of message. Valid values are: • Deliver-SM (normal message) • Status Report • SRI-SM Request • SRI-SM Response
Originator SSI		This condition is evaluated against the SSI information of the originator. It enables you to specify which services the originator must or must not have. If the MTO rule set is evaluated while the originator MSISDN is not available (such as for SRI-SM requests issued by an external SMSC with the RP-SMEA field not present, and the subsequent responses), no originator SSI is available. If SSI is not used, this condition should not be specified.
Recipient SSI		This condition is evaluated against the SSI information of the recipient. It enables you to specify which services the recipient must or must not have. If the MTO rule set

Condition	Format	Description
		is evaluated while the recipient MSISDN is not available (such as for unsolicited MT messages issued by an external SMSC), no recipient SSI is available. If SSI is not used, this condition should not be specified.
Traffic Type		This condition is evaluated against the trusted/suspect categorization of the external SMSC, which issued the SRI-SM request or MT message. If the RTR issued the message, it is considered trusted.
Message Concatenated Match		This condition is evaluated against the Deliver-SM's UDH in the IEI parameter. If the MT message is a Status Report or if the MTO rule set is evaluated against a SRI-SM request issued by an external SMSC (or its response), the condition evaluates as if the UDH in IEI parameter were set to 0 or 8.

10.7.3 MTOR Rule Set

The RTR evaluates the MTOR rule set to filter and block certain messages.

The MTOR rule set has certain limited routing capabilities (described below), but they are deprecated and should not be used. Instead, the SRI-SM Request and Response rule sets should be used.

10.7.3.1 MTOR Routing Action

The primary effect of the evaluation of the MTOR rule set is that the RTR determines if a message should be passed or blocked, which is implemented through the matching MTOR rule's routing action. The possible actions are:

Action	Effect
Pass	When the MTOR rule set is evaluated for an SRI-SM request, this action causes the RTR to send the SRI-SM request to the HLR, so that the HLR will send its response back to the RTR. When the MTOR rule set is evaluated for the response to an SRI-SM request issued by an external SMSC, this action means that SRI-SM response processing will continue by the inbound SRI-SM processing logic's evaluation of the SRI-SM Response rule set. When the MTOR rule set is evaluated for an MT message, this action means that the MT message shall be sent to the MSC/SGSN, so that the MSC/SGSN will send its response back to the RTR.
Block with temporary error	This action means that the requestor of the outbound SRI-SM or MT message will consider the requested outbound service to have failed with an error classified as temporary.
Block with permanent error	This action means that the requestor of the outbound SRI-SM or MT message will consider the requested outbound service to have failed with an error classified as permanent.

Action	Effect
Block with no response	This action means that if the SRI-SM request or MT message was issued by an external SMSC, the RTR will discard the inbound message and return no response. For MT delivery attempts requested by the RTR, this action produces the same behavior as the "block with temporary error" action.
Block with acknowledgment	When the MTOR rule set is evaluated for an MT message, this action causes the RTR to not send the MT message to the MSC/SGSN, but to indicate successful delivery to the requestor of the outbound MT service. When the MTOR rule set is evaluated for a SRI-SM request or response, this action produces the same behavior as the "pass" action.
Release	When the MTOR rule set is evaluated for a SRI-SM request issued by an external SMSC, this action causes the RTR to relay the SRI-SM request to the HLR so that the HLR will send its response directly to the external SMSC (not to the RTR). When the MTOR rule set is evaluated for the response to an SRI-SM request issued by an external SMSC, this action means that the RTR skips evaluation of the SRI-SM Response rules of the inbound SRI-SM processing, and subsequent MT messages are therefore not get Home-Routed. In all other cases, this action has the same effect as the "pass" action. **Note:** The "release" action is deprecated. The SRI-SM Request and SRI-SM Response rule sets should be used.

If no MTOR rule matches, the RTR applies routing logic that is the same as for the "pass" action.

10.7.3.2 MTOR Modifier

MTOR rules can refer to an MTO Modifier. If the matching MTOR rule refers to an MTO Modifier, that modifier is applied to the evaluated message after the MTOR rule set evaluation. For information about MTO modifiers, refer to *Modifiers*.

10.7.3.3 MTO Throughput Regulation

The RTR supports rule-based throughput regulation when evaluating the MTOR rule set. You can specify the maximum number of times that each MTOR rule does not match. If such a rule would match (due to its priority and conditions), but the rule's throughput counter has not reached the provisioned threshold for the current second, the rule does not match. The rule will only match if the rule's throughput counter has reached the provisioned threshold. This mechanism enables you to block certain MT messages if their throughput exceeds a threshold.

10.7.3.4 MTOR Rule Matching Ratio

The MTOR rule matching ratio enables you to Home-Route a fraction of inbound MT traffic. However, this functionality is deprecated. The matching fraction mechanism of the SRI-SM Response rule set should be used instead.

10.7.3.5 MT Outgoing Address Conversion

An outgoing originator address conversion rule set may be specified for each MTO routing rule.

See *Outgoing Address Conversion* for details of Outgoing Conversion Rules.

Note: In case both output TON and output NPI for MT outgoing address conversion are set to `default` for a given output address prefix then the RTR will use some older TON/NPI conversion semantics in order to avoid a possible upgrade issue. Following explains how the older TON/NPI conversion works:

1. If the output address matches the configured E164 international prefix (see *internationalprefix*), then the Output TON/NPI will be 1/1.
2. If the output address starts with the configured E164 country code(see *countrycode*), then the Output TON/NPI will be 0/1. Also the country code present in the output address will be replaced by the configured national prefix.
3. If the output address matches the configured E164 national prefix (see *nationalprefix*), then the Output TON/NPI will be 2/1.
4. For other scenarios the Output TON/NPI will be 0/0.

The outgoing MT originating address conversion affects the MT status report only if the semi-static `applyoutgoingrulesetonmtstatusreport` item is set to 'true' (see *applyoutgoingrulesetonmtstatusreport*).

In case of MT SMS-Deliver message where the originating address is a short number outgoing address conversion is only applied if the semi-static `applyoutgoingaconmtdeliverwithorigsn` item is set to 'true' (see *applyoutgoingaconmtdeliverwithorigsn*). (This limitation does not affect MT status report if the semi-static `applyoutgoingrulesetonmtstatusreport` item is set to 'true'.)

Outgoing address conversion is not applied for delivery to IMS domain (SIP-MT).

10.7.3.6 MTOR Billing

MTOR rules can refer to a billing profile that will be associated to outbound MT messages. The actual generation of CDRs is not part of the outbound MT processing, but is rather part of the inbound message control's post-processing logic. If a matching MTOR rule causes a "default" billing profile to be associated with a message, then the determination of which profile is the default profile is performed during the post-processing of the inbound message. Therefore, the "default" billing profile in an MTOR rule may be the default billing profile designated for inbound MO, inbound AO, or inbound MT traffic, depending on the origin of the message.

The MTOR-based billing profiles that are used to generate CDRs depend on the MTOR routing action and on the message's exact routing path and delivery result(s).

The billing profile for delivery notifications (that is, for Status Reports) is generally used in all cases where a CDR is generated for a Status Report. Otherwise, if the MTOR rule's action is a "block" action, the billing profile for blocked delivery is used. Delivery or non-delivery CDRs, respectively, are created using the billing profile for successful or failed delivery. If submission CDRs are created after the outbound MT processing, the billing profile for submission will be used.

For information about the billing profile for B-IMSI retrieval, refer to the Billing Manual. This billing profile should be used with care.

The billing profile configured for the Blocked Delivery can be used to create the CDRs for the rejected messages if the following conditions are met:

1. Applied MTO routing rule action is set as **Block with permanent error** or **Block with no response**.
2. The field **Not Delivered Status** is set as **Rejected** in the billing profile used for Blocked Delivery.

Only the FCDR format will be supported for Rejected CDR generated by the RTR.

In case of MT-MT scenario, billing profile configured for the Blocked Delivery can be used to create the CDRs for the rejected messages if the following conditions are met:

1. The applied MTO routing action is set as **Block with permanent error** or **Block with temporary error** or **Block with no response**.
2. The semi-static parameter *rtrcreatemtmtcdrforerrorscenarios* is configured as true.
3. The configured Billing profile is of 3G CDR format.

When the AMS is used to perform the MT delivery and the MTOR routing action is set to **Block with no response**, no CDR will be generated, because in this case the messages will be stored again in the AMS for further retries.

Note: Reject CDRs will not be generated if the early SRISM request for the MO message is rejected due to the routing action set to **Block with no response** in the MTOR rule.

For more information about the CDR formats that the RTR supports, refer to the Billing Manual.

Note: Supported CDR formats for Return Messages are the same as with Notification Messages. Please refer to Billing Manual for Details (4.9 CDR Formats by Billing Profile).

10.7.3.7 Unicode Character Conversion

The Unicode Character Conversion Map setting allows to customize the character translation logic that is applied on the final user data (excluding UDH) of outgoing MT messages matching a given MTOR rule.

Supported path for Unicode Character Conversion are AO-ST-MT, MO-ST-MT, and MT-MT paths.

Note: Character Conversion is not performed on SIP-Terminated messages.

See *Unicode Character Conversion* for details of the Unicode Character Conversion functionality.

10.7.4 MTOX Rule Set

The RTR evaluates the MTOX rule set so that EC applications can process the outbound MT message or SRI-SM request/response. MTOX rules are most commonly used to apply additional personalized services to Deliver-SMs.

MTOX rules get evaluated using the logic common to all external condition rule sets (refer to *Rule Evaluation*).

For information about the circumstances in which the MTOX rule set is evaluated, refer to *MTO Rule Evaluation*.

10.7.4.1 MTOX Failure Action

If the ECI evaluation produces, after the optional inversion of the corresponding MTIX rule's external condition, a result of FALSE, then, the processing of the sorted list of matching MTOX rules [see the generic description of the evaluation of X rules in the introduction section] stops, and the Failure Action, associated with that MTOX rule gets applied. If the Failure Action is set to "None", then the result of the external evaluation is ignored. Whenever the purpose of the EC application is other than to block certain messages, this Failure Action should be used. All other Failure Actions behave like their MTOR counterparts (see above).

If the ECI evaluated produces a result of false (after the optional inversion of the corresponding MTOX rule's external condition), then the processing of the sorted list of matching MTOX rules stops and the failure action of the MTOX rule is applied.

If the failure action is set to "none", then the result of the external evaluation is ignored. If the purpose of the EC application is anything other than blocking certain messages, this failure action should be used. All other failure actions behave like their MTOR counterparts (see *MTOR Routing Action*).

Note:

CDRs will be generated using the billing profile (if configured) for `Discarded Messages` when the message is discarded due to the application of any of the following routing action:

1. Discard with permanent error
2. Discard with no response

Apart from the above stated condition for the MT-MT scenario, if the semi-static parameter *rtrcreatemtmtcdrforerrorscenarios* is configured as true, CDRs will also be generated using the billing profile (if configured) for Discarded Messages when the configured billing profile is of 3G CDR format and the message is discarded due to the application of any of the following routing actions:

1. Discard with permanent error
2. Discard with no response
3. Discard with temporary error

Only the FCDR format will be supported for generating CDRs for messages discarded by the RTR.

Note: Reject CDRs will not be generated if the early SRISM request for the MO message is rejected due to the failure action set as **Block with no response** in the MTOX rule.

10.7.5 MTOC Rule Set

The MTOC rule set is evaluated to generate statistics about the handling of outbound SendRoutingInfoForSm and MT messages. Each MTOC rule has a set of per-result counters in addition to the "total" counter. The result counters pertain to the result as received from the HLR, MSC, or SGSN.

MTOC rules are also evaluated in the case of an outbound ReportSmDeliveryStatus operation toward the HLR. The evaluation of MTO conditions is similar to the evaluation against a SendRoutingInfoForSm request.

10.8 Using Alternative Global Titles for MT Routing

The RTR supports alternative identities for GT routing through the use of configurable alternative global titles (GTs). Each RTR instance can have up to 10 alternative identities. The alternative GTs are used on the same physical network connection; additional physical network connections are not added.

Note: This feature is not supported for point code (PC) routing.

When the RTR is going to initiate an outgoing TCAP dialog in which the MAP operation is MtForwardSm, SendRoutingInfoForSm, or ReportSmDeliveryStatus, it applies a best-matching algorithm to the MAP-layer SMSC address to determine which identity to use as the SCCP calling party address (CGPA) within the scope of the TCAP dialogue. This algorithm compares the GTs

digit-by-digit, starting with the country code. If the same number of digits matches for two or more candidate GTs, then the best-matching GT is unpredictable; however, if one of them is the RTR's own GT, then that is considered to be the best match.

When multiple MT messages are delivered on the same TCAP dialogue, the RTR only applies the best-matching algorithm on the first MAP operation.

The billing records (CDRs) and log records that the RTR writes will contain the GT that it sends.

Note: The RTR will not apply this feature in a configuration where transparent routing or interception of TCAP CONTINUE dialogues is done.

For information about configuring alternative identities, refer to *Configuring Alternative GTs*.

10.8.1 MT Use Case for Alternative GTs

The RTR can use multiple alternative GTs to support an operator that uses dual IMSI SIM cards to facilitate roaming agreements.

For example, there are three operators:

- Operators A and B have a roaming agreement and SS7 interconnect
- Operators B and C have a roaming agreement and SS7 interconnect
- Operators A and C do not have a roaming agreement and do not have SS7 interconnect

This figure illustrates the scenario.

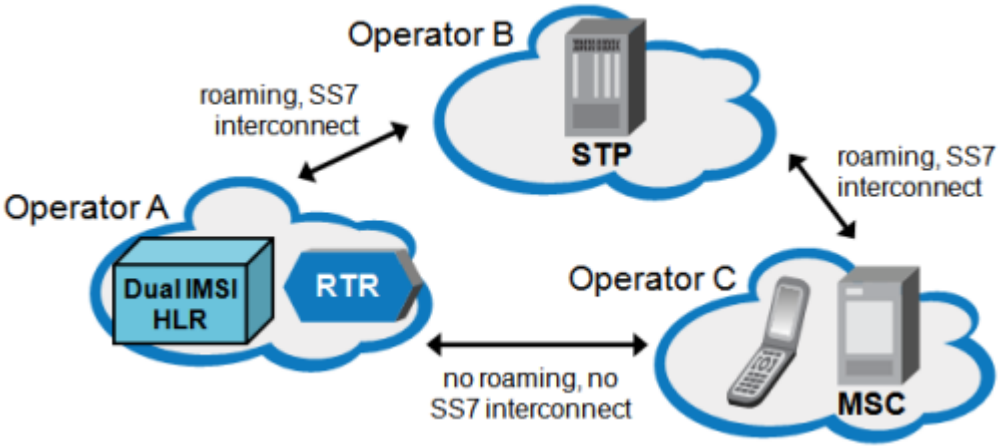


Figure 40: Operators with roaming agreements

Operator A does not have many roaming agreements, but Operator B does. Therefore, they agree that A's subscribers can roam into networks with which B has a roaming agreement (including the network of Operator C). To ensure that A's subscribers can register with C's network, A uses SIM cards that contain two IMSIs:

- One of A's own IMSIs, which the phone uses whenever possible
- An alternative IMSI that belongs to a range that B has set aside for A's subscribers, which the phone uses when attempting to register with the networks of B's roaming partners

When an A subscriber roams in C's network, C recognizes the alternative IMSI as belonging to B and allows the subscriber to register with the network. Also, B's STPs recognize the SMSC address that is associated with the IMSI and route messages to A.

To ensure that the lack of SS7 interconnect between A and C does not block MO responses and MtForwardSm requests, the RTR manipulates the GT in the SCCP CGPA.

When the RTR attempts to deliver an MT message to a subscriber of A who is roaming in C's network, the delivery must be routed through B, because C must see the message as coming from Operator B. To accomplish this, both the MAP SMSC address and the GT in the CGPA must represent a B identity.

To change the MAP SMSC address, use an MTO modifier to change the SMSC address to the desired value.

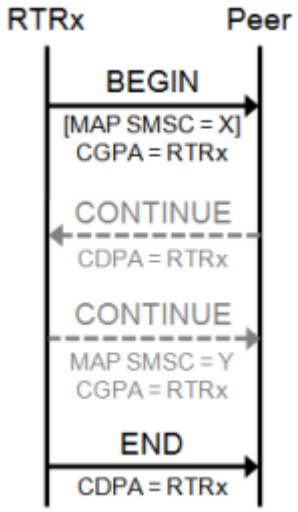


Figure 41: MT TCAP dialogue with altenative GT

10.8.2 Limitations on MT-MT Routing

This section describes limitations on the alternative GT functionality for MT-MT routing.

Incoming Dialogue

For incoming TCAP dialogues, the RTR selects its GT based on the SCCP CDPA. Therefore, when the incoming CDPA address is from Operator B, the dialogue will contain the alternative RTR SCCP address from Operator B.

Outgoing Dialogue

For outgoing TCAP dialogues, the RTR selects its GT based on the MAP address that was used when the dialogue began. Therefore, when the outgoing MAP SMSC address is from Operator B, the dialogue should have the RTR SCCP address from Operator B. This requires you to use an MT modifier to set the Operator B MAP SMSC address.

Home Routing

When Home Routing is applied, each incoming MT message addresses a specific RTR instance: the one that has the correlation record for that message. Therefore, the SCCP CDPA will contain the RTR instance's own GT. In this case, the RTR sets its CGPA to the received CDPA, overriding the best-matching algorithm's output.

Unsolicited MT Messages

An unsolicited MT message is an MT message that does not have a corresponding previous SendRoutingInfoForSm operation and does not have a correlation record on the RTR.

When the RTR receives an unsolicited MT message and the incoming TCAP dialogue does not contain a "components" part:

- The RTR will not use an alternative identity in the corresponding outgoing dialogue. This is because the RTR will forward the first BEGIN message to the MSC, at which point the RTR does not know what value the MAP layer SMSC field will have.
- In the incoming dialogue for the first CONTINUE (which is sent back to the SMSC that initiated the dialogue with the RTR), the RTR will use an alternative identity. This is because the CONTINUE must contain an address that is specific to a RTR instance.

When the RTR receives an unsolicited MT message and the incoming TCAP dialogue is a simple BEGIN-END dialogue, the RTR places the terminating MSC's address into the SCCP CGPA of its response to the SMSC, overriding the best-matching algorithm's output. This functionality ensures that the SMSC sees the response as coming from the MSC.

10.9 Home Routing

The Home Routing feature allows you to act as a home PLMN (HPLMN) when routing messages that originate in a foreign PLMN and are destined for your outbound-roaming subscribers. This enables you to control messages that are addressed to your subscribers without performing a complete MT spoofing check. Home Routing can be used to:

- Block certain messages, such as welcome messages from the visited PLMN
- Ensure that your subscribers can access their Personalized Services, whether or not they are roaming in foreign networks
- Take advantage of interconnect agreements that may exist between the foreign PLMN and the HPLMN
- Take advantage of interconnect agreements that may exist between the HPLMN and the visited PLMN

When Home Routing is not used, the foreign PLMN SMSC delivers messages to the visited PLMN MSC without the involvement of the HPLMN.

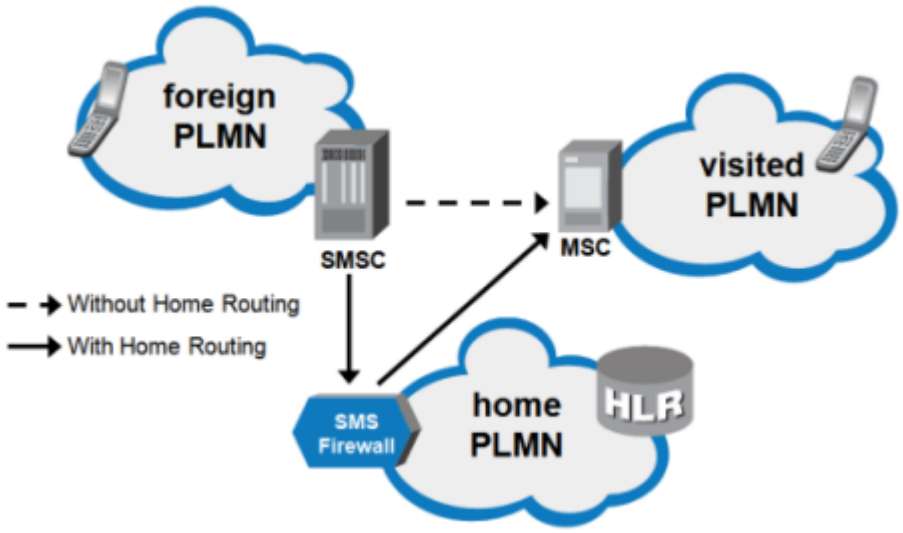


Figure 42: Home Routing

The FWL forwards SendRoutingInfoForSm (SRI-SM) requests to the HLR. After the HLR sends an SRI-SM response to the FWL, the FWL modifies the response's MSC address. This ensures that the originating SMSC will see the FWL as the MSC and will send the subsequent MtForwardSm operation to the FWL. The FWL stores the actual MSC/SGSN in its local correlation records.

After the FWL receives the MtForwardSm, it uses a correlation key to look up the record and retrieve the correct MSC/SGSN. The composition of the correlation key depends on the type of Home Routing in use:

Type	Description
"Plain" Home Routing	The FWL uses the recipient's IMSI as a correlation key, rather than a scrambled IMSI. This means that the originating SMSC will receive the recipient's true IMSI.
"Scrambled" Home Routing	The FWL uses a scrambled IMSI as a correlation key. The scrambled IMSI is a number that is randomly selected from a range that you define in the MGR interface. This means that the originating SMSC will not receive the recipient's true IMSI; it will receive the scrambled IMSI instead. This is the same correlation key mechanism that the FWL uses for MT anti-spoofing.

You can use plain Home Routing and scrambled Home Routing together by creating sets of IMSI prefix ranges in **Routing ➤ Home Routing** in the MGR. You associate each IMSI prefix range with a range of numbers from which the FWL randomly selects a scrambled IMSI; an empty scrambling range results in plain Home Routing. You can then choose to apply the set to trusted traffic, suspect traffic, or both.

10.9.1 Home Routing Process

The Home Routing process flows as follows:

1. The STP intercepts the SendRoutingInfoForSm (SRI-SM) operation from the SMSC to the HLR and redirects it to the FWL.

2. The FWL modifies the SRI-SM request to ensure that the SRI-SM response will be sent back to the FWL.
3. The FWL passes the SRI-SM operation to the HLR.
4. When the FWL receives the SRI-SM response from the HLR, it:
   a. Stores information about the response in a correlation record; if "scrambled" Home Routing is in use, the record includes a randomly generated key (scrambled IMSI)
   b. Modifies the response as follows:
      - Substitutes an address randomly selected from the list in `firewallmscsgsnaddressinsuspectsrismresponse` (or the FWL's GT, if a list is not provisioned) for the MSC and/or SGSN
      - If "scrambled" Home Routing is in use, substitutes the correlation key for the IMSI
      - Removes the LMSI, if it is present
5. The FWL sends the modified SRI-SM response to the SMSC.
6. The SMSC sends an MtForwardSm operation that:
   a. Terminates at the FWL (as a result of the MSC/SGSN substitution in the SRI-SM response)
   b. If "scrambled" Home Routing is in use, passes the correlation key as the IMSI (as a result of the IMSI substitution)
   c. Specifies the IMSI as the reference for the destination mobile (as a result of the LMSI removal)
7. The FWL looks up the correlation record:
   - If the look-up succeeds, the FWL combines the information from the correlation record and the MtForwardSm operation and issues an MtForwardSm operation toward the MSC or SGSN using the actual IMSI. In this case, the originator address on the SCCP level contains the SCCP address of the FWL.
   - If the look-up fails, the FWL rejects the MT message.

10.9.2 MAP Phase Translation in Home Routing

In home-routed scenario, the external SMSC does not have the actual MSC/SGSN address and hence it cannot determine the MAP Phase of Terminating MSC/SGSN which leads to more dialogues if there are "Application-Context-Name-Not-Supported" responses for the delivered MtForwardSm operation.

The FWL can be configured with the parameter **MAP Phase Translation** under the **Firewall ➤ MT ➤ Properties** in the MGR GUI to determine whether the MAP phase translation is to be supported or not for home routing scenarios.

This configuration provides the following three options:

S. No.	MAP Phase Translation option	FWL behavior
1.	No translation	With this configuration: 1. FWL sends the outgoing MtForwardSm using incoming MAP Phase. 2. Any error including Abort due to "Application-Context-Name-Not-Supported" received by the FWL is sent back to the external SMSC.

S. No.	MAP Phase Translation option	FWL behavior
		3. External SMSC has the responsibility of retrying with lower MAP version.
2.	Translation based on App Context Not Supported Error	With this configuration: **1.** In Case the FWL receives the TCAP Abort due to "Application-Context-Name-Not-Supported" in response to MtForwardSm request, the FWL will try forwarding the outbound MtForwardSm using the supported map phase value received in the response from the other entity. **2.** If the message is not delivered, then the error received for outgoing MtForwardSm is converted to incoming MtForwardSm MAP phase format while sending the response back to the external SMSC. **3.** This is the default behavior of the FWL. **Note:** The RTR will perform the map-phase translation irrespective of whether the incoming message is received from a Japanese Operator or an Oversea Operator.
3.	Translation based on Destination MAP Phase and App Context Not Supported Error	With this configuration: **1.** FWL will check the MAP phase of the incoming MtForwardSm message. **2.** If the MAP phase is 1 or 2, then FWL will behave as defined for "No translation" operation. **3.** If the MAP phase is 2+, FWL will convert and send the outgoing MtForwardSm using MAP Phase configured in Destination network (determined based on MSC/SGSN address). **4.** If the destination network is unknown, FWL uses the incoming MAP phase version. **5.** In case FWL received TCAP Abort due to "Application-Context-Name-Not-Supported" in response to MtForwardSm request, FWL tries to forward outbound MtFowardSm in decreasing order of map phase i.e. either 3>2 or 3>1. **6.** If the message is not delivered, then the error received for outgoing MtForwardSm is converted to incoming MtForwardSm MAP phase format while sending the response back to the external SMSC. **Note:** The RTR will perform the map-phase translation irrespective of whether the incoming message is received from a Japanese Operator or an Oversea Operator.

The following table specifies how the MAP phase translation is performed when the outgoing MtForwardSm is a success, failure or receives the TCAP abort with "Application-Context-Name-Not-Supported".

Incoming MAP Phase	Configured Destination Network MAP Phase	1st MtForwardSm delivery attempt	2nd MtForwardSm delivery attempt	3rd MtForwardSm delivery attempt	MAP-Phase translations	Response translation (while sending the response to the External SMSC)
3	3	Success				
3	3	Error				
3	3	App context not sup	Success		3 -> 2	
3	3	App context not sup	Error		3 -> 2	2 -> 3
3	3	App context not sup	App context not sup	Success	3 -> 2, 3 -> 1	
3	3	App context not sup	App context not sup	Error	3 -> 2, 3 -> 1	1 -> 3
3	2	Success			3 -> 2	
3	2	Error			3 -> 2	2 -> 3
3	2	App context not sup	Success		3 -> 2, 3 -> 1	
3	2	App context not sup	Error		3 -> 2, 3 -> 1	1 -> 3
3	1	Success			3 -> 1	
3	1	Error			3 -> 1	1 -> 3
2	Don't care	Success			No translation, phase 2 used	No translation
2	Don't care	Error			No translation, phase 2 used	No translation
2	Don't care	App context not sup			No translation, required for 29.002 compliant behavior phase 2 used.	No translation required, application context error send towards SMSC.
1	Don't care	Success			No translation	No translation
1	Don't care	Error			No translation, phase 1 used	No translation

10.9.3 Home Routing Ratio

Home Routing can offer financial benefits by enabling a network operator to avoid termination fees from other operators. Because of this, some operators have contractual agreements about the percentage of MT traffic that each operator is allowed to Home Route.

The FWL enables you to configure this percentage by adding a rule matching ratio to outgoing mobile-terminating routing (MTOR) rules (this is sometimes referred to as "decimation"). The ratio determines the number of messages to which the RTR will apply the routing action of a rule, out of all MT messages that match the rule's conditions.

The ratio is in the format N/M, where:

- N is the number of messages to which the RTR will apply the routing action of the rule
- M is the number of messages in a "set"

For example, if the ratio is 13/50, the RTR will apply the routing action to the first 13 messages of the set, and will not apply the outing action to the following 37 messages. A new set of messages then begins: the RTR applies the action to the next 13 messages, and does not apply the action to the 37 messages after that.

N and M can be 1 through 9999, and M must be greater than or equal to N. The default ratio is 1/1, which means that the RTR will apply the routing action to all messages that match the rule.

To control the amount of traffic that is Home Routed, create MTOR rules that will match trusted SendRoutingInfoForSm (SRI-SM) responses and use the rule matching ratio to pass and release portions of the responses ("pass" means proceed to the next-lowest priority MTOR rule, while "release" means release the operation without further MTOR rules processing).

CAUTION: Do not apply a ratio to suspect traffic when the FWL MT anti-spoofing license is enabled. This will cause incorrect blocking of unsolicited MT messages. The ratio should only be applied to trusted traffic.

10.10 Unicode Character Conversion

The RTR supports twenty different default Unicode Character Map Tables that translate a Unicode character into another Unicode character in an outgoing MTFSM.

10.10.1 Configuring Unicode Character Map

The RTR supports updating of Unicode Character Map configuration in a transactional manner, i.e. in case of incorrect configuration in any Unicode Character Map entry RTR aborts the complete configuration update action and continues to use the existing Character Map.

Unicode Character Map entries can be configured on MGR in the following two ways:

- One translation character entry at a time.
- Multiple translation character entries at a time by uploading a CSV file.

Unicode character conversion (UCC) feature has two parts:

1. Unicode character conversion feature that may be configured per MT routing rule on normal SMS deliver messages (NOT on error messages, NOT on MAP phase 1 or any other status reports). Will not be done on internally generated messages such as copied or forwarded messages, for AO-ST-MT, MO-ST-MT, and MT-MT paths.
2. New enhanced character conversion feature that may be enabled per AMS storage queue, for MO-ST-MT and AO-ST-MT paths.

Note:

- Adding a new Unicode Character Map table or deleting any existing Unicode Character Map table is not supported.
- A maximum of 32000 translation character entries can be configured for a single Unicode Character Map.
- Maximum 20 Unicode Character Map table are supported.
- Currently only Unicode codepoints are supported from MGR. and UTF-16 encoded Unicode code points for RTR.
- Provisioning of the translation character entries is done in such a way that only those entries for which a translation is required are considered for provisioning. Hence Input Character should not be same as Output Character in any Translation Character entry.
- For CDR, only converse 3G format is supported, also Message Data in CDR will contain the original userdata received in message.

For more information about configuring Unicode Character Map, refer to the MGR Operator Manual (section 4.15).

10.10.2 Character Translation

For Unicode Character Conversion, the *Unicode Character Conversion* setting allows you to do user data translation based on:

- destination network
- presence or absence of concatenated message headers
- source and destination handset type as determined by LDAP query using the PBC (over ECI) and reported in external attributes bits.

The Unicode Character Conversion Map settings allow you to do user data translation based on source SMSC address, presence or absence of concatenated message headers, and destination handset type.

Translation is performed just before sending out the message, if the matching MTOR rule has the Unicode Character Map configured and DCS is UCS-2. Hence only the final user data content (excluding UDH) is translated.

Currently the Unicode Character Conversion is limited to outgoing MT messages. Translation is not performed on SIP-Terminated messages. The supported routing paths are:

- MT-MT
- MO-ST-MT
- AO-ST-MT

However, there are no restrictions on the following paths:

- MT-ST-MT
- MO-MT-ST
- AO-MT-ST

10.10.3 Unsplit Surrogate Pairs

Existing behavior of UCC conversion may separate the pairs into 2 segments by fully using the space in the segment. This leads to issues in certain handsets (android phones where the software version is less than 6.0) from not being able to display messages when multi Unicode characters/surrogate pairs are split into 2 segments.

This feature prevents certain Unicode characters (surrogate pairs and multi-Unicode characters) on the SMSC from splitting into 2 segments of a concatenated message, thus this feature will move the whole pair of Unicode characters to one of the segments. Consequently, the whole surrogate pair is unsplit.

Once UCC conversion is applied to the incoming message, the RTR always performs the check for the unsplit surrogate pair and Configured Multiple Unicode characters by using the *pairedunicodecharlist* semi-static parameter, if an incoming message is not segmented for RTR.

Note: The router will not perform the unsplit surrogate pair check in case the incoming message is a concatenated message, or if Unicode Character Conversion not applied.

Limitation: In case of Modifiers are applied, then this feature is not applicable.

10.10.4 Unique TP-SCTS in Additional Segments After Applying the Unicode Character Conversion

Currently, while the RTR applies the UCC conversion to the single (unsegmented) incoming message, the RTR can create extra segments after the UCC conversion (Max 2 segment), so both the outgoing MT segments can have the same SCTS. This applies for incoming MT message or DeliverSmRequest MXP message from the AMS.

In the above scenario, the RTR makes unique SCTS. This means all segments created by the RTR will have different SCTS for the same recipient.

This is applicable for MT-MT and STORE-MT flows of the RTR UCC conversion.

Limitation of this solution:

1. The uniqueness of SCTS only has the scope of a single RTR instance, means RTR can generate the duplicate SCTS for the same recipient if multi-instance RTR is configured.
2. Same SCTS can be used by RTR and AMS (if the system is configured for MO/AO-ST-MT and MT-MT flow together)

10.11 TP-OA Modification Using MTO Modifier

If for the matching MTOR rule the **Outgoing Address Conversion** field is set to `Originator` and the originator address is not an alphanumeric or a short number, the outgoing conversion rule(s) would be applied on the Originator Address of the MT message.

For scenarios where outgoing conversion rule(s) is not applied, originator address modification is done as per the MTO modifier configuration.

This modifier overrides the format specified in the `mtoriginatorformatfordomestictraffic` and `mtoriginatorformatformtmtdomestictraffic` parameters in the semi-static configuration file. These parameters take effect only when the modifier is set to `Transparent`.

The parameter `mtoriginatorformatfordomestictraffic` is applicable for MO/AO/Store-MT and MT-MT (where the SRIQ routing rule action is set to '`Accept and Respond to SMSC immediately`') traffic.

The parameter `mtoriginatorformatformtmtdomestictraffic` is applicable for MT-MT traffic (except in the case where the SRIQ routing rule action is set to '`Accept and Respond to SMSC immediately`'),

A special value of -1 is supported for MT modifier Originator TON and NPI, that preserves the received TON and NPI value in the TP-OA.

Note: For the following scenarios, the TON/NPI value is always encoded as 0/1 in the TP-OA:

1. If the received TON/NPI is 6/1 (regardless of value configured in the MTO modifier)
2. If the originator input format is short, and any of the following case matches :
   a. The MTO modifier originator format is national/international.
   b. The MTO modifier originator format is transparent and TON/NPI is any value other than -1/-1.

If the originator input format is short, the received TON/NPI value will be preserved when the matched MTO modifier is configured with the following values:

1. The originator format is transparent.
2. The originator TON/NPI is set as -1/-1.

The below table summarizes how TP-OA modification is done using MTO Modifier for different originator types:

Originator Input Format	**MT modifier Originator Format**	**TP-OA Modification**
Alphanumeric	National / International / Transparent	Received TON/NPI is preserved
Short number (A number is defined as short number: • If the address length is less than or equal to the configurable parameter `maxlengthforshortnumber`. • If an application is configured with a number, then it is defined as a short number regardless of length)	National / International / Transparent	If in the MT modifier, the Originator format is set as `transparent` and TON/NPI as -1/-1 Received TON/NPI is preserved Else TON/NPI is updated as 0/1

Originator Input Format	MT modifier Originator Format	TP-OA Modification
International / National MSISDN	International	If TON/NPI configured in the MT modifier as 1/1 If received NPI is 1 TON/NPI is updated as per MTO modifier configuration, i.e. 1/1 Else Received TON/NPI is preserved Else TON/NPI is updated as per MTO modifier configuration.
International / National MSISDN	National	The TON/NPI is updated as per MTO modifier configuration. If the normalized address starts with an E164 country code and the received NPI is `unknown`(0) or `isdnTelephony`(1), the E164 country code is replaced with the national prefix. In this scenario also, the TON/NPI is updated as per MTO modifier configuration. **Note:** When the incoming TON/NPI = 2/1 and the normalized MSISDN does not start with an E164 country code and the TON/NPI in MTO modifier is 0/1 and semi-static parameter "`preservenationalorigton`" is set to "true", the TON/NPI in the outgoing TP-OA will be 2/1. This is for backward compatibility.
International / National MSISDN	Transparent	TON/NPI is updated as per MTO modifier configuration.

Note: Some handsets cannot cope with the address type TON as `abbreviated` (6) and NPI as `isdnTelephony` (1). The RTR therefore overrules this particular TON/NPI combination with TON as `unknown` (0) and NPI as `isdnTelephony` (1). This functionality is applicable for below routing paths:

- AO/MO/Store-MT/SIPT scenarios
- Home routed MT-SIPT scenarios.
- Home routed MT-MT scenarios in the case where the SRIQ routing rule action is set to '`Accept and Respond to SMSC immediately`'

Few examples for TP-OA modification using MTO modifier:

Input Number format	Destination	Desired TON/NPI in TP-OA	Required Configuration
MSISDN national number	National	0/0	Select Originator TON as 'national' and Recipient condition as national network in MTOR and the attached modifier should contain the below configuration: Originator Format : National Originator TON : 0 Originator NPI : 0
MSISDN national number	International	1/1	Select Originator TON as 'national' and Recipient condition as international network in MTOR and the attached modifier should contain the below configuration: Originator Format : International Originator TON : 1 Originator NPI : 1
MSISDN international number	International	1/1	Select Originator TON as 'international' in MTOR and the attached modifier should contain the below configuration: Originator Format : International Originator TON : 1 Originator NPI : 1
Short number	National	0/1	Select Originator = Short Number condition in MTOR and the attached modifier should contain the below configuration: Originator Format : National
Alphanumeric	International	5/0	MTO modifier not required as this is the default behavior. TP-OA modification is not done for Alphanumeric originator.

Chapter 11

AO Routing

Topics:

11.1 Introduction

Application-originating (AO) routing is the generic name for the processing of incoming AO messages. The HUB works in conjunction with the RTR and, in the case of routing with storage, the AMS to route AO messages to their destinations.

For more information about AO routing, refer to the HUB Operator Manual. This manual discusses AO-MT routing, which is subject to the RTR's outgoing mobile-terminating (MTO) rules.

11.2 AO Routing Paths

Supported AO routing paths are:

- AO-MT (route to mobile station)

  Note: AO-MT messages are subject to AO and MTO routing rules.

- AO-AT (route to application)
- AO-AO (route to SMSC)
- AO-MT-AO (route to mobile station, fallback to SMSC)
- AO-MT-Store (route to mobile station, fallback to storage)
- AO-AT-Store (route to application, fallback to storage)
- AO-AO-Store (route to SMSC, fallback to storage)
- AO-Store-MT (store for delivery to mobile station)
- AO-Store-AT (store for delivery to application)
- AO-Store-AO (store for forwarding as AO)
- AO-Discard:
  - Discard with NACK
  - Discard with ACK

Note: During the AT delivery via store, the configured value of the "outside transmit window size" is used as the `maxtransactions` in the store request. For the AT delivery "outside transmit window size" of the configured application is used for load balancing the traffic towards the HUB.

11.3 AO-MT, AO-MT-Store and AO-Store-MT Routing

The HUB can support AO-MT routing (route to mobile station) . The HUB provides the functionality to process incoming AO messages and the RTR performs an optimised MT delivery. AO-MT routing provides the following features:

- Optimised direct delivery of MT to mobile
- Throughput control
- Notification generation, if configured
- CDR generation, if configured

Figure 43: AO-MT routing

AO-MT routing can provide SMSC offload and SMSC overload protection. The direct MT delivery of AO-MT routing can use optimised routing on a per-application basis.

When the Mobile Messaging system includes the AMS, the HUB can provide AO-MT-Store (route to mobile station, fallback to storage) and/or AO-Store-MT (store for delivery to mobile station) routing.

Note: The AO-MT messages use the SMSC address that is configured in the `commonaddress` attribute as the MAP SMSC address in the MT message.

Important: In case of AO-MT-Store (route to mobile station, fallback to storage), the message is sent by the RTR to Store (AMS) before even making a FDA to the MS. Here the message is not stored in the AMS database but it is placed in the appropriate message queue; now the AMS immediately sends an Ack. to the RTR and then sends the message back to the RTR for performing the FDA. If the FDA is successful, the RTR generates a billing record (CDR); otherwise the routing result is returned to the AMS for storing it in the database for later retries. In the AO routing rule counters on the RTR, when the message is sent to the AMS, it is always counted as the primary destination and never as a fallback.

Note: In the AO-MT scenario, if early HLR query for AO/SM is configured (see **Routing-➤ Properties Early SRI-SM for AO/SM Whitelist** and **Early SRI-SM for AO/SM** in MGR), then during AO Rule evaluation, early SRISM is sent irrespective of Recipient Mobile Network Domain. MT delivery is also attempted in SS7 domain irrespective of Recipient Mobile Network Domain.

Note: The AO Rule condition (**Terminating MSC/SGSN** [cond]) is evaluated against the MSC or SGSN address as returned by the HLR. If the HLR returns both addresses, the rule set is evaluated against either the MSC or the SGSN address, as selected by the semi-static attribute `preferredmtdestination`. If the Network configuration is available according to MSC and/or SGSN (i.e. received in the HLR query), the **Preferred MT Destination** in the Network configuration overrides the semi static attribute `preferredmtdestination` for the rules evaluation.

Note: During the AT delivery via store, the configured value of the "outside transmit window size" is used as the `maxtransactions` in the store request. For the AT delivery "outside transmit window size" of the configured application is used for load balancing the traffic towards the HUB.

Important: In case of AO-MT, AO-MT-ST and AO-ST-MT billing if Source address of AO message is an alphanumeric address and reflecting the service provider name or address then the content vendors should send an SMPP message where an optional field TLV should reflect the real short code. The SMSC should retrieve this field and put it in the FCDR's OrigAddress fields.

The RTR will receive an `originatorAddressForBillingOverride` in receivedSubmitSmRequest from HUB over the MXP interface and will retrieve the short code belonging to the optional TLV in range 0x1400 to 0x3fff (5120 to 16383).

The following sub-fields will be affected in the FCDR's OrigAddress:

- `ton` will be short (4)
- `npi` will be private (5)
- `msisdn` will be an integer value (up to 9 digit) received in TLV 0x1403
- `msisdnUTF8` will be an integer value (up to 9 digit) received in TLV 0x1403.

Note:

1. It should be applicable for the submitted, rejected, Delivery FCDRs,
2. there should not be any impact on Routing rules, log and events.
3. Following routing path can be impacted:
   a. AO-MT
   b. AO-Store-MT
   c. AO-MT-Store

11.3.1 Setting SRI-SM Priority

SRI-SM Priority configuration for an Application/ AMS Queue controls the setting of the priority field in the SRI-SM Requests for messages originated from an application and to be delivered to a MT recipient, either directly (FDA by RTR) or via the AMS. This parameter can be configured independently for each Application as well as for each AMS Queue, and it can have three possible settings: 'High', 'Low' and 'Use message priority'.

If the SRI-SM Priority parameter is set to 'High' or 'Low', the value of the sm-RP-PRI in the SRI-SM Request will be set to 'TRUE' (1) or 'FALSE' (0), respectively. Note that in case a message gets stored in the AMS and retried later, then the SRI-SM Priority setting for the AMS queue will override the corresponding setting for the Application; refer to the AMS Operator Manual for more details.

In case the parameter is set to 'Use message priority':

- For an application, it means that the value of the sm-RP-PRI in the SRI-SM will be set as per the value of the Priority field in individual AO-MT messages originated from that Application, if the Priority field is actually present in a message; in case no Priority field is present in a particular message, the value of the sm-RP-PRI in the SRI-SM will be set to 'FALSE'.
- For an AMS Queue, it means that the value of the sm-RP-PRI in the SRI-SM will not be affected by the Queue configuration setting, i.e. the sm-RP-PRI value will remain the same as it would have been in the case of a direct FDA by the RTR.

By default the SRI-SM Priority parameter is configured as 'High' for an Application as well as an AMS Queue.

Note: In case of early SRI-SM for AO message, the SRI-SM Request will always be sent with sm-RP-PRI as 'TRUE', irrespective of the configured "SRI-SM Priority" setting in the Application or the value of the priority field received in the AO message.

11.4 AO-MT-AO Routing

AO-MT-AO routing provides the functionality to process incoming AO messages where the HUB will route the AO message to the RTR for a first delivery attempt (FDA). The HUB will only forward the AO message to an SMSC if the FDA fails. AO-MT-AO routing provides the following features:

- Traffic distribution and load balancing traffic over RTRs and SMSCs
- Throughput regulation of the AO traffic
- Optimised direct delivery of MT to mobile
- Throughput control

- Notification generation, if delivered successfully and if configured
- CDR generation, if configured
- Forward to SMSC in case of an unsuccessful delivery attempt

To relieve the SMSC of excessive application traffic, the HUB can also provide the first delivery attempt (MT) for application-originated (AO) traffic.

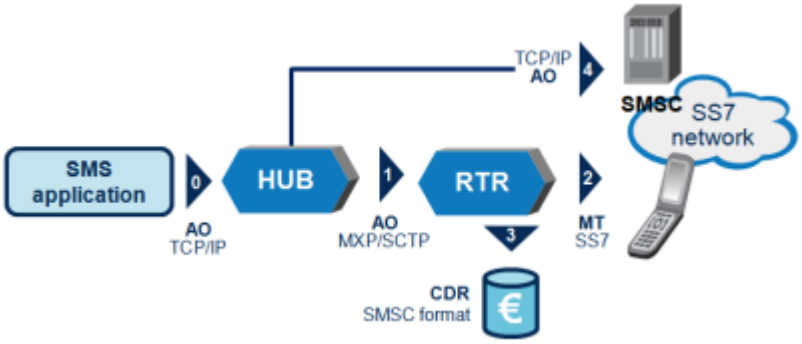


Figure 44: AO-MT-AO routing

The application submits an AO message (via SMPP, UCP, or CIMD2) to the HUB (flow 0). When the routing path AO-MT-AO is defined for the incoming SMS message, the HUB routes the AO message to the RTR (flow 1). Immediately, the RTR performs one delivery attempt to the recipient (flow 2), which in this example is a mobile phone. If the delivery attempt is successful, a billing record is generated (flow 3); if the delivery failed, the message is forwarded as an AO submit message to the appropriate SMSC (flow 4) for further delivery. Now the SMSC will take care of the delivery (retries) of the message and will generate a billing record when the message is delivered.

11.4.1 AO-MT-AO Message Flow

A typical message flow for regular AO-MT-AO routing is:

1. The HUB accepts a connect request from an SMS application on one of the configured AO-MT-AO ports.
2. The HUB receives a UCP60 log-in request from the SMS application on the established session.

   If the UCP60 log-in is valid, the HUB:

   a) Forwards the log-in request to the RTR configured
   b) Establishes a connection to the SMSC configured in the service class
   c) Logs in to the SMSC on behalf of the SMS application
   d) Responds to the UCP60 log-in request to the SMS application
   e) Logs in to the RTR on behalf of the SMS application
3. The HUB receives a UCP51 submit message from the SMS application.
4. The HUB investigates the properties of the UCP51 message to determine one of the following required actions:

   a) If the message can be delivered by the RTR, the HUB forwards the message to the RTR
   b) If the RTR's delivery attempt is not successful, the message is forwarded to the SMSC for further retries
5. If the HUB receives a valid UCP message (not UCP60, UCP51, UCP54), the HUB forwards the message to the SMSC.

6. If the HUB receives a disconnect request from the SMS application, it disconnects the corresponding session to the SMSC and forwards the disconnect request to the RTR.

The HUB actively manages the session set up to the SMSCs on behalf of the SMS applications by issuing UCP31 as keep-alive messages.

Note: Forwarding to the SMSC requires that the system wait on the response from the SMSC to return a response to the application, due to the identifier that the SMSC assigns.

11.4.2 AO-MT-AO Failure Scenarios

This section describes some AO-MT-AO failure scenarios.

Scenario	Result
There is not an SMSC connection when the message is submitted (UCP51 message is received)	The AO-MT-AO rule will not match the message.
All SMSC connections are overloaded (throughput limitation or window size is exceeded)	The AO-MT-AO rule will not match the message.
When the fallback AO message is submitted, the SMSC returns an error	If an acknowledgement has already been returned to the application, the Mobile Messaging system can only notify the application of this failure if it requested a delivery notification. The delivery status in the notification would indicate failure. If the application did not request delivery notification and logging, the log record will show that the message was dropped. However, the application sees the message as having been delivered successfully.
The SRI-SM or MT operation performed by the RTR returns a permanent error	If an acknowledgement has already been returned to the application, the Mobile Messaging system can only notify the application of this failure if it requested a delivery notification. The delivery status in the notification would indicate failure. If the application did not request delivery notification and logging, the log record will show that the message was dropped. However, the application sees the message as having been delivered successfully.
The connection to the SMSC fails after the RTR performs a delivery attempt (MtFwdSm)	If an acknowledgement has already been returned to the application, the Mobile Messaging system can only notify the application of this failure if it requested a delivery notification. The delivery status in the notification would indicate failure. If the application did not request delivery notification and logging, the log record will show that the message was dropped. However, the application sees the message as having been delivered successfully.

Scenario	Result
Segment of a concatenated message is greater than 140 bytes on the MT path.	If an AO message, submitted via SMPP, contains *sar* fields and the "total messages" value is greater than 1, then the message is a segment of a sequence of concatenated messages; according to specifications. To forward such an AO message through an MT path, requires the *sar* fields be converted to a user data header. This requires the RTR to prepend six or seven bytes to each segment. There may exist scenarios that such prepending will result in an individual segment greater than 140 bytes. In this case the message is undeliverable by the MT path and a line will be logged to syslog (saying,"`Application <xxx> of ID <xx> sent unexpected data`"). `noSpaceForSegmentingHeader` will be logged as `rejectCause`. Applications are required to explicitly divide long messages into segments of 133 bytes or less, allowing just enough space for the user data header.

11.4.3 Configuring the Application Entity for AO-MT-AO Routing

In the case of AO-MT-AO routing, RTR routing properties must be adapted determine when to generate the ACK/NACK response for a submit operation. These properties can be configured on an individual RTR application basis.

In the MGR interface, the SMS application entity has the following attributes:

- **AO-MT-AO Enabled**—When selected, the RTR always generate an ACK/NACK response that reflects the result of the delivery attempt. (This functionality requires the license for the AO-MT-AO routing path.)
- **Respond After Delivery**—When selected, the RTR will generate an ACK/NACK response that reflects the result of the delivery attempt. This attribute is mandatory for AO-MT-AO routing, but it can also be applied to the AO-MT path.

11.5 Multi-SIM Support for AO-MT Routing

Multi-SIM is an operator service that enables a customer to have more than one SIM card, but be reachable by only one MSISDN, which is called the master MSISDN. The non-master MSISDNs are called hidden MSISDNs.

The customer selects which MSISDN is the master. The device that the master MSISDN redirects to is called the Active Paging Device (APD).

Normally, SMS messages can only be delivered to the master MSISDN. If a message is sent toward a hidden MSISDN, the HLR rejects the SendRoutingInfoForSm request for the message with an error. If a message is sent toward the master MSISDN, the HLR responds to the SendRoutingInfoForSm request with the IMSI and MSC location of the SIM card in the APD.

However, in some scenarios, a message must be delivered to a specific SIM card; for example, an AO binary message to update the preferred roaming list in the SIM. In such a scenario, the HLR redirection mechanism must be overridden so the message can be delivered to the specific MSISDN, even if it is hidden.

The RTR supports HLRs that achieve the override functionality by requiring that the SMSC number in the SendRoutingInfoForSm operation be set to a special number. This number indicates to the HLR that it should override the rejection of the message and return the IMSI for the requested MSISDN, whether it is hidden or not. The RTR supports this method for AO-MT messages, on a per-application basis. When an application is configured for this functionality, the RTR:

- Queues messages from that application separately from other messages to the same recipients
- Sets the SMSC number in SendRoutingInfoForSm operations from that application to the configured special value

To configure the RTR:

- In the common configuration file, set the `tpconfig` attribute `smscaddressformultisimhlrredirectionbypass` to the special SMSC number (0-15 digits).
- In the MGR, select the **Multi SIM HLR Redirection Bypass** option in the SMS application configuration.

11.6 AO Routing Action Billing Parameters

This section describes the billing parameters for AO routing actions.

Parameter	Description	Default
Submission	Billing profile to use for submission; applies to all AO routing actions.	None
Successful Delivery	Billing profile to use when the routing action succeeds. Applies to: • Path AO-AO (to SMSC) • Path AO-AT (to Application) • Path AO-MT (to MT) • Path AO-MT-AO (Try-and-Forward MT) • Discard with ACK • Route to SMSC, Fallback to Storage	None
Failed Delivery	Billing profile to use when the routing action fails. Applies to: • Path AO-AO (to SMSC) • Path AO-MT (to MT) • Path AO-MT-AO (Try-and-Forward MT)	None

Parameter	Description	Default
Delivery Notification	Billing profile to use for delivery notification. Applies to: • Path AO-AO (to SMSC) • Path AO-AT (to Application) • Path AO-MT (to MT) • Path AO-MT-AO (Try-and-Forward MT) • Discard with ACK	None
Successful Delivery on Fallback	Billing profile to use when the fallback leg of the routing action succeeds. Applies to: • Path AO-MT-AO (Try-and-Forward MT)	None
Failed Delivery on Fallback	Billing profile to use when the fallback leg of the routing action fails. Applies to: Path AO-MT-AO (Try-and-Forward MT)	None
Discarded Messages	Billing profile to use when routing action discard the message. Applies to: • Discard with NACK **Note:** Only the FCDR format will be supported for generating CDRs for messages discarded by the RTR.	None

11.7 AO External Condition Routing

AO external condition (AOX) routing processes incoming AO messages and forwards selected message fields to a configured external condition (EC) application.

AO external condition routing provides one of the following responses:

Response	Description
True	The rule condition evaluates to true and the message processing continues normally.
False	The rule condition evaluates to false and the failure action is applied.

Response	Description
EC attributes	A returned matrix of result flags that the EC application sets and upon which the RTR can base its routing decision. **Note:** To use EC attributes in a rule condition, all used EC attributes must be configured in the EC attribute entry.

AOX rules get evaluated using the logic common to all external condition rule sets (refer to *Rule Evaluation*).

The possible failure actions are:

Action	Effect
None	Ignore the false result and continue to process the list of matching AOX rules, or assume that the message "passed" the AOX rule evaluation if there are no more matching rules in the list.
Discard with negative acknowledgement	Return an error to originator and discard the message.
Discard with acknowledgement	Return an acknowledge to originator and discard the message.

Note:

CDRs will be generated using the billing profile (if configured) for `Discarded Messages` when the message is discarded due to the application of any of the following failure actions:

1. Discard with negative acknowledgement

Only the FCDR format will be supported for generating CDRs for messages discarded by the RTR.

11.8 Early SRI-SM Behavior for Store Cases

The following table describes the behavior of **Early SRI-SM** for AO-Store-MT and AO-MT-Store Flow:

Early SRISM	Early SRI-SM Behavior against Paths
Disable	AO-ST-MT • Early SRI-SM **will not be** performed AO-MT-ST • Early SRI-SM **will not be** performed

Early SRISM	Early SRI-SM Behavior against Paths
Enable	AO-ST-MT • Early SRI-SM **will be** performed AO-MT-ST • Early SRI-SM **will be** performed

There are two ways by which the RTR evaluates if the early SRI-SM is enabled or not:

1. There is a white list including the recipient
2. The parameter *hlrqueryforrecipientofaobeforeapproval* is enabled

If the white list is configured, the parameter *hlrqueryforrecipientofaobeforeapproval* will not be used. The white list overrides the configuration of the parameter *hlrqueryforrecipientofaobeforeapproval*.

Chapter 12

AT Routing

Topics:

12.1 Introduction

Application-terminated (AT) routing is the generic name for the processing of incoming (ATI) and outgoing (ATO) application-terminated messages.

The RTR and HUB work in conjunction to route AT messages to their destinations. In the case of AT routing with storage, the AMS acts as a message store. The AMS can also provide a transaction database (called the Intermediate Cache, or Icache) that stores message state and parameters while the message itself is stored in an external SMSC. For more information about the Icache, refer to the AMS Operator Manual.

Note: MIB items that are related to ATO rules use the acronym AT. MIB items that are related to ATI rules use the acronym ATI.

Up to 500 ATIR rules and up to 500 ATOR rules can be defined.

Incoming AT Messages

When an incoming AT message arrives at the RTR, it is evaluated by the following rules, in the following order:

1. Incoming AT external condition (ATIX) rules
2. Incoming AT routing (ATIR) rules
3. Incoming AT counting (ATIC) rules

Outgoing AT Messages

When outgoing AT message is ready to leave the RTR, it is evaluated by the following rules, in the following order:

1. Outgoing AT external condition (ATOX) rules
2. Outgoing AT routing (ATOR) rules
3. Outgoing AT counting (ATOC) rules

12.2 AT Routing Paths

The available AT routing paths are:

- AT-AT (route to application)
- AT-AT-Store (route to application, fallback to storage)
- AT-Store-AT (store for delivery to application)
- AT-AO (route to SMSC as AO)
- AT-AO-Store (route to SMSC as AO, fallback to storage)
- AT-Store-AO (store for delivery to SMSC as AO)
- AT-Discard:
  - Discard with ACK
  - Discard with temporary error
  - Discard with permanent message error

- Discard with permanent recipient error

Note: During the AT delivery via store, the configured value of the "outside transmit window size" is used as the `maxtransactions` in the store request. For the AT delivery "outside transmit window size" of the configured application is used for load balancing the traffic towards the HUB.

12.3 AT-AT Routing

AT-AT routing allows for monitoring and controlling traffic toward applications. In AT-AT routing, the RTR receives incoming AT messages from a service centre and routes them to an application. AT-AT messages are first evaluated by the incoming AT routing (ATIR) rules, then by the outgoing AT (ATOR) routing rules.

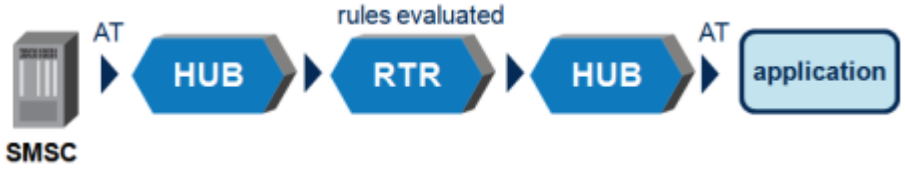


Figure 45: AT-AT routing

The **Destination Application** parameter in the ATIR rule determines the application to which the RTR routes the message:

- The application that sent the message
- The recipient application that is specified in the message
- An application that the user specifies in the ATIR rule
- An application that is determined by the Intermediate Cache (Icache)

Note: During the AT delivery via store, the configured value of the "outside transmit window size" is used as the `maxtransactions` in the store request. For the AT delivery "outside transmit window size" of the configured application is used for load balancing the traffic towards the HUB.

Note: For more information about the Icache, refer to the AMS Operator Manual.

12.4 AT-AT-Store Routing

In AT-AT-Store routing, if the application rejects a message with a temporary error, the message can fall back to storage in the AMS. The AMS delivery scheme determines when and how often message delivery is retried.

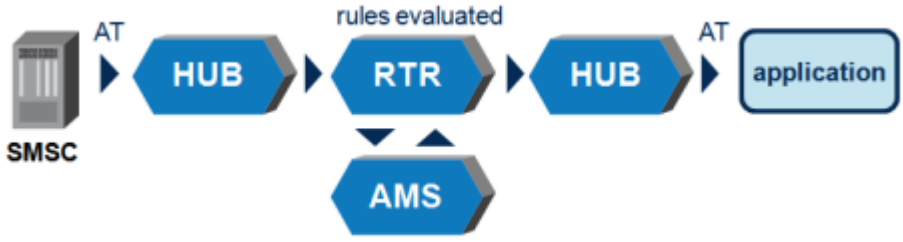


Figure 46: AT-AT-Store routing

The **AMS Queue** parameter in the ATIR rule determines the queue in which the message is stored (and, therefore, the delivery scheme that applies to the message).

Note: During the AT delivery via store, the configured value of the "outside transmit window size" is used as the `maxtransactions` in the store request. For the AT delivery "outside transmit window size" of the configured application is used for load balancing the traffic towards the HUB.

12.5 AT-Store-AT Routing

In AT-Store-AT routing, the RTR does not perform a first delivery attempt of the message. Instead, it immediately sends the message to the AMS for storage. The AMS delivery scheme determines when and how often message delivery is tried.

Note: During the AT delivery via store, the configured value of the "outside transmit window size" is used as the `maxtransactions` in the store request. For the AT delivery "outside transmit window size" of the configured application is used for load balancing the traffic towards the HUB.

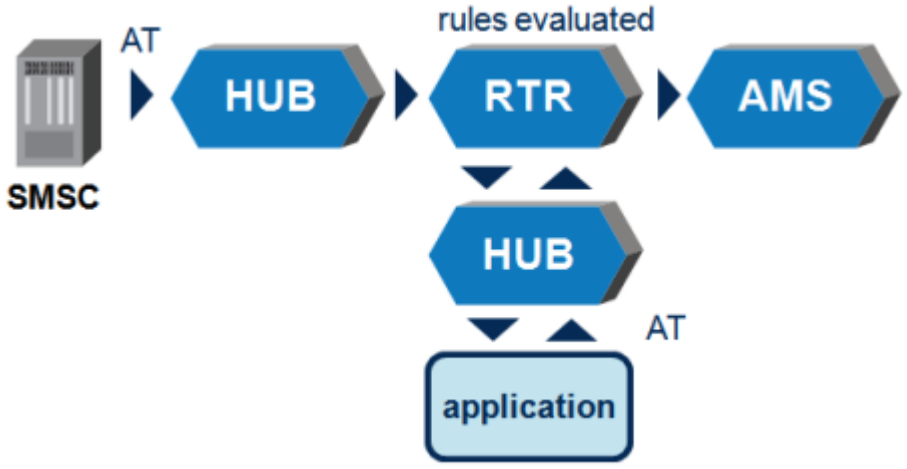


Figure 47: AT-Store-AT

12.6 AT-AO Routing

AT-AO routing allows a carrier to receive inter-carrier peer-to-peer AT messages, convert them to AO messages, and route them to the appropriate home network SMSC. AT-AO can also enable intra-carrier SMSCs to route AT messages that arrive at the wrong SMSC to the correct SMSC as AO messages.

AT-AO routing requires the AT-AO license.

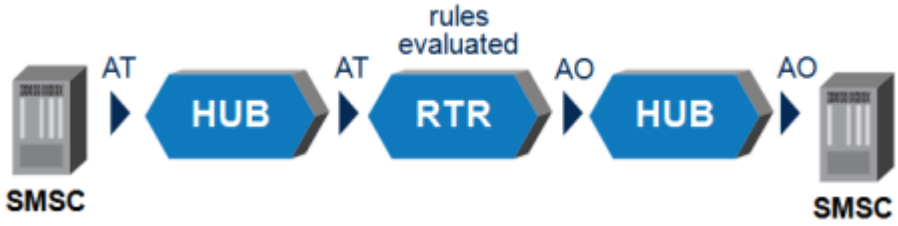


Figure 48: AT-AO

AT-AO routing flows as follows:

1. An inbound AT message arrives at the HUB
2. The HUB sends the AT message to the RTR for rule evaluation
3. The RTR evaluates the ATIR rules for the message, and it matches an AT-AO rule
   a. If the protocol of the incoming AT message does not match the protocol that is accepted by the destination application, the RTR blocks the message with a permanent error and processing of the message stops
   b. If the protocol of the incoming AT message matches the protocol that is accepted by the destination application, the RTR converts the AT message to AO and sends the AO message to the HUB
4. The HUB sends the AO message to the SMSC
5. The SMSC acknowledges (ACKs) or negatively acknowledges (NACKs) the AO message to the HUB
6. The HUB relays the SMSC's response to the RTR
   a. If the AO message was ACKed, the RTR sends an ACK for the AT message to the HUB
   b. If the AO message was NACKed, the RTR sends a NACK for the AT message to the HUB
7. The HUB relays the RTR's response to the AT originator

Note: This routing path is not supported for CIMD messages.

12.6.1 AT-AO Configuration

The **Destination Application** parameter in the ATIR rule determines which application the Mobile Messaging system uses to submit the message to the service centre:

- The application that sent the message
- The recipient application that is specified in the message
- An application that you specify in the ATIR rule

The destination application should be an application that has an inside connection to the service center(s) to which the message will be submitted. In the most common scenario, it would be set to an application that you specify in the ATIR rule.

Note: The **Destination Application** parameter must not be set to Icache-based application determination.

The **SMSC Group** parameter in the ATIR rule determines the group of service centres to which the Mobile Messaging system will submit the message.

12.6.2 Introduction

Application-terminated (AT) routing is the generic name for the processing of incoming (ATI) and outgoing (ATO) application-terminated messages.

The RTR and HUB work in conjunction to route AT messages to their destinations. In the case of AT routing with storage, the AMS acts as a message store. The AMS can also provide a transaction database (called the Intermediate Cache, or Icache) that stores message state and parameters while the message itself is stored in an external SMSC. For more information about the Icache, refer to the AMS Operator Manual.

Note: MIB items that are related to ATO rules use the acronym AT. MIB items that are related to ATI rules use the acronym ATI.

Up to 500 ATIR rules and up to 500 ATOR rules can be defined.

Incoming AT Messages

When an incoming AT message arrives at the RTR, it is evaluated by the following rules, in the following order:

1. Incoming AT external condition (ATIX) rules
2. Incoming AT routing (ATIR) rules
3. Incoming AT counting (ATIC) rules

Outgoing AT Messages

When outgoing AT message is ready to leave the RTR, it is evaluated by the following rules, in the following order:

1. Outgoing AT external condition (ATOX) rules
2. Outgoing AT routing (ATOR) rules
3. Outgoing AT counting (ATOC) rules

12.7 AT-AO-Store Routing

In AT-AO-Store routing, if the SMSC NACKs the AO message with a temporary error, the message can fall back to storage in the AMS. The AMS delivery scheme determines when and how often message delivery is retried.

AT-AO-Store routing requires the following licenses:

- AT-AO

- AT-Store
- Store-AO

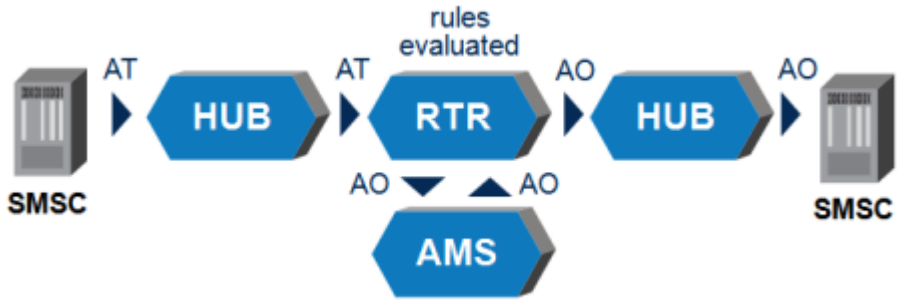


Figure 49: AT-AO-Store

AT-AO-Store routing flows as follows:

1. An inbound AT message arrives at the HUB
2. The HUB sends the AT message to the RTR for rule evaluation
3. The RTR evaluates the ATIR rules for the message, and it matches an AT-AO-Store rule
   a. If the protocol of the incoming AT message does not match the protocol that is accepted by the destination application, the RTR blocks the message with a permanent error and processing of the message stops
   b. If the protocol of the incoming AT message matches the protocol that is accepted by the destination application, the RTR converts the AT message to AO and sends the AO message to the HUB
4. The HUB sends the AO message to the SMSC
5. The SMSC ACKs or NACKs the AO message to the HUB
6. The HUB relays the SMSC's response to the RTR
   a. If the AO message was ACKed, the RTR sends an ACK for the AT message to the HUB (this is the AT-AO routing path) and steps 7, 9, and 10 are omitted from the flow
   b. If the AO message was NACKed with a temporary error, the RTR attempts to store the AO message in the AMS
7. The AMS ACKs or NACKs the storage request
   a. If the storage request was ACKed, the RTR sends an ACK for the AT message to the HUB
   b. If the storage request was NACKed, the RTR sends a NACK for the AT message to the HUB
8. The HUB relays the RTR's response to the AT originator
9. When the delivery scheme indicates that the message should be delivered, the AMS notifies the RTR
10. The RTR sends the message to the SMSC
    a. If the SMSC ACKs the message, the RTR notifies the AMS, which then deletes its internal copy of the message
    b. If the SMSC NACKs the message with a temporary error, the RTR notifies the AMS, which continues to store the message until the next scheduled delivery attempt

The **AMS Queue** parameter in the ATIR rule determines the queue in which the message is stored (and, therefore, the delivery scheme that applies to the message).

Note: This routing path is not supported for CIMD messages.

12.8 AT-Store-AO Routing

In AT-Store-AO routing, the RTR does not perform a first submission attempt of the message. Instead, it immediately sends the message to the AMS for storage. The AMS delivery scheme determines when and how often message delivery is tried.

AT-Store-AO routing requires the following licenses:

- AT-Store
- Store-AO

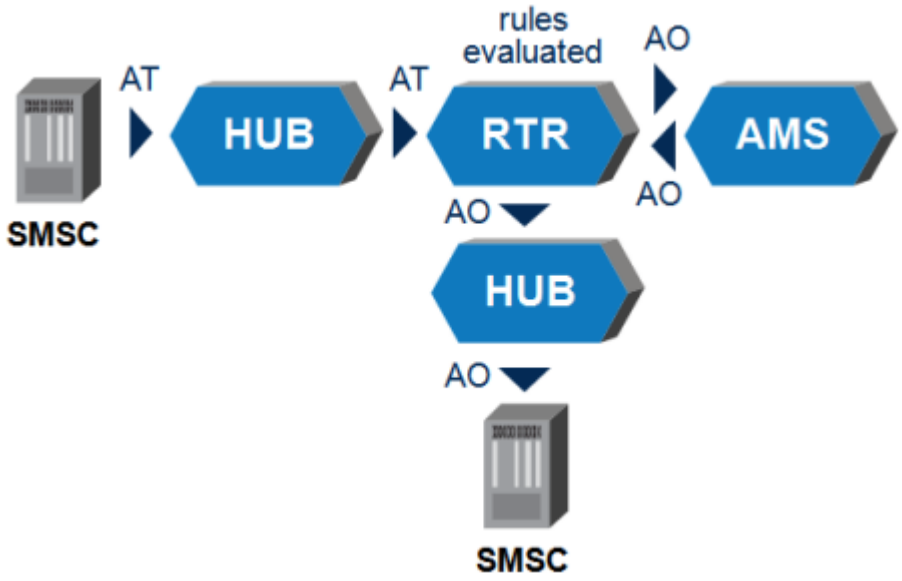


Figure 50: AT-Store-AO

AT-Store-AO routing flows as follows:

1. An inbound AT message arrives at the HUB
2. The HUB sends the AT message to the RTR for rule evaluation
3. The RTR evaluates the ATIR rules for the message, and it matches an AT-Store-AO rule
   a. If the protocol of the incoming AT message does not match the protocol that is accepted by the destination application, the RTR blocks the message with a permanent error and processing of the message stops
   b. If the protocol of the incoming AT message matches the protocol that is accepted by the destination application, the RTR converts the AT message to AO and attempts to store it in the AMS
4. The AMS ACKs or NACKs the storage request

   a. If the storage request was ACKed, the RTR sends an ACK for the AT message to the HUB
   b. If the storage request was NACKed, the RTR sends a NACK for the AT message to the HUB

5. The HUB relays the RTR's response to the AT originator
6. When the delivery scheme indicates that the message should be delivered, the AMS notifies the RTR
7. The RTR sends the message to the SMSC

   a. If the SMSC ACKs the message, the RTR notifies the AMS, which then deletes its internal copy of the message
   b. If the SMSC NACKs the message with a temporary error, the RTR notifies the AMS, which continues to store the message until the next scheduled delivery attempt

The **AMS Queue** parameter in the ATIR rule determines the queue in which the message is stored (and, therefore, the delivery scheme that applies to the message).

Note: This routing path is not supported for CIMD messages.

12.9 ATIR Rule Billing

The ATIR rules can refer to a billing profile that will trigger the generation of CDRs representing the processing of the inbound AT messages. When processing inbound AT traffic, the RTR creates CDRs for an inbound AT message that has been rejected based on the following routing actions:

1. Block with permanent message error
2. Block with permanent recipient error

For more information about the CDR formats that the RTR supports, refer to the Billing Manual.

12.10 AT Outgoing Address Conversion

An outgoing originator address conversion rule set and an outgoing recipient address conversion rule set may be specified for each ATO routing rule.

See *Outgoing Address Conversion* for details of Outgoing Conversion Rules.

12.11 ATOR Rule Billing

The ATOR rules can refer to a billing profile that will be associated to outbound AT messages. The ATOR-based billing profiles that are used to generate CDRs depend on the ATOR routing action and on the message's exact routing path and delivery result(s).

The billing profile for delivery notifications (that is, for internally generated AT Notification) is generally used in all cases where a CDR is generated for an internally generated AT Notification. Otherwise, if the ATOR rule's action is a "block" action, the billing profile for blocked delivery is used. Delivery or non-delivery CDRs, respectively, are created using the billing profile for successful or failed delivery.

If submission CDRs are created after the outbound AT processing, the billing profile for submission will be used.

Note:

1. The billing profile configured for the Blocked Delivery can be used to create the CDRs for the rejected messages due to applied ATO routing rule action (where action is **Block with permanent error**). For getting the desired status value with the ATOR rule applied for AT messages, configure the **Not Delivered Status** field as **Rejected** in the billing profile used for Blocked Delivery.
2. Only the FCDR format will be supported for Rejected CDR generated by RTR.
3. In case of AO-AT routing path, with AT delivery failure, CDR will only be generated when the condition specified in point 1 is met. Otherwise there will be no CDR generated.
4. If AMS is used to perform AT delivery, then no CDR will be generated when the ATOR routing action is set as **Block with temporary error** as in this case message will again be stored in the AMS for the next retry.
5. In case of MO-AT routing path or AO-ST-AT or AO-AT-ST, if the AT message is blocked due to permanent error then the status field in the CDR generated will be "Expired". The only exception is if the condition specified in point 1 is met. In that case status field in the CDR will be set as "Rejected".

For more information about the CDR formats that the RTR supports, refer to the Billing Manual.

12.12 ATIX Rule Set

The RTR evaluates the ATIX rule set so that EC applications can process the inbound AT message. EC processing may include providing extra personalized services, filtering messages.

ATIX rules get evaluated using the logic common to all external condition rule sets (refer to *Rule Evaluation*).

12.12.1 ATIX Rule Failure Action

If the ECI evaluation produces a result of false (after the optional inversion of the corresponding ATIX rule's external condition), then the processing of the sorted list of matching ATIX rules stops and the failure action of the ATIX rule is applied.

The possible failure actions are:

Action	Effect
None	Ignore the false result and continue to process the list of matching ATIX rules, or assume that the message "passed" the ATIX rule evaluation if there are no more matching rules in the list.
Block with temporary error	Leave the ATIX rule evaluation and behave as if an ATIR rule with action "Block with temporary error" had matched.
Block with permanent error	Leave the ATIX rule evaluation and behave as if an ATIR rule with action "Block with permanent error" had matched.

Action	Effect
Block with acknowledgment	Leave the ATIX rule evaluation and behave as if an ATIR rule with action "Block with ACK" had matched.

Note:

CDRs will be generated using the billing profile (if configured) for `Discarded Messages` when the message is discarded due to the application of any of the following failure actions:

1. Discard with permanent error

Only the FCDR format will be supported for generating CDRs for messages discarded by the RTR.

12.13 ATOX Rule Set

The RTR evaluates the ATOX rule set so that EC applications can process the outbound AT message. EC processing may include providing extra personalized services.

ATOX rules get evaluated using the logic common to all external condition rule sets (refer to *Rule Evaluation*).

12.13.1 ATOX Rule Failure Action

If the ECI evaluation produces a result of false (after the optional inversion of the corresponding ATOX rule's external condition), then the processing of the sorted list of matching ATOX rules stops and the failure action of the ATOX rule is applied.

The possible failure actions are:

Action	Effect
None	Ignore the false result and continue to process the list of matching ATOX rules, or assume that the message "passed" the ATOX rule evaluation if there are no more matching rules in the list.
Block with temporary error	Leave the ATOX rule evaluation and behave as if an ATOR rule with action "Block with temporary error" had matched.
Block with permanent error	Leave the ATOX rule evaluation and behave as if an ATOR rule with action "Block with permanent error" had matched.
Block with acknowledgment	Leave the ATOX rule evaluation and behave as if an ATOR rule with action "Block with ACK" had matched.

Note:

CDRs will be generated using the billing profile (if configured) for `Discarded Messages` when the message is discarded due to the application of any of the following failure actions:

1. Discard with permanent error

Only the FCDR format will be supported for generating CDRs for messages discarded by the RTR.

Chapter 13

IGM Routing

Topics:

13.1 Introduction

The RTR implements logic dedicated to the processing of *internally generated SMs*, i.e. short messages that are created by the RTR, and need to be processed and delivered or relayed in some way. Among other capabilities, this logic includes the evaluation of the Internally Generated Message (IGM) rule sets. This chapter describes that logic.

There are three types of IGM rules:

- IGM routing rules (IGMR)
- IGM external condition rules (IGMX)
- IGM counting rules (IGMC)

Note: Even though the logic has been designed to be generic for any kind of internally generated SM, IGM rules are currently **only applied to Auto Reply (ARP) messages** (refer to *Auto Reply Service*).

13.2 IGM Rule Evaluation

The evaluation of the IGM logic on the RTR consists of the following consecutive steps:

1. **SSI Query:** If a Subscriber Service Information (SSI) is available, and if the SSI of the originator or recipient of the IGM are unknown, the RTR issues a query to retrieve the SSI.
2. **SCTS Generation:** The RTR generates a Service Centre Timestamp (SCTS), optionally involving the AMS, for the IGM.
3. **Early SRI-SM:** Under the control of MGR GUI properties (**Routing ➤ Properties**, refer to MGR Operator Manual for more information), an Early SRI-SM query may be issued, primarily in order to retrieve a routing number for the recipient of the IGM.
4. **IGMX Rule Set Evaluation:** The RTR evaluates the IGM External Condition (IGMX) rule set according to the normal rules for evaluating an External Condition Rule set. If this does not reject/discard the IGM, then
5. **CAMEL Charging:** If an EC application (typically, the PBC) requested CAMEL charging, the RTR applies CAMEL charging, using SMSC and MSC parameters as configured through the semi-static configuration parameters *localsmscaddressincameltrigger* and *localmscaddressincameltrigger* respectively. If CAMEL charging does not reject the IGM, then
6. **IGMR Rule Set Evaluation:** The RTR evaluates the IGM Routing rule set, primarily in order to determine how to route the IGM. Additionally, this may associate Billing Profiles with the IGM in order to generate CDRs.
7. **Route IGM:** Route the IGM according to the matching rule's Routing Action.
8. **Post-process IGM:** Evaluate the IGM Counting (IGMC) rule set, complete any pending CAMEL and ECI communication (mostly evolving around real-time charging) and generated CDRs.

13.3 IGM Rule Conditions

The IGM rule sets share the following set of supported rule conditions:

Condition	Format	Description
Time Schedule		This condition does not depend on any parameter of the IGM, it evaluates against the current time (local to the RTR instance) at the moment that the rule set is evaluated.
Originator	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the normalized originator address, if it is categorized as MSISDN[13].
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the normalized MSISDN. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges and/or network ranges. Successful association of the MSISDN with a provisioned mobile network can only happen if mobile number portability for originator is not supported for that network, and if the network and its number range(s)/prefix(es) have been provisioned.
	List	This condition evaluates the normalized MSISDN against a list of MSISDNs, enabling logical OR operation.
Originator SSI		This condition is evaluated against the originator's SSI. It enables you to specify which services the originator must or must not have. If SSI is not used, this condition should not be specified.
Recipient	General	If an early SRI-SM query was executed for the IGM, both the recipient's MSISDN and IMSI may be available.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the normalized recipient address, if it is categorized as MSISDN[13].
	Country	If the recipient's IMSI has been retrieved, this condition is evaluated against the country, as derived from extracting the mobile country code (MCC) from the IMSI. Otherwise, the condition is evaluated against the country, as derived from extracting the E.164 country code from the normalized MSISDN. Successful extraction of the country depends on the provisioned countries.
	Network	If the recipient's IMSI has been retrieved, this condition is evaluated against the mobile network, as derived

[13] While only ARP messages pass through these rules, both the IGM's originator and recipient are expected to always be categorized as MSISDNs.

Condition	Format	Description
		from extracting the mobile network code (MNC) from the IMSI. Otherwise, the condition is evaluated against the network, as derived from matching the normalized MSISDN against the provisioned mobile network number ranges and/or network prefixes. Successful extraction of the mobile network depends on the provisioned mobile networks.
	List	This condition evaluates the normalized MSISDN or IMSI against a list of MSISDNs or IMSIs, enabling logical OR operation.
	Single IMSI, IMSI range or IMSI prefix	This condition is evaluated against the recipient IMSI, if that IMSI has been retrieved prior to the evaluation of the rule set.
Recipient SSI		This condition is evaluated against the recipient's SSI. It enables you to specify which services the recipient must or must not have. If SSI is not used, this condition should not be specified.
User Data		This condition is evaluated against the user data of the IGM.
External Attributes		This condition is evaluated against the external attributes as set by the EC application(s) consulted during the evaluation of the IGMX rule set. Due to the nature of the EC rule set evaluation, this condition is only supported in the IGMR and IGMC rule sets.
XS Message		This condition is evaluated against the XS message type of the IGM. As currently, IGM processing only applies to Auto Reply (ARP) messages, this condition should not be used.
Recipient RN Group		This condition is evaluated against the recipient's Routing Number (RN) group. A routing number can be retrieved by issuing an early SRI-SM query, and routing numbers can only ever be extracted when they were provisioned.
Terminating MSC/SGSN	General	The terminating MSC or SGSN address is only available during rule evaluation after a successful early SRI-SM query. If that query returned both an MSC and an SGSN address the condition is evaluate against the address selected by the semi-static configuration setting `preferredmtdestination` only. **Note:** If the Network configuration is available according to the MSC and/or SGSN (i.e. received in the HLR query), The '**Preferred MT Destination**' in the Network configuration overrides the semi-static

Condition	Format	Description
		attribute '`preferredmtdestination`' for the rules evaluation.
	Single MSISDN, MSISDN range or MSISDN prefix	This condition is evaluated against the MSC or SGSN E.164 number.
	Country	This condition is evaluated against the country, as derived from extracting the E.164 country code from the MS or SGSN address. Successful extraction of the country code depends on the provisioned countries.
	Network	This condition is evaluated against the network, as derived from matching the E.164 address against the provisioned mobile network number ranges and/or network prefixes. Successful association of the MSC or SGSN address with a provisioned mobile network can only happen if the network and its number range(s)/prefix(es) have been provisioned.
	List	This condition evaluates the MSC or SGSN address against a list of E.164 numbers, enabling logical OR operation.

13.4 IGMR Rule Set

The RTR evaluates the IGM Routing (IGMR) rule set to determine how IGMs will be routed. In addition, the evaluation of the IGMR rule set can associate a Billing Profile with the IGM in order to generate CDRs. For information about the circumstances in which the IGMR rule set is evaluated, refer to *IGM Rule Evaluation*.

13.4.1 IGMR Routing Action

The possible routing actions are:

Action	Effect
Discard	Discard the IGM, and do the post-processing as if the message was successfully delivered.
Reject	Discard the IGM, and do the post-processing as if the delivery of the message failed and the message got dropped.
Route to MS	Try to deliver the IGM to a Mobile Station (MS), no fallback upon failure.
Route to MS, Fallback to Storage	Try to deliver the IGM to an MS, or try to store the IGM in the specified AMS queue upon temporary failure of the first MT delivery attempt.
Store for Delivery to MS	Try to store the IGM in the specified AMS queue, such that the AMS takes care of requesting the delivery of the IGM to an MS. Such IGMR rules only match if, at the time of rule evaluation, at least one AMS is available, which

Action	Effect
	indicates the capability for storing messages (as opposed to Icache functionality only).
Route to Application	Try to deliver the IGM as AT to an application. The destination application is determined by the **Application Selection** field: • By Rule: The IGMR needs to specify the destination application. • By Load Balancing Group: The IGMR needs to specify the load balancing group to be used when determining the destination application. Such IGMR rules only match if, at the time of the rule evaluation, the destination application is available, i.e. there are active outside sessions for the destination application(s).
Route To Application, Fallback to Storage	Try to deliver the IGM as AT to an application, or try to store the IGM in the specified AMS queue upon temporary failure of the first AT delivery attempt. The destination application is determined in the same way as it is for the Route to Application action. Such IGMR rules only match if, at the time of the rule evaluation, either the destination application or the AMS is available.
Store for Delivery to Application	Try to store the IGM in the specified AMS queue, such that the AMS takes care of requesting the delivery of the IGM to an application. The destination application is determined in the same way as it is for the Route to Application action. Such IGMR rules only match if, at the time of rule evaluation, at least one AMS is available.
Route to SMSC as AO	Try to forward the IGM as an AO message to an external SMSC. The IGMR needs to specify both the application to use when forwarding the AO message, and the SMSC group to which the IGM is supposed to be forwarded. Such IGMR rules only match if, at the time of rule evaluation, at least one of the SMSCs in the SMSC group is available to receive AO messages from the designated application.
Route to SMSC as AO, Fallback to Storage	Try to forward the IGM as an AO message to an external SMSC, or try to store the IGM in the specified AMS queue upon temporary failure of the first AO forwarding attempt. The IGMR needs to specify both the application to use when forwarding the AO message, and the SMSC group to which the IGM is supposed to be forwarded. Such IGMR rules only match if, at the time of rule evaluation, at least one of the SMSCs in the SMSC group is available to receive AO messages from the designated application, or if at least one AMS is available.
Store for Forwarding to SMSC as AO	Try to store the IGM in the specified AMS queue, such that the AMS takes care of requesting the forwarding of the IGM as AO to an external SMSC. The IGMR needs to specify both the application to use when forwarding the AO message, and the SMSC group to which the IGM is supposed to be forwarded. Such IGMR rules only match if, at the time of rule evaluation, at least one AMS is available.
Route to MS, Fallback to SMSC as AO	Try to deliver the IGM to an MS, or try to forward the IGM as an AO message to an external SMSC upon temporary failure of the first MT delivery attempt. The IGMR needs to specify both the application to use when

Action	Effect
	forwarding the AO message, and the SMSC group to which the IGM is supposed to be forwarded.

If no IGMR rule matches, the IGM processing continues as if an IGMR with Routing Action "Reject" had matched.

Note: When the selected routing action leads to the an MT or AT delivery attempt, the MTOX or ATOX rule set only gets evaluated for IGMs if the semi-static configuration attribute `outboundextcondrulesenabledforigsm` is set to *true*.

13.4.2 IGMR Billing

The IGMR rule set allows associating a billing profile by means of the matching IGMR rule, in order to generate (non-)delivery CDRs during the post-processing of the IGM. CDRs can only be generated for IGMs if the IGM logic evaluates the IGMR rule set for the IGM. If the IGM gets discarded before matching the IGMR rules, no CDRs get created for the IGM.

If the selected routing action leads to the an MT or AT delivery attempt, billing profiles assigned to the IGM by means of a matching MTOR or ATOR rule also trigger the creation of a CDR.

If any billing profile assigned to the IGM is the *default profile*, the default profile designated to IGMs will be used. The default profile for IGM is configured on the MGR through **Billing ➤ Post-paid Billing ➤ Properties ➤ Default Profile For IGM**.

For each IGMR rule, two separate billing profiles can be referred to:

- Billing Profile for Successful Delivery
- Billing Profile for Failed Delivery

Billing Profile for Successful Delivery

This billing profile is used for the following IGMR routing actions:

Routing Action	Remarks
Discard	Use of a billing profile for this routing action may only make sense in rare cases.
Route to Ms or Route to MS, Fallback to Storage	Billing Profile used upon successful MT delivery or MTOR "block with ack" (see *MT Routing*).
Route to Application or Route to Application, Fallback to Storage	Billing Profile used upon successful AT delivery or ATOR "block with ack" (see *AT Routing*).
Route to SMSC as AO or Route to SMSC as AO, Fallback to Storage	Billing Profile used upon successful AO forwarding to an external SMSC as AO. Where possible, the message status in the CDR would indicate "submitted" rather than "delivered".
Route to MS, Fallback to Forwarding to SMSC as AO	Billing Profile used upon successful MT delivery or MTOR "block with ack", or for successful forwarding to an external SMSC as AO.

If the IGM is successfully stored in the AMS, no CDR is generated. Later on, if the IGM gets delivered from the AMS, or if the IGM gets deleted from the AMS, Billing Profiles assigned through IGMR rules are *not* considered. Instead, use billing profiles assigned through the MTOR or ATOR rule set.

If the message is successfully forwarded to an external SMSC as AO, CDRs get created regardless of the use of the Icache (see *IGMR Icache*). If the Icache is in use, and the parameters of an IGM are successfully retrieved from the Icache, the IGMR rules get (re-)evaluated in order to determine the Billing Profile for generating the Final Delivery CDR.

Billing Profile for Failed Delivery

This billing profile is used for the following IGMR routing actions:

Routing Action	Remarks
Reject	Use of a billing profile for this routing action may only make sense in rare cases.
Route to MS	Billing Profile used upon MT delivery failure, or MTOR "block with error" (see *MT Routing*).
Route to MS, Fallback to Storage	Billing Profile used upon permanent MT delivery failure or MTOR "block with permanent error", or upon failure to store the IGM in the AMS.
Store for Delivery to MS, Store for Delivery to Application or Store for Forwarding to SMSC as AO	Billing Profile used upon failure to store the IGM in the AMS.
Route to Application	Billing Profile used upon AT delivery failure, or ATOR "block with error" (see *AT Routing*).
Route to Application, Fallback to Storage	Billing Profile used upon permanent AT delivery failure or ATOR "block with permanent error", or upon failure to store the IGM in the AMS.
Route to SMSC as AO	Billing Profile used upon AO forwarding failure.
Route to SMSC as AO, Fallback to Storage	Billing Profile used upon temporary AO forwarding failure, or upon failure to store the IGM in the AMS.
Route to MS, Fallback to Forwarding to SMSC as AO	Billing Profile used upon permanent MT delivery failure or MTOR "block with permanent error", or upon failure to forward the IGM to an external SMSC.

13.4.3 IGMR Icache

The Icache functionality is designed to enable *charging on delivery*, while the message (IGM) is delivered by some external SMSC. This functionality depends on the availability of one or more AMS nodes with Icache capability. For more information about Icache, refer to the AMS Operator Manual.

The Icache functionality is supported for IGMs that are successfully forwarded to an external SMSC as AO. To use this functionality, it must be turned on explicitly for IGMs in the MGR GUI (**Storage ➤ Intermediate Cache ➤ IGM Intermediate Cache Support**). For more information about this setting, refer to the MGR Operator Manual.

When creating Final Delivery CDRs, the IGMR rule set gets (re-)evaluated (refer to *IGMR Billing* for more information).

13.5 IGMX Rule Set

The IGMX rule set enables the following functionality:

- Real-time charging (using the PBC)
- Message screening/filtering (using the FAF)
- Providing extra (personalized) services.

IGMX rules get evaluated using the logic common to all external condition rule sets (refer to *Rule Evaluation*).

For information about the circumstances in which the IGMX rule set is evaluated, refer to *IGM Rule Evaluation*.

13.5.1 IGMX Failure Action

If the ECI evaluation produces a result of false (after the optional inversion of the corresponding IGMX rule's external condition), then the processing of the sorted list of matching IGMX rules stops and the failure action of the IGMX rule is applied.

Possible failure actions are:

Action	Effect
None	Ignore the false result and continue to process the list of matching IGMX rules, or assume that the message "passed" the IGMX rule evaluation if there are no more matching rules in the list.
Reject	Leave the IGMX rule evaluation and proceed with the post-processing for the IGM, indicating that the message was not delivered, i.e. dropped.
Discard	Leave the IGMX rule evaluation and proceed with the post-processing for the IGM, indicating that the message was "delivered successfully".

13.6 IGMC Rule Set

The IGMC rule set is evaluated in order to generate statistics about the routing of IGMs. Each IGMC rule has a set of per-routing result counters in addition to the "total rules matched" counter (igmCntRuleMatchedCounter).

The IGMC rules have the same conditions as the IGMR rules.

Chapter 14

IMS Routing

Topics:

14.1 Introduction

The RTR and the IIW work in conjunction to provide IPSMGW functionality. The IPSMGW can be deployed in three ways:

Integrated IPSMGW

Integrated IPSMGW acts as a gateway between IMS domain and SS7 domain and provides ability to receive text messages from IMS domain and deliver text messages to subscriber in the IMS domain. It is tightly coupled with other components like RTR, AMS, and HUB. It supports all the paths for IMS Originating messages as supported for Mobile Originated messages. It provides transport level interworking.

Stand-Alone IPSMGW

Stand-Alone IPSMGW acts as a gateway between IMS domain and SS7 domain and provides ability to receive text messages from IMS domain and deliver text messages to subscriber in the IMS domain. It can be deployed as a separate server in operator's network and can be integrated with the existing "SMS Network" product to seamlessly enable SIP-based messaging. It is logically located between the legacy SMSC domain and the IP Multi-media Subsystem (IMS) Domain. Apart from text, it also supports Registration, Subscribe and Notify. It provides transport level interworking

Service Level Interworking with Krypton

IPSM-GW can be deployed with Krypton to provide ability to deliver messages to recipient not registered in IMS domain. It also allows to deliver messages originated from SS7 domain to subscriber in IMS domain. Messages are exchanged with Krypton using Service level interworking. In the current release only simple text messages as supported.

14.2 Integrated IPSM-GW

14.2.1 Rule Evaluation for IMS Messages

The Existing Mobile Originated and Mobile Terminated Outgoing rules are applied on IMS Originated and IMS Terminated messages respectively.

14.2.1.1 Rule Evaluation for IMS Originated Messages

IMS Originated Messages are handled similarly to an MO-ForwardSM, applying the MOX/MOR/MOC rules.

14.2.1.2 Rule Evaluation for IMS Terminated Messages

Existing MTOX/MTOR/MTOC rules can be applied on IMS Terminated messages.

14.2.2 IMS Originated Routing Paths

SIP Originated (SIPO) routing is the generic name for the processing of incoming IMS Originated messages. The IIW works in conjunction with the RTR and, in the case of routing with storage, the AMS to route SIPO messages to their destinations. The IMS Originated message handling requires MO-MO 3G routing path license.

Supported SIPO routing paths are:

- SIPO-MT (route to mobile station)
- SIPO-MO (route to SS7 SMSC)
- SIPO-MT-MO (route to mobile station, fall back to SS7 SMSC)
- SIPO-MT-AO (route to mobile station, fall back to SMSC)
- SIPO-MT-AT (route to mobile station, fall back to application)
- SIPO-AT (route to application)
- SIPO-Store-AT (store for delivery to application)
- SIPO-AT-Store (route to application, fallback to storage)
- SIPO-MT-Store (route to mobile station, fall back to storage)
- SIPO-Store-MT (store for delivery to mobile station)
- SIPO-AO (route to SMSC as AO)
- SIPO-Discard
  - Discard with NACK
  - Discard with ACK

For more information about SIPO routing paths, please refer to the IIW Operator Manual.

14.2.3 IMS Terminated Routing Paths

The RTR and IIW work in conjunction to route IMS Terminated messages to their destinations. In the case of routing with storage, the AMS acts as a message store.

The delivery to IMS domain requires the license for the MT-MT 3G routing path.

The IMS Terminated Routing supports the following domains:

- Delivery to IMS Domain
  - SIPO-SIPT
  - AO-SIPT
  - MT-SIPT
- Delivery to IMS Domain with fall back to SS7 Domain
  - MO-SIPT-MT
  - SIPO-SIPT-MT

  When the Mobile Messaging system includes an AMS, the system can provide SIPO-SIPT-Store or

  MO-SIPT-Store (route to the UE's in the IMS domain, fall back to storage) routing.

  Important: In case of fall back to storage, the message is sent by the RTR to the Message Store (AMS) before even attempting an FDA to the UE in IMS domain. Here, the message is not stored in the AMS database but it is placed in the appropriate message queue; then, the AMS immediately

sends an acknowledgement to the RTR and then sends the message back to the RTR to perform the FDA. If the FDA is successful, the RTR generates a billing record (CDR); otherwise the routing result is returned to the AMS for storing it in the database for later retries.

14.2.3.1 Delivery to IMS Domain

SIPO-SIPT

When the recipient mobile network domain is '`IMS only`', then:

- The RTR forwards the message to the IIW to perform a first delivery attempt (FDA) to the recipient in the IMS domain.
- If the delivery attempt is successful, a billing record can optionally be generated.
- If the delivery fails in the IMS domain with a temporary error, the message can fall back to the storage in the AMS. The AMS delivery scheme determines when and how often the message delivery is retried.

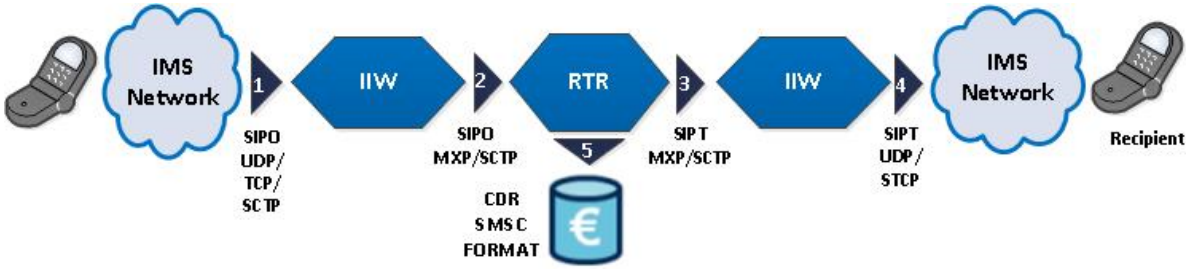


Figure 51: Sample Flow (SIPO-SIPT Scenario)

AO-SIPT

The AO-SIPT routing flows as follows:

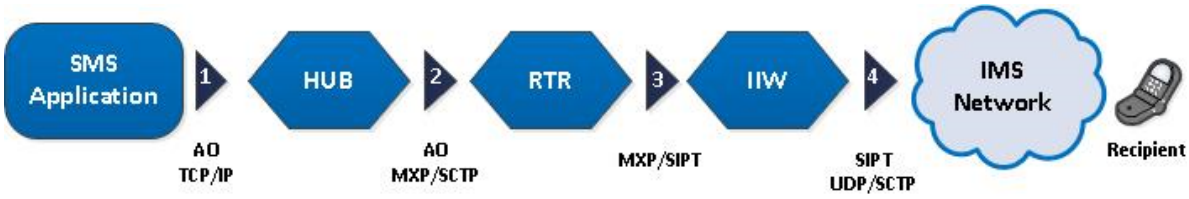


Figure 52: Sample Flow (AO-SIPT Scenario)

1. The Application submits the Short Message using SMPP/UCP/CIMD, which arrives in the Integrated IPSM-GW via the HUB.
2. The Integrated IPSM-GW determines the Recipient Network Mobile Domain as specified in the section Mobile Network Domain Selection.
3. If the domain is IMS, the RTR forwards the message to the IIW to perform a delivery attempt to the recipient using the IMS domain.
4. The IIW delivers the message to the IMS domain.
   a. If the delivery attempt is successful, a billing record can optionally be generated.
   b. If the delivery attempt is not successful, the message is dropped and the originator can receive a message delivery status, depending on the configuration.

Note: In above scenario if early HLR query is configured for AO/SM (see Routing➤Properties Early SRI-SM for AO/SM Whitelist and Early SRI-SM for AO/SM in MGR), then early recipient query is sent to HLR irrespective of Recipient Mobile Network Domain. MT delivery is attempted in SS7 domain.

MT-SIPT

The MT-SIPT Routing path allows the capability to receive the messages from a foreign subscriber in the 2G/3G network and deliver it to an own subscriber in IMS/4G network.

In this routing path, message from foreign SMSC is home routed to RTR. RTR, via IIW, delivers the message in the IMS domain.

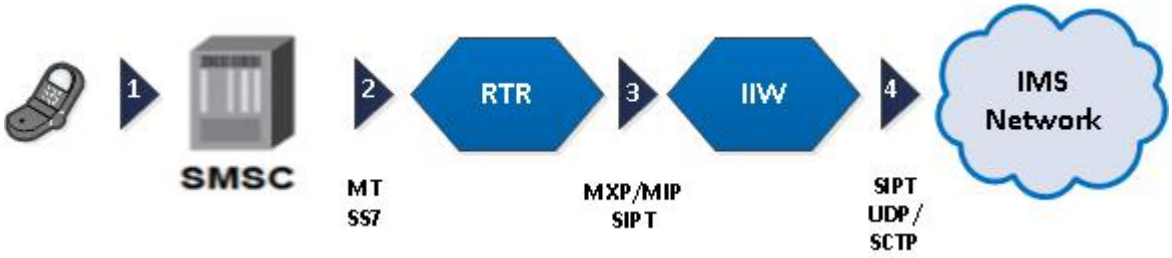


Figure 53: Sample Flow (MT-SIPT Scenario)

1. The message arrives at SMSC from the subscriber in the 2G/3G network.
2. The SMSC forwards the message to RTR via the MT and SS7 interface.
3. The RTR forwards the message to IIW for further delivery, via internal MXP and MIP interface.
4. The IIW forwards the message to IMS network via the SIP network. The CSCF will perform delivery retries of the message and generate a billing record when the message is delivered.

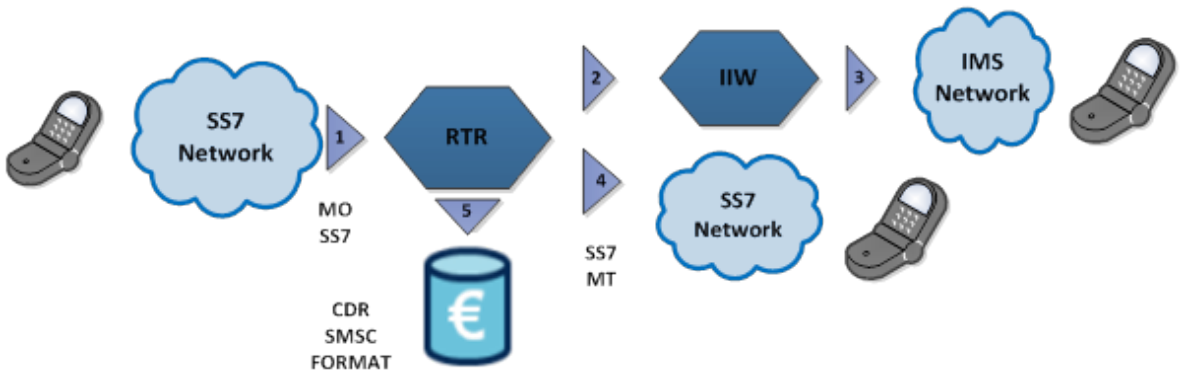
14.2.3.2 Delivery to IMS Domain with Fall Back to SS7 Domain

MO-SIPT-MT

When the recipient mobile network domain is '`IMS then SS7`', then:

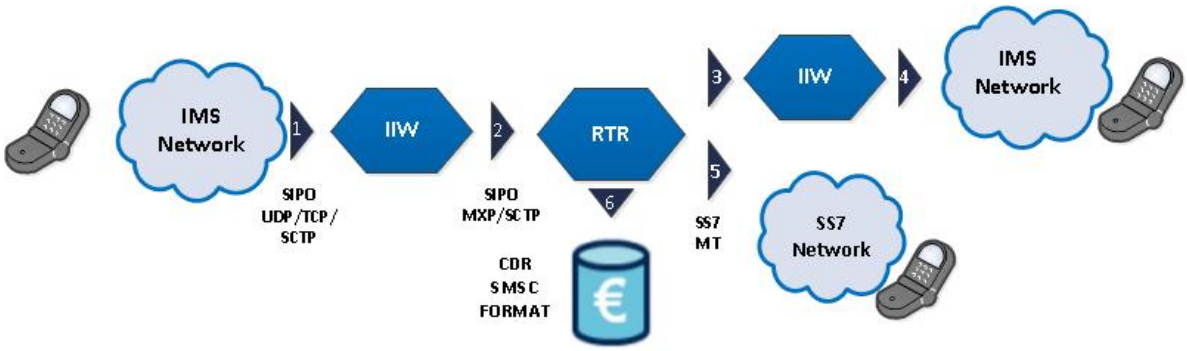
- The RTR forwards the message to the IIW to perform a FDA to the recipient in the IMS domain.
- If the delivery attempt is successful, then IIW informs the RTR about the status of the delivery attempt, and RTR generates billing record if configured.
- If the delivery attempt is not successful, then IIW informs the RTR about the status of the delivery attempt, and RTR falls back to the SS7 domain.
- The RTR performs a first delivery attempt (FDA) to the recipient via the SS7 domain.
- If the delivery attempt is successful, then IIW informs the RTR about the status of the delivery attempt, and RTR generates billing record if configured.
- If delivery fails in both IMS and SS7 domain, then the error class and error result calculation are based of the 'last error' i.e. on fallback to SS7 the RTR will present SS7 outcome to the other components.
- If the delivery fails in both IMS and SS7 domain and the error is a temporary error, the message can fall back to storage in the AMS. The AMS delivery scheme determines when and how often the message delivery is retried.

Sample flow (MO-SIPT-MT scenario)



SIPO-SIPT-MT

The routing flow is as follows:



1. The message arrives at the IIW via the IMS network.
2. The IIW parses the SIP message and forwards it to the RTR via the internal MXP interface.
3. The RTR determines the Recipient Network Mobile Domain as specified in the section Mobile Network Domain Selection. If the domain is IMS fallback to SS7, the RTR forwards the message to the IIW.
4. The IIW performs the FDA to the recipient in the IMS domain, which in the above diagram is a UE.
   a. If the delivery attempt is successful, then IIW informs the RTR about the status of the delivery attempt, and RTR generates billing record if configured.
   b. If the delivery attempt is not successful, then IIW informs the RTR about the status of the delivery attempt, and RTR falls back to the SS7 domain.
5. The RTR performs a FDA to the recipient via SS7 domain, which in the above diagram is a mobile phone.
6. If the delivery attempt is successful, then IIW informs the RTR about the status of the delivery attempt, and RTR generates billing record if configured.
7. If the delivery attempt is not successful, the message is dropped and the originator can receive a message delivery status, depending on the configuration. If the delivery fails in both IMS and SS7 domain and the error is a temporary error, the message can fall back to storage in the AMS. The AMS delivery scheme determines when and how often the message delivery is retried.

Note:

- SIPO-SIPT-MT messages are subject to MO and MTO routing rules. The same rules apply to MO-SIPT-MT as well.
- The RTR maintains separate MT Queues for IMS and SS7 delivery. In case, some segments of a message end up in different queues, then out of order delivery of messages can occur on SS7.

14.2.4 IMS Billing

14.2.4.1 IMS Originated Messages Billing

The system supports both CDR and Real-time billing for IMS Originated messages. To identify IMS Originated messages coming from the home network, the system supports following parameters

- `pseudoOriginatingAddress`: Pseudo A-Party MSC address
- `pseudoOriginatingPointCode`: Pseudo A-Party MSC Point Code

For IMS Originated messages, the FCDR fields `ogtiAddress` and `ogtiAddressGSM` (if included in the FCDR) would be set to the configured pseudo A-party MSC Address.

Also the `origPointCode` field (if included in the CDR) would be set to a configured pseudo A-party MSC Point Code.

For IMS Originated messages, the FCDR fields `originatorPaniUE`, `originatorPaniNP` and `originatorPcni` (if included in the FCDR billing profile) would be set to the received values of the originator `P-Access-Network-Info` (User-Equipment provided header and Network-Provided header) and originator `P-Cellular-Network-Info` header in the message.

The IIW module parses the last occurrence of the received originator `P-Access-Network-Info` (User-Equipment and Network-Provided) and originator `P-Cellular-Network-Info` header and sends it over to the RTR for capturing in the generated FCDR.

Note:

1. For more details on the parsing of the received originator `P-Access-Network-Info` (User-Equipment and Network-Provided) and originator `P-Cellular-Network-Info` header, refer to IIW Operator Manual.
2. These new fields are applicable only on the Transport Level Interworking.

Billing programs can use these CDR Fields to recognize IMS Originated messages. This will accomplish two things:

1. Prevent the billing program from applying roaming charges to the A-party.
2. Allow the billing program to apply any special processing to IMS Originated text messages.

The configured Pseudo A-Party MSC Address can also be used in Diameter Charging Requests sent by the PBC. The back-end systems can recognize them and calculate the charges correctly.

14.2.4.2 IMS Terminated Messages Billing

The system supports both CDR and Real-time billing for IMS Terminated messages. To identify IMS Terminated messages delivered to the home network, the system supports two parameters:

- `pseudoTerminatingMscAddress`: Pseudo B-Party MSC address
- `pseudoTerminatingMscPointCode`: Pseudo B-Party MSC Point Code

For IMS Terminated messages, the FCDR fields `dgtiAddress` and `dgtiAddressGSM` (if included in the CDR) would be set to the configured pseudo B-party MSC Address.

Also the `destPointCode` field (if included in the FCDR) would be set to a configured pseudo B-party MSC Point Code.

For IMS Terminated messages, the FCDR field `recipientPaniNp` (if included in the FCDR billing profile) would be set to the received values of the `P-Access-Network-Info` header in the received 200 OK message from network for delivery or from the SIP message containing the delivery report in response to the delivered IMS Terminating messages (SIPT).

The IIW module parses the last occurrence of the recipient `P-Access-Network-Info` header and send it over to the RTR for capturing in the generated FCDR. The recipient `P-Access-Network-Info` header is included in the FCDR only if the message is successfully delivered in IMS network.

Note:

1. For more details on the parsing of the received recipient `P-Access-Network-Info` header, refer to the IIW Operator Manual.
2. These new fields are applicable only on the Transport Level Interworking.

14.3 Stand-Alone IPSM-GW

14.3.1 Rule Evaluation for IMS Messages

The Existing Mobile Originated and Mobile Terminated Outgoing rules are applied on IMS Originated and IMS Terminated messages respectively.

Rule Evaluation for IMS Originated Message s

IMS Originated Messages are handled similarly to an MO-ForwardSM, applying the MOX/MOR/MOC

rules. The Operator should use the below conditions to distinguish between GSM Originated and IMS Originated messages:

- Originating MSC Address: The Originating MSC address for IMS Originating messages is the pseudo MSC address that is provisioned in the IIW semi-static configuration file.
- Originating MSC Point Code: The Originating MSC Point Code for IMS Originating messages is the pseudo MSC Point Code that is provisioned in the IIW semi-static configuration file.

Rule Evaluation for IMS Terminated Messages

Existing MTOX/MTOR/MTOC rules can be applied on IMS Terminated messages. The Operator should use the below conditions in MTO rules to distinguish between GSM Terminated and IMS Terminated messages.

- Terminating MSC Address: The Terminating MSC Address for IMS Terminated messages is the pseudo Terminating MSC Address that is provisioned in the RTR semi-static file.
- Terminating MSC Point Code: The Terminating MSC Point Code for IMS Terminated messages is the pseudo Terminating MSC Point Code that is provisioned in the RTR semi-static file.

14.3.2 IMS Originated Routing Paths

Stand-Alone IPSM-GW is deployed between Legacy SMSC and IMS network, so it supports only one routing path SIPO-MO.

Note : For more information about routing paths, please refer to the IIW Operator Manual.

14.3.3 IMS Terminated Routing Paths

Stand-Alone IPSM-GW is deployed between Legacy SMSC and IMS network, so it supports only one path on Terminating side: MT-SIPT.

Note: For more information about SIPT routing paths, please refer to the IIW Operator Manual.

14.3.4 IMS Billing

IMS Originated Messages Billing

Please refer to Section : *IMS Originated Messages Billing*

IMS Terminated Messages Billing

Please refer to Section: *IMS Terminated Messages Billing*

14.4 IPSM-GW Service Level Interworking with RCS Server

14.4.1 IPSM-GW Service Level Interworking with RCS Server

SERVICE LEVEL INTERWORKING is a termination side function.Unlike TRANSPORT LEVEL (which transport SMS-over-IP originations to the SMSC), SERVICE LEVEL is invoked by either an RCS Application Server or an SMSC after the origination function has been completed and the termination function needs to be executed.

Since it is on terminating side so SIPT will be used as generic term for messages incoming from RCS Server. The Existing Mobile Terminated Incoming and Mobile Terminated Outgoing rules are applied on Incoming RCS Server and Outgoing RCS Server messages respectively.

Rule Evaluation for incoming RCS Server Messages

Incoming RCS Server Messages are handled similarly to an MT-Incoming, applying the MTIX/MTIR/MTIC rules. The Operator should use the below conditions to distinguish between GSM Originated and RCS Server Originated messages:

- Originating SMSC Address: The Originating SMSC address for incoming RCS Server messages is the pseudo SMSC address that is provisioned in the IIW semi-static configuration file.
- Originating SMSC Point Code: The Originating SMSC Point Code for incoming RCS Server messages is the pseudo SMSC Point Code that is provisioned in the IIW semi-static configuration file.

Rule Evaluation for Outgoing RCS Server Messages

Existing MTOX/MTOR/MTOC rules can be applied on outgoing RCS Server messages. The Operator should use the below conditions in MTO rules to distinguish between GSM Terminated and RCS Terminated messages.

- Terminating MSC Address: The Terminating MSC Address for outgoing RCS Server messages is the pseudo Terminating MSC Address that is provisioned in the RTR semi-static file.
- Terminating MSC Point Code: The Terminating MSC Point Code for outgoing RCS Server messages is the pseudo Terminating MSC Point Code that is provisioned in the RTR semi-static file.

14.4.2 Incoming RCS Server message Routing Paths

RTR and IIW process incoming RCS Server messages and routes them to their destination.

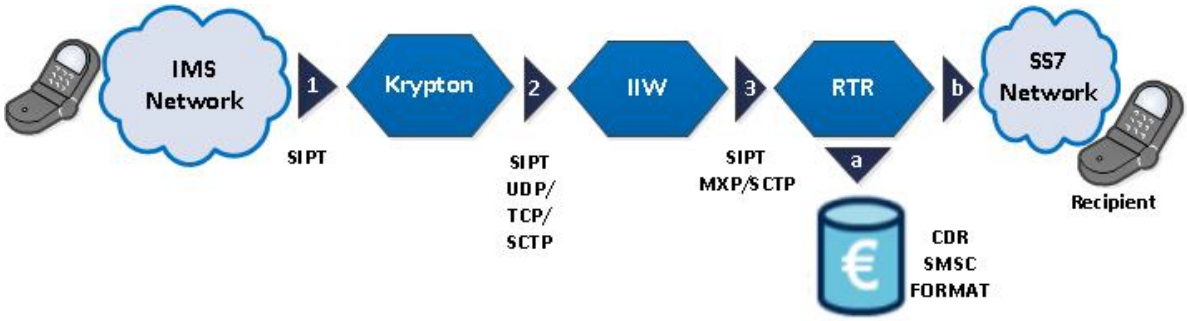
The following paths are supported for messages incoming from RCS Server:

- SIPT-MT (route to mobile station)
- SIPT-AO (route to SMSC as AO)
- SIPT-AT (route to application)

SIPT-MT

The IIW, in conjunction with RTR supports the standard configuration of SIPT-MT. The IIW can be deployed to receive the messages from Krypton and deliver it to subscriber in 2G/3G network. In this routing path, the IIW processes incoming SIPT messages and routes them to SS7 network.

The SIPT-MT routing flow is as follows:



1. The Krypton receives message from UE.
2. The Krypton sends the message to IIW via UDP, TCP or SCTP interface.
3. The IIW parses the SIP message and forwards it to the RTR via the internal MXP interface. Immediately, the RTR performs a first delivery attempt (FDA) to the recipient, which in the above diagram is a mobile phone.
   a. If the delivery attempt is successful, a billing record can optionally be generated.
   b. If the delivery attempt is not successful, the message is dropped and the originator can receive a 'message not sent' message, depending on the configuration.

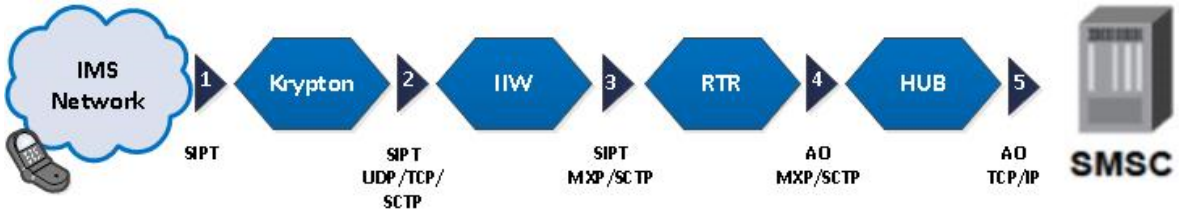
Note: SERVICE LEVEL INTERWORKING is a termination side function so term SIPT is used for messages incoming from Krypton.

SIPT-AO

The IIW, in conjunction with RTR and HUB, supports the configuration of SIPT-AO. In this routing path, the IIW can be deployed to receive IMS-terminated (SIPT) messages from Krypton are forwarded

as Application-originated (AO) messages to a service centre or to a message gateway that accepts AO messages.

The SIPT-AO routing flow is as follows:

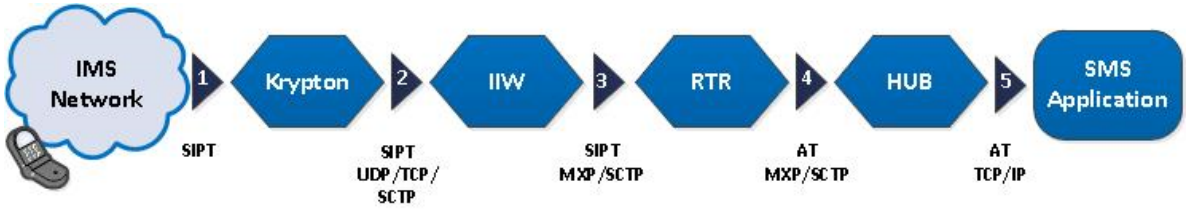


1. The message arrives at the Krypton via the IMS network via SIPT interface.
2. The Krypton sends the SIPT message to IIW via UDP, TCP or SCTP interface.
3. The IIW parses the message and forwards it to the RTR via the internal MXP interface.
4. The RTR forwards the message to HUB through AO interface.
5. The HUB forwards the message as an AO message to the SMSC using SMPP/CIMD/UCP over TCP/IP.

SIPT-AT

The IIW, in conjunction with RTR and HUB, supports the configuration of SIPT-AT. In this routing path, the IIW processes incoming IMS-terminated (SIPT) messages from Krypton and routes them to routes them to towards SMS application.

The SIPT-AT routing flow is as follows:



1. The message arrives at the Krypton via the IMS network via SIPT interface.
2. The Krypton sends the SIPT message to IIW via UDP, TCP or SCTP interface.
3. The IIW parses the message and forwards it to the RTR via the internal MXP interface.
4. The RTR forwards the message to HUB through AT interface.
5. The HUB forwards the message as an AT message to the SMS Application using SMPP/CIMD/UCP over TCP/IP.

Note: All the routing paths in transport-level interworking also apply for service-level Interworking.

14.4.3 Long message Support

IPSM-GW supports delivery of long messages received by service level interworking from Krypton. The IPSM-GW divides the messages in small segments, depending on maximum data that can be copied in one message. The IPSM-GW supports long message delivery in following scenarios:

RCS to CS Long Message Handling

The IPSM-GW supports long message delivery from RCS Server to CS. It receives long messages from the server and delivers them to CS.

IPSM-GW performs following actions bases on the content length of the SIP MESSAGE:

- If the RCS Server sends the SIP MESSAGE with “charset=us-ascii”, then the IPSM-GW allows the content up to 640 bytes. However, if the length of the content is more than 640 bytes, then the IPSM-GW rejects that message and displays “413 Request too Large” error result code.
- If the RCS Server sends the SIP MESSAGE has “charset” other than “us-ascii”, then the IPSM-GW allows the total content length upto 320 bytes. However, if the total length is longer than 320 bytes, then the IPSM-GW rejects that message and displays “413 Request too Large” error result code.

In both the above scenarios, if the RCS Server sends the SIP MESSAGE with length more than 160 bytes for “charset=us-ascii”, or more than 70 bytes for “non us-ascii”, then the IPSM-GW performs the following steps:

1. Segment the text message depending on maximum data that can be copied in one message.
2. For each segment
    a. Prepare MT-FSM
    b. Add Concatenated message User Data Header
    c. Set More message to send
    d. Deliver the segment to MS

Note: If any of the segment delivery fails to reach CS, then complete delivery will be treated as failed.

RCS Server to AO Long Message Handling

The IPSM-GW supports long message delivery from RCS Server to AO. If message length of the SIP MESSAGE sent by RCS Server is more than 160 for “charset=us-ascii” or more than 70 for “non ascii”, then IPSM-GW forward the complete text as a single message to AO.

CS to RCS Server Long Message Handling

In the network, there can be multiple IIWs and RTRs that support long message delivery from CS to RCS Server. There is a possibility that the concatenated message segments can arrive on different RTR and also forwarded to different IIW. As a result, the IPSM-GW might not be able to following tasks:

- Combine all the segments and send one long message to RCS Server
- Send Segments in correct order

To manage this situation, RTR supports a new semi-static configuration parameter `rtrdeliverconcatmessagetorcs`.

- If ` rtrdeliverconcatmessagetorcs ` is set to false, RTR shall force SS7 delivery of concatenated messages regardless of whether recipient domain is RCS.
- If ` rtrdeliverconcatmessagetorcs ` is set to true, RTR shall deliver concatenated messages to RCS Server if recipient domain is RCS.

Note: It is recommended to keep the value for ‘rtrdeliverconcatmessagetorcs’ parameter as false (which is default value), so that the concatenated messages are delivered via SS7 domain. In case, the value for ‘rtrdeliverconcatmessagetorcs’ parameter is true, then following issues might occur:

- Since system cannot enforce correct ordering of segments, individual segments may be sent to RCS Server in random order.
- RCS Server will not be able to identify User Data Header for Concatenation in `text/plain`.

14.4.4 Krypton Billing

Incoming RCS Server Messages Billing

The system supports CDR billing for incoming RCS Server messages. To identify incoming RCS Server messages coming from the home network, the system supports following parameters

- pseudoOriginatingAddress: Pseudo A-Party SMSC address

For incoming RCS Server messages, the FCDR field's ogtiAddress and ogtiAddressGSM (if included in the CDR) would be set to the configured pseudo A-party SMSC Address.

Billing programs can use these CDR Fields to recognize incoming RCS Server messages. This will accomplish two things:

1. Prevent the billing program from applying roaming charges to the A-party.
2. Allow the billing program to apply any special processing to incoming RCS Server incoming text messages.

Note : The configured Pseudo A-Party SMSC Address can also be used in Diameter Charging Requests sent by the PBC. The back-end systems can recognize them and avoid the real-time Billing.

14.5 Mobile Network Domain Selection

14.5.1 Integrated IPSM-GW

The Mobile-Terminated messages can be delivered to either SS7 domain or IMS domain. The supported options are:

- Delivery to SS7 domain (Mobile-Terminated messages are delivered to UE via GSM network)
- Delivery to IMS domain (Mobile-Terminated messages are delivered to UE via IMS network)
- Delivery to IMS domain fall back to SS7 domain (Mobile-Terminated message are first attempted on IMS network. If delivery fails then delivery is re-attempted in GSM network)

To configure domain for recipient mobile network, the operator can apply either of the below methods:

- Configure domain through semi-static file
- Configure domain through LDAP Database Lookup Domain Information query
- Configure domain through selection MTOR rule

If all the above options are provisioned, the default domain (from semi-static configuration file) superseded by domain from LDAP Query (caused by MTOX rule) is superseded by domain in MTOR Rule.

14.5.1.1 Configure the Domain via Semi-static File

The operator can configure the default domain in the Semi-Static Configuration file via the following parameters:

- `rtrdefaultdomainselection`

  This parameter is used to set delivery domain for the SS7 Originated traffic.

- `rtrdefaultdomainfor4goriginatedmessage`

  This parameter is used to set delivery domain for the IMS originated traffic.

14.5.1.2 Configure the Domain Selection via LDAP Database Lookup Domain Information Query

The domain information can be provisioned on the LDAP server. IPSM-GW can retrieve this information via PBC. The following configuration must be performed to retrieve domain information via LDAP:

1. The operator must maintain a LDAP database with the domain information for each recipient. The domain can be:
   a. SS7 only
   b. IMS only
   c. IMS then SS7
2. The MTOX rules must be provisioned on the RTR to send ECI requests to the PBC.
3. The PBC must be configured to fetch the recipient mobile network domain from the LDAP database and send this information back in the ECI evaluation response. Refer to the PBC Operator Manual for details.

If the system is configured as per above, the RTR will send the ECI evaluation request to the PBC. The PBC will retrieve the recipient mobile network domain information using a LDAP Query. The RTR will record the recipient mobile network domain received from the PBC in the ECI evaluation response.

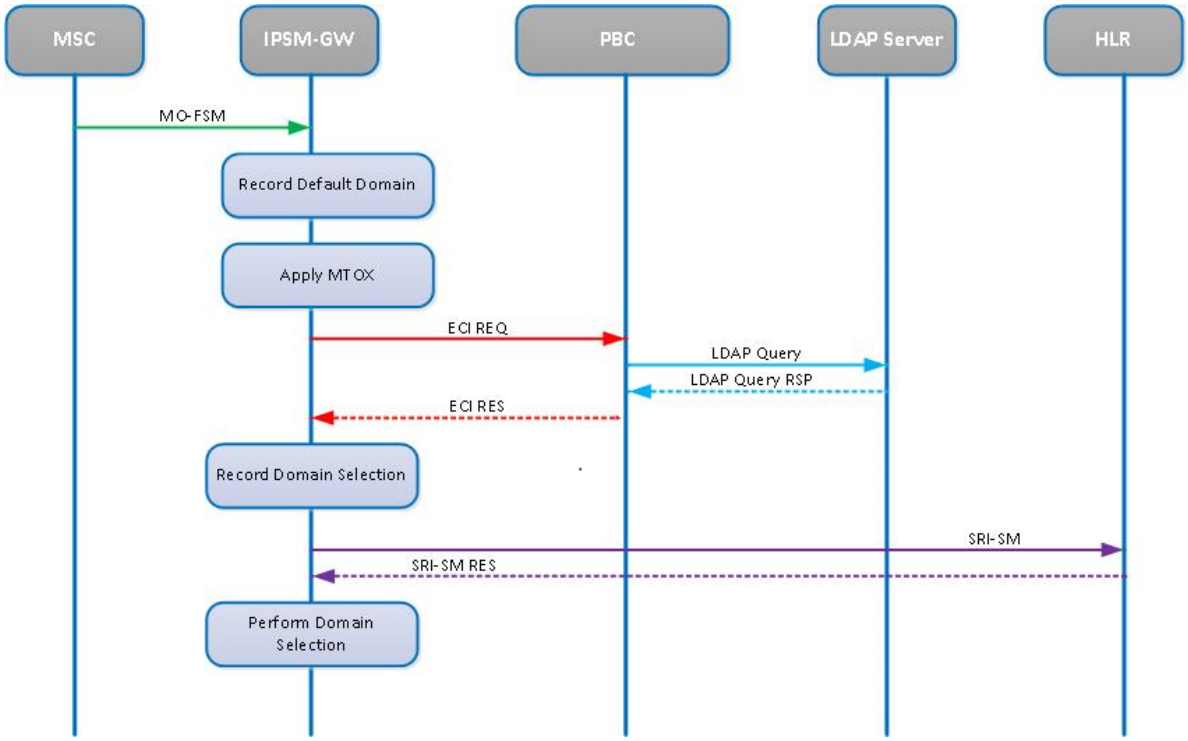


Figure 54: Mobile Domain via PBC and LDAP Server

14.5.1.3 Configure the Domain Selection via MTOR Rule

IPSM-GW supports Recipient Domain Selection via MTOR Rules. The MTOR rules contain the **Mobile domain** parameter which indicates the recipient domain.

The **Mobile Domain** supports the following values:

- No Change
- IMS Domain
- IMS Then SS7 Domain
- SS7 Domain

Important Considerations:

- The default value of Mobile Domain will be **No Change**.
- If the Domain Selection License is disabled, the **Mobile Domain** will not be visible in the MTOR rules on the MGR GUI.
- If the Domain Selection License is disabled, `tp_walk/tp_set` on the Mobile domain oid will give the value as **noChange**.
- If the Domain Selection License is enabled, `tp_walk/tp_set` on the Mobile domain oid will give the value same as provisioned on the **MGR GUI ➤ Routing ➤ MTOR ➤ Mobile Domain**.

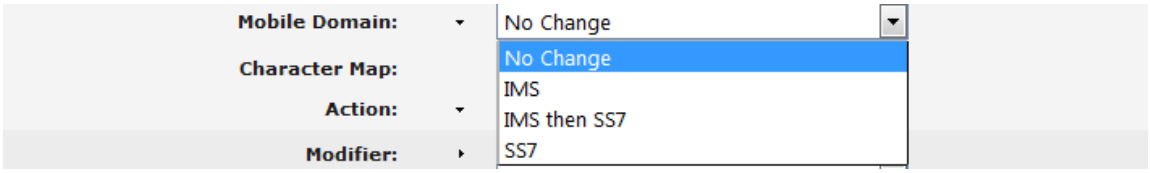


Figure 55: MTOR Rule Mobile Domain

Note :

If the matching MTOR rule has Mobile Domain as '**No Change**', then the Recipient Domain determined using LDAP Query (if performed) will be used for Delivery. If the LDAP query was not performed, the global default domain will be used.

14.5.1.4 Domain Selection Scenarios

14.5.1.4.1 MT Delivery Scenario

The domain can be configured at the following places:

1. Default domain
2. MTOX on SRISM (via LDAP Query)
3. MTOR (parameter **Mobile Domain**) on SRISM
4. MTOX on MTFSM (via LDAP Query)
5. MTOR (parameter **Mobile Domain**) on MTFSM

During message processing the domain is recorded at these places (in the same order as above 1-2-3-4-5).

The final recorded domain is the selected domain.

The figure below highlights places where domain value is recorded and applied.

Note:

1. The flow in the figure below is MO-SIPT **fallback to SS7**.
2. Similar order applies to AO, SIPO and Store to MT delivery.

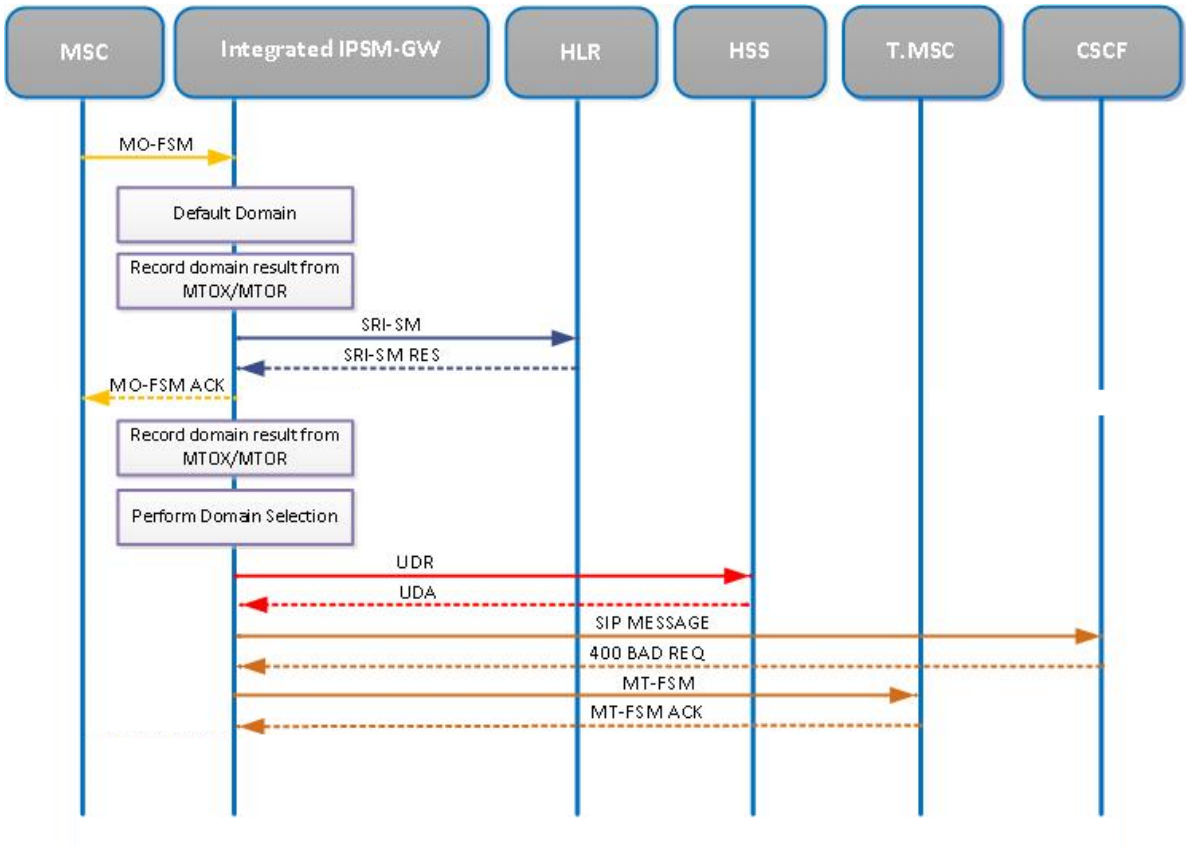


Figure 56: Domain Selection Mechanism in Case MTFSM

14.5.1.4.2 Home Routed Scenario

The domain result is recorded in the following order for delivery from external SMSC scenario, however it is only applied at the time of sending MTFSM.

1. Default domain
2. MTOX (via LDAP Query) on SRISM
3. MTOR (parameter **Mobile Domain**) on SRISM
4. MTOX (via LDAP query) on SRISM Response
5. MTOR (parameter **Mobile Doman**) on SRISM Response
6. MTOX (via LDAP query) on MTFSM
7. MTOR (parameter **Mobile Domain**) on MTFSM

During message processing the domain is recorded at these places (in the same order as above 1-2-3-4-5-6-7).

The final recorded domain is the selected domain.

The figure below highlights places where domain value is recorded and applied.

Note:

1. The flow in the figure below is MT-SIPT **fallback to SS7**.
2. Similar order applies to AT and Store to MT delivery.

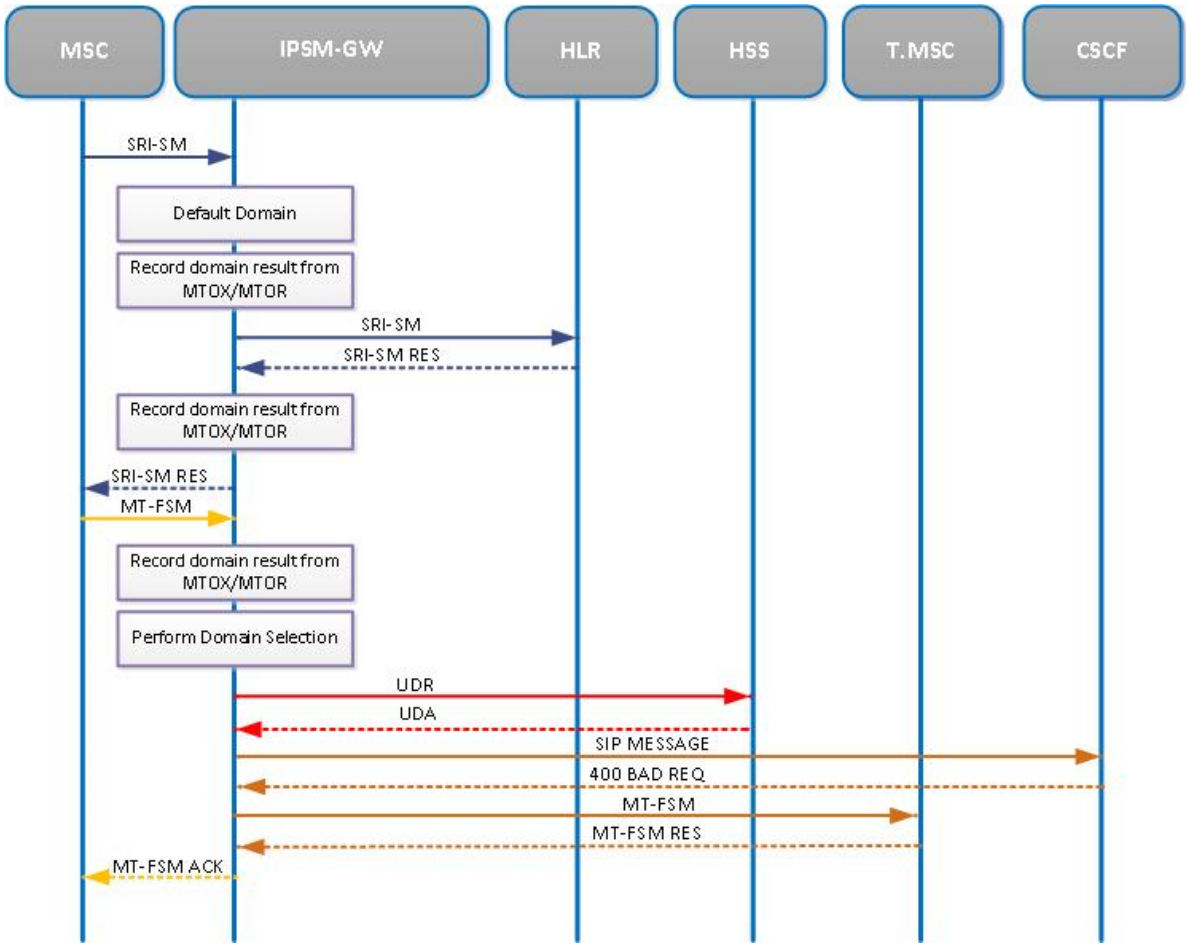


Figure 57: Domain Selection Mechanism Delivery for Home Routed Scenario

14.5.2 Standalone IPSM-GW

The Mobile-Terminated messages can be delivered to either a SS7 domain or an IMS domain. The supported options are:

- Delivery to IMS domain (Mobile-Terminated messages are delivered to UE via IMS network)
- Delivery to IMS domain fall back to SS7 domain (Mobile-Terminated message are first attempted on IMS network. If delivery fails then delivery is re-attempted in GSM network)

The Stand-Alone IPSM-GW configure the recipient network domain via semi-static parameter `defaultdomainselection` only. Possible values are:

- `imsdomain`
- `imsthenss7domain`

The default value is `imsthenss7domain`.

To enable the recipient mobile network selection, set:

```
defaultdomainselection=imsthenss7domain
```

The selected domain is the last recorded domain; it is only applied at the time of sending MTFSM.

Note: If you set the value for `defaultdomainselection` parameter as `legacy` or `ss7Domain`, then the value of the parameter value is changed back to the default value `imsthenss7domain`.

14.6 SIP Message Barring

The functionality allows the RTR along with the IIW to restrict the sending/receiving of SMS to a subscriber. In the IMS domain, the functionality is provided by the Integrated or Stand-Alone IPSM-GW solution for the messages exchanged through TRANSPORT LEVEL Interworking.

14.6.1 SIPO Barring

The below two mechanisms for SIPO message barring are mutually exclusive, that is, only one of these two barring mechanisms should be enabled or used at any point in time.

14.6.1.1 Barring Based on Route Header

The RTR and IIW support a mechanism for barring SIPO messages, which is based on comparing the 'Route' header field received in a SIP 'MESSAGE' method (carrying a SIPO message as per transport level Interworking) against the configured values of the semi-static parameters *rtrsipauthenticationtokena* and *rtrsipauthenticationtokenb*.

14.6.1.2 Barring Based on HSS Query

This section describes the specific SIPO barring functionality supported in the RTR and IIW by means of querying the HSS for retrieving SMS barring-related information.

If the RTR is configured for SIPO barring action through the semi-static parameter *sipsmsbarringaction*, then it performs the following processing upon receiving a new message from the IIW over the MXP interface:

- The RTR generates an HSS query request for the originator of the received SIPO message and forwards this request to an IIW.

  Note: While sending the "RecipientQueryRequest", the RTR encodes the field `sipMsgtype` as `sipo` to indicate that this query is for retrieving the SMS Barring information for SIPO Barring.

  The result of the HSS query indicates if the originating subscriber is barred from sending the message.

  Note: While forwarding an HSS query request to the IIW, the RTR considers all available IIW instances that have indicated their connectivity with the HSS, and selects one IIW instance in an adaptive round-robin manner. Hence, the IIW instance that had originally received the SIPO message and sent it to the RTR need not necessarily be responsible for performing the HSS query for the purpose of checking the SMS barring status. Also, in case none of the IIW instances have connectivity with the HSS, then the RTR does not perform any barring action, but continues with the normal processing of the received message.

- If the HSS response indicates that the SIPO message barring is activated for the originating subscriber (refer to the IIW Operator Manual, Section 5.2.2), then the IIW responds to the RTR with the call barred error (`MXIP_ERR_SRISM_CALL_BARRED`). Accordingly, the RTR discards the message and sends back an MXP response indicating a routing error to the IIW instance that had originally received the SIPO message.
- If the originating subscriber is not barred from sending messages, then the RTR proceeds with the processing of the message.
- If a timeout occurs while the RTR is waiting for a response to the HSS query request from the IIW, then the subsequent processing in the RTR is controlled by the semi-static configuration parameter *sipsmsbarringonresponsetimeout*. If this parameter is set to TRUE (default is FALSE), then the RTR considers the originating subscriber as barred from sending SMS, and performs the same processing as mentioned above.

  Note: A timeout can occur under the following circumstances:

  - Timeout on the Diameter Sh interface between the IIW and HSS, due to the HSS response not being received by IIW in time. There is an IIW configuration parameter (`iiwDiamQueryTimeout`) which is used to configure the Diameter Sh query timeout in seconds.
  - Timeout on the internal MIP interface between the RTR and IIW, before IIW can send a response back to RTR for the HSS query request. The value of this timeout is set to 5 seconds internally and is not configurable. It is recommended to set the value of the IIW parameter "`iiwDiamQueryTimeout`" to 3 seconds otherwise internal MIP timer (on RTR) will expire prematurely.

- In case the RTR receives any error other than timeout and call barred from IIW in response to the HSS query request, then the subsequent processing in RTR is controlled by the semi-static configuration parameter *sipsmsbarringonerrorresponse*. If this parameter is set to TRUE (default is FALSE), then the RTR considers the originating subscriber as barred from sending SMS, and performs the necessary processing as mentioned above.

14.6.2 Barring Using MO Routing Rules

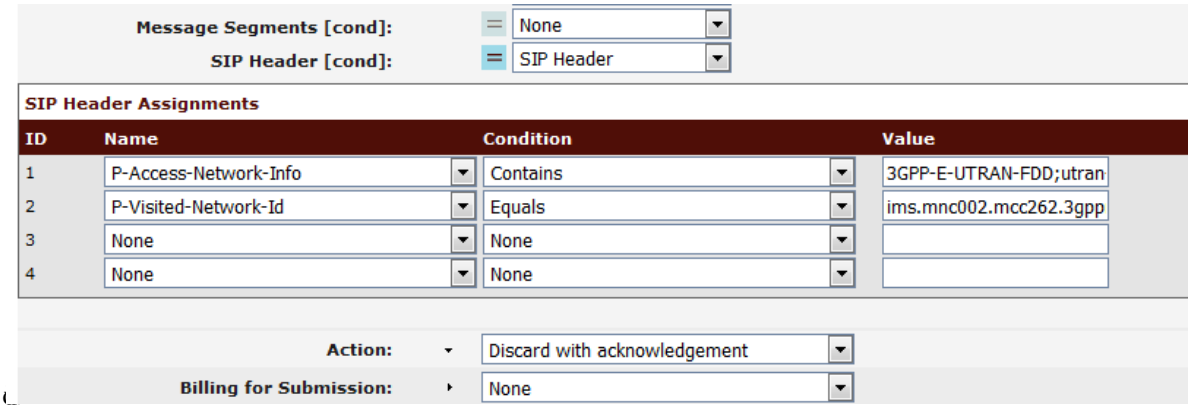
MO Routing rules support SIP Headers conditions which can be used to determine Routing Action based on SIP Header values received in incoming SIP messages.

For barring SIP Originated message:

1. Header on which decision is performed must be provisioned in SIP Header screen under IPSM-GW tab.
2. In MO Routing Rule, SIP Header condition should be selected as "SIP Header"
3. SIP Header sub-condition should be added for the Header.
4. Routing Action is added as "Discard with ack"

For example: If the **P-Access-Network-Info** header contains the value "`3GPP-E-UTRAN-FDD; utran-cell-id-3gpp=262096ea10014104`" and the **P-Visited-Network-Id** header contains the value "`ims.mnc002.mcc262.3gppnetwork.org`", the SIP Header sub-condition should be added

for the Header as mentioned in the figure



14.6.3 SIPT Barring

14.6.3.1 Barring Based on HSS Query

While sending the SIPT message towards the CSCF, the RTR initiates the "RecipientQueryRequest" over the MIP interface and performs the following steps:

1. The RTR checks if the semi-static parameter *sipsmsbarringaction* is set to `siptBarring` or `sipoSiptBarring`. If the configuration parameter is set as `noBarring`, the RTR triggers the MIP message "RecipientQueryRequest" towards the IIW to initiate the HSS query for the recipient to retrieve IMS User State and S-CSCF name.

   While sending the "RecipientQueryRequest", the RTR encodes the field `avpValueSelection` as "0x03" and the field `sipMsgtype` as `sipt` to indicate that this query is for retrieving the IMS User State and S-CSCF name.

2. If the semi-static parameter *sipsmsbarringaction* is set as `siptBarring` or `sipoSiptBarring`, the RTR triggers the MIP message "RecipientQueryRequest" towards the IIW to initiate the HSS query for the recipient to retrieve Barring information, Service Indication, IMS User State and S-CSCF name.

   While sending the "RecipientQueryRequest", the RTR encodes the field `avpValueSelection` as "0x0F" and the field `sipMsgtype` as `sipt` to indicate that this query is for retrieving the SMS Barring information pertaining to the IPSM-GW.

   Note: The `avpValueSelection` value "0x0F" indicates that the IIW enquires the below information from the HSS server corresponding to the recipient:

   - IMS user state
   - SCSCF Name
   - SMS Barring
   - HSS service indication

   Note: If SIPT Barring is configured then the RecipientQuery Request is performed even if the SIP End Point is configured.

3. Based on the "RecipientQueryResult", the RTR decides if the SIPT message is to be barred. If the response contains the result as successful, the RTR continues to process it as a non-barred message.
4. If the response contains the result as failure, the `errorCode` determines the SIPT barring (i.e. applicable for domain 'IMS' as well as 'IMS then SS7').

a) If the `errorCode` received by the RTR is `MXIP_ERR_SRISM_CALL_BARRED`, the RTR considers the message as failed with permanent error. No fallback to SS7 (in case of IMS then SS7) is performed.
b) If the `errorCode` `MXIP_ERR_SRISM_TIMEOUT` (0x01000001) is received, then the configuration parameter *sipsmsbarringonresponsetimeout* controls the barring behavior of the SIPT message as follows:

- If the parameter is set to TRUE, the RTR considers the message as failed with permanent error. No fallback to SS7 (in case of IMS then SS7) is performed.
- If the parameter is set as FALSE, RTR handles the error as SRISM time-out error.

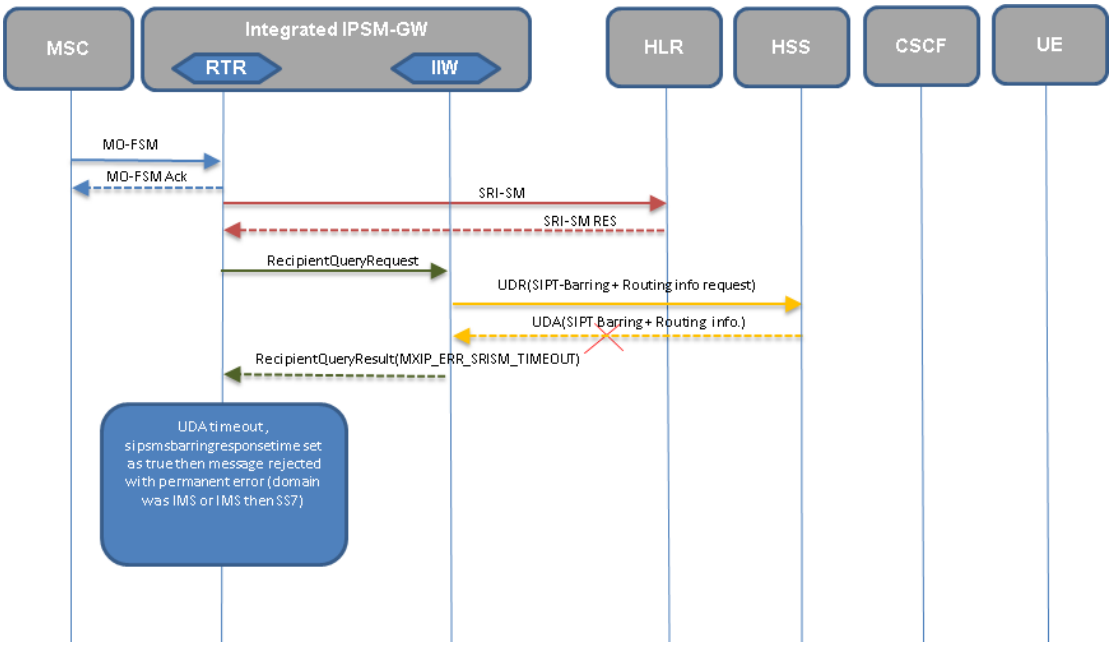


Figure 58: MO-SIPT message flow when the HSS query from the IIW times out

Note: SIPT-Barring + Routing info = Service Indication + SMS Barring + S-CSCF Name + IMS User State

Note: If the HSS query request (UDR) of the IIW times-out, that is the UDA is not received within the default 3 seconds (the time-out value is configurable), then the IIW informs the RTR using the corresponding error code in the "RecipientQueryResult" MIP response. If the configuration parameter *sipsmsbarringonresponsetimeout* is set to TRUE, the SIPT message is barred.

Note: A timeout can occur under the following circumstances:

- Timeout on the Diameter Sh interface between the IIW and HSS, due to the HSS response not being received by IIW in time. There is an IIW configuration parameter (`iiwDiamQueryTimeout`) which is used to configure the Diameter Sh query timeout in seconds.
- Timeout on the internal MIP interface between the RTR and IIW, before IIW can send a response back to RTR for the HSS query request. The value of this timeout is set to 5 seconds internally and it is not configurable. It is recommended to set the value of the IIW parameter "`iiwDiamQueryTimeout`" to 3 seconds, otherwise the internal MIP timer (on RTR) will expire prematurely.

c) Similarly, if any `errorCode` other than `MXIP_ERR_SRISM_CALL_BARRED` is received, then the configuration parameter *sipsmsbarringonerrorresponse* defines if the message is barred.

- If the parameter is set to TRUE, the RTR considers the message as failed with permanent error. No fallback to SS7 (in case of IMS then SS7) is performed.
- If the parameter is set to FALSE, the RTR handles the error accordingly.

d) If the "ResponseQueryResult" is timed out (i.e. if there is a timeout on the MIP interface before any response is received from IIW side), then the configuration parameter *sipsmsbarringonresponsetimeout* controls the barring behavior of SIPT message as follows:

- If the parameter is set to TRUE, the RTR considers the message as failed with permanent error. No fallback to SS7 (in case of IMS then SS7) is performed.
- If the parameter is set to FALSE, the RTR handles the error accordingly.

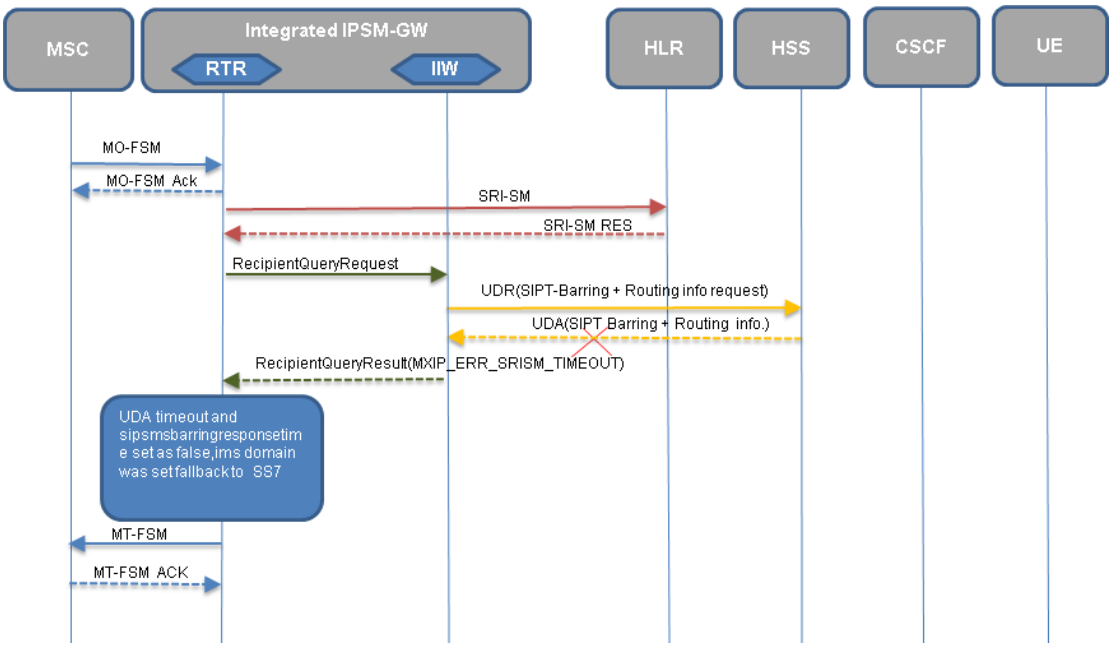


Figure 59: MO-SIPT message flow when the HSS query from the IIW times-out with fallback

Note: SIPT-Barring + Routing info = Service Indication + SMS Barring + S-CSCF Name + IMS User State

Note: If the HSS query request (UDR) of the IIW times-out, that is, the UDA is not received within the default 3 seconds (the time-out value is configurable), then the IIW informs the RTR using the corresponding error code in the "RecipientQueryResult" MIP response. If the configuration parameter *sipsmsbarringonresponsetimeout* is set to FALSE and the domain is set to Fallback to SS7, the SIPT message is delivered to the SS7 domain.

5. If the SIPT message is not barred after the previous steps, the RTR attempts the SIP-T Delivery.

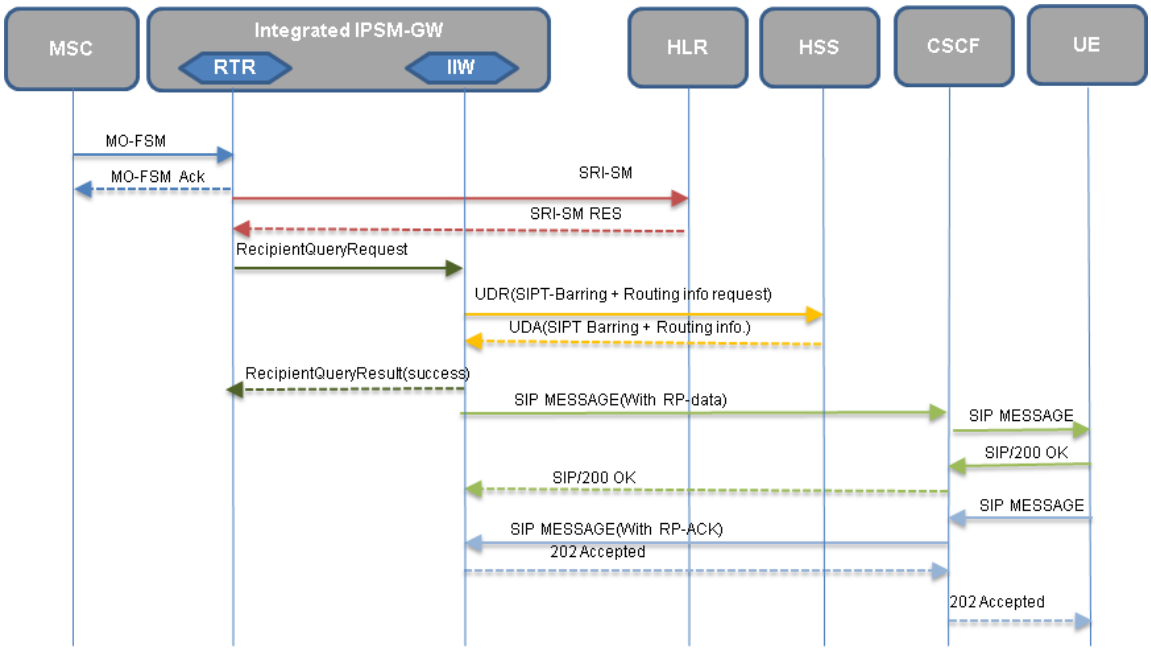


Figure 60: MO-SIPT message flow when the SIPT message does NOT get barred

Note: SIPT-Barring + Routing info = Service Indication + SMS Barring + S-CSCF Name + IMS User State

Note: The above example of a message flow shows the successful delivery of a non-barred MO-SIPT message. However, the functionality addressed in this feature does not depend on whether a SIPT message is eventually coming as MT, SIPO, AO etc.

6. In SIPO-SIPT case, if the SIPO message is not barred but the SIPT message is barred, the IP-SM-GW (i.e. RTR + IIW) behavior is as in the following figure:

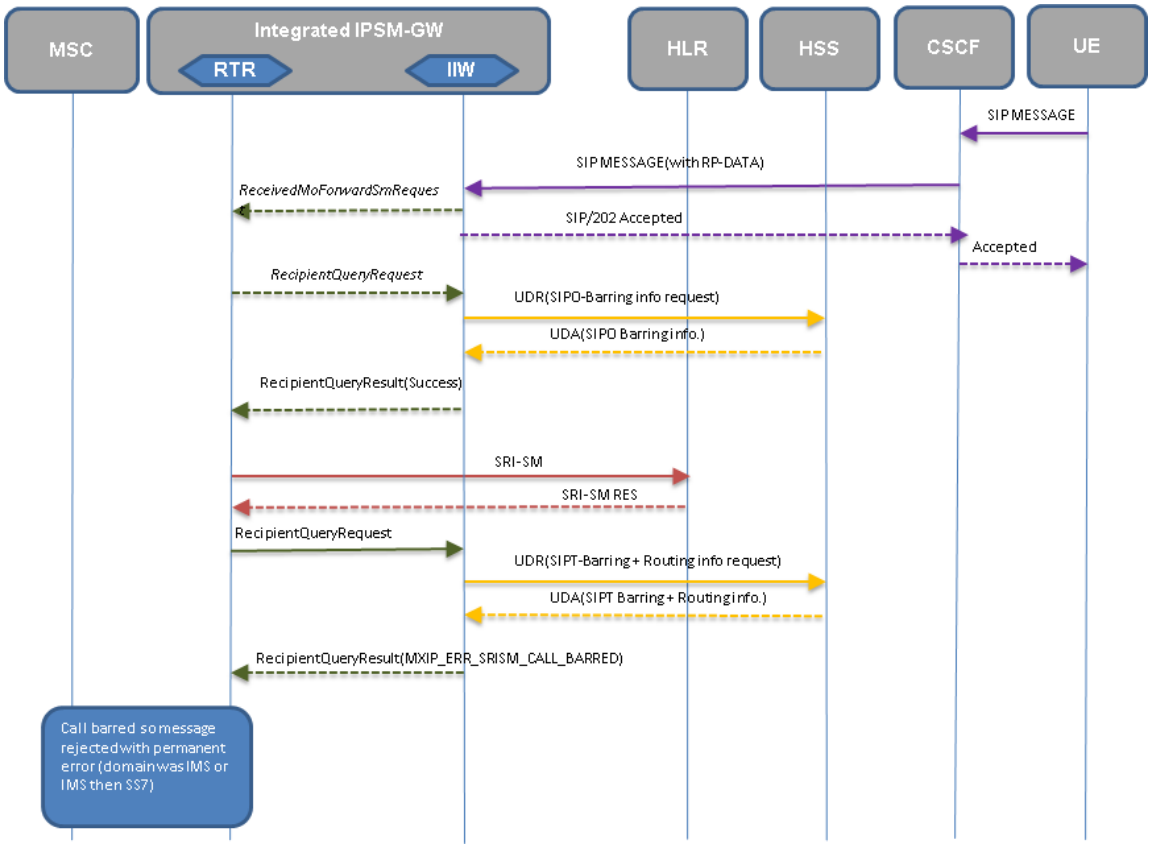


Figure 61: SIPO-SIPT scenarios where SIPO is not barred and SIPT is barred

Note: SIPT-Barring + Routing info = Service Indication + SMS Barring + S-CSCF Name + IMS User State

7. In case of MT-SIPT scenarios with Accept and Respond Immediately, on receiving an MT-FSM, if the domain is set to "IMS" or "IMS then SS7", then the RTR initiates the HSS query request (i.e. via IIW) to HSS for SIPT barring information. Upon receiving the HSS query response for SIPT barring, the RTR rejects the SIPT Message with permanent error. Refer Figure 5 for flow diagram.

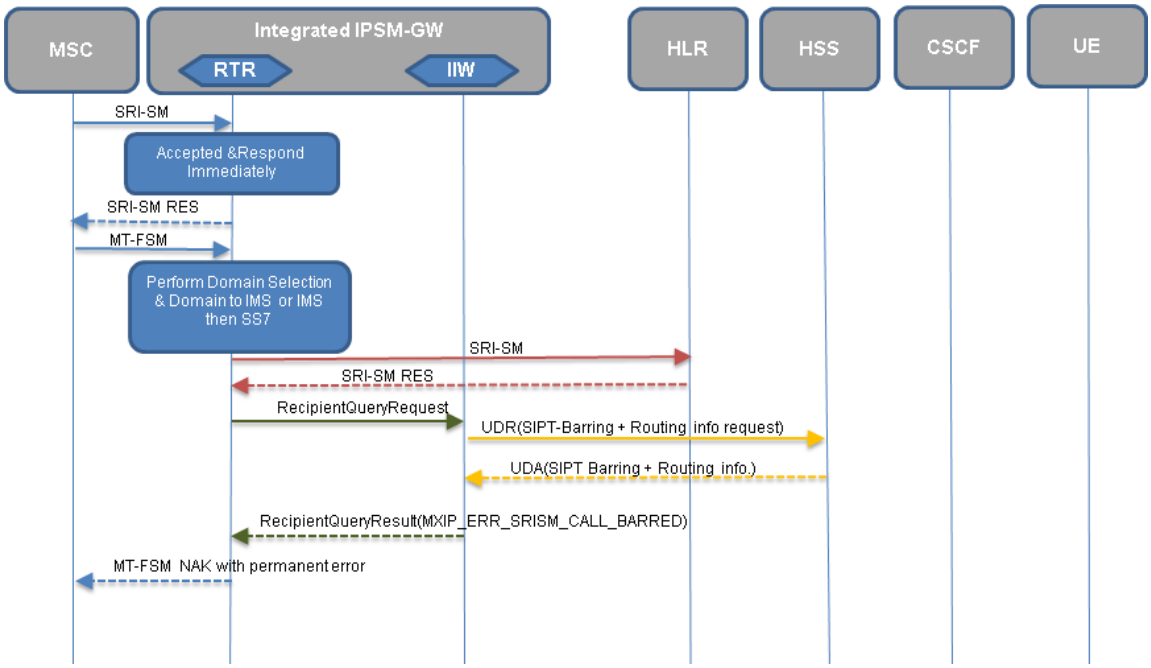


Figure 62: MT-SIPT scenario where SRISM performed After MT-FSM

Note: SIPT-Barring + Routing info = Service Indication + SMS Barring + S-CSCF Name + IMS User State

8. In case of MT-SIPT scenarios with Send to HLR., on receiving an MT-FSM, if the domain is set to "IMS" or "IMS then SS7", then the RTR initiates the HSS query request (i.e. via IIW) to HSS for SIPT barring information. Upon receiving the HSS query response for SIPT barring, RTR rejects the SIPT Message with permanent error. Refer Figure 6 for flow diagram.

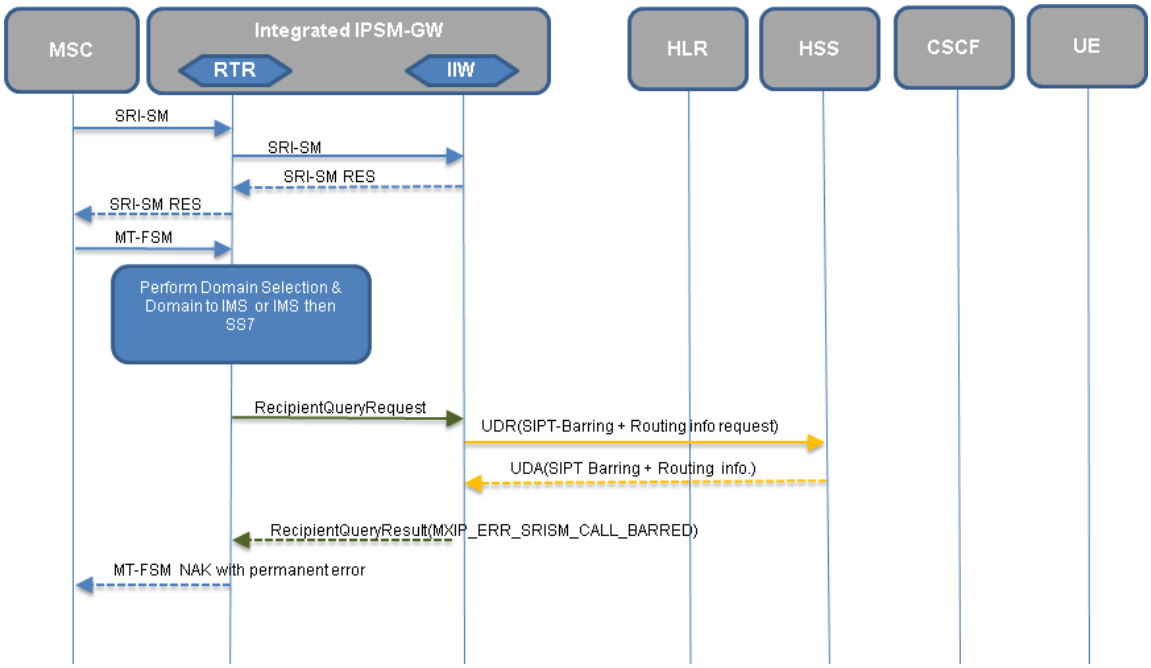


Figure 63: MT-SIPT scenario where SRISM performed before MT-FSM

Note: SIPT-Barring + Routing info = Service Indication + SMS Barring + S-CSCF Name + IMS User State

14.7 Mapping of SIP Error Codes to Internal Errors

SIP Error Code	Internal Error
404	UE-Deregistered Error
410	UE-Deregistered Error
503	UE-Deregistered Error
408	No Response Via IPSMGW
480	No Response Via IPSMGW
486	No Response Via IPSMGW
504	No Response Via IPSMGW
Between 300-399	System Failure
All Others	Other Error

14.8 Counters for IMS Delivery Scenarios

This section describes the counters for the IMS delivery for the following scenarios:

- MO-SIPT
- MO-SIPT-MT
  - SIPT delivery failed fallback to MT
  - HSS query failed fallback to MT
- MO-SIPT fallback to Store
- MO-SIPT-MT fallback to Store
- MT-SIPT
  - SRIQ rule with action 'Send to HLR'
  - SRIQ rule with action 'Accept and Respond to SMSC immediately'
- MT-SIPT-MT
  - SRIQ rule with action 'Send to HLR'
    - SIPT delivery failed fallback to MT
    - HSS query failed fallback to MT
  - SRIQ rule with action 'Accept and Respond to SMSC immediately'
    - SIPT delivery failed fallback to MT
    - HSS query failed fallback to MT

Note:

1. In the following scenarios, the MTFSM failure counters can be `smsCntMtTimeoutCounter`, `smsCntMtAbsSubErrorCounter`, `smsCntMtSysFailErrorCounter`, `smsCntMtDataMisErrorCounter`, etc.
2. The SRISM failure counters can be `smsCntSriSmTimeoutCounter`, `smsCntSriSmSysFailErrorCounter`, `smsCntSriSmDataMisErrorCounter`, `smsCntSriSmAbsSubErrorCounter`, etc.
3. In the following scenarios, Mobile Network Domain is set to "IMS then SS7". For more details, refer to the section *Mobile Network Domain Selection*.
4. In the following scenarios, few counters are incremented twice, thrice and four times. Below are the explanation for those counters:
   - Incremented Twice: The counters are incremented for the first time in case of SIPT failure, and second time in case of MT successful delivery.
   - Incremented Thrice: The counter is incremented for the first time in case of SIPT failure, second time in case of SS7 temporary failure, and third time when message is retried from AMS (via RTR) to IMS and the delivery gets failed.
   - Incremented Four Times : The counters are incremented for the first time in case of SIPT failure, second time in case of SS7 temporary failure, third time when message is retried from AMS (via RTR) to IMS and the delivery gets failed, and last time when the message is delivered to SS7.

14.8.1 MO-SIPT

Below are the counters and their values for successful delivery of a MO message into IMS domain.

MO Counters	Incremented/Not Incremented
smsCntMoTotalCounter	Incremented Once
smsCntMoSuccessfulCounter	Incremented Once
smsCntRecvMoFwdSmCounter	Incremented Once
smsCntRecvMoFwdSmWithoutStatusReportRequestCounter	Incremented Once
smsCntMoMtSuccess	Incremented Once

MT Delivery Counters	Incremented/Not Incremented
smsCntMtTotalCounter	Incremented Once
smsCntMtSuccessfulCounter	Incremented Once
smsCntSentMtFwdSmWithOrdinaryMessageCounter	Incremented Once
smsCntMtFirstDeliveryCounter	Incremented Once
smsCntSentMtFwdSmCounter	Incremented Once
MTFSM failure counter	Not Incremented
smsCntSriSmTotalCounter	Incremented Once
smsCntSriSmSuccessCounter	Incremented Once
smsCntSentSriSmCounter	Incremented Once
SRISM failure counter	Not Incremented

14.8.2 MO-SIPT-MT

Case 1: SIPT delivery failed fallback to MT

Below are the counters and their values for successful delivery of a MO message into SS7 domain, if IMS delivery failed in first attempt.

MO Counters	Incremented/Not Incremented
smsCntMoTotalCounter	Incremented Once
smsCntMoSuccessfulCounter	Incremented Once
smsCntRecvMoFwdSmCounter	Incremented Once
smsCntRecvMoFwdSmWithoutStatusReportRequestCounter	Incremented Once
smsCntMoMtSuccess	Incremented Once

MT Delivery Counters	Incremented/Not Incremented
smsCntMtTotalCounter	Incremented Twice
smsCntMtSuccessfulCounter	Incremented Once
smsCntSentMtFwdSmWithOrdinaryMessageCounter	Incremented Twice
smsCntMtFirstDeliveryCounter	Incremented Twice
smsCntSentMtFwdSmCounter	Incremented Twice
MTFSM failure counter	Incremented Once
smsCntSriSmTotalCounter	Incremented Once
smsCntSriSmSuccessCounter	Incremented Once
smsCntSentSriSmCounter	Incremented Once
SRISM failure counter	Not Incremented

Case 2: HSS query failed fallback to MT

Below are the counters and their values for successful delivery of a MO message into SS7 domain, if HSS query failed in first attempt.

MO Counters	Incremented/Not Incremented
smsCntMoTotalCounter	Incremented Once
smsCntMoSuccessfulCounter	Incremented Once
smsCntRecvMoFwdSmCounter	Incremented Once
smsCntRecvMoFwdSmWithoutStatusReportRequestCounter	Incremented Once
smsCntMoMtSuccess	Incremented Once

MT Delivery Counters	Incremented/Not Incremented
smsCntMtTotalCounter	Incremented Once
smsCntMtSuccessfulCounter	Incremented Once
smsCntSentMtFwdSmWithOrdinaryMessageCounter	Incremented Once
smsCntMtFirstDeliveryCounter	Incremented Once
smsCntSentMtFwdSmCounter	Incremented Once
MTFSM failure counter	Not Incremented
smsCntSriSmTotalCounter	Incremented Once
smsCntSriSmSuccessCounter	Incremented Once
smsCntSentSriSmCounter	Incremented Once
SRISM failure counter	Not Incremented

Note: When the HSS query fails, the SRISM failure counters will not increment.

14.8.3 MO-SIPT Fallback to Store

Below are the counters and their values for the successful delivery of an MO message in IMS domain, when the SIPT delivery failed in the first attempt followed by message getting stored in the AMS.

MO Counters	Incremented/Not Incremented
smsCntMoTotalCounter	Incremented Once
smsCntMoSuccessfulCounter	Incremented Once
smsCntRecvMoFwdSmCounter	Incremented Once
smsCntRecvMoFwdSmWithoutStatusReportRequestCounter	Incremented Once
smsCntMoMtSuccess	Not Incremented
smsCntMoMtAmsPrimaryFailure	Incremented Once
smsCntMoMtAmsFallbackSuccess	Incremented Once
smsCntMoMtFromAmsSuccess	Incremented Once

MT Delivery Counters	Incremented/Not Incremented
smsCntMtTotalCounter	Incremented Twice
smsCntMtSuccessfulCounter	Incremented Once
smsCntSentMtFwdSmWithOrdinaryMessageCounter	Incremented Twice
smsCntMtFirstDeliveryCounter	Incremented Once
smsCntSentMtFwdSmCounter	Incremented Twice
MTFSM failure counter	Incremented Once
smsCntSriSmTotalCounter	Incremented Twice
smsCntSriSmSuccessCounter	Incremented Twice
smsCntSentSriSmCounter	Incremented Twice
SRISM failure counter	Not Incremented

14.8.4 MO-SIPT-MT Fallback to Store

Below are the counters and their values for the successful delivery of an MO message in SS7 domain when the SIPT delivery failed followed by MT delivery failure followed by message being stored in the AMS.

MO Counters	Incremented/Not Incremented
smsCntMoTotalCounter	Incremented Once
smsCntMoSuccessfulCounter	Incremented Once
smsCntRecvMoFwdSmCounter	Incremented Once

MO Counters	Incremented/Not Incremented
smsCntRecvMoFwdSmWithoutStatusReportRequestCounter	Incremented Once
smsCntMoMtSuccess	Not Incremented
smsCntMoMtAmsPrimaryFailure	Incremented Once
smsCntMoMtAmsFallbackSuccess	Incremented Once
smsCntMoMtFromAmsSuccess	Incremented Once

MT Delivery Counters	Incremented/Not Incremented
smsCntMtTotalCounter	Incremented Four Times
smsCntMtSuccessfulCounter	Incremented Once
smsCntSentMtFwdSmWithOrdinaryMessageCounter	Incremented Four Times
smsCntMtFirstDeliveryCounter	Incremented Twice
smsCntSentMtFwdSmCounter	Incremented Four Times
MTFSM failure counter	Incremented Thrice
smsCntSriSmTotalCounter	Incremented Twice
smsCntSriSmSuccessCounter	Incremented Twice
smsCntSentSriSmCounter	Incremented Twice
SRISM failure counter	Not Incremented

14.8.5 MT-SIPT

Case 1: SRIQ rule with action 'Send to HLR'

Below are the counters and their values for successful delivery of an MT message into IMS domain.

MT Counters	Incremented/Not Incremented
smsCntRecvMtPassedCounter	Incremented Once
smsCntRecvMtHomeRoutedSuspectScrambledCounter	Incremented Once
smsCntRecvMtFwdSmCounter	Incremented Once
smsCntRecvSriSmPassedCounter	Incremented Once
smsCntRecvSriSmCounter	Incremented Once
smsCntMtMtSuccess	Incremented Once

MT Delivery Counters	Incremented/Not Incremented
smsCntMtTotalCounter	Incremented Once
smsCntMtSuccessfulCounter	Incremented Once

MT Delivery Counters	Incremented/Not Incremented
smsCntSentMtFwdSmWithOrdinaryMessageCounter	Incremented Once
smsCntMtFirstDeliveryCounter	Not Incremented
smsCntSentMtFwdSmCounter	Incremented Once
MTFSM failure counter	Not Incremented
smsCntSriSmTotalCounter	Incremented Once
smsCntSriSmSuccessCounter	Incremented Once
smsCntSentSriSmCounter	Incremented Once
SRISM failure counter	Not Incremented

Case 2: SRIQ rule with action 'Accept and Respond to SMSC immediately'

Below are the counters and their values for successful delivery of an MT message into IMS domain.

MT Counters	Incremented/Not Incremented
smsCntRecvMtPassedCounter	Incremented Once
smsCntRecvMtHomeRoutedSuspectScrambledCounter	Incremented Once
smsCntRecvMtFwdSmCounter	Incremented Once
smsCntRecvSriSmPassedCounter	Not Incremented
smsCntRecvSriSmCounter	Incremented Once
smsCntMtMtSuccess	Incremented Once

MT Delivery Counters	Incremented/Not Incremented
smsCntMtTotalCounter	Incremented Once
smsCntMtSuccessfulCounter	Incremented Once
smsCntSentMtFwdSmWithOrdinaryMessageCounter	Incremented Once
smsCntMtFirstDeliveryCounter	Not Incremented
smsCntSentMtFwdSmCounter	Incremented Once
MTFSM failure counter	Not Incremented
smsCntSriSmTotalCounter	Incremented Once
smsCntSriSmSuccessCounter	Incremented Once
smsCntSentSriSmCounter	Incremented Once
SRISM failure counter	Not Incremented

14.8.6 MT-SIPT-MT

Case 1: SRIQ rule with action 'Send to HLR'

a. SIPT Failure

Below are the counters and their values for successful delivery of an MT message into SS7 domain, If IMS delivery failed in first attempt.

MT Counters	Incremented/Not Incremented
smsCntRecvMtPassedCounter	Incremented Once
smsCntRecvMtHomeRoutedSuspectScrambledCounter	Incremented Once
smsCntRecvMtFwdSmCounter	Incremented Once
smsCntRecvSriSmPassedCounter	Incremented Once
smsCntRecvSriSmCounter	Incremented Once
smsCntRecvMtMatchingMtRoutingRuleCounter	Incremented Once
smsCntMtMtSuccess	Incremented Once

MT Delivery Counters	Incremented/Not Incremented
smsCntMtTotalCounter	Incremented Twice
smsCntMtSuccessfulCounter	Incremented Once
smsCntSentMtFwdSmWithOrdinaryMessageCounter	Incremented Twice
smsCntMtFirstDeliveryCounter	Incremented Twice
smsCntSentMtFwdSmCounter	Incremented Twice
MTFSM failure counter	Incremented Once
smsCntSriSmTotalCounter	Incremented Once
smsCntSriSmSuccessCounter	Incremented Once
smsCntSentSriSmCounter	Incremented Once
SRISM failure counter	Not Incremented

b. HSS query failure

Below are the counters and their values for successful delivery of an MT message into SS7 domain, If HSS query failed in first attempt.

MT Counters	Incremented/Not Incremented
smsCntRecvMtPassedCounter	Incremented Once
smsCntRecvMtHomeRoutedSuspectScrambledCounter	Incremented Once

MT Counters	Incremented/Not Incremented
smsCntRecvMtFwdSmCounter	Incremented Once
smsCntRecvSriSmPassedCounter	Incremented Once
smsCntRecvSriSmCounter	Incremented Once
smsCntMtMtSuccess	Incremented Once

MT Delivery Counters	Incremented/Not Incremented
smsCntMtTotalCounter	Incremented Once
smsCntMtSuccessfulCounter	Incremented Once
smsCntSentMtFwdSmWithOrdinaryMessageCounter	Not Incremented
smsCntMtFirstDeliveryCounter	Not Incremented
smsCntSentMtFwdSmCounter	Incremented Once
MTFSM failure counter	Not Incremented
smsCntSriSmTotalCounter	Incremented Once
smsCntSriSmSuccessCounter	Incremented Once
smsCntSentSriSmCounter	Incremented Once
SRISM failure counter	Not Incremented

Note: No counter is incremented for HSS query failure or pass.

Case 2: SRIQ rule with action 'Accept and Respond to SMSC immediatly'

a. SIPT Failure

Below are the counters and their values for successful delivery of an MT message into SS7 domain, If IMS delivery failed in first attempt.

MT Counters	Incremented/Not Incremented
smsCntRecvMtPassedCounter	Incremented Once
smsCntRecvMtHomeRoutedSuspectScrambledCounter	Incremented Once
smsCntRecvMtFwdSmCounter	Incremented Once
smsCntRecvSriSmPassedCounter	Not Incremented
smsCntRecvSriSmCounter	Incremented Once
smsCntRecvMtMatchingMtRoutingRuleCounter	Incremented Once
smsCntMtMtSuccess	Incremented Once

MT Delivery Counters	Incremented/Not Incremented
smsCntMtTotalCounter	Incremented Twice

MT Delivery Counters	Incremented/Not Incremented
smsCntMtSuccessfulCounter	Incremented Once
smsCntSentMtFwdSmWithOrdinaryMessageCounter	Incremented Twice
smsCntMtFirstDeliveryCounter	Incremented Twice
smsCntSentMtFwdSmCounter	Incremented Twice
MTFSM failure counter	Incremented Once
smsCntSriSmTotalCounter	Incremented Once
smsCntSriSmSuccessCounter	Incremented Once
smsCntSentSriSmCounter	Incremented Once
SRISM failure counter	Not Incremented

b. HSS query failure

Below are the counters and their values for successful delivery of an MT message into SS7 domain, If HSS query failed in first attempt.

MT Counters	Incremented/Not Incremented
smsCntRecvMtPassedCounter	Incremented Once
smsCntRecvMtHomeRoutedSuspectScrambledCounter	Incremented Once
smsCntRecvMtFwdSmCounter	Incremented Once
smsCntRecvSriSmPassedCounter	Not Incremented
smsCntRecvSriSmCounter	Incremented Once
smsCntMtMtSuccess	Incremented Once

MT Delivery Counters	Incremented/Not Incremented
smsCntMtTotalCounter	Incremented Once
smsCntMtSuccessfulCounter	Incremented Once
smsCntSentMtFwdSmWithOrdinaryMessageCounter	Incremented Once
smsCntMtFirstDeliveryCounter	Incremented Once
smsCntSentMtFwdSmCounter	Incremented Once
MTFSM failure counter	Not Incremented
smsCntSriSmTotalCounter	Incremented Once
smsCntSriSmSuccessCounter	Incremented Once
smsCntSentSriSmCounter	Incremented Once
SRISM failure counter	Not Incremented

Note: No counter is incremented for HSS query failure or pass.

14.9 SCSCFName Support over MIP/MXP Interface

To deliver the SIPT message, first RTR initiates the recipient query towards the IIW side and then the IIW initiates the HSS query to get the CSCF address.

In successful case, the IIW receives the `<SCSCFName>` value with additional parameters. The exact same information of `<SCSCName>` will be transferred to the RTR over the MIP interface.

In SIPT Message delivery, the RTR will copy the same information of `<SCSCFName>` value and transfer towards the IIW over the MXP interface.

Note: The maximum length of `SCSCFName` which can be transferred over the MIP/MXP interface is 256 bytes. The `scscfName` is an optional field over the MIP/MXP interface and it will be added only when `iiwrouteheadertemplateforsipt` is configured with a route URI template in the IIW components. Please refer to section 3.5.3 of the IIW Operator Manual.

Chapter 15

Logging

Topics:

15.1 Introduction

The RTR supports two types of logging:

- Transactional logging, also called message logging, in which log records are created post-transaction
- Event logging, in which log records are created instantaneously, as events occur (limited to short messages and unexpected TCAP messages)

15.2 Message Logging

Transaction logging, also called message logging, is the RTR's mechanism for logging inbound SMSC traffic. Log records are created post-transaction. These records provide information about each short message's origins, message fields, and how it was routed.

To enable message logging, create message logging profiles in the MGR (**Logging ➤ Messages ➤ Profile**) and optionally assign as defaults for categories such as MO messages, MT violations, etc. (**Logging ➤ Messages ➤ Properties**). Then, when you create a routing or counting rule, you can select whether the messages that match the rule are logged according to the applicable default profile, according to a specific profile, or not at all. You can create up to 100 message log profiles.

Important: The logging of MT status reports must be configured in the MOR rule, the MTOR rule and the default MO log profile `logPropDefaultProfileForMo` to enable MT status report logging. The logging of AT notifications must be configured in the AOR rule, the ATOR rule and the default AO log profile `logPropDefaultProfileForAo` to enable AT notification logging.

Note: While logging the addresses, the values of the addresses captured will be same as the addresses present in the messages received and transmitted by the RTR. The RTR can change the value of the TON/NPI based on the following logic:

1. In case of ASN1 extended format Ton/NPI value of the address is retained.
2. In case of ASN1 extended with Country and Network
   a. TON/NPI of the Short number is logged as 6/0.
   b. If NPI of the msisdn is set as ISDN Telephony then the TON/NPI is set as 1/1.
   c. If NPI of the msisdn is not ISDN Telephony then the original TON/NPI is retained.

15.2.1 Logging Fatal Protocol Violations

Messages may contain protocol violations that will cause the RTR to reject them before the rule engine evaluates them. These messages are not subject to routing or counting rules, and are therefore logged according to separate profiles.

A violation occurs when one or more of the following conditions apply to an inbound operation:

- An invalid SMSC address at MAP layer
- An invalid recipient address
- An invalid originator address
- An invalid IMSI

- An invalid MSC address
- A forged MSC address
- A forged IMSI
- A forged LMSI
- An unknown SMSC address at SCCP layer
- An unknown SMSC address at MAP layer
- Conflicting SMSC addresses
- A spoofed SMSC address at SCCP layer
- A spoofed SMSC address at MAP layer
- An unsolicited MtForwardSm operation (that is, one not preceded by a SendRoutingInfo operation)
- A spoofed originator address

15.2.2 Logging CDMA- and TDMA-Specific Fields

The RTR supports logging of CDMA- and TDMA-specific SMPP message fields.

The CDMA-specific SMPP message fields are:

- `privacy_indicator`
- `source_subaddress`
- `dest_subaddress`
- `user_response_code`
- `language_indicator`
- `number_of_messages`
- `callback_num`
- `display_time`
- `ms_validity`
- `alert_on_message_delivery`
- `its_reply_type`
- `its_session_info`

The TDMA-specific SMPP message fields are:

- `callback_num_pres_ind`
- `callback_num_atag`
- `sms_signal`
- `alert_on_message_delivery`

15.2.3 Creating Message Logging Profiles

To create a logging profile:

1. In the left navigation bar, select **Logging ➤ Messages ➤ Profile**.
   The Logging Profiles tab appears.
2. Click **Add New**.
   A new Logging Profiles tab appears.
3. Enter a unique name for the profile in the **Name** box (maximum 31 characters).
4. Optionally enter a description of the profile in the **Description** box.

5. Select the message type(s) that the profile applies to:
6. In the **Processing Directory** box, enter the location in which to store the log files while they are being created (defaults to `/var/TextPass/log/processing`).

   Note: In a multi-instance setup, the processing directory will be shared by all the RTR instances running on a node.

7. In the **Finished Directory** box, enter the location in which to store the log files after they are created (defaults to `/var/TextPass/log/available`).

   Note: In a multi-instance setup, the finished directory will be shared by all the RTR instances running on a node.

8. In the **Copy 1 of Finished Directory** through **Copy 9 of Finished Directory** boxes, enter directories in which to created hard links to the files in the finished directory (by default, there are no copies of the finished directory).

   Note: The finished directory and all finished directory copies must be on the same disk partition as the processing directory.

9. In the **Filename Template** box, enter the template to use to name the log files (defaults to `log_%h_%U_%Y%m%d_%H%M%S_%3.dat`).

   Important: If multi-instances of RTR are running on the same node, then it is important to include `%U` escape sequence, which will be translated to `UID` (operating system user identifier). This ensures that multiple instances of RTR do not try to create files with identical names.

10. In the **Max. File Size** box, enter the maximum size of a log file in bytes (defaults to 1048576 bytes, which is 1 MB). The range is 1024 byes (1 KB) to 1073741824 bytes (1 GB).
11. In the **Max. File Duration** box, enter the maximum duration of a log file in seconds (defaults to 3600 seconds, which is 1 hour). The range is 1 second to 2,678,400 seconds (1 month).
12. In the **Max. File Records** box, enter the maximum number of records to allow in a log file (defaults to 10000 records). The range is 1 record to 10,000,000 records.
13. Select the file format from the **File Format** list:

    - ASN.1 Extended
    - ANS.1 Extended with country and network info (default)

14. In the **Starting Sequence Number** box, enter the number with which to start the log file numbering sequence (defaults to 0).
15. From the **Suspect/Trusted Messages** list, select the type of messages to log:

    - Only suspect
    - Only trusted
    - Both suspect and trusted (default)

    Suspect/Trusted Messages logging pertains to whether the RTR/FWL considers the message source to be suspect or trusted. Inbound MO messages may come from a suspected or trusted MSC, while inbound SendRoutingInfoForSm operations and MT messages may come from a suspected or trusted SMSC. Refer to the Firewall Guide for more information about suspect and trusted qualifications.

16. From the **Failed/Succeeded Messages** list, select the type of messages to log:

    - Only failed

- Only succeeded
- Both failed and succeeded (default)

Failed/Succeeded Messages logging pertains to whether a message was successfully delivered from the Mobile Messaging system to the destination. For outbound MT messages, the destination is an MSC (MS). For outbound AT messages, the destination is an application.

17. From the **Accepted/Rejected Messages** list, select the type of messages to log:

- Only accepted
- Only rejected
- Both accepted and rejected (default)

Accepted/Rejected Messages logging pertains to whether the Mobile Messaging system accepts a message or not. This applies to inbound MO and inbound AO messages only.

18. From the **Legitimate/Violated Messages** list, select the type of messages to log:

- Only legitimate
- Only violated
- Both legitimate and violated (default)

Legitimate/Violated Messages logging pertains to whether a message passes or fails a spoof check. Legitimate messages are messages that passed the spoof check. Violated messages are messages that failed the spoof check.

19. From the **Expired/Deleted Messages** list, select the type of messages to log:

- Do not log (default)
- Only expired
- Only deleted
- Both expired and deleted
- Only replaced
- Both expired and replaced
- Both deleted and replaced
- Expired, deleted and replaced

Expired/Deleted Messages logging pertains to the AMS delivery result. Expired messages reached their validity period expiration or their maximum number of delivery attempts. Deleted messages were manually deleted from the AMS by a user or by an application. Replaced messages were replaced in the AMS.

20. From the **Status Report Messages** list, select the type of messages to log:

- Do not log (default)
- Status reports

21. From the **Copied/Forwarded Messages** list, select the type of messages to log:

- Do not log (default)
- Only copied
- Only forwarded
- Both copied and forwarded

22. From the **Transparent User Data Level** list, select the level of user data logging:

- Use Global Setting
- Always
- Protocol Violation
- Never
- Encrypt Always

Note: If the value of the logging profile parameter is `Use Global Setting`, the RTR will use the semi-static parameter `logtransparentuserdatalevel`.

23. Click **Save**.

    The MGR creates the logging profile and closes the tab.

24. Activate the profile.

15.2.4 Configuring Message Logging Properties

The message logging properties are used to set a log profile as the default log profile for certain messages or violation types.

Note: Changing the default profile will change the logging for all rules that are configured with this default profile.

Prerequisites:

- Logging profile

To configure logging properties:

1. In the left navigation bar, select **Logging ➤ Messages ➤ Properties**.

   The Logging Properties tab appears.

2. Select a logging profile for mobile-originating or IMS-originating traffic from the **MO Messages** list.
3. Select a logging profile for mobile-terminating traffic from the **MT Messages** list.
4. Select a logging profile for application-originating traffic from the **AO Messages** list.
5. Select a logging profile for application-terminating traffic from the **AT Messages** list.
6. Select a logging profile to use in case of a fatal protocol violation in a mobile-originating message from the **MO Violations** list.
7. Select a logging profile to use in case of a fatal protocol violation in a mobile-terminating message from the **MT Violations** list.
8. Select a logging profile to be used for mobile-originating SMS commands from the **MO Commands** list.
9. Select a logging profile to be used for application-originating SMS commands from the **AO Commands** list.
10. Select a logging profile to be used for mobile number portability (MNP) violations of originator(in case of MO message) from the **MNP Violations** list.
11. Click **Save**.

    The MGR saves the logging properties and closes the tab.

15.2.5 Configurable User Data Logging

The level of user data logging can be configured to meet local privacy regulations. The text of messages, for which user data should not be logged, will be masked by a string of Xs.

To allow flexibility and privacy protection, the maximum logging level is determined and locked by the license key. Therefore, the log level that is configured in the semi-static configuration file and per logging profile can never exceed the maximum log level that is defined in the license.

The following table specifies information for the semi-static variable `logtransparentuserdatalevel` and per logging profile parameter **Transparent User Data Level**.

logtransparentuserdatalevel	This governs the system-wide setting for the transparent User data level. If the variable is less than the License key, the RTR gives an error.
Transparent User Data Level	This parameter can be configured per logging profile. If this parameter is configured with a value less than the license key, the RTR gives an error.

The following table specifies the possible configuration values for the semi-static variable `logtransparentuserdatalevel` and the logging profile parameter **Transparent User Data Level** for different License key values:

License Key values	**Allowed logtransparentuserdatalevel values**	**Allowed Transparent User Data Level values**
always	always, protocolViolationsOnly, never	always, protocolViolationsOnly, never, Use Global Setting
protocol violations only	protocolViolationsOnly, never	protocolViolationsOnly, never, Use Global Setting
never	never	never, Use Global Setting

The following tables describe different possible configuration for the semi-static parameter `logtransparentuserdatalevel` and per logging parameter **Transparent User Data Level**. Based on the license key, the possible configuration values for semi-static & per logging profile parameter are:

License Key value is "always"

logtransparentuserdatalevel	**Transparent User Data Level**	**User-data Logged**
always	always	Yes
always	protocolViolationsOnly	Protocol-Violations
always	never	No
protocol violations only	always	Protocol-Violations

logtransparentuserdatalevel	Transparent User Data Level	User-data Logged
protocol violations only	protocolViolationsOnly	Protocol-Violations
protocol violations only	never	No
never	always	No
never	protocolViolationsOnly	No
never	never	No
always	encrypt-always	Yes (encrypt Data)
encrypt-always	always	Yes (encrypt Data)

License Key value is "protocolViolationsOnly"

logtransparentuserdatalevel	Transparent User Data Level	User-data Logged
never	never	No
never	protocolViolationsOnly	No
protocol violations only	never	No
protocol violations only	protocolViolationsOnly	Protocol-Violations
never	always	Not possible
always	always	Not possible
always	protocolViolationsOnly	Not possible
always	never	Not possible
protocolViolationsOnly	always	Not possible
any value	encrypt-always	Not possible
encrypt-always	any value	Not possible

License Key value is "never"

logtransparentuserdatalevel	Transparent User Data Level	User-data Logged
never	never	No
protocol violations only	protocolViolationsOnly	Not possible
never	protocolViolationsOnly	Not possible
protocol violations only	never	Not possible
never	always	Not possible
always	always	Not possible
always	protocolViolationsOnly	Not possible
always	never	Not possible

logtransparentuserdatalevel	Transparent User Data Level	User-data Logged
protocol violations only	always	Not possible
any value	encrypt-always	Not possible
encrypt-always	any value	Not possible

15.3 Event Logging

Event log records are created instantaneously, when an event occurs. Each event record is defined in ASN.1 form, and expresses what event has occurred to which object (such as a short message) in what moment. Multiple events for the same object can be correlated and sorted by timestamp, producing the event trail for that object. You can use the Event Logs Search within the Customer Care Interface (CCI) to view the event trail of a short message.

To enable event logging, create an event logging profile in the MGR (**Logging ➤ Events ➤ Profile**) and assign it to a property (**Logging ➤ Events ➤ Properties**). The supported objects are short messages and unexpected TCAP messages. You can create up to 100 event log profiles.

15.3.1 Logging of Unexpected TCAP Messages

In case of fraud attempts between operators, unexpected TCAP end messages or TCAP continue messages with a ReturnResult will be received by an operator. These unexpected messages are identified as messages with no existing dialog and can be logged as stipulated in section 1.1.3 of AA.50 and section 3.1.3 of IR.71, industry-standard documents for SMS fraud detection and prevention.

Only the unexpected TCAP messages will be logged when they arrive at the RTR.

Note: Late responses on outgoing TCAP dialogs (i.e. responses after a timeout) will result in logging these responses as unexpected TCAP messages.

The following TCAP information will be logged:

- MTP3 originating point code
- SCCP calling party address (including country and network when provisioned)
- SCCP called party address (including country and network when provisioned)
- TCAP message type (end or continue)
- TCAP originating transaction ID (in case of TCAP continue)
- TCAP destination transaction ID
- Application context name

Logging of unexpected TCAP messages only logs messages that are received directly on the RTR/FWL. Unexpected TCAP messages going directly to other SMS components (for example, the SMSC in FWL-only deployments) are not logged. Those messages should be logged by the SMSC, as the RTR/FWL does not see these messages. If these other SMS components do not have unexpected TCAP logging capabilities, all MT traffic should be directed through the RTR/FWL, so unexpected TCAP message logging of the RTR/FWL can be used for these SMS components too.

15.3.2 Creating Event Logging Profiles

To create a logging profile:

1. In the left navigation bar, select **Logging ➤ Events ➤ Profile**.
   The Event Logging Profiles tab appears.
2. Click **Add New**.
   A new Event Logging Profiles tab appears.
3. Enter a unique name for the profile in the **Name** box (maximum 31 characters).
4. Optionally enter a description of the profile in the **Description** box.
5. In the **Processing Directory** box, enter the location in which to store the log files while they are being created (defaults to `/var/TextPass/log/processing`).

   Note: In a multi-instance setup, the processing directory will be shared by all the NMM component instances running on a node.
6. In the **Finished Directory** box, enter the location in which to store the log files after they are created (defaults to `/var/TextPass/log/available`).

   Note: In a multi-instance setup, the finished directory will be shared by all the NMM component instances running on a node.
7. In the **Filename Template** box, enter the template to use to name the log files (defaults to `%N_event_%U_%h_%Y%m%d_%H%M%S_%3.dat`).

   Important: As multiple components on the same system may share an event logging profile configuration, it is important to include the `%N` escape sequence, which will be translated to the component name. This ensures that multiple components will not try to create files with identical names.

   Important: If multi-instances of NMM components are running on the same node, then it is important to include `%U` escape sequence, which will be translated to `UID` (operating system user identifier). This ensures that multiple components will not try to create files with identical names.
8. In the **Max. File Size** box, enter the maximum size of a log file in bytes (defaults to 1,048,576 bytes, which is 1 MB). The range is 1024 byes (1 KB) to 1,073,741,824 bytes (1 GB).
9. In the **Max. File Duration** box, enter the maximum duration of a log file in seconds (defaults to 3600 seconds, which is 1 hour). The range is 1 second to 2,678,400 seconds (1 month).
10. In the **Max. File Records** box, enter the maximum number of records to allow in a log file (defaults to 10,000 records). The range is 1 record to 10,000,000 records.
11. In the **Starting Sequence Number** box, enter the number with which to start the log file numbering sequence (defaults to 0).
12. Click **Save**.
    The MGR creates the logging profile and closes the tab.
13. Activate the profile.

15.3.2.1 Configuring Event Logging Copies

For each event logging profile, you can create a list of directories in which the LGP will save copies of the files in the profile's **Finished Directory**. You can use this functionality to ensure that an automatic backup of completed files exists. The list for each event logging profile can contain up to 10 directories.

Note: The **Finished Directory** and all directories containing copies must be on the same disk partition as the **Processing Directory**.

Prerequisites:

- Event logging profile

To add a directory to an event logging copies list:

1. In the left navigation bar, select **Logging ➤ Events ➤ Profile**.
   The Event Logging Profiles tab appears.
2. Click the name of an event logging profile.
3. In the Event Logging Copies section, click **Add New**. A new Event Logging Copies List tab appears.
4. In the **Copy Directory** box, enter a directory in which the LGP should create hard links to the files in the **Finished Directory** (defaults to `/var/TextPass/backup`).
   You can only add a directory to the list if the event logging profile is deactivated.
5. From the **Event Log Profile** list, select the profile to use for this copy location (defaults to the profile that you clicked earlier).
6. Click **Save**.
   The MGR closes the tab and adds the directory to the Event Logging Copies list.
7. On the event logging profile tab, click **Add New** to add another directory to the list, or click **Save** to save the profile.

15.3.3 Configuring Event Logging Properties

The event logging properties are used to set a specific log profile for certain events.

Prerequisites:

- Event logging profile

To configure event logging properties:

1. In the left navigation bar, select **Logging ➤ Events ➤ Properties**.
   The Event Logging Properties tab appears.
2. Select an event logging profile for:

Option	Description
Short Message Events	Events related to the processing of Short Messages, that are used for the Event Logs Search within the Customer Care Interface (CCI) component.
Rogue TCAP Events	Events that are used for unexpected TCAP messages (that is, TCAP messages for which no TCAP dialog exists). All unexpected TCAP End

Option	Description
	and TCAP Continue messages with a `ReturnResult` message will be logged to this profile when they arrive at the RTR.

3. Click **Save**.
   The MGR saves the event logging properties and closes the tab.

15.4 Log File Creation

Log files are always generated in the processing directory. When the file has been generated, it is moved to the finished directory. Files in the finished directory can be further processed by the operator.

The log record is written to the log file that is currently open. This log file will be closed and physically written to disk based when any of the following conditions become true:

- Maximum file duration time limit reached. If the time since the creation of the log file has exceeded the value defined in the maximum file duration as configured in the log profile, the log file is closed and written to disk, and a new log file is created.
- Maximum file size limit reached. If the log file size reaches the maximum file size as configured in the log profile, the log file is closed and written to disk, and a new log file is created.
- Maximum file records limit reached. If the number of log records reaches the maximum log records as configured in the log profile the log file is closed and written to disk, and a new log file is created.

Chapter 16

SMS Statistics

Topics:

16.1 Introduction

A prerequisite before improving the quality of service (QoS) of the SMS service is determining the traffic profile and the key performance indicators, such as message success rate, message volume per destination, and differentiated peak throughput figures in several time intervals.

These performance indicators can be viewed in the routing rule counters and counting rules.

16.2 Routing Statistics

For every routed message per network layer, the RTR stores statistical information in counters. Signalling network counters are available on the MTP3, SCCP, and TCAP levels. The following table provides an overview of the counters:

Entity	Originator	Destination
Application	AO (short number)	AT (short number)
Network	MO (originating global title)	MT (destination global title)
Country	MO (originating global title)	MT (destination global title)
Router	MO	MT

For each entity, totals counters are broken down into error and success counters.

16.3 SMS Firewall Statistics

The FWL can provide a specific set of statistical counters tailored to its functionality. These counters fall into the following categories:

- Detailed applied counters for MO routing rules
- Detailed counters for validation and action statistics on MT-MT routing rules
- Country and network specific counters on MO spoofing

The MT routing counters differentiate between SRI-SM and MtForwardSm.

16.4 User-Defined Counting

User-defined counting rules count messages that match specific rule conditions. Counting rules are defined in the MGR.

Counting rules have the same flexible rule structure as routing rules. The main difference is that counting rules do not have an associated action; their implicit action is to count the number of messages that match the rule conditions.

All active mobile-originated counting (MOC) rules are executed for each incoming MO from the SS7 network and are counted if the conditions apply. If a message generates an error (for example, "service center congested"), the corresponding error counter is incremented. In this way, specific error conditions can be monitored by user-defined counting rules.

All active outgoing mobile-terminated counting (MTOC) rules are executed for outgoing MT messages, which consist of a SendRoutingInfoForSm (SRI-SM) operation to an HLR and an MTForwardSm operation to the MSC. If an error occurs in one of these messages (for example, "absent subscriber"), the corresponding error counter is incremented. If the MT message is successfully delivered, the success counter is incremented.

Note: The conditions in the counting rules operate on message requests. The message response determines the counter that will be updated. For example, when an MTOC rule is active based on an IMSI or IMSI range condition, the SRI-SM counters of the MTOC rule are not updated. This is because the IMSI is not part of a SRI-SM request, but part of the SRI-SM response. The MT total and the MTForwardSm counters are updated.

Examples of user-defined counting rules are:

- Count voicemail traffic (has a high "absent subscriber" error rate)
- Count MO messages from outbound roamers (home network subscribers using a foreign network but the home SMSC)
- Count MO-MT messages of test phones to specifically see the results messages sent and received by the test phones (enables testing while the RTR handles other traffic)

You configure MOC and MTOC counting rules using the MGR's Web-based interface. The conditions that are available for counting rules are described in the MGR Operator Manual.

Chapter 17

OAM Interface (SNMP)

Topics:

17.1 Introduction

The RTR uses the Simple Network Management Protocol (SNMP) to configure and monitor interfaces, system statuses, and settings. SNMP is a widely used industry standard for managing and configuring network components.

Note: Because the RTR device stores its configuration in volatile memory, the default configuration is always restored after booting the RTR device.

17.2 MIB Files

All statistical and configuration information (including internal values) that can be configured and/or viewed with SNMP are described in the Management Information Base (MIB) files (`*.my`).

The following MIB files apply to RTR:

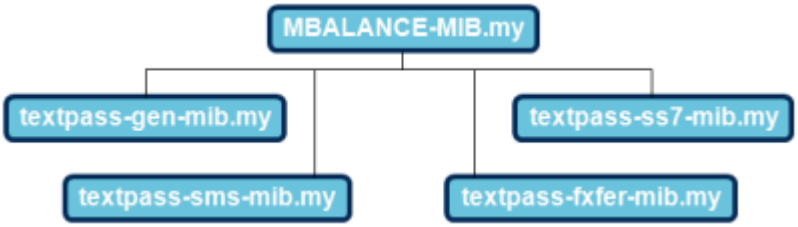


Figure 64: MIBs

Each MIB is stored in a separate `*.my` file. Due to the size of the MIB files, they are not included in this manual. However, they can easily be viewed in the RTR system. The MIB files are located in `/usr/local/share/snmp/mibs/`.

17.3 SNMP Manager

For configuration and monitoring purposes, an SMNP Manager or Management Station issues SNMPv1 requests to the RTR. SNMP Managers should send such requests to UDP port 11661 of the RTR. The device does not enforce an SNMP Manager to originate requests from any specific UDP port (any UDP port can be used for this purpose).

The device requires an SNMP Manager to use a community string equal to:

- `public` for read operations
- `private` for set operations

The RTR silently discards any request that does not satisfy these requirements.

Note: If '`snmpPropListenAddressType`' parameter in semi-static configuration file is set to 'dual', then RTR will accept requests on both IPv4 and IPv6.

17.4 Trap Service

Up to seven SNMP managers can subscribe to the RTR trap service. When a trap condition occurs, the RTR sends an SNMP trap to any SNMP management station that is subscribed to the trap service.

To subscribe an SNMP manager to the trap service, add an entry to the alarm station table that contains:

- The IP address (IPv4 or IPv6) or Hostname of the SNMP manager
- A UDP port number to which traps should be sent for that particular SNMP manager

The alarm station table is also SNMP manageable; refer to the `TEXTPASS-GEN` MIB for more information about this table.

The RTR always originates SNMP traps from UDP port 11162 and terminates them in the UDP ports that are specified in the alarm station table. The community string that the RTR specifies in SNMP traps is always equal to `public`.

The RTR uses an SMNP trap daemon to log generated SNMP traps locally in `/var/log/messages`. The daemon uses UDP port 11173.

Note:

1. If '`snmpPropAlarmOwnIpv6Address`' parameter in semi-static configuration file is set, then specified address will be used as source address for sending SNMP traps to SNMP Manager with address of type IPv6.
2. If '`snmpPropAlarmOwnIpAddress`' parameter in semi-static configuration file is set, then specified address will be used as source address for sending SNMP traps to SNMP Manager with address of type IPv4.

17.5 Trap Filtering

SNMP trap filters to be applied on the NewNet Mobile Messaging component(s) and can be customised per configured alarm station. This filtering can be configured using a combination of black-listing and white-listing of traps in two tables that are associated with the alarm stations table:

- **Whitelist table**—Contains a list of all traps that should be sent toward an alarm station (wild-cards are allowed)
- **Blacklist table**—Contains a list of traps that should be blocked for a particular alarm station (wild-cards are allowed)

Note: The whitelist is applied before the blacklist. An empty whitelist is identical to a whitelist of "*". An empty blacklist does not block any trap.

The following rules and restrictions apply:

- Creating a whitelist for a trap belonging to a specific MIB, implicitly blacklists all other traps from that MIB, for the alarm station the whitelist is configured on.
- It is *not* possible to have a black- and whitelist for traps that belong to the same MIB and for the same alarm station. It is possible to combine both a black- and whitelist for a specific trapreceiver, as long as the black- and whitelist do not contain entries from the same MIB.

17.6 Device Type Variable Binding

When an SNMP trap occurs, the generic SNMP library that the RTR uses automatically adds an extra variable binding to the trap. This variable contains the product name as specified in the global variable module. The product name is the last variable in the trap message. This feature allows trap receivers to distinguish among traps from different products.

The following are examples of traps with the device type variable:

```
$11:28:41 TEXTPASS-GEN-MIB::deviceOperationalStateChanged TEXTPASS-
GEN-MIB::deviceOperationalState.0 = INTEGER: starting(1) TEXTPASS-
GEN-MIB::deviceType.0 = STRING: "AMS" from system1.asd.mbalance.com

11:28:41 TEXTPASS-GEN-MIB::deviceOperationalStateChanged TEXTPASS-
GEN-MIB::deviceOperationalState.0 = INTEGER: synching(4)
TEXTPASS-GEN-MIB::deviceType.0 = STRING: "AMS" from
system1.asd.mbalance.com

11:28:48 TEXTPASS-GEN-MIB::deviceOperationalStateChanged TEXTPASS-
GEN-MIB::deviceOperationalState.0 = INTEGER: operating(2)
TEXTPASS-GEN-MIB::deviceType.0 = STRING: "AMS" from
system1.asd.mbalance.com

11:28:56 TEXTPASS-AMS-MIB::rtrUnAvailable TEXTPASS-GEN-
MIB::deviceType.0 = STRING: "AMS" from system1.asd.mbalance.com

11:28:57 TEXTPASS-GEN-MIB::deviceOperationalStateChanged TEXTPASS-
GEN-MIB::deviceOperationalState.0 = INTEGER: adminDisabled(0)
TEXTPASS-GEN-MIB::deviceType.0 = STRING: "AMS" from
system1.asd.mbalance.com

11:28:57 TEXTPASS-GEN-MIB::deviceOperationalStateChanged TEXTPASS-
GEN-MIB::deviceOperationalState.0 = INTEGER: synching(4)
TEXTPASS-GEN-MIB::deviceType.0 = STRING: "AMS" from
system1.asd.mbalance.com

11:28:58 TEXTPASS-GEN-MIB::networkDiscoveryNodeAdded TEXTPASS-GEN-
MIB::lastSnmpErrorString.0 = STRING: "node_type=RTR, port=25092,
ip1=10.0.0.46"       TEXTPASS-GEN-MIB::deviceType.0 = STRING: "AMS"
from system1.asd.mbalance.com
```

Chapter 18

PLMN Interface (SS7)

Topics:

18.1 Introduction

The RTR uses the Mobile Application Part (MAP) protocol over SS7 to interface with the mobile network. The RTR specifically uses the MSC/SGSN and SMSC mobile network components.

18.2 SS7 Addressing

The core components of a mobile network, the MSC and the HLR, are connected through the SS7 protocol. Each mobile operator has its own SS7 network. The international SS7 network arranges interconnection of an operator's SS7 network with other SS7 networks.

The SS7 networks are thus arranged in two planes: the top plane of the international SS7 network and the bottom plane of the SS7 networks of various operators. The network indicator that is sent in each SS7 packet reflects the network type on which it is conveyed.

18.2.1 Signalling Link Selection (SLS)

The valid values of SLS depend on the SCCP flavour supported by the RTR:

- ITU-T - 0 to 15
- ANSI - 0 to 255
- Japanese SS7 - 0 to 255

For Japanese SS7 flavour, the RTR ignores bits 4-7 of the SLS when a value greater than 15 is received and only transmits out the SLS value within the range 0-15.

18.2.2 Signaling Point Code (SPC) Addressing

Each entity within a SS7 network is addressable with a Signaling Point Code (SPC). An entity can only be addressed with its SPC if it is accessed from within the same SS7 network, because SPCs are only unique within one network.

The valid values and format of signaling point codes depend on the SCCP flavour supported by the RTR. The SCCP flavour can be any one of the following:

- ITU-T
- ANSI
- Japanese SS7

The actual SCCP flavour is controlled by the *Software License*.

For the ITU-T flavour, the RTR supports 14-bit signaling point codes. A valid ITU-T SPC can be represented as follows:

- Decimal integer (**Range**: 0-16383)
- String (3-8-3 format indicating the Area/Network, Cluster, and Member)
  - Area/Network is represented by the most significant 3 bits (**Range**: 0-7)
  - Cluster is represented by the next 8 bits (**Range**: 0-255)

- Member is represented by the least significant 3 bits (**Range**: 0-7)

For the ANSI flavour, the RTR supports 24-bit signaling point codes. A valid ANSI SPC can be represented as follows:

- Decimal integer (**Range**: 65536-16777215)
- String (8-8-8 format indicating the Area/Network, Cluster, and Member)
  - Area/Network is represented by the most significant 8 bits (**Range**: 1-255)
  - Cluster is represented by the next 8 bits (**Range**: 0-255)
  - Member is represented by the least significant 8 bits (**Range**: 0-255)

Note: The Network value cannot be 0 (zero) in an ANSI SPC string.

For the Japanese SS7 flavour, the RTR supports 16-bit signaling point codes. A valid Japanese SS7 SPC can be represented as follows:

- Decimal integer (**Range**: 0-65535)
- String (5-4-7 format indicating the Main Number Area/Network, Sub Number Area/Cluster and Unit Number/Member)
  - Main Number Area/Network is represented by the least significant 5 bits (**Range**: 0-31)
  - Sub Number Area/Cluster is represented by the middle 4 bits (**Range**: 0-15)
  - Unit Number/Member is represented by the most significant 7 bits (**Range**: 0-127)

The following formula is used by the RTR for computing the decimal integer value of a Japanese SS7 SPC that is given in the string format:

```
Integer value of SPC = [Unit Number * 512] + [Sub Number Area * 32] + Main Number
Area
```

18.2.3 Global Title (GT) Addressing

To enable access to entities in other SS7 networks, most SS7 entities are also addressable with one or more global titles (GTs). Unlike an SPC, a GT is a worldwide unique identification of an SS7 entity over all SS7 networks. Therefore, GT addressing is used for inter-network addressing. GT addressing is also widely used for intra-network addressing as well.

The following diagram illustrates intra-network addressing (between 3 and 4) and inter-network addressing (between 1 and 3). The network elements 1 and 3 have the same SPC. However, none of the network elements 1, 2, 3, or 4 have the same GT.

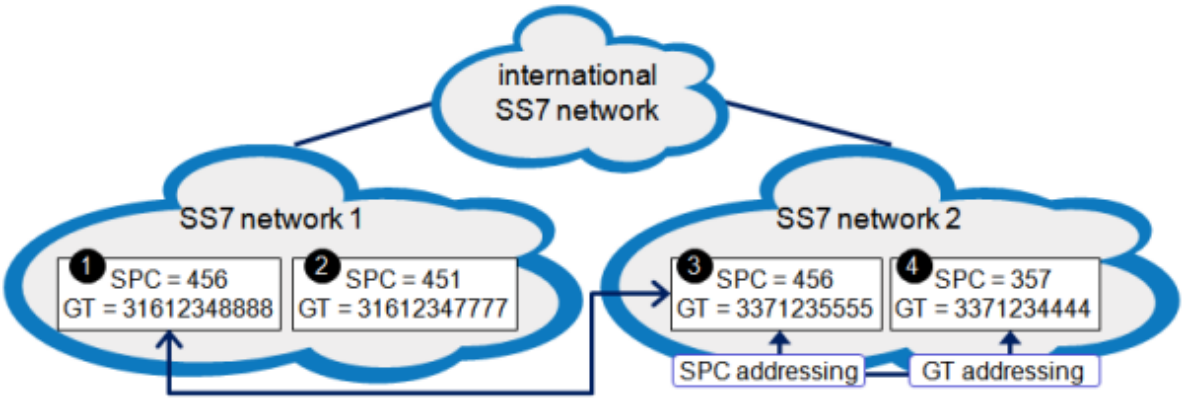


Figure 65: GT addressing

A global title consists of several fields. The most important fields are:

Field	Description
Global Title Address Information (GTAI)	Usually contains an E164 address. Network entities such as MSCs, HLRs, and SMSCs have an E164 address that uniquely identifies them. An HLR is addressable by multiple GTs: the HLR's specific E164 address, and GTs with an E164 address of any mobile for which the HLR holds subscriber data.
SubSystem Number (SSN)	Identifies the type of SS7 entity: • 6—HLR • 7—VLR • 8—MSC
Translation Type (TT)	Used for routing purposes.

Note: In certain cases the GT Address in an incoming message (i.e. the SCCP Calling Party or Called Party Address) may contain an IMSI as per the E.212/E.214 numbering plan format. This does not affect the processing of incoming messages when the MAP screening functionality is used. The MAP Screener can intercept an incoming message irrespective of whether the SCCP addresses are in the E.164 format or the E.212/E.214 format.

18.2.4 Signalling Transfer Point (STP)

The signalling transfer point (STP) is an SS7 entity that is primarily concerned with the routing of packets for which GT addressing is used. When two entities interact, traffic normally flows from the originating entity, through one or more STPs, to the terminating entity. An STP decides the entity (another STP or the terminating entity) to which a packet should be routed.

The STP carries out routing based on the GT that is specified as the destination address of the packet. Sometimes, an STP may need to change the GT to another GT, or to revert to SPC addressing. This process is called global title translation (GTT).

18.2.5 Router Specifics

The RTR is associated with a specific SPC and a specific GT. Also, the RTR can be associated with a virtual SPC, which multiple RTRs can share. The virtual SPC enables addressing a group of RTRs, using a single SPC.

For example, in the following configuration:

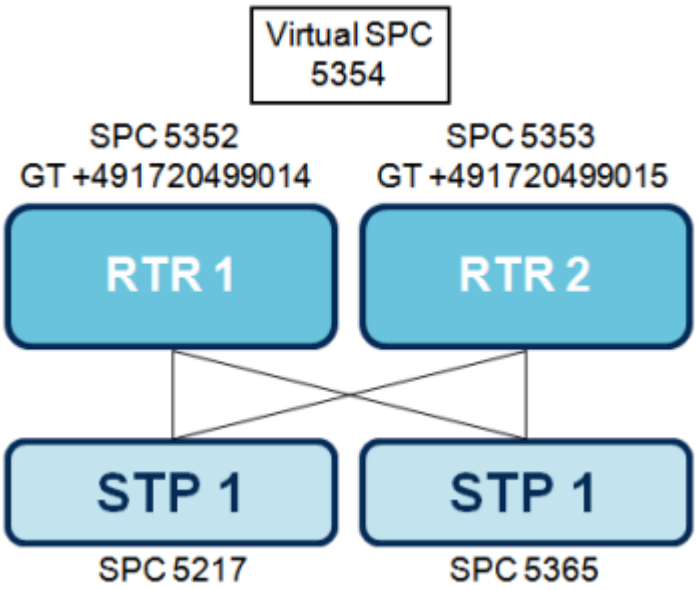


Figure 66: SS7 addressing interface

On STP1 and STP2, the following should be configured:

- SPC 5352 reachable directly through linkset with adjacent SPC 5352
- SPC 5353 reachable directly through linkset with adjacent SPC 5353
- SPC 5354 reachable indirectly through linkset with adjacent SPC 5352 and through linkset with adjacent SPC 5353

The following information about RTR addressing uses RTR 1 as an example.

18.2.5.1 MSUs on the MTP Level

On the MTP level, an incoming MSU is processed when the destination point code in the MTP routing label equals the specific SPC (5352) or the virtual SPC (5354). Any other MSU is discarded.

When an RTR sends an MSU, the originating point code in the MTP routing label always equals the specific SPC (5352).

18.2.5.2 MSUs on the SCCP Level

On the SCCP level, the RTR outputs UDTs with a routing indicator in the SCCP called party address and in the SCCP calling party address equal to the GT or to the SSN. The RTR always sets the routing indicators in the two addresses to the same value. This method improves efficiency, as it reduces the number of GT translations that the network must perform.

18.2.5.3 Addressing Using GT: Specific SPC

When addressing the RTR using GT and the destination point code in the MTP routing label equals the specific SPC (`5352`), the GT in the SCCP called party address must be the same length or longer than the RTR's global title (11 digits or more).

The corresponding digits in the GT in the SCCP called part must be the same as the RTR's global title (`+49172049901`). Any extra digits are ignored.

When addressing the RTR using GT and:

- The destination point code in the MTP routing label equals the specific SPC, and
- The translation type equals the semi-static configuration file attribute `ttwhenincludingmscaddrinmofwdsmtosmsc`

The message is accepted, regardless of the GT used to address the RTR.

18.2.5.4 Addressing Using GT: Virtual Point Code

When addressing the RTR using GT and the destination point code in the MTP routing label equals the virtual point code (`5354`), every valid GT in the SCCP called party address is accepted. If this is not the case, the RTR will discard the UDT.

18.2.5.5 Addressing Using SSN

When addressing RTR1 using SSN, the GT (if present) in the SCCP called party address is not checked at all. Each incoming UDT is accepted as long as the destination point code in the MTP routing label equals the specific SPC or the virtual SPC.

18.2.5.6 Outputting a UDT

When an RTR outputs a UDT, the SCCP calling party address always contains the RTR's GT and SSN 8, provided the routing indicator is set to GT. When the routing indicator is set to SSN, the SCCP calling party address only contains SSN 8. However, the exception to this behaviour is when optimised MO routing is in use.

When the `includemscaddressinmoforwardsm` variable is set, the RTR uses the MSC address as the SCCP calling party address for MoForwardSm operations.

18.3 MO Routing

18.3.1 Conventional MO Routing

MO traffic can be routed to SMSCs in a conventional way or in an optimised way. The following diagram illustrates the conventional method:

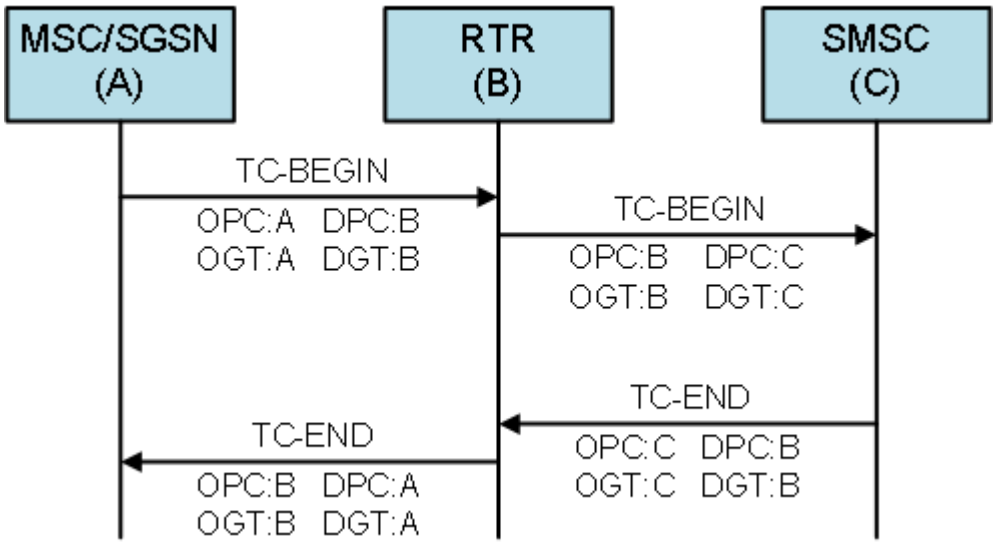


Figure 67: Conventional MO routing

The DPC and DGT in the TC-BEGIN from the MSC/SGSN to the RTR are the specific SPC and the specific GT for that RTR. When the virtual point code functionality is in use, the DPC is equal to the virtual point code, while the DGT can have any value.

18.3.2 Optimised MO Routing

The RTR's MO optimisation functionality saves resources on the RTR and on the STP. Optimisation comprises the RTR spoofing the SCCP calling party addressing when sending the TC-BEGIN toward the SMSC in a way that will cause the SMSC to send the TC-END directly to the MSC/SGSN. With this method, the RTR is not involved in relaying the TC-END to the MSC/SGSN. The 'Optimized MO routing' affects only the TCAP dialogues comprising of a TC-BEGIN and a TC-END. It does not apply to dialogues that include a TC-Continue.

The following diagram illustrates optimised MO routing:

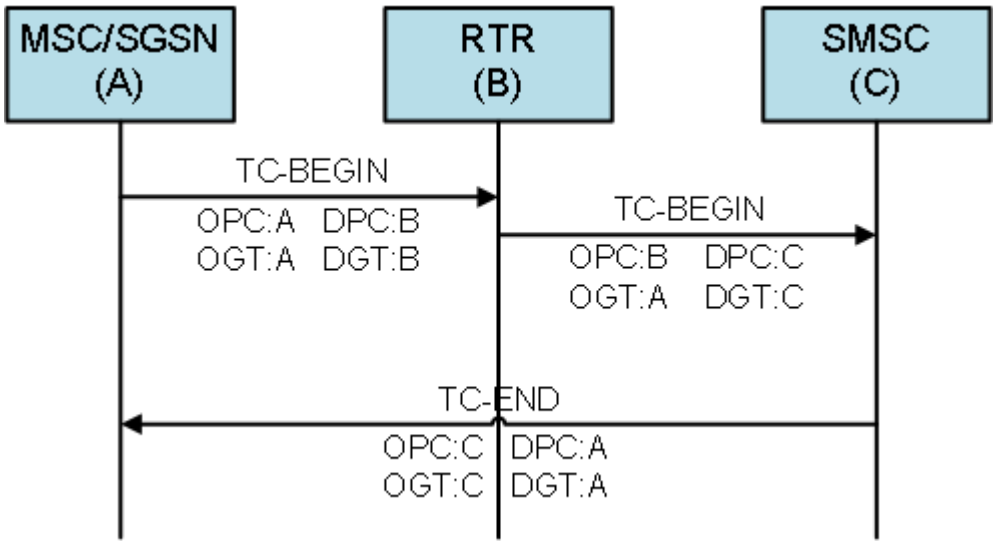


Figure 68: Optimised MO routing

The DPC and DGT in the TC-BEGIN from the MSC/SGSN to the RTR are the specific SPC and the specific GT for that RTR. When the virtual point code functionality is in use, the DPC is equal to the virtual point code, while the DGT can have any value.

18.3.3 Segmented TCAP Dialogue

The following diagram illustrates how the RTR handles an MO message that the MSC offers to the RTR as a segmented TCAP dialogue.

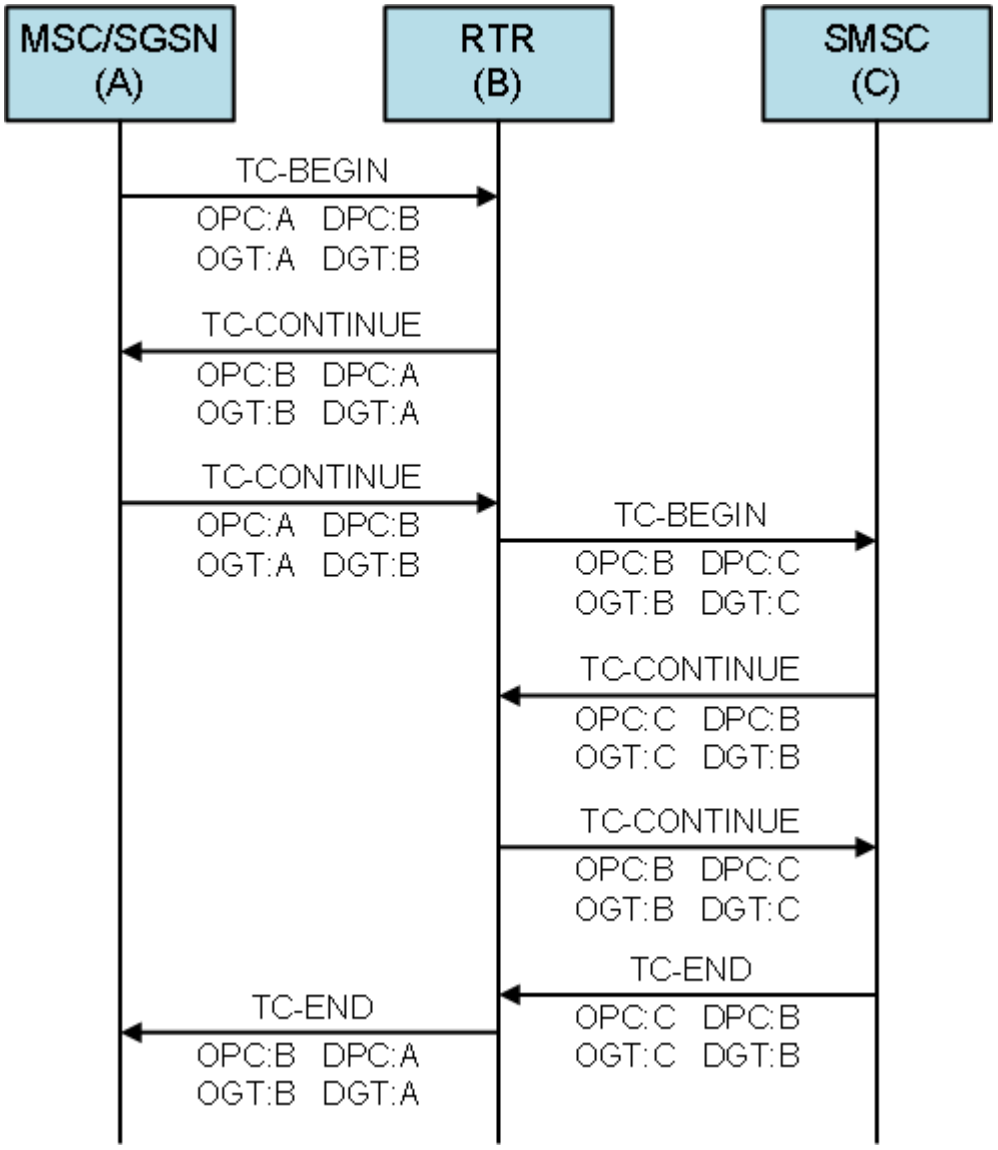


Figure 69: Segmented TCAP dialogue

The DPC and DGT in the TC-BEGIN from the MSC/SGSN to the RTR are the specific SPC and the specific GT for that RTR. When the virtual point code functionality is in use, the DPC is equal to the virtual point code, while the DGT can have any value.

18.3.4 Tracking SMSC Status

MTP and SCCP management offer methods to track SMSC status. However, some SMSC brands are not available at the application level. Therefore, the RTR uses an alternative method for tracking the SMSC status. In this method, the RTR starts a segmented TCAP dialogue for an MO message toward the SMSC and aborts it after receiving a TC-CONTINUE from the SMSC.

The following diagram illustrates the method:

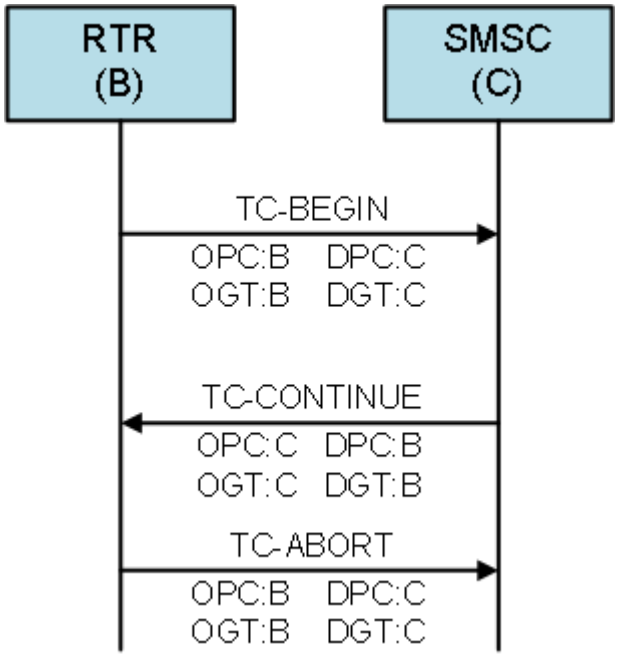


Figure 70: Tracking SMSC status

18.4 MT Routing and Delivery

An attempt to deliver an MT message consists of a sequence of operations:

1. SRI-SM—Queries the HLR for information about the destination, including the address of the serving MSC and flags specifying the availability for MT messages.
2. MtForwardSm—Requests the serving MSC to deliver the message to the destination.
3. ReportSmDeliveryFailure—Only issued when any of the flags that specify the availability for MT messages has changed.

   The operation updates these flags.

Delivery attempts may fail for various reasons. Most commonly, the destination is not reachable (for example, the mobile phone is switched off). This case leads to an AbsentSubscriber error.

Another common error is MemoryCapacityExceeded, which indicates that the destination mobile phone does not have enough memory to store the message.

18.4.1 Optimized MT Routing

In MAP phase 2+, the HLR's availability flags indicate whether the `AbsentSubscriber` and/or `MemoryCapacityExceeded` error conditions are in effect. When optimized MT delivery is enabled, the RTR takes these flags into account for certain paths. If the flags specify that the destination is unavailable, the RTR may consider the delivery attempt to be undesirable and not issue a MT delivery request to the MSC or SGSN.

For the paths starting with MO-MT, optimized MT delivery is enabled by default. To disable it, set the `optimisedmtdelivery` parameter in the semi-static configuration file to "false".

For the paths starting with AO-MT, optimized MT delivery can be specified on a per-application basis.

For delivery attempts from the AMS, the RTR does not take these flags from the HLR into account and continues to issue a request to the MSC or SGSN.

Note:

When the following conditions are true, RTR will treat the HLR query result for that destination as a temporary failure even if the concerned subscriber's IMSI is provided in the SRI-SM response:

- HLR's availability flags for a MS destination indicate that it is unavailable
- Optimized MT delivery is enabled

In case the result of an Early Recipient Query for a MO message is considered as a temporary failure due to the above reasons, then the RTR does not use the recipient subscriber's IMSI for the purpose of matching a MOR rule condition (even if the IMSI is known). Hence any MOR rule configured with a 'Recipient IMSI' condition would not match in this scenario.

In such a case it is recommended to configure an appropriate 'Recipient Query Result' condition instead of a 'Recipient IMSI' condition for the relevant MOR rule(s).

18.4.2 Preferred MT Destination

SMS over GPRS is available as of MAP phase 2+. This functionality provides the RTR with two paths toward the destination:

- The conventional path through the MSC
- A new path, through the SGSN

If the `enablegprssupportindicator` semi-static parameter is set to true, the RTR will include the GPRS support indicator in the SRISM Request to inform the external network that the RTR is capable of combined delivery via MSC and/or via SGSN.

If both `enablegprssupportindicator` and `enablegprssupportindicatorfordomestichlrqueryonly` semi-static parameters are set to true, the RTR will add GPRS support indicator in SRI-SM only if the HLR is domestic. The following table describes various scenarios related to these parameters:

enablegprssupportindicator fordomestichlrqueryonly	**enablegprssupportindicator**	**GPRS Support Indicator in SRI-SM to Domestic HLR**	**GPRS Support Indicator in SRI-SM to International HLR**
true	true	yes	no
true	false	no	no
false	true	yes	yes
false	false	no	no

The **SRISM GPRS Support Indicator** in the **Firewall ➤ MT ➤ Properties** configuration, provides a finer control over the usage of the configuration parameter `enablegprssupportindicator` in the home routed scenario. The **SRISM GPRS Support Indicator** supports the following options:

- **Default**: With this configuration, the RTR transparently forwards the received value of the GPRS support indicator in the incoming SRI-SM request. When the SRI-SM request is being modified due to a modifier or TCAP User Info addition then the inclusion/absence of the GPRS support indicator field is governed using `smsPropEnableGprsSupportIndicatorForSriSmRequest` parameter.
- **Off**: With this configuration, the RTR will not set the "GPRS support indicator" in the SRI-SM request regardless of the inclusion/absence of the GPRS support indicator in incoming SRI-SM. This behavior is only applicable when the MTOR action is configured as "Pass". However, in case the MTOR action is set as "Release", then the SRI-SM request is forwarded transparently.
- **On**: With this configurations, the RTR will set the "GPRS support indicator" in SRI-SM request regardless of the inclusion/absence of GPRS support indicator in incoming SRI-SM. This behavior is only applicable when the MTOR action is configured as "Pass". However, in case the MTOR action is set as "Release", then the SRI-SM request is forwarded transparently.

Note:

1. This parameter is only applicable when the Japanese MNP functionality is enabled in the RTR and the country determined from SCCP CDPA / MSISDN is same as the home country. If any of the mentioned conditions fail then RTR will behave as if the configured value of **SRISM GPRS Support Indicator** as "Default".
2. In case of Japanese MNP if the MNP action for the first SRI-SM is forward, then second SRI-SM is sent. This second SRI-SM will never have the GPRS support indicator enabled.

By default, the RTR's preferred MT destination is the MSC. To change the preferred destination to the SGSN, set the `preferredmtdestination` parameter in the semi-static configuration file to "`sgsn`".

If the Network configuration is available according to the MSC and/or SGSN (i.e. received in the HLR query), the '**Preferred MT Destination**' in the Network configuration overrides the '`preferredmtdestination`' semi-static parameter. The '**Preferred MT Destination**' supports the following options (go to **MGR ➤ Environment ➤ Networks**):

- **MSC**
- **SGSN**
- **Use Global Setting**

If the '**Preferred MT Destination**' is set to '**Use Global Setting**', the RTR's preferred MT destination is determined based on the '`preferredmtdestination`' semi-static parameter.

The RTR will always issue an MT message through the preferred path first. If delivery through this path fails, the RTR attempts to delivery through the alternative path (provided this is a valid option; refer to 3GPP TS 29.002 for more information).

If the Network configuration is available according to MSC and/or SGSN (i.e. received in the HLR query) and the delivery through the preferred path fails, the RTR attempts to deliver through the alternative path based on the following Network configuration's parameter (go to **MGR ➤ Environment ➤ Networks**):

- Enable fallback to Secondary dest.

If this parameter is set (i.e. checked in the MGR), then only the RTR attempts the alternative path for MT delivery; otherwise, the RTR considers the MT delivery as failed with temporary error.

If the Preferred MT Destination is configured as either MSC or SGSN in the RTR and the RTR receives only one destination address in the SRISM Response which is not same as the Preferred MT Destination, then the MT Delivery depends on the '`Enable Fallback to Secondary Dest`'.

If it is enabled, then the message deliver to destination which was received in SRISM response. Otherwise the RTR considers MT delivery as failed with temporary error.

The semi-static configuration parameter *firewallallowfallbacktosecdest* allows the fallback to secondary destination functionality to be applicable on the home-routed scenarios as well.

If the `firewallallowfallbacktosecdest` is set to true, on receiving both MSC and SGSN address in the SRISM response from HLR, the RTR will return only one address in the SRISM response to the external SMSC which is RTR's own GT address. On receiving the MtForwardSm, the RTR will attempt delivery on preferred destination as configured in the terminating network (If the network is not configured preferred MT destination is determined based on the *preferredmtdestination* semi-static parameter). In case of failure, if **Enable Fallback to Secondary Dest** is set, then the RTR will re-attempt delivery on secondary destination.

If the option **Enable Fallback to Secondary Dest** is not set, then the RTR will not attempt delivery to secondary destination and sends back error to the SMSC.

If **Preferred MT Destination** is configured as either `MSC` or `SGSN` in the RTR but in SRI-SM Response message the RTR received only one destination address which is not same as the Preferred MT Destination, then the RTR will attempt delivery on secondary destination irrespective of the value configured for **Enable Fallback to Secondary Dest** in the recipient network settings.

In case of Home-Routing scenario, if the `firewallallowfallbacktosecdest` is set to false (this is the default behaviour), on receiving both MSC and SGSN address in the SRISM response from the HLR, the RTR will include its own GT address in both the MSC and SGSN addresses in the SRISM response towards external SMSC.

Note: The RTR will attempt delivery on secondary destination in home routing scenario, irrespective of the value configured for **Enable Fallback to Secondary Dest** in the recipient network settings, if in the SRISM Response message only one destination address from HLR is received and the received destination address is not same as the Preferred MT Destination.

The following table summarizes the RTR's behavior based on the MT-FSM errors encountered on delivery attempt to the preferred destination:

MT FSM Error	RTR behavior
SystemFailure	Delivery attempt is made through the alternative path.
DataMissing	Delivery attempt is made through the alternative path.
UnexpectedDataValue	Delivery attempt is made through the alternative path.
FacilityNotSupported	Delivery attempt is made through the alternative path.
UnidentifiedSubscriber	Delivery attempt is made through the alternative path.
IllegalSubscriber	No delivery attempt is made through the alternative path.
IllegalEquipment	No delivery attempt is made through the alternative path.
SubscriberBusyForMT-SMS	For AO-MT, MO-MT, and Storage then fallback to MT routing paths, if the `gprs_connection_suspended` indicator is set to true, the delivery attempt is made through the alternative path. Otherwise, no delivery attempt is made through the alternative path.

MT FSM Error	RTR behavior
	For MT-MT routing path, when the parameter `fwPropAllowFallbackToSecDest` is set to true, if the first delivery attempt is to the SGSN and the RTR receives a subscriber Busy for MT response without `gprs_connection_suspended` set, the RTR still perform the fallback delivery attempt to the MSC. **Note:** For this particular error, retry is done to MSC only if the first MT-FSM delivery attempt was made to SGSN (as the preferred destination) and the `gprs_connection_suspended` flag was set in the response. In case the first MT-FSM delivery attempt was made to MSC, then there would be no retry for this error.
SM-DeliveryFailure	No delivery attempt is made through the alternative path.
AbsentSubscriberSM	Delivery attempt in this case depends upon whether `absentSubscriberDiagnosticSM` parameter is present in MT-FSM error message. This is applicable for MAP Phase 2+ version. If `absentSubscriberDiagnosticSM` parameter is present in MT-FSM error, then delivery attempt is made through the alternative path based on the value of below diagnostics: • 1 [IMSI detached] • 2 [Roaming Restriction] • 6 [GPRS Detached] • 11 [UE Deregistered] If `absentSubscriberDiagnosticSM` parameter is not present in MT-FSM error, then delivery attempt is made through the alternative path based on the below condition: • MT-FSM Nak response time should be less than value of semi-static configuration parameter `mtfmsnopaingtimeout`. Otherwise, No delivery attempt is made through the alternative path.
MT FSM Timeout	If `fallbacktosecdestonpreferredmtdesttimeout` is set to true, then a delivery attempt is made through the alternative path. When set to false, a retry on secondary destination will not occur. Please refer to section *fallbacktosecdestonpreferredmtdesttimeout* for the semi-static parameter.

18.4.3 More-Messages-to-Send

When multiple messages to a single destination are pending, the messages can be delivered to the destination using a single TCAP dialogue toward the MSC. This feature is called More-Messages-to-Send (MMTS), and is fully supported by the RTR.

18.4.4 Status Reports

Status reports, requested by the originator, are available as of MAP phase 2. A status report is a special message that informs the originator of the status of the MO message.

Status reports are disabled by default. To enable them, set the `statusreportenabled` parameter in the semi-static configuration file to true.

The status report functionality is based on the following parameters:

MO SMS status report requested?	RTR status report enabled?	Modifier on status report	Status report generated?
Yes	Yes	None	Yes
Yes	No	None	No
Yes	Yes or No	Force On	Yes
Yes	Yes or No	Force Off	No
No	Yes or No	Yes or No	No

Note: The RTR does not generate status reports if the MO message is forwarded to the SMSC.

The following `tpconfig` attributes in the semi-static configuration file control the actions for status reports:

- For MT status reports—`actionformtstatusreports`
- For AT status reports—`actionforatstatusreports`

The options are:

Value	Description
route	Try to deliver the message and discard the message if the first attempt fails.
store	Store the message (requires the AMS).
routefallbacktostorage	Try to deliver the message and store the message if the first attempt fails (requires the AMS).

18.4.4.1 Route

If `actionformtstatusreports` is set to route, the following attributes provide control over the RTR's retry scheme:

Attribute	Description	Valid Values	Default
maxstatusreportretries	Maximum number of times that the RTR retries delivery before it considers the status report to be expired. The RTR only retries status report delivery if this attribute is not 0 (zero).	0-20	0
statusreportretryinterval	Interval (in seconds) that the RTR maintains between two consecutive delivery attempts.	1-900	60

18.4.4.2 Store and Route Fallback to Storage

If `actionformtstatusreports` is set to store or routefallbacktostorage, the RTR will send status reports to the AMS (in the case of routefallbacktostorage, the RTR only sends a status report to the AMS if the initial routing of the status report failed with a temporary error).

The following `tpconfig` attributes control the AMS queues in which the status reports are stored:

- For MT status reports, `mtstatusreportsamsqueue`.
- For AT status reports, `regularatstatusreportsamsqueue`.

Set each attribute to the index of the AMS queue, as assigned by (and viewable in) the Manager.

18.4.5 Dialout Delivery Notifications

Normally, the SMSC sends status reports to the originating application. However, in the UCP protocol, applications can specify a notification address to which the SMSC should send status reports. This type of status report is called a dialout delivery notification (DDN). DDNs require the SMSC to set up a session before delivering the status reports.

The AMS can deliver DDNs more quickly when a specific queue is configured for them. In the semi-static configuration file, the `tpconfig` attribute `dialoutatstatusreportsamsqueue` references this queue.

To enable the RTR to generate AMS store requests with the message type dialoutNotification, set the `enabledialoutnotificationasamsmessagetype` attribute to true.

18.4.5.1 Alternative SMSC Selection Scheme for DDNs

The RTR supports an alternative SMSC selection scheme for AO messages that include a request for a notification to be delivered using a dial-out session to a notification server. In this alternative scheme, the RTR distributes AO messages to SMSCs based on the notification address (instead of using a distribution key derived from originator and recipient). A notification server will receive all its notifications from only one SMSC.

By default, the alternative scheme is disabled. To enable is, in the semi-static configuration file, set the `tpconfig` attribute `alternativescselectionforaosmwithdnenabled` to true.

The RTR selects the HUB to send the notification based on the notification address. Therefore, a notification server will always receive dialout sessions for notification deliveries from the same HUB.

18.4.6 Phase 1 Status Reports

For MAP phase 1, the 3GPP 23.040 standard does not define status report messages or a means to request that such messages be generated. Therefore, the RTR supports "phase 1 status reports" that are regular, MT-only messages that are generated by an SMSC, based on provisioned templates.

The RTR supports the following templates:

Status	Semi-Static Configuration Parameter
Succeeded	phase1statusreporttemplateforsucceededstatus
Failed	phase1statusreporttemplateforfailedstatus
Discarded	phase1statusreporttemplatefordiscardedstatus
Expired	phase1statusreporttemplateforexpiredstatus
Deleted	phase1statusreporttemplatefordeletedstatus
Buffered	phase1statusreporttemplateforbufferedstatus

All templates support run-time interpolation of message-specific or delivery-specific variables. These variables can be inserted into a template using the following format:

```
$(<VARNAME>)
```

Where `<VARNAME>` is the name of the variable to be interpolated at that location in the message template.

The following table lists the supported variables and the status report templates in which they can be used:

VARNAME	Description	Support
DESTINATION	Address of the message's recipient	All templates
DISCHARGE_TIME	Discharge time, formatted according to `dttemplateforphase1statusreport`	All templates
ERROR	Error string, formatted as specified by one of the `XYZerrorstringforphase1statusreport` templates, where `XYZ` depends on the delivery error.	Failed, Discarded
SCTS	Service centre timestamp, formatted according to `sctstemplateforphase1statusreport`	All templates

Status report templates and error string templates are configured as UTF-8. Templates containing Unicode characters that cannot be mapped to the UCS2 character set are rejected.

Note: If a template that contains characters that are not part of the GSM 7-bit default alphabet is provisioned, the phase 1 status report will be encoded in UCS2, implying a maximum length of 70 characters.

18.4.6.1 Controlling Phase 1 Status Reports

Phase 1 status reports are triggered when the SMSC recognises MO tags. The SMSC scans the received MO message to find a tag at the beginning of the message (usually starting with `*<TAG>#`). The tag must be in GSM 7-bit format. UCS2 format tags cannot be recognized.

The exact value of `<TAG>` is configured in the `string` attribute of the `motag` entity in the semi-static configuration file. The `function` attribute for requesting a phase 1 status report is phase1statusreport.

For example, the following line from a RTR semi-static configuration file has the effect that messages beginning with `*SR#` trigger the generation of a status report:

```
<motag string="*SR#" function="phase1statusreport"/>
```

If a phase 2 MO message requests both a phase 1 and a phase 2 status report, the configuration parameter `phase1statusreportoverrules` determines whether a phase 1 or a phase 2 status report is returned.

Use the configuration parameter `forcestatusreportfordroppedmomessage` to force the RTR to always generate a phase 1 status report when an MO message was accepted but had to be dropped later, even if the message did not request it.

Note: The RTR only supports `forcestatusreportfordroppedmomessage` for MO-MT routing.

18.4.7 MAP Phase Negotiation

For outgoing MT messages, the RTR supports negotiation of the MAP phase. The initial MAP phase that the RTR uses in negotiation can be set per mobile network entity in the MGR.

18.4.8 MAP Phase Optimization

When the property `smsPropEnableMapPhaseOptimisation` is true (default configuration), the RTR will send SRI-SM to the HLR and MtForwardSM messages to the MSC using MAP phase 1 whenever possible.

For the SRI-SM to the HLR the RTR would use MAP phase 1 under the following conditions:

- Optimised MT delivery (controlled primarily through smsPropOptimisedMtDelivery, but also through an application's corresponding flag and in some cases hardcoded to off) is off for the message.
- The preferred MAP phase is 2.
- The RTR does not intend to update (reportSmDeliveryStatus) the HLR about delivery failure for this message, or that feature is globally disabled (smsPropEnableHlrUpdates). The value of the message-specific flag is only set if the routing path does not involve storage, and not for MO messages.

For the MtForwardSM to the MSC the RTR would use MAP phase 1 under the following conditions:

- the message is delivered to/through an MSC
- TP-MTI is SMS-DELIVER
- TP-MMS is set (i.e. NO more-messages-to-send)
- TP-SRI is false
- TP-UDHI is false
- TP-RP is false

- TP_DCS is 0
- TP-PID is in range of 0-63

18.4.9 TCAP Segmentation for Outgoing MTFSM

TCAP segmentation is the process in which the message information is transferred not as a single TCAP message but is split into two parts, TCAP Dialogue setup and TCAP components (with MAP data) exchange. TCAP segmentation is not supported in case of MAP phase 1.

RTR performs TCAP Segmentation of outgoing MTFSM and MT Status Report based on the following conditions:

1. If SCCP length is more than the value configured in semi-static parameter `sccpMaxPduLengthForTcapSegmentation`, then TCAP Segmentation shall be performed. For more details, please refer section *sccpmaxpdulengthfortcapsegmentation*.
2. TCAP segmentation can also be done based on the MTFSM user data length in bytes.

   The RTR will do TCAP segmentation based on the following configurations:

   1. If the terminating network matches one of the configured network, TCAP segmentation will be performed when MT-FSM user data length is equal to or greater than the minimum of the value configured for the semi-static parameter *rtrmaxuserdatalengthfortcapsegmentation* and the configured value of **MTFSM Max User Data Length for TCAP Segmentation** in the matching network (refer to point 19 of section 7.3 in the MGR OM for more details of this field).
   2. If the terminating network does not match one of the configured network, TCAP segmentation will be performed when the MT-FSM user data length is equal to or greater than the value configured for the semi-static parameter *rtrmaxuserdatalengthfortcapsegmentation*. In this scenario, if the value configured for the parameter `rtrmaxuserdatalengthfortcapsegmentation` is 141, then no TCAP segmentation will be performed.
   3. If the semi-static parameter *rtrmaxuserdatalengthfortcapsegmentation* is configured as "0", then TCAP segmentation will always occur irrespective of the network matching.

      Note:

      1. User data length in octets will includes both TP_UDL and TP_UDH.
      2. In case of GSM7 encoding:

         a. Received TP_UDL represents number of characters
         b. RTR will convert TP_UDL from number of characters to number of octets and then compare it against the configured value of `rtrmaxuserdatalengthfortcapsegmentation` and/or **MTFSM Max User Data Length for TCAP Segmentation** in the matching network.

      3. In case of GSM8 and UCS2 encoding:

         a. Received TP_UDL will represent number of bytes so TP_UDL will directly be compared with the configured value of `rtrmaxuserdatalengthfortcapsegmentation` and/or **MTFSM Max User Data Length for TCAP Segmentation** in the matching terminating network.

The RTR performs TCAP segmentation when the message is delivered using the MAP phase 2 or MAP phase 2+.

When the MAP phase optimization is applied, the RTR will send MT-FSM using MAP phase 1, then TCAP segmentation will not happen irrespective of value of the parameter `mobNetworkMaxUserDataLengthForTcapSegmentation` and semi-static parameter `rtrmaxuserdatalengthfortcapsegmentation`. Please refer to section *MAP Phase Optimization* for more information about the MAP phase optimization.

TCAP Segmentation for Outgoing MTFSM and MT Status Report will be determined based on the following priority order:

1. Based on the value of `sccpMaxPduLengthForTcapSegmentation`.
2. Based on the value of the semi-static parameter `rtrmaxuserdatalengthfortcapsegmentation` and the value of **MTFSM Max User Data Length for TCAP Segmentation** in the configured network as explained in point 2 above.

18.5 Prepaid Triggers

This section describes the RTR's support for CAMEL primitives. For detailed information about prepaid charging, refer to the PBC Operator Manual.

Note: For incoming MO messages, CAMEL charging occurs only after all MOX rule processing is complete. Therefore, the MOX rule for the PBC should be provisioned as the lowest priority MOX rule.

18.5.1 CAMEL Phase 2 Operations

In conjunction with the PBC, the RTR supports the following the CAMEL Phase 2 primitives:

- CAP-InitialDp
- CAP-ContinueSms

Refer to the PBC Operator Manual for more information about these CAMEL operations.

18.5.2 CAMEL Phase 3 Operations

In conjunction with the PBC, the RTR supports the following CAMEL Phase 3 primitives:

- CAP-InitialDpSms
- CAP-RequestReportSmsEvent
- CAP-FurnishChargingInfoSms (optional)
- CAP-ContinueSms
- CAP-ReleaseSms
- CAP-ReportSms [o-smsSubmitted]
- CAP-ReportSms [o-smsFailure]

Refer to the PBC Operator Manual for more information about these CAMEL operations.

18.6 Graceful Start Up and Shutdown

To support graceful start up and shutdown of the RTR, the RTR should be associated with a unique virtual point code.

18.6.1 Start Up

When the RTR process starts, it must first be configured. During configuration, the RTR should not receive any requests from the GSM network or from applications.

To prevent the SS7 network from sending requests to the RTR during its configuration, the RTR sends signals to the SS7 network, indicating that its virtual point code is unavailable. If the network ignores the signals and sends requests to the RTR, the RTR will discard them.

18.6.2 Shutdown

When the RTR process shuts down, it should reject any new request from the SS7 network and from applications. However, it should attempt to complete all pending requests.

To prevent the SS7 network from sending requests to the RTR during its shutdown, the RTR sends signals to the SS7 network, indicating that its virtual point code is unavailable.

18.7 Configuration Basics

Note: This section is obsolete and scheduled for removal.

A RTR is associated with the following addresses:

- Specific SPC (signalling point code)
- Virtual SPC
- Specific GT (global title)

To enable the RTR to interact with other SS7 entities, the entities must be defined in its configuration.

18.7.1 SPC Addressing

Each SS7 entity that the RTR accesses using SPC addressing has an entry in the RTR's MTP destination table. This entry specifies the name and SPC of the SS7 entity.

The MTP destination table entry is linked to one or more entries in the MTP route table. Each entry specifies detailed information about a possible route to reach the SS7 entry.

18.7.2 GT Addressing

SS7 entities that the RTR accesses using GT addressing do not have to be configured. However, the STPs to which the RTR forwards GT-addressed traffic must be configured.

Each STP requires an entry in the MTP destination table and in the MTP route table. Each STP also requires an entry in the SCCP STP table. This entry specifies how the RTR should distribute GT-addressed traffic over the STPs.

18.7.3 Adjacents and Non-Adjacents

The RTR can connect to SS7 entities through a direct physical connection or through other SS7 entities. Directly connected SS7 entities are called adjacents, while indirectly connected entities are called non-adjacents.

In the following example, entities 1 and 2 are adjacents. Entities 3, 4, and 5 are non-adjacents.

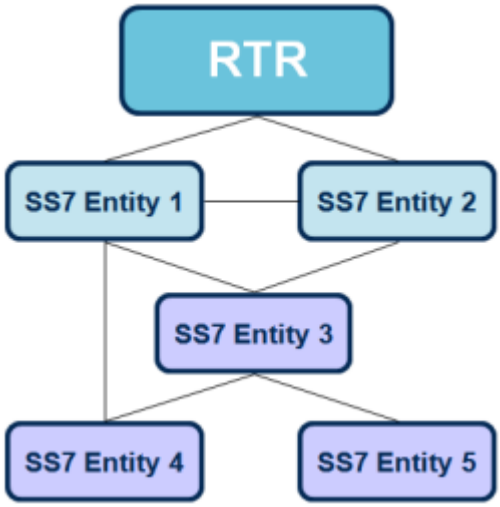


Figure 71: Adjacents and non-adjacents

The physical connection to an adjacent consists of one or more E1 trunks, each of which comprises 32 timeslots. Each timeslot can transfer 64 Kbit per second in both directions (full duplex). Timeslot 0 is always used for synchronisation. Each remaining timeslot can be used for speech or signalling.

In the case of narrowband links, each timeslot that conveys signalling data maps to a single link. When using high speed link, all timeslots of an E1 trunk (excluding timeslot 1 and timeslot 16) map to a single link.

18.7.3.1 Links Between Adjacents and the Router

All the links between an adjacent and the RTR are organised into a linkset. Each link in a linkset is associated with a unique signalling link code (SLC). The range of values for the SLC is 0-15. Therefore, the number of links in a linkset cannot exceed 16.

Each linkset has an entry in the RTR's MTP linkset table. This entry specifies the adjacent by referring to an SS7 entity defined in the MTP destination table.

Each subordinate link has an entry in the MTP link table. This entry specifies:

- Which E1 trunk to use for the link
- Which timeslot maps to the link
- The SLC of the link

18.7.3.2 Configuring Adjacents on the Router

In the RTR's semi-static configuration file, you must configure a `destination` entity for each adjacent. Normally, the adjacent will be an STP; however, an adjacent can also be an SS7 node running a MAP application (e.g. SMSC).

The main attributes of the `destination` entity are:

- `name`
- `type` (stp, msc, hlr, or smsc)
- `pointcode`

The `destination` entity has a subordinate entity, `route`. Each `destination` entity can have zero or more `route` entities.

Each `route` entity specifies a path to reach the destination by making a reference to an entity that provides a path to the destination. Entities that can be referenced are:

- `linkset`
- `m3uasgp`
- `m3uaas`

When the RTR maintains an MTP linkset with an adjacent, the `destination` entity must have a subordinate entity called `linkset` that specifies the linkset name (if no name is specified, it defaults to the superordinate's name).

18.7.3.3 Configuring Non-Adjacents on the Router

In the RTR's semi-static configuration file, you must configure a `destination` entity for each non-adjacent in which the RTR terminates messages. Normally, the RTR will only terminate messages in non-adjacent SS7 nodes running a MAP application (e.g. SMSC).

The main attributes of the `destination` entity are:

- `name`
- `type` (stp, msc, hlr, or smsc)
- `pointcode`

The `destination` entity has a subordinate entity, `route`. Each `destination` entity can have zero or more `route` entities.

Each `route` entity specifies a path to reach the destination by making a reference to an entity that provides a path to the destination. Entities that can be referenced are:

- `linkset`
- `m3uasgp`
- `m3uaas`

18.7.3.4 Advanced Destination Configuration

The `destination` entity's optional `throughput` attribute defines a threshold (maximum number of MTP user messages per second) to restrict the number of MTP user messages that the RTR terminates on the MTP destination. When the throughput is exceeded, the RTR silently discards MTP user messages for the MTP destination until the start of a new second.

The `throughput` attribute can be between 0-10000, where 0 indicates that no maximum is imposed for the throughput (this is the default).

When the `throughput` setting is applied to a destination that is defined as an STP, the number of messages that are terminated on the STP's point code are restricted.

18.7.3.5 Advanced Route Configuration

The route entity has the following optional attributes:

Attribute	Description	Valid Values	Default
throughput	Defines a threshold (maximum number of MTP user messages per second) to restrict the number of MTP user messages that the RTR terminates on the MTP destination. When the throughput is exceeded, the RTR does not use the MTP destination until the start of a new second.	0-65535	0
priority	Sets the priority for the route, allowing for the configuration of preferred routes. Lower priority routes will only be used when the higher priority routes are not available.	0-7	0
weight	Sets the weight for a route. When more than one route has the same priority, the RTR shares the load equally among the routes by default. The `weight` attribute allows for adjustment of the load sharing.	0-100	0

For example, in the following configuration:

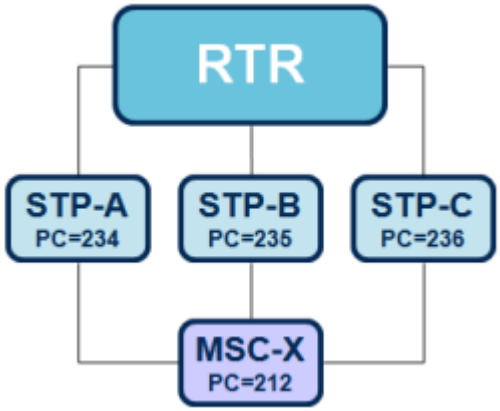


Figure 72: Advanced route configuration

With the following configuration file:

```
<destination name="STP-A" type="stp" pointcode="234">
    <linkset>
      ...
    <linkset/>
</destination>
<destination name="STP-B" type="stp" pointcode="235">
    <linkset>
```

```
      ...
    <linkset/>
</destination>
<destination name="STP-B" type="stp" pointcode="236">
    <linkset>
      ...
    <linkset/>
</destination>
<destination name="MSC-X" type="msc" pointcode="212">
    <route linkset="STP-A" priority="7" throughput="100"/>
    <route linkset="STP-B" priority="0" weight="3">
    <route linkset="STP-C" priority="0" weight="1"/>
</destination>
```

When the RTR sends messages to MSC-X, it will attempt to use STP-A, if possible. The route through STP-A will not convey more than 100 messages per second. When STP-A is not available, the RTR will use STP-B and STP-C. The RTR will send STP-B 75percent of the traffic and will send STP-C 25 percent of the traffic.

18.8 Global Title Translations

Use the RTR's global title translation (GTT) function to manipulate the SCCP called party address in outgoing UDTs.

The GTT function can filter on the following fields:

- GT nature of address indicator (only works for Home Routing, hard-coded for all other message paths)
- GT numbering plan (only works for Home Routing, hard-coded for all other message paths. If not specified, all numbering plans apply.)
- GT address digits (wildcards allowed)

The GTT function can change to the following fields:

- National use bit
- Routing indicator
- GT indicator
- Point code
- Subsystem number
- GT translation type
- GT nature of address indication
- GT address digits (wildcard allowed, provided that the related field in filter is a wildcard)
- MTP destination to which to route UDT (if not specified, UDT will be routed to an STP)

Note: The GTT function may also refer to a SCCP load share set containing one or more member entities, each of which is associated with a MTP destination (refer *SCCP Load Balancing*) . In this case the GTT function cannot change the Point code or the MTP destination directly, but only through the SCCP load balancing mechanism; the load balancing mechanism selects a particular member from the load share set and provides the corresponding Destination Point code and optionally the Subsystem number as output of the GTT function.

There are two types of GTT rules:

- Exactly matching rules—To match, the E164 address that identifies the destination should equal the translation rule's address.
- Wildcard rules—The address is specified as a number of digits, followed by an asterisk (*). To match, the E164 address that identifies the destination must begin with the digits of the wildcard rule.

If multiple rules apply:

- Exactly matching rules take precedence over wildcard rules.
- Among wildcard rules, the rule containing the most digits takes precedence.

If there is no GTT rule configured and the outgoing traffic is routed via configured "`STP`" or `mtp` destinations, the router will not be aware of the destination point code, so in transaction, CDRs and event logs will not have the destination point code.

Note: If the GTT rule is configured and applied in the outgoing route, CDRs and event logs will contain the destination point code.

18.8.1 SCCP Load Balancing

While routing messages to the SS7 network, the RTR can load balance the outgoing SCCP traffic over multiple MTP destinations, if those destinations are configured as the members of one or more load share sets that are referenced by the GTT rule(s) matching the outgoing messages. Refer to *sccploadshareset Entity* and *member Entity* for descriptions of the relevant semi-static configuration attributes. Refer to Appendix G.2 for a sample configuration of a load share set and its member destinations.

Note: The RTR also performs GTT on incoming SCCP UDTs if the Routing Indicator in the Calling Party Address is set to 'route on GT' (0), because the Calling Party Address of a received message can be later used as the Called Party Address while sending back the corresponding response message. However in this scenario the RTR does not use the SCCP load balancing mechanism even if a load share set is referenced by the matching GTT rule; instead it always selects the first available member (in terms of SNMP index) from the load share set.

Each load share set may contain up to eight members. Each member in a load share set is uniquely associated with a MTP destination and may also optionally be assigned a Subsystem Number (SSN). Note that either SSN can be specified for all the members belonging to a single load share set or it cannot be specified for any member. However, in case SSN is specified for all the members of a load share set then the SSN values may be different for different members.

Apart from the MTP destination and the SSN, each member of a load share set is also assigned a "priority" value in the range 0-7 and a "weight" value in the range 1-100. Different members may have different or same priority and weight assigned to them, and these values form the basis of the Load Balancing Mechanism. The MAP Screener always selects the member having the highest priority value in a load share set, and in case there are more than one members having the highest priority value then the load sharing is done based on the respective weights of those members.

Once a member is selected from a load share set as per the load sharing mechanism, the corresponding MTP destination's point code and the SSN assigned to the member (if any) are considered as the output of the matching GTT rule that referenced the load share set. In case no SSN is assigned to the member but an output SSN is configured for the GTT rule itself, then the latter is taken as part of the output.

Important: Although the system allows to configure the SSN values '0' and '1' for a load share set member, it is strongly recommended not to assign these SSN values to any member because doing so may cause routing failures for the outgoing SCCP messages.

18.8.1.1 Load Balancing Mechanism

The SCCP load balancing mechanism takes into account the following parameters pertaining to the members of a load share set:

- Priority
- Weight
- Accessibility of the MTP destination

As mentioned above, for each load share set member a "priority" value between 0 (least urgent) and 7 (most urgent) can be specified. The "priority" value is relevant only when more than one member is included in the load share set. By default (if not configured explicitly) the "priority" of a member is considered as zero.

Similarly, for each load share set member a weight between 1 (least weightage) and 100 (highest weightage) can be specified. The "weight" is relevant only when multiple members have the same "priority" value, specifically the highest "priority" value. This is because the load balancing mechanism is designed to select the member having the highest priority out of all the members in the 'active' state. But in case there are more than one members having the highest "priority" value then the load balancing mechanism has to distribute the traffic load among these members according to the ratio of their respective weights.

Apart from the "priority" and "weight", the load balancing mechanism also considers the accessibility of the load share set members before selecting a particular member. The accessibility status of a member at any given point in time depends upon the following events or factors:

- If the MTP destination associated with a member becomes inaccessible, e.g. either due to the SS7 links or routes at the MTP3/M3UA layer getting disconnected or due to the reception of a MTP3/M3UA management message indicating the unavailability of the destination endpoint, then the member is also considered as inaccessible. In this case the member is again considered as accessible only when the MTP destination becomes accessible.
- If a specific MTP3/M3UA management message called "User Part Unavailable" or "Destination User Part Unavailable" is received indicating that the SCCP layer at a certain destination node is not accessible, then the member corresponding to that destination is also considered as inaccessible. In this case the member is again considered as accessible when a valid SCCP message (UDT or XUDT) is received from the concerned destination node. However, in case the above MTP3/M3UA management message indicates that the SCCP layer is not even present at a certain destination node ("unequipped remote user"), then the member corresponding to that destination is considered as permanently inaccessible.
- If an SCCP management message is received indicating that the remote subsystem at a certain destination node has been "prohibited" from carrying traffic or it is congested, then the member corresponding to that destination is considered as inaccessible. In such a case the member would again be considered as accessible only when another SCCP management message is received indicating that the concerned remote subsystem at the destination node is operational and available for carrying traffic.
- If an SCCP error message (UDTS) is received from a certain destination point-code with any of the below return cause, then there is no impact on the accessibility status of the member corresponding to that destination:
  - `0 0 0 0 0 0 0 0 (0x00) 'no translation for an address of such nature'`
  - `0 0 0 0 0 0 0 1 (0x01) 'no translation for this specific address'`
  - `0 0 0 0 0 1 1 1 (0x07) 'unqualified'`

However, if an SCCP error message is received from a certain destination point-code with the return causes excluding the one mentioned above, then the member corresponding to that destination is considered as inaccessible In such a case the member would again be considered as accessible when a valid SCCP message (UDT or XUDT) is received from the concerned destination node.

Note: The RTRs do not support/process incoming XUDTS messages, because they never send out any XUDT. Hence, it will not impact on the accessibility status of the member.

Note that a load share set member's operational state, as indicated by the SNMP object sccpLoadShareSetMemberOperationalState , can also be used to check its accessibility status. The following table describes the possible operational states of a member:

Operational State	Description
adminDisabled	The load share set member is currently deactivated; hence this member is not considered for the load balancing mechanism.
inaccessible	The load share set member's destination is currently inaccessible; hence this member is not selected by the load balancing mechanism (irrespective of its "priority" and "weight") till it becomes accessible again.
accessible	The load share set member's destination is currently accessible; hence this member is available for selection by the load balancing mechanism.

The number of outgoing SCCP messages sent to a particular load share set member's destination can be checked by accessing the SNMP counter sccpLoadShareSetMemberTxCounter. Note that this counter is incremented only when the load balancing mechanism is actually applied for selecting a member, as opposed to the scenario in which the RTR simply selects the first accessible member of the load share set (i.e. while performing GTT on the Calling Party Address of an incoming message).

The load balancing mechanism for a given load share set is initially set up when the set is activated for the first time. Subsequently, if the load share set gets deactivated and then activated again, then the load balancing mechanism is set up afresh. It is also re-evaluated every time a load share set member gets activated or deactivated.

Note:

In order to change the priority, weight, MTP destination, or SSN assigned to a load share set member, it is required to first deactivate the member; once the necessary configuration change is done, the member can be re-activated.

18.8.1.2 Load Balancing Examples

Equal Priority, Equal Weights

Consider the following scenario:

- 8 load share set members
- All members have priority ‘3’ and weight ‘1’
- Traffic throughput of 600 messages per second.
- Traffic duration is 60 seconds (total of 36,000 messages)

In this case each members will receive 36000/8 = 4500 messages (appx.).

Equal Priority, Mixed Weights

Consider the following scenario:

- 2 load share set members with both having priority '5'
- One member having weight '60'
- The other member having weight '40'
- Traffic throughput of 600 messages per second.
- Traffic duration is 60 seconds (total of 36,000 messages)

Member having weight '60' will receive 36000 * 60 / (60 + 40) = 21600 messages (appx.).

Member having weight '40' will receive 36000 * 40 / (60 + 40) = 14400 messages (appx.).

Note: It has been assumed that the GTT rule is applied only once for all the messages.

18.8.1.3 Limitation of SCCP Load Balancing

The SCCP load balancing mechanism does not work correctly under the following scenarios, in which the RTR performs GTT on a destination address and then the same destination address is later used repeatedly without any further translation for sending out a large number of messages:

- Routing outbound MO messages to a pre-configured SMSC that is associated with a matching MOR rule. In this scenario, GTT is performed only at the time of configuring the SMSC address and activating the SMSC.
- Sending multiple outbound messages using the same TCAP dialogue in the case of MT-MT, AO-MT, SIPO-MT, SIPT-MT or MO-MT routing. In this scenario, GTT is performed only once at the time of creating the outbound TCAP dialogue. Note that the GTT is also applied on the Calling Party Address of each received PDU (i.e. TCAP-Continue). As already mentioned, on each such occasion the first accessible member of the load share set is selected (i.e. the load balancing mechanism is not used).

In both the above scenarios the `sccpLoadShareSetMemberTxCounter` is incremented only at the beginning, i.e. when the GTT is actually performed and the load balancing mechanism is applied.

18.9 Japanese Mobile Number Portability Support

The RTR supports a configurable Mobile Number Portability (MNP) functionality for specific Japanese network(s). As part of this functionality, the RTR performs customized processing and routing for messages originated from or destined to subscribers belonging to a different Japanese Mobile Network Operator (MNO). Additionally, the RTR performs special processing and routing for messages originated from or destined to international subscribers as well.

The Japanese MNP functionality in the RTR can be enabled or disabled through the semi-static configuration parameter *enablejapanesemnp*. By default this parameter is set to FALSE, to maintain backwards compatibility.

18.9.1 Overview of Japanese MNP

If the Japanese MNP functionality is enabled, the RTR needs to determine whether the recipient of an incoming message or SRI-SM Request is a ported subscriber (i.e. belonging to a different Japanese network). For this purpose the RTR first sends a SRI-SM Request towards a special network element

called the Flexible Number Register (FNR) in the HPLMN; this initial SRI-SM Request contains the recipient number of the incoming message or SRI-SM (provided the recipient is neither an application nor an MSISDN representing a ported application).

Note that in case the recipient number is an international number, then the initial SRI-SM needs to be eventually routed to the HLR in the destination (international) network via an International SMS Hub; this can be accomplished by configuring suitable GTT rules with specific prefixes, which would be applied on the outgoing SCCP CdPA.

The IMSI contained in the response to the initial SRI-SM mentioned above controls the subsequent processing in the RTR. If the recipient is a local subscriber or an international subscriber, then the actual IMSI of the recipient would be received in the SRI-SM Response. However, if the recipient is a ported subscriber then a Generated IMSI (GIMSI) would be received in the SRI-SM Response. The GIMSI is basically a "fake" IMSI that cannot be used for actual MT message delivery, but its MNC and MSIN portions are used by the RTR in order to determine the other Japanese network (if any) to which a subsequent SRI-SM Request would need to be sent.

Using the IMSI (actual or generated) received in the initial SRI-SM Response and, optionally, a prefix string consisting of the first five digits of the CdPA GT address of an incoming SRI-SM Request, the RTR performs a search on a set of pre-configured records in a table. The data in this table (henceforth referred to as the "MNP table") are configured using the MGR GUI (refer to Section 4.16 of the MGR Operator Manual for details).

The search is considered successful if a matching record is found in the MNP table corresponding to the recipient IMSI and (optionally) the CdPA Prefix received in an incoming SRI-SM. In case multiple matching records containing a common "IMSI prefix" (i.e. a partial string of IMSI digits followed by the wildcard character '*') are found, then the record having the longest matching IMSI prefix is selected.

From the matching record, the RTR finds out the nature of the subsequent processing action to be taken.

The following table describes the different Japanese MNP Actions that can be configured using the MGR GUI:

MNP Action	Description
Accept	Indicates that the recipient of the message is not a ported subscriber, i.e. the recipient either belongs to the HPLMN or is an international number. In this case, no further processing related to number portability is required, hence RTR should continue with its normal functionality in order to deliver the message.
Forward	Indicates that the recipient of the message is a ported subscriber. In this case it is required to send a second SRI-SM Request or forward the received SRI-SM Request towards another operator's network, in order to determine the actual destination network for the delivery of the message. A special prefix (string of digits) needs to be inserted before the outgoing CdPA GT address of the second SRI-SM; this prefix is also obtained from the matching MNP table record.
Discard	Indicates that the message should be discarded with a permanent error.

In case the search in the MNP table is not successful, then the nature of the subsequent RTR processing is determined by the semi-static parameter *defaultactionwhennotfoundinmnptable*.

The Japanese MNP functionality mainly impacts the routing paths mentioned below:

- MO-MT

- MO-MT-Store
- MO-Store-MT
- AO-MT
- AO-MT-Store
- AO-Store-MT
- SIPO-MT
- SIPO-MT-Store
- SIPO-Store-MT
- MT-MT (Home-routed)
- MT-Store-MT
- SIPT-MT

The following sub-sections briefly describe the customized processing and routing performed by the RTR for supporting Japanese MNP w.r.t. the above routing paths.

Note: Depending on the Japanese MNP Action and the routing path applied on a message (or on an incoming SRI-SM Request), the performance of the RTR may be impacted due to the additional processing.

18.9.2 Japanese MNP Processing For Incoming MO, AO and SIPO Messages

Japanese MNP is applicable on incoming MO/AO/SIPO messages only when the recipient number is an MSISDN that does not represent a ported application.

- If the semi-static parameter *enablejapanesemnp* is set to "true" and if Early SRI-SM Request for Recipient (B-number) is enabled, then the RTR sends an SRI-SM with the recipient MSISDN and with high priority (i.e. sm-RP-PRI set as `1`) towards the local HLR/FNR or the International SMS Hub for retrieving the recipient IMSI and the destination MSC address (if available).
- Using the IMSI received in the SRI-SM Response, the RTR performs a look-up on the configured MNP table.
- In case of a successful match in the MNP table, the RTR determines the Action from the matching record. Otherwise the RTR uses the semi-static parameter *defaultactionwhennotfoundinmnptable* to determine the MNP Action.
- If the MNP Action is **Discard**, the received message is considered to be failed, and is rejected by the RTR. For other MNP Actions no additional processing is performed at this point.

Note: In case the MNP Action is **Forward**, then the second SRI-SM Request is initiated later, i.e. during the outgoing MT delivery of the message.

Note: If the semi-static parameter *enablejapanesemnp* is set to "true" and if Early SRI-SM Request for Recipient (B-number) is enabled and the MNP action is **Forward**, then recipient IMSI condition is only applicable with IMSI list in the MOR rule (i.e. MGR->Routing rules->MOR->Recipient = List of IMSI).

Note: If the semi-static parameter *enablejapanesemnp* is set to "true" and if Early SRI-SM Request for Recipient (B-number) is enabled and the MNP action is **Accept** for concatenated MO-MT-Store flow, the RTR sends the early SRI-SM request for recipient for the first segment only and it does not send the early SRI-SM request for the second segment.

18.9.3 Japanese MNP Processing While Delivering Outgoing MT Messages

If the semi-static parameter *enablejapanesemnp* is set to "true", then the RTR performs the following processing steps while delivering an outgoing MT message, either as FDA or through a retry from the AMS.

Note: The following steps are relevant for MT short messages only and not for MT status reports, because MT status reports are always sent to originating subscribers of MO messages, i.e. local subscribers.

- If the outgoing MT message is being retried from the AMS, the RTR first sends a SRI-SM Request towards the local HLR/FNR or the International SMS Hub for retrieving the recipient IMSI and the destination MSC address, as described in the previous section.
- Using the IMSI received in the SRI-SM response the RTR performs a look-up on the configured MNP table and eventually determines the MNP action, as described in the previous section.

  Note: The above two steps are not required while trying to deliver a message through FDA, since they are already performed while processing the incoming message (refer to the previous section).

- If the MNP action is found to be **Accept**, the recipient is considered to be either a local subscriber or an international subscriber. RTR uses the received IMSI and MSC address during the first SRI-SM request for the delivery of the message.
- If the MNP Action is found to be **Discard**, then the received message is considered as failed and the RTR sends back a permanent error for the recipient to the AMS. This would cause all the messages stored for the same recipient to be deleted from the AMS.
- If the MNP action is found to be **Forward**, the recipient is considered to be a ported subscriber. Hence the RTR issues a second SRI-SM with high priority (i.e. sm-RP-PRI set as `1`) and the SCCP CdPA being populated as follows (before GTT):
  - CdPA GT address = <Forward Prefix in the matching MNP table record><MSIN>;,
  - Subsystem Number = 6;,
  - Nature of Address Indicator = 0x03;,
  - TT = Value of the semi-static parameter *cdpattforjapanesemnp*;
- If the semi-static parameter *enablegprssupportindicatorfordomestichlrqueryonly* is set to true, the RTR will not add GPRS Support Indicator in the second SRI-SM request. Otherwise, the inclusion of GPRS Support Indicator in SRI-SM will be based on the parameter `gprssupportindicatorforsrismrequest`.
- Recipient IMSI and MSC address received in the second SRI-SM Response are used for the actual delivery of the message to the recipient.

Note: If the Copy To Phone (CPY), Forward To Phone (FWD) or Auto-Reply (ARP) personalized service(s) is activated on the recipient subscriber of an outgoing MT message, then the RTR does not perform any lookup on the MNP table while delivering the copied message or forwarded message or auto-reply message. In such cases it is assumed that the recipients of such service-specific messages will always be local subscribers only.

Note: If the semi-static parameter *enablejapanesemnp* is set to "true" and if Early SRI-SM Request for Recipient (B-number) is enabled and MNP action is forward, then the recipient IMSI condition is only applicable with IMSI list in MT rule (i.e. MGR->Routing rules->MTOR->Recipient = List of IMSI).

18.9.4 Japanese MNP Processing For Incoming SRI-SM And Home-routed MT Messages

If the semi-static parameter *enablejapanesemnp* is set to "true", then the RTR performs the following processing steps for incoming SRI-SM Requests and home-routed MT-FSM messages.

- If an incoming SRI-SM request is received with the Nature of Address Indicator in the CdPA set as 0x03 (**National**), then the RTR extracts the CdPA prefix from the received CdPA GT address. First five digits of the GT address are considered to be the CdPA prefix. This extracted CdPA prefix is later used by the RTR for the look-up in the Japanese MNP table.

  Note: If the RTR receives a SRI-SM request with the Nature of Address Indicator in CdPA set as0x04 ("International"), then the RTR transparently forwards it to the International SMS Hub, using the same CgPA, TCAP transaction_id and dialogue as in the incoming request. Thus the behaviour of the RTR in this case is similar to its behaviour when the SRI-SM Request (SRIQ) Rule's routing action is set to **Have HLR respond to SMSC directly**.

- If the SRIQ rule's routing action is **Send to HLR**, the RTR sends an SRI-SM with the recipient MSISDN and with high priority (i.e. sm-RP-PRI set as 1) to the local HLR/FNR.

  Note: If the SRIQ rule's routing action is different from **Send to HLR**, then the RTR does not perform any further processing related to Japanese MNP and continues with the normal functionality.

- The RTR performs lookup on the MNP table using the IMSI returned in response to the above SRI-SM, and the CdPA Prefix extracted from the incoming SRI-SM.
- In case of successful match in the Japanese MNP table, the configured Action determines how the message is going to be handled. In case no Japanese MNP record matches, the semi-static parameter *defaultactionwhennotfoundinmnptable* determines the MNP Action.
- If the MNP action is found to be **Accept** and the SRI-SM Response (SRIP) Rule's routing action is **Home Routing**, then the RTR returns an SRI-SM Ack. with either a Scrambled IMSI or the actual IMSI (of the recipient) and RTR's own GT address to the originating SMSC.

  Note: If the SRIP rule's routing action is different from **Home Routing** then the RTR does not perform any further processing related to Japanese MNP and continues with the normal functionality.

- If the MNP Action is found to be **Discard**, the RTR sends back a failure response to the external SMSC. For the purpose of sending this Nack. to the SMSC, the RTR treats the "discard" MNP action as an "unknown subscriber" error received in response to its outgoing SRI-SM Request.
- If the MNP action is found to be **Forward**, it means that the recipient subscriber does not belong to the HPLMN. In such a case trying to home-route the (subsequent) MT-FSM is not logically justified. Hence in this case the RTR forwards the SRI-SM using the same CgPA, TCAP transaction_id and dialogue as in the original incoming request. However the CdPA of the forwarded SRI-SM is modified as follows:

  - CdPA GT address = <Forward Prefix in the matching MNP table record><MSIN>;
  - Subsystem Number = 6;
  - Nature of Address Indicator = 0x03;
  - TT = Value of the semi-static parameter *cdpattforjapanesemnp*.

Since the SRI-SM Response will be directly routed to the external SMSC, the RTR has no further role to play in the above scenario.

Note: In case home-routing is performed, the RTR executes its normal functionality upon receiving the incoming MT-FSM. However, if the home-routed MT-FSM gets stored in the AMS (i.e. due to the MTIR Rule routing action being **Store for Delivery to MS**), then during the subsequent retry from the AMS no further lookup is performed by the RTR in the MNP table, since it has already confirmed that the recipient subscriber belongs to the HPLMN and the MNP Action is **Accept**.

18.9.5 Japanese MNP Processing When Delivery is Attempted From AMS

This section describes the Japanese MNP processing for both segmented and non-segmented messages, when delivery is attempted from AMS. There are two scenarios where delivery is attempted from store:

- MO-Store-MT
- AO-Store-MT

The following sub-sections will focus on the details of these scenarios and their exceptions.

18.9.5.1 MO-Store-MT Routing

Case: MO-Store-MT with MMS disabled:

In this scenario, the MOFSM messages will be stored in the AMS and the AMS will request the RTR to deliver the MT messages with MMS disabled.

The following points need to be considered for this scenario:

- If "Early SRI-SM for MO/SM" is enabled, then for each MOFSM, the RTR will perform the SRI-SM but never store the SRISM result.
- When the MTFSM delivery is attempted from AMS with TP-MMS=1 that is, no more messages are waiting for the MS in the SC, the RTR will perform another SRI-SM because the RTR does not store the SRISM response received during Early-SRISM.
- If the MNP action is evaluated as accept, the RTR will deliver the MTFSM.
- If the MNP action is evaluated as forward, the RTR will perform another SRISM to get the actual IMSI and then the RTR will deliver the MTFSM.

The figure describes the forward scenario, with two MOFSM messages received by the RTR.

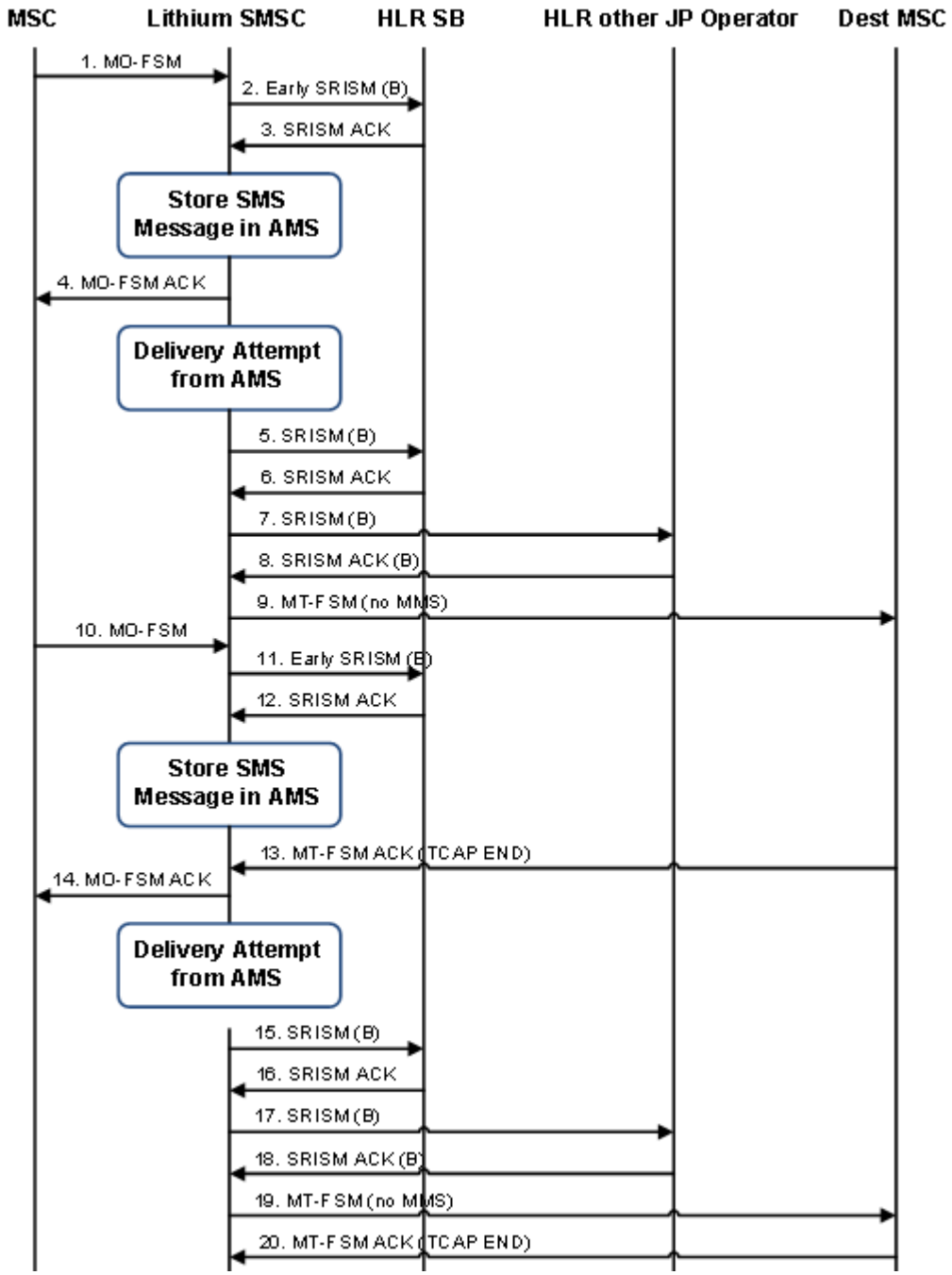


Figure 73: MO-Store-MT Scenario with MMS Disabled

Case: MO-Store-MT with MMS enabled:

In this scenario, a segmented MOFSM message will be stored in AMS and AMS will request RTR to deliver the MT messages with MMS enabled.

The following points need to be considered for this scenario:

- If "Early SRI-SM for MO/SM" is enabled, then for each segment of MOFSM message, RTR will perform individual SRI-SM but never store the SRISM result.
- When MTFSM delivery is attempted from AMS with TP-MMS=0 that is, more messages are waiting for the MS in the SC, the RTR will perform another SRI-SM as RTR doesn't stores the SRISM response received during Early-SRISM.
- If MNP action is evaluated as accept, RTR will deliver MTFSM.
- If MNP action is evaluated as forward, RTR will perform another SRISM to get the actual IMSI and stores the SRISM response.
- If subsequent segmented MTFSM message delivery is attempted from AMS within 3 seconds then RTR will not perform the SRISM as RTR will use the previously stored SRISM result and it will deliver the message on the same TCAP dialogue.

Note: The counter 'mtRtgRuleAppliedCounter' will be incremented for those segments also for which no SRISM action is performed but instead cached SRISM result is used for delivery.

The following figure describes the forward scenario:

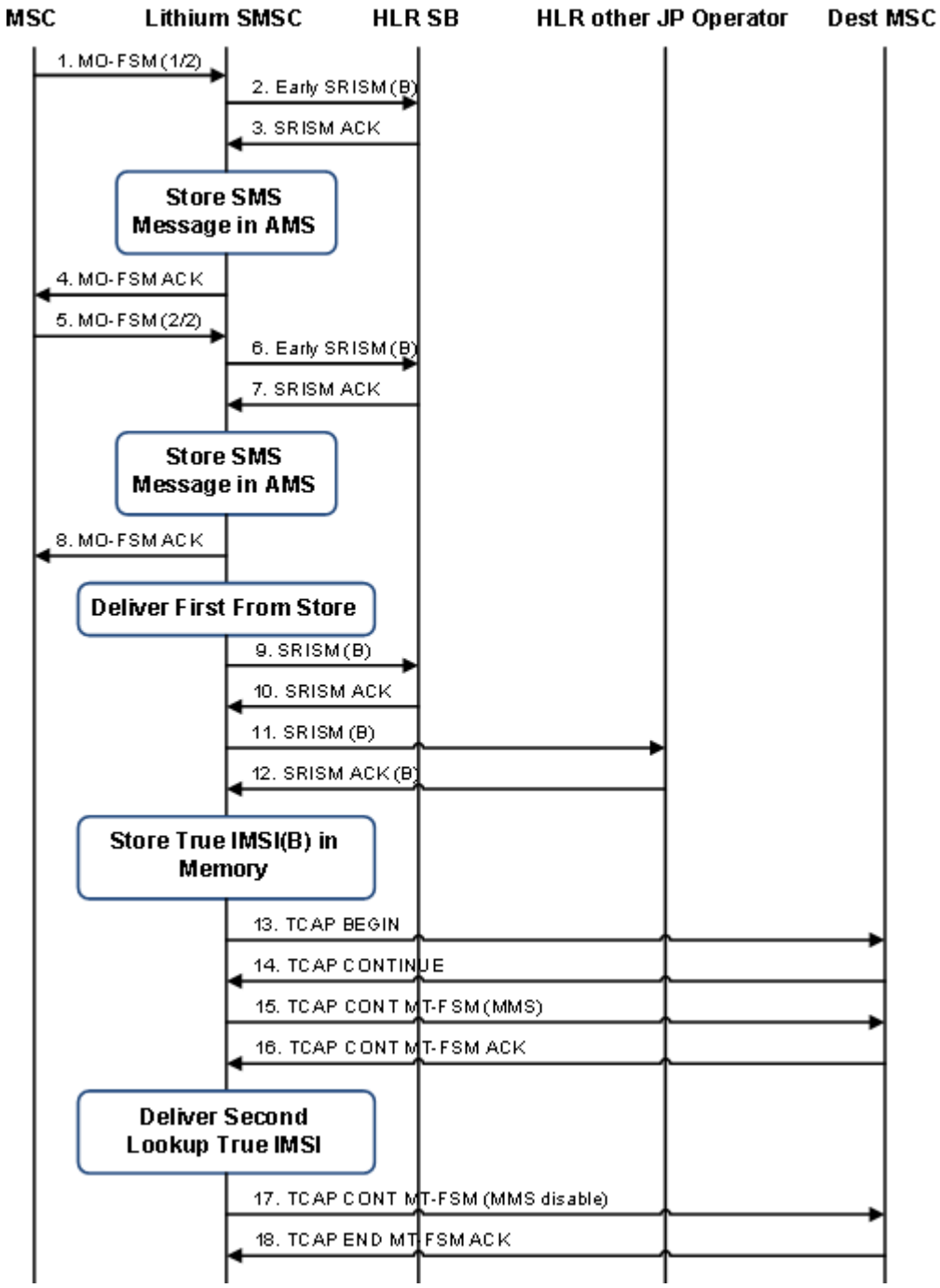


Figure 74: MO-Store-MT Scenario with MMS Enabled

Case: Exception in MO-Store-MT with MMS enabled:

There is one exception in this scenario where a Single MOFSM is stored in the AMS but when delivery is attempted by AMS, the MT conversion configured in the MT Outgoing Rule causes the RTR to segment the message in two parts.

In this case RTR perform SRI-SM procedure for the first segment only irrespective of whether we receive TC-End or TC-Continue for the first segment.

The following figure describes the forward scenarios:

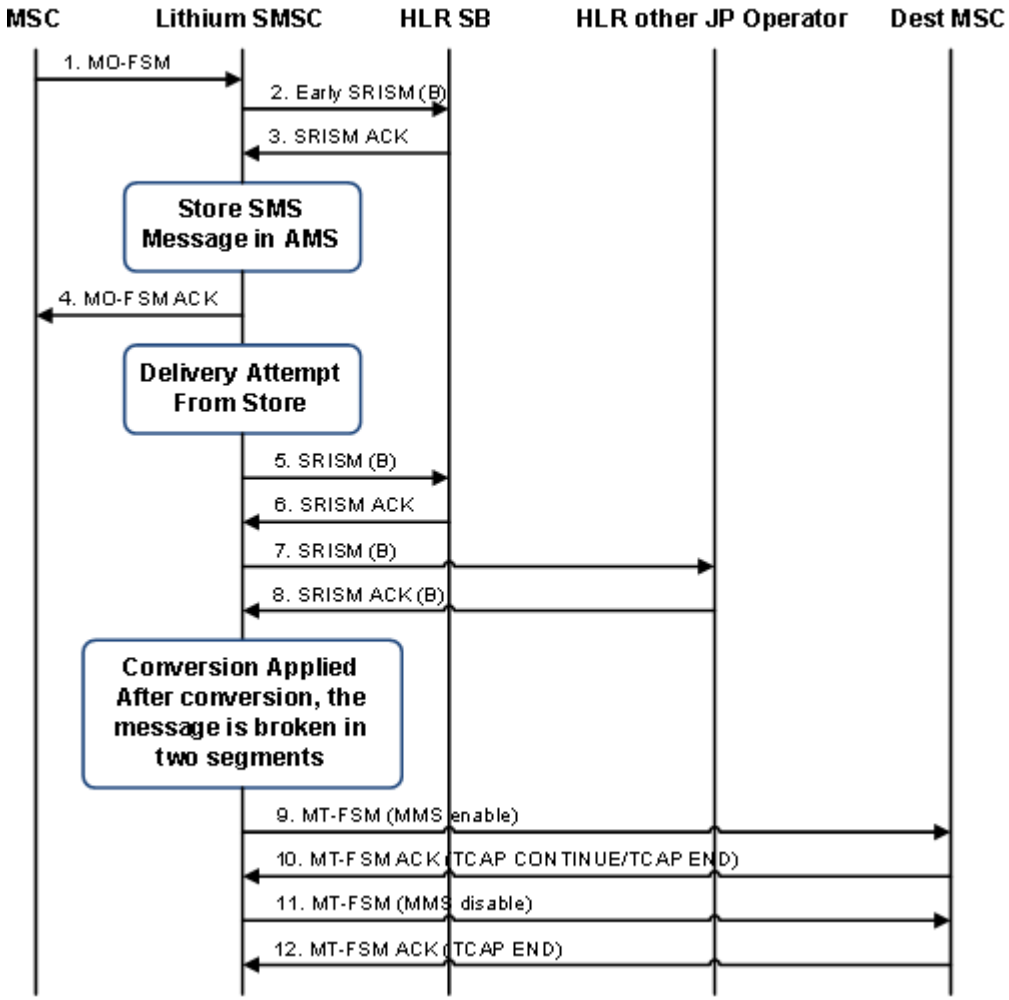


Figure 75: 1 Normal MO-Submit, 2 MT messages after Conversion

18.9.5.2 AO-Store-MT Routing

Case: AO-Store-MT with MMS disabled:

In this scenario, AO messages will be stored in AMS and AMS will request RTR to deliver the MT messages with MMS disabled.

The following points need to be considered for this scenario:

- If "Early SRI-SM for AO" is enabled, then for each AO message the RTR will perform SRI-SM but never store the SRISM result.
- When MTFSM delivery is attempted from AMS with TP-MMS=1 that is, no more messages are waiting for the MS in the SC, RTR will perform another SRI-SM as RTR does not store the SRISM response received during Early-SRISM.

- If MNP action is evaluated as accept, RTR will deliver MTFSM.
- If MNP action is evaluated as forward, RTR will perform another SRISM to get the actual IMSI and then RTR will deliver the MTFSM.

The following figure describes the forward scenario:

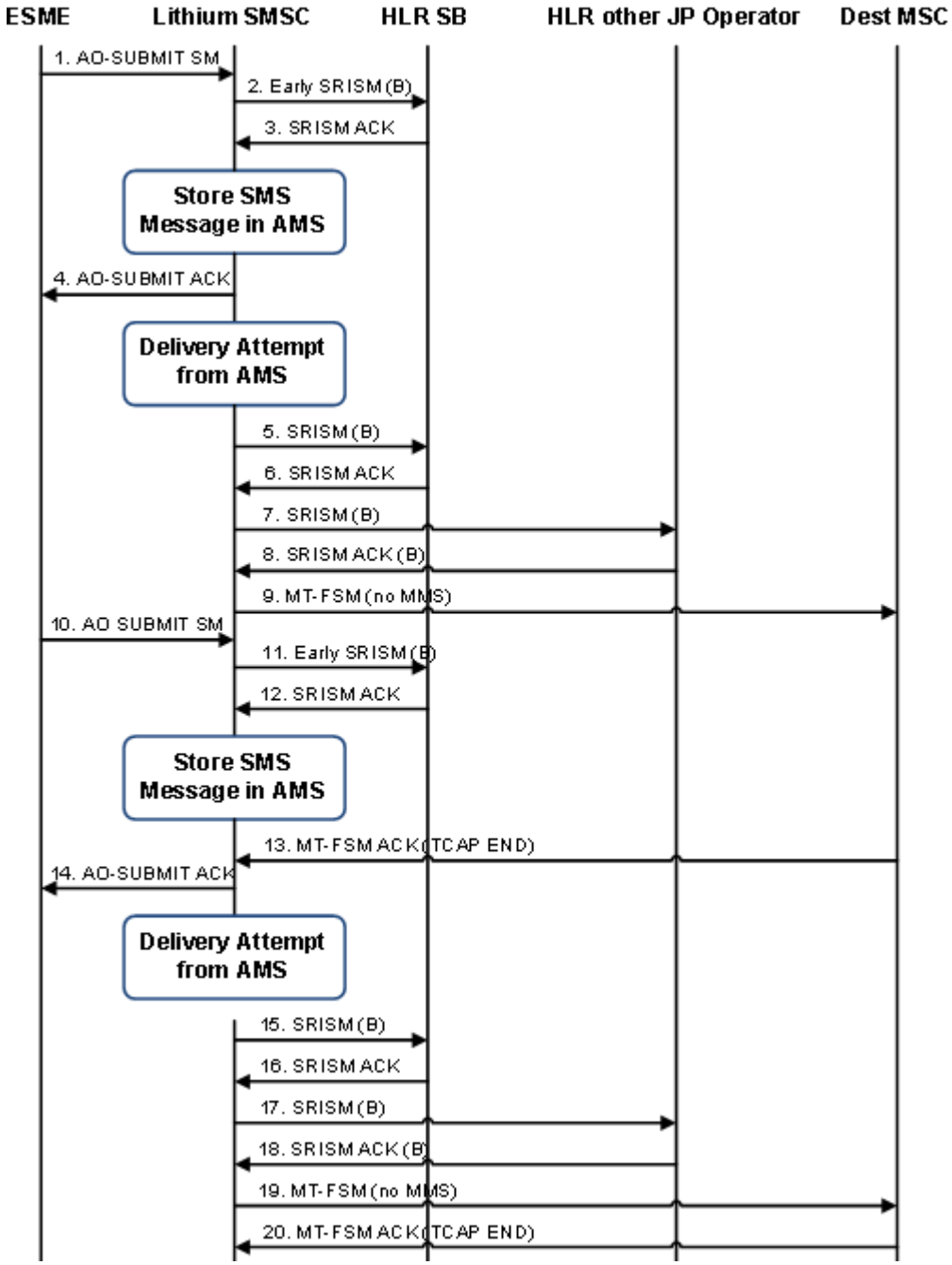


Figure 76: AO-Store-MT Scenario with MMS Disabled

Case: AO-Store-MT with MMS enabled:

In this scenario, AO messages will be stored in AMS and AMS will request RTR to deliver the MT messages with MMS enabled.

The following points need to be taken care for this scenario:

- If "Early SRI-SM for AO" is enabled, then for each AO message the RTR will perform SRI-SM but never store the SRISM result.
- When MTFSM delivery is attempted from AMS with TP-MMS=0 that is, more messages are waiting for the MS in the SC, RTR will perform another SRI-SM as RTR does not store the SRISM response received during Early-SRISM.
- If MNP action is evaluated as accept, RTR will deliver MTFSM.
- If MNP action is evaluated as forward, RTR will perform another SRISM to get the actual IMSI and stores the SRISM response.
- If subsequent segmented MTFSM message delivery is attempted from AMS within 3 seconds then RTR will not perform the SRISM as RTR will use the previously stored SRISM result and will deliver the message on the same TCAP dialogue.

The following figure describes the forward scenario of two independent AO messages with store to the same recipient, where AMS attempted MT delivery with MMS enabled:

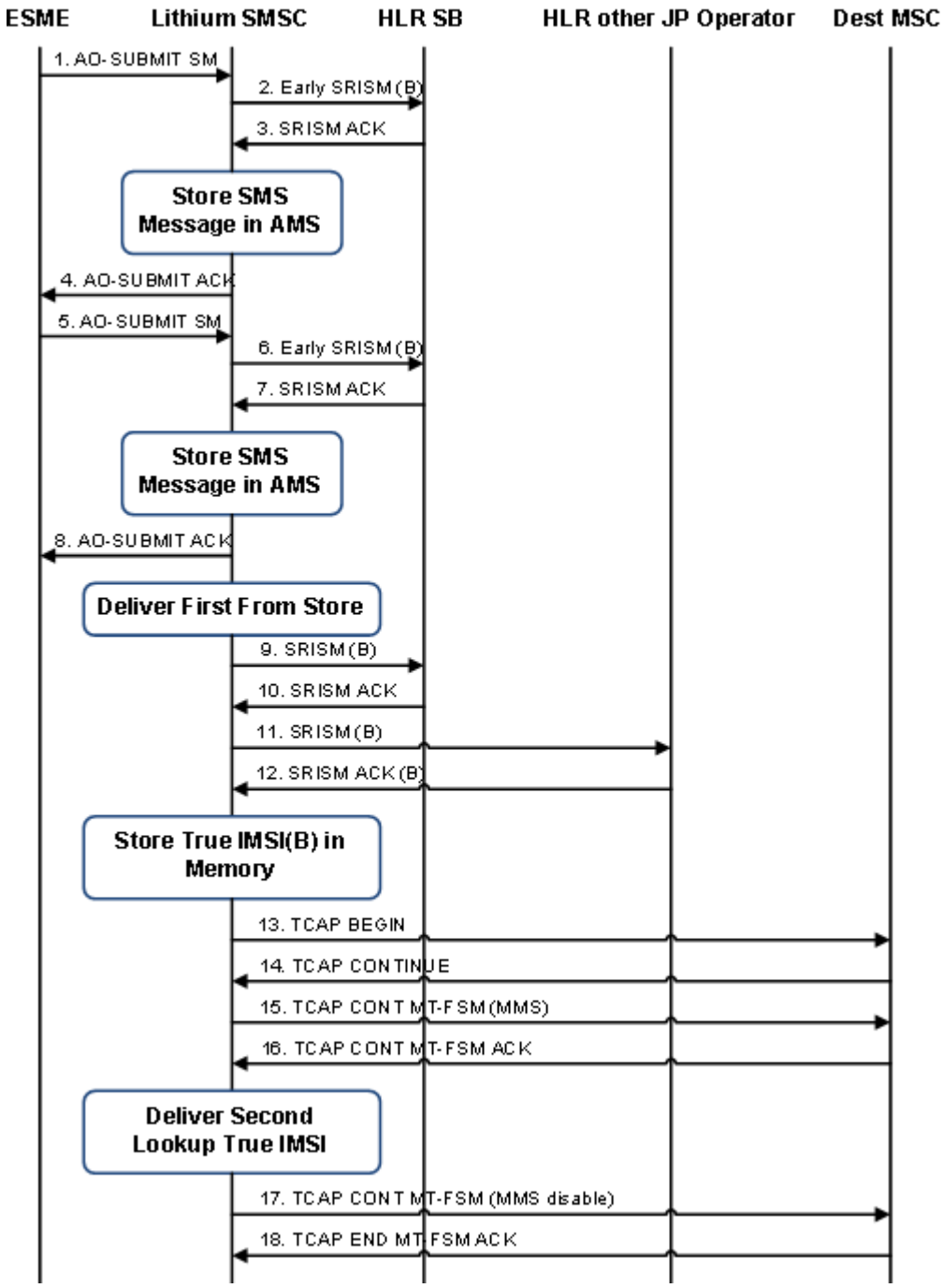


Figure 77: AO-Store-MT Scenario with MMS Enabled

Case: Exception in AO-Store-MT with MMS enabled:

There is one exception in this scenario where a single long AO message (i.e. >140 byes) is stored in the AMS, but when delivery is attempted by AMS, 160 characters limitation in GSM 7-bit encoding causes the RTR to segment the message in two parts.

In this case RTR perform SRI-SM procedure for the first segment only irrespective of whether we receive TC-End or TC-Continue for the first segment.

The following figure describes the forward scenario:

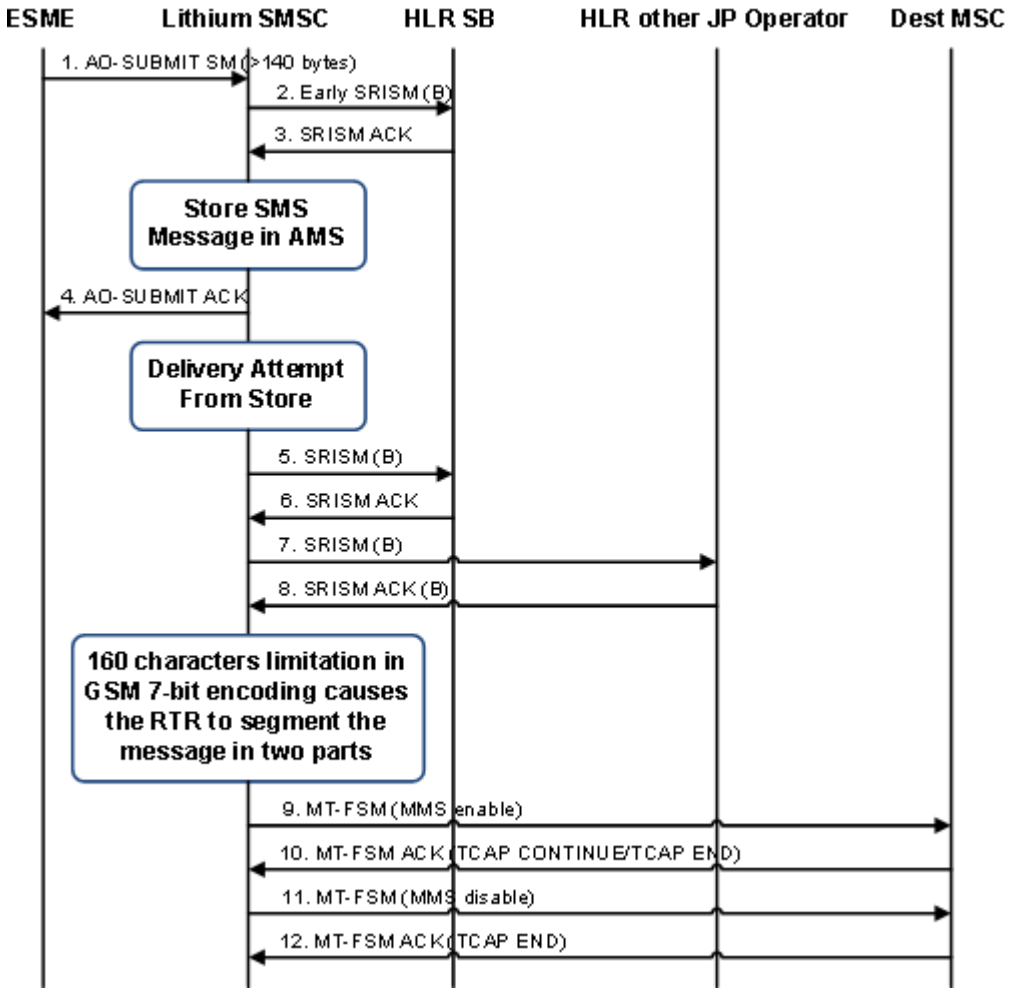


Figure 78: 1 Long AO Submit, 2 MT Message after Conversion

18.9.5.3 Caching Scenario When Delivery Is Attempt From AMS

In this scenario, when the MTFSM delivery is attempted from AMS for a recipient, MMS is enabled (i.e. MMS = 0), the RTR will perform SRI-SM as the RTR does not store the SRISM response received during Early-SRISM.

If another MTFSM delivery is attempted from AMS after 3+ seconds for the same recipient and MAP transaction dialogue is open (i.e. TCAP-continue received in response of the first MTFSM), then the RTR will again perform the SRISM as the RTR clears the previously stored SRISM result.

Note: The HLR query result will be stored for another 3 seconds only when the RTR receives the MT-FSM ack. If the MTFSM ack has not been received and the dialog is still open, then the RTR will not perform the new SRISM request but it will reuse the existing result instead.

The following figure describes the forward scenario:

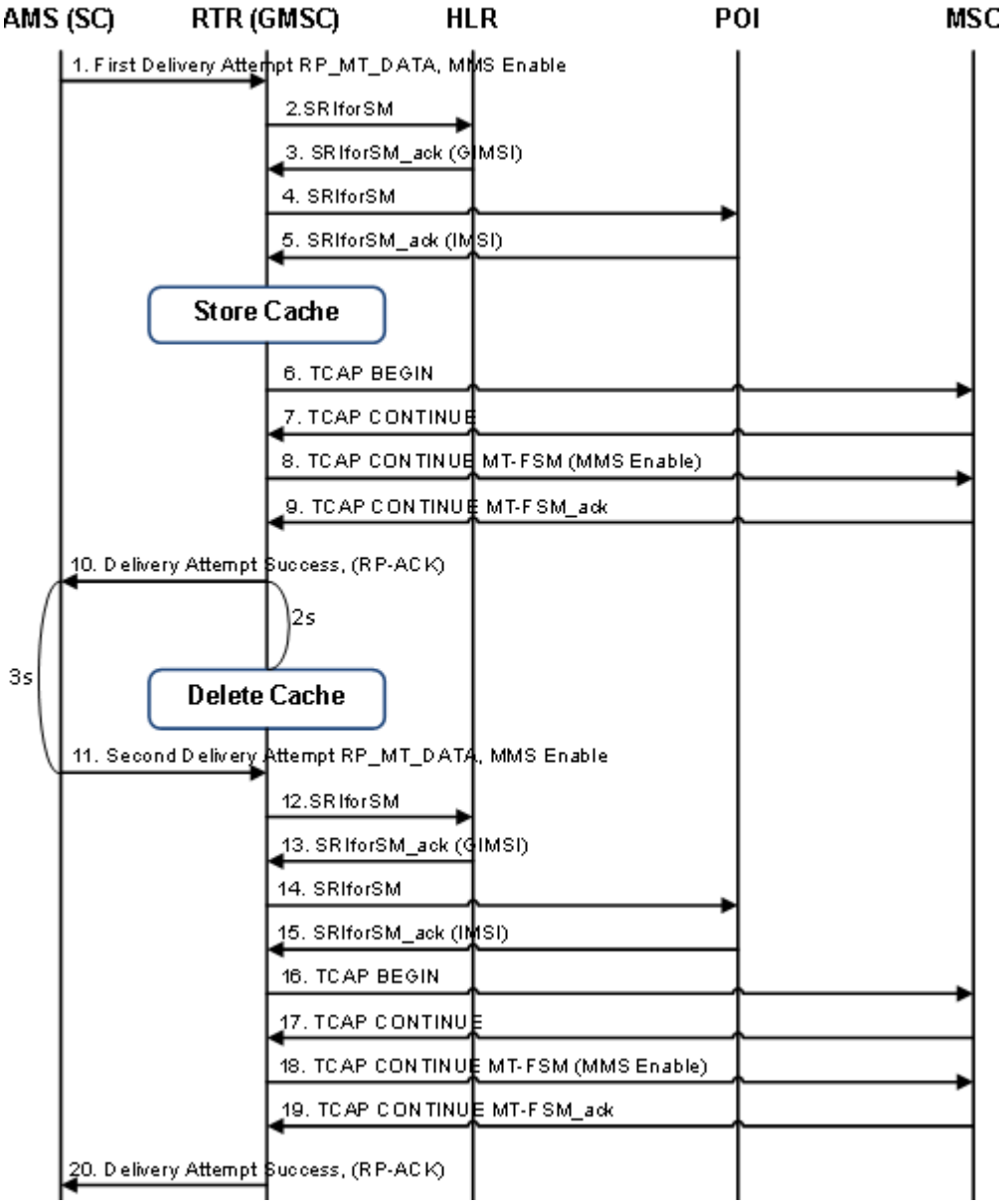


Figure 79: Cache Scenario for Segmented Message

18.9.6 Japanese MNP Processing While Receiving a Report SM Delivery Status

When the RTR receives a Report SM Delivery Status message from the SMSC, then, based on whether the message is addressed to the RTR or not, the RTR either forwards the message based on the Recipient number or it forwards the message as per the CdPA GTA of the message received.

1. When the RTR receives an incoming Report SM Delivery Status request, it checks if Japanese MNP is ON. If Japanese MNP is OFF, the RTR forward the Report SM Delivery Status message to the local HLR using CdPA GTA as the recipient number.
2. If Japanese MNP is ON, the RTR forwards the Report SM Delivery Status message to the local HLR using:

a. CdPA GTA as the recipient number, CdPA TT=0x00 and CdPA NAI=0x04.
b. If the outgoing network to which the Report SM Delivery Status is being forwarded has TCAP User Info Set, then TCAP user info is also added to the message.

3. The RTR receives a Report SM Delivery Status response from the HLR and sends it back to the Originating SMSC.

   a. If the incoming network has TCAP User Info Set, then TCAP user info is added to the Report SM Delivery Status response sent back to SMSC.

Note:

1. With Japanese MNP ON, the RTR has the same behavior for handling the Report SM Delivery Status message received from a Japanese Operator or an Overseas Operator.
2. The RTR also creates a valid outgoing Report SM Delivery Status message for incoming Report SM Delivery Status message destined to an HLR, as per the MAP Phase configured in Destination network, if any of the below conditions return true:

   a. If the MGR GUI configuration option **ReportSmDeliveryStatus GPRS Support Indicator** (**Firewall ➤ MT ➤ Properties**) is set as either ON/OFF.
   b. If the option **Inc. TCAP user info.** is checked in the configured destination network.

   For more details refer to *Modification of the TCAP and MAP Portion of the Incoming Report SM Delivery Status Message*

18.9.7 Japanese MNP Processing While Sending a Report SM Delivery Status

The RTR sends a Report SM Delivery Status message to the HLR under the following scenarios, irrespective of whether Japanese MNP is enabled or not:

1. In case the MT-FSM delivery attempt is successful, but the HLR had earlier indicated that MWD status flag(s) was set for the recipient subscriber (in response to the SRI-SM sent with priority, or in the Inform-SC);
2. In case the MT-FSM delivery attempt is not successful and the error received is such that the MWD status for the recipient subscriber in the HLR should be updated (e.g. absent subscriber, memory capacity exceeded), and if the HLR has not already indicated that the relevant MWD status flag(s) was set for the recipient.
3. If the semi-static parameter *repstsaddgprssupportindicatorifbothmscsgsnpresent* is set to true and in the SRI-SM response both MSC and SGSN destinations are present, only then GPRS Support Indicator will be present in the Report SM Delivery Status. The following table describes various scenarios related to this parameter:

repstsaddgprssupportindicatorifbothmscsgsnpresent	Both MSC & SGSN Present in SRI-SM Response	GPRS Support Indicator in Report SM Delivery Message
true	yes	yes
true	no	no
false	yes	yes
false	no	yes

Note: In the second scenario mentioned above, the RTR does not send a Report SM Delivery Status if the message was originally received as MO, unless there is a fallback option to the Store (AMS).

However, if the semi-static parameter *enablejapanesemnp* is set to "true" then the RTR performs the following customized processing steps while sending a Report SM Delivery Status:

- The RTR first does a lookup on the Mobile Network Table based on the MCC/MNC from the recipient IMSI. Note that the actual IMSI of the recipient is already known at this point, since it would have been included in the preceding MT-FSM
- If a matching Network entry is found, the MNP prefix ("mobNetworkMnpPrefix") and the Translation Type for the Fallback SRI-SM ("mobNetworkTtForFallbackSriSm") are retrieved. Note that if the TT for the Fallback SRI-SM is not configured then by default the TT value is taken as 0x0.

  Note: If a matching entry is not found in the Network table, or if the MNP prefix is not configured in the matched entry, then the RTR does not perform any further customized processing related to Japanese MNP and continues with its normal functionality.

The RTR sends the Report-SM-Delivery-Status message with its SCCP CdPA and CgPA being populated (before GTT) as below for national recipient:

If the MTO modifier's field "Apply SCCP CdPA Modifier for Report SM operation" is checked and Recipient country belongs to national (i.e. own country), the MTO modifiers will not be applied on the SCCP called party address (CdPA) of the Report SM Delivery Status Message.

CdPA for Report SM Delivery Status will be prepared as:

- CdPA GT address = <MNP Prefix retrieved from Network Table entry><MSIN>;
- Subsystem Number = 6;
- Nature of Address Indicator = 0x03;
- TT = <Fallback SRI-SM TT retrieved from Network Table entry, default 0x0 if not found>;
- CgPA GT address = <RTR's own GT>;
- Subsystem Number = 8;
- Nature of Address Indicator = 0x04;

If the MTO modifier's field "Apply SCCP CdPA Modifier for Report SM operation" is checked and Recipient country belongs to international, the MTO modifiers will be applied on the SCCP called party address (CdPA) of the Report SM Delivery Status Message.

CdPA for Report SM Delivery Status will be prepared as:

- CdPA GT address = <MTO modifier provisioned SCCP CdPA>;
- Subsystem Number = 6;
- Nature of Address Indicator = 0x04;
- TT = <Fallback SRI-SM TT retrieved from Network Table entry, default 0x0 if not found>;
- CgPA GT address = <RTR's own GT>;
- Subsystem Number = 8;
- Nature of Address Indicator = 0x04;

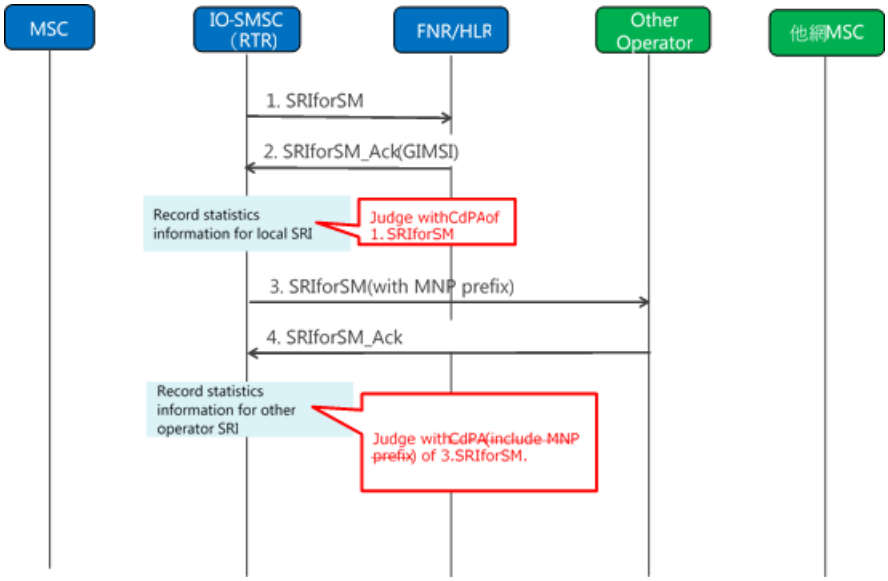
Note: We can distinguish the national and international subscribers in the following way:

- If the *mobilecountrycode* configured in semi-static configuration file is the same as the mobile country code received in the IMSI provided by the HLR in the SRISM Response, then the subscriber belongs to national country; otherwise it will be international.

18.9.8 Japanese MNP Processing for Statistics Information per Destination Operator When Action Is Forward

The RTR will be enhanced to have:

- Per Country/Network SRISM counter increment based on Recipient for First SRISM.
- Per Country/Network SRISM counter increment based on Forwarded Network in case of Second SRISM (for MNP Action = Forward)



The RTR increments the Per Country/Network SRI-SM statistics counter only if "`MNP network Info`" is configured in Number Portability Table.

The MNP network Info value is configured only if below conditions are true:

1. Japanese MNP action set as FORWARD.
2. The Network is present in Network Table.
3. The configured network state is ACTIVE .

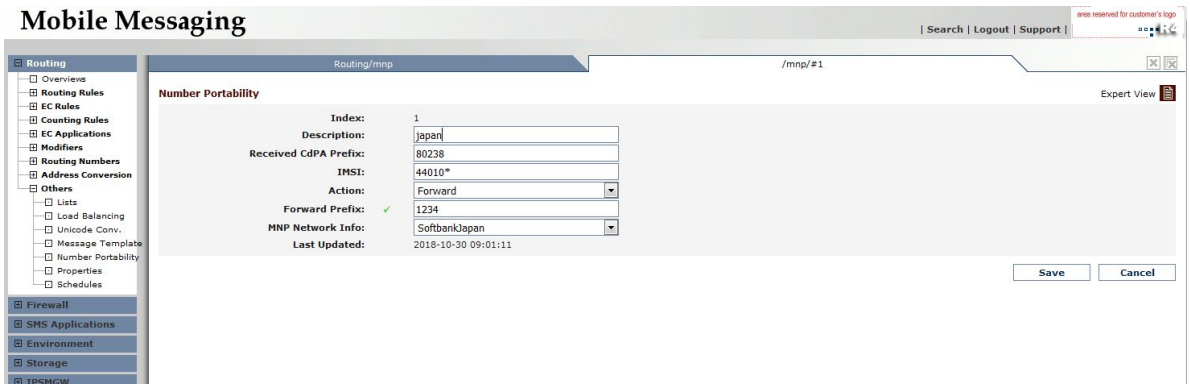


Figure 80: MNP Network Info in MNP Table

This functionality mainly impacts the following counters available in the Statistics Viewer, selectable per Country or per configured Network:

Network Statistics	Country Statistics
mobNetworkSriSmTotalCounter	countrySriSmTotalCounter
mobNetworkSriSmSuccessCounter	countrySriSmSuccessCounterCounter
mobNetworkSriSmTimeoutCounter	countrySriSmTimeoutCounterCounter
mobNetworkSriSmSysFailErrorCounter	countrySriSmSysFailErrorCounter
mobNetworkSriSmDataMisErrorCounter	countrySriSmDataMisErrorCounter
mobNetworkSriSmUnexpDataValErrorCounter	countrySriSmUnexpDataValErrorCounter
mobNetworkSriSmFacNotSuppErrorCounter	countrySriSmFacNotSuppErrorCounter
mobNetworkSriSmUnkSubErrorCounter	countrySriSmUnkSubErrorCounter
mobNetworkSriSmAbsSubErrorCounter	countrySriSmAbsSubErrorCounter
mobNetworkSriSmCallBarredErrorCounter	countrySriSmCallBarredErrorCounter
mobNetworkSriSmTeleServNotProvErrorCounter	countrySriSmTeleServNotProvErrorCounter
mobNetworkSriSmOtherErrorsCounter	countrySriSmOtherErrorsCounter
mobNetworkSriSmTcapAbortedCounter	countrySriSmTcapAbortedCounter
mobNetworkSriSmSccpAbortedCounter	countrySriSmSccpAbortedCounter
mobNetworkSriSmFallbackToVersion2Counter	countrySriSmFallbackToVersion2Counter
mobNetworkSriSmFallbackToVersion1Counter	countrySriSmFallbackToVersion1Counter

18.9.9 Japanese MNP Behavior With MTO Modifier

1. MTO modifier behavior for MO-ST-MT:

Scenario	MNP Action=Accept	MNP Action=Forward
SRI-SM Message triggered due to Early SRISM	MTO modifiers are applied on the message's SCCP CdPA	MTO modifiers are applied on the message's SCCP CdPA
SRI-SM Message Triggered through AMS	MTO modifiers are applied on the message's SCCP CdPA	MTO modifiers are applied on the message's SCCP CdPA
SRISM Message Triggered through MNP Action as Forward	N/A	MTO modifier should not be configured for this case

	Recipient Country is own country (National)	Recipient Country is not own country (International)
RSMDS Message	MTO modifiers are not applied on the message's SCCP CdPA	MTO modifiers are applied on the message's SCCP CdPA

2. MTO modifier behavior for AO-ST-MT:

Scenario	MNP Action=Accept	MNP Action=Forward
SRI-SM Message triggered due to Early SRISM	MTO modifiers are not applied on the message's SCCP CdPA	MTO modifiers are not applied on the message's SCCP CdPA
SRI-SM Message Triggered through AMS	MTO modifiers are applied on the message's SCCP CdPA	MTO modifiers are applied on the message's SCCP CdPA
SRISM Message Triggered through MNP Action as Forward	N/A	MTO modifier should not be configured for this case

	Recipient Country is own country (National)	Recipient Country is not own country (International)
RSMDS Message	MTO modifiers are not applied on the message's SCCP CdPA	MTO modifiers are applied on the message's SCCP CdPA

3. MTO modifier behavior for MT-MT:

   In this scenarios the routing action is configured with '`send to HLR`' in SRI_SM request rules and the country belongs to the RTR's own country.

Scenario	MNP Action=Accept	MNP Action=Forward
Outgoing SRI-SM Message triggered due to home-routing	MTO modifier **Replace SCCP CdPA** is applied on the message's SCCP CdPA	MTO modifier **Replace SCCP CdPA** is applied on the message's SCCP CdPA
Outgoing SRI-SM Message Triggered through AMS	MTO modifier **Replace SCCP CdPA** is applied on the message's SCCP CdPA	MTO modifier **Replace SCCP CdPA** is applied on the message's SCCP CdPA
Outgoing SRISM Message Triggered through MNP Action as Forward	N/A	MTO modifier **Replace SCCP CdPA** is not applied on the message's SCCP CdPA

	Recipient Country is own country (National)	Recipient Country is not own country (International)
RSMDS Message	MTO modifier **Replace SCCP CdPA** is not applied on the message's SCCP CdPA	MTO modifier **Replace SCCP CdPA** is applied on the message's SCCP CdPA

18.10 Inclusion of TP-MR in Outgoing MT-FSM Towards CDMA-based Networks

As per 3GPP TS 23.040, the TP-MR value is supposed to be generated by each mobile station for each message (including each individual segment of a concatenated message) originated from it, in the strict ascending order from 0 to 255; once the value reaches 255 it rolls over and restarts from 0 again.

Hence, for MO (and also SIPO) messages, the TP-MR provides the means to uniquely identify each message sent from a particular Originator within a reasonable period of time, irrespective of the Destination(s) of such messages.

Inclusion of TP-MR in MT short messages (carrying the SMS-DELIVER PDU) is not addressed in the relevant protocol specifications and there is no standard field defined for such a purpose. However, in certain scenarios it might be useful to include the TP-MR in an outgoing MT-FSM, e.g. while sending a message from a GSM-based network to a CDMA-based network.

The maximum allowed size of a single short message is less in CDMA-based networks as compared to GSM-based networks. Hence if the RTR is operating in a GSM network then the peer entity in the external network would need to split many of the single messages received from the RTR into 2 messages. In such a case, a unique TP-MR value per Originator would enable the external network entity to correctly keep track of each pair of split messages w.r.t. the original "parent" message received from RTR; this can help prevent potential duplicate deliveries of the split messages.

The RTR supports the capability of including the 'TP-MR' field as a customized "private extension container" in outgoing MT-FSM messages destined for certain Japanese networks (which are supposed to be using CDMA based operations). In accordance with 3GPP TS 29.002, the private extension container carrying the TP-MR value is included in an outgoing MT-FSM only if MAP Phase 2+ is being used. The inclusion of this field in the MT-FSM is controlled through a new configuration option "Inc. TP-MR in MT-ForwardSM" associated with the matching MTOR rule (refer to Section 4.4.5 of the MGR Operator Manual),

For each MO or SIPO message that gets delivered as an MT-FSM, the RTR includes the original TP-MR value that was received in the incoming message in the outgoing PDU; this is also true for individual segments of a concatenated message.

On the other hand, for each AO message that gets delivered as an MT-FSM, the RTR internally generates a TP-MR value such that for any sequence of 255 consecutive messages originated from a particular ESME, the generated values remain unique across all RTR instances. Moreover, if a long AO message is received and internally segmented by the RTR into multiple MT "parts", the RTR ensures that each such part is assigned a unique TP-MR value.

Note:

1. The above functionality is independent of the support for Japanese MNP in the RTR.
2. The above functionality is relevant only for MT short messages (i.e. MT-FSMs carrying SMS-DELIVER PDUs). For an MT Status Report, the RTR always includes the TP-MR value received in the corresponding original MO message, as specified in 3GPP TS 23.040.
3. In case the TP-MR is received in an inbound MT-FSM message (i.e. as a custom field encapsulated within a private extension container) then it is ignored by the RTR, irrespective of whether the inbound message is an Unsolicited MT-FSM or a Home-routed MT-FSM.

18.11 Inclusion of TCAP User Information in Outgoing PDU(s)

As per 3GPP 29.002 [6] Section 16.1.2.3, the User information parameter in TC dialogue primitives is used to carry the MAP dialogue application PDUs.

The RTR supports the capability of including the user information in the TCAP dialogue portion for outgoing requests and responses based on a per network configuration. The network table parameter **mobNetworkIncludeTcapUserInfo** controls the inclusion of the TCAP user info. If the network corresponding to the CdPA GT in the outgoing PDU has the parameter **mobNetworkIncludeTcapUserInfo** enabled, then RTR adds the respective TCAP user information.

The TCAP User Information comprises of the following:

1. MAP-DialogueAS

   As per 3GPP 29.002 [6] Section 17.1, the ASN.1 syntax for MAP-DialogueAS is as follows:

   ```
   map-DialogueAS  OBJECT IDENTIFIER ::=
    {gsm-NetworkId as-Id map-DialoguePDU (1) version1 (1)}
   ```

   Note: The value for the map-DialogueAS in request/response is: "0.4.0.0.1.1.1.1".

2. MAP-DialoguePDU

   As per 3GPP 29.002 [6] Section 17.1, the ASN.1 syntax for MAP-DialoguePDU is as follows:

   ```
   MAP-DialoguePDU ::= CHOICE {
    map-open            [0] MAP-OpenInfo,
    map-accept          [1] MAP-AcceptInfo,
    map-close           [2] MAP-CloseInfo,
    map-refuse          [3] MAP-RefuseInfo,
    map-userAbort       [4] MAP-UserAbortInfo,
    map-providerAbort   [5] MAP-ProviderAbortInfo}
   ```

   The following list the MAP-DialoguePDU(s) that shall be used in RTR:

   - **map-open**

     ASN1 syntax of MAP-OpenInfo is:

     ```
     MAP-OpenInfo ::= SEQUENCE {
      destinationReference    [0] AddressString OPTIONAL,
      originationReference    [1] AddressString OPTIONAL,
      ...,
      extensionContainer ExtensionContainer OPTIONAL
      -- extensionContainer must not be used in version 2
      }
     ```

     Note: Only the optional destinationReference is supported by RTR.

   - **map-accept**

     ASN1 syntax of map-AcceptInfo is:

     ```
     MAP-AcceptInfo ::= SEQUENCE {
      ...,
      extensionContainer ExtensionContainer OPTIONAL
      -- extensionContainer must not be used in version 2
      }
     ```

     Note: The optional extensionContainer is not supported by RTR.

   - **map-refuse**

ASN1 syntax of map-RefuseInfo is:

```
MAP-RefuseInfo ::= SEQUENCE {
 reason Reason,
 ...,
 extensionContainer ExtensionContainer OPTIONAL,
 -- extensionContainer must not be used in version 2
 alternativeApplicationContext OBJECT IDENTIFIER OPTIONAL
 -- alternativeApplicationContext must not be used in version 2
 }

Reason ::= ENUMERATED {
 noReasonGiven (0),
 invalidDestinationReference (1),
 invalidOriginatingReference (2)}
```

Note: Of these, only the Reason “invalidDestinationReference(0)” is supported by RTR.

- **map-userAbort**

  ASN1 syntax of map-userAbortInfo is:

```
MAP-UserAbortInfo ::= SEQUENCE {
 map-UserAbortChoice MAP-UserAbortChoice,
 ...,
 extensionContainer ExtensionContainer OPTIONAL
 -- extensionContainer must not be used in version 2
 }

MAP-UserAbortChoice ::= CHOICE {
 userSpecificReason [0] NULL,
 userResourceLimitation [1] NULL,
 resourceUnavailable [2] ResourceUnavailableReason,
 applicationProcedureCancellation [3] ProcedureCancellationReason}
```

  Note: Of these, only the map-UserAbortChoice “userSpecificReason(0)” is supported by RTR.

- **map-providerAbort**

  ASN1 syntax of map-providerAbort is:

```
MAP-ProviderAbortInfo ::= SEQUENCE {
 map-ProviderAbortReason MAP-ProviderAbortReason,
 ...,
 extensionContainer ExtensionContainer OPTIONAL
 -- extensionContainer must not be used in version 2
 }

MAP-ProviderAbortReason ::= ENUMERATED {
 abnormalDialogue  (0),
 invalidPDU  (1)}
```

  Note: Of these, only the map-ProviderAbortChoice “abnormalDialogue(0)” is supported by RTR.

18.11.1 Handling for Incoming Requests by RTR

The RTR adds the following TCAP User Information in response to incoming requests:

- The TCAP user information "map-accept" is included in ACK/NACK **response** of incoming Requests (MTFSM, SRISM, MOFSM or Report Status Delivery Status), if the CgPA network of incoming request has TCAP user information parameter **mobNetworkIncludeTcapUserInfo** enabled.

- If the incoming message has MAP-DialoguePDU with invalid IMSI (i.e.: "IMSI too long") in the destination reference and MAP Phase is 2 or 2+, then RTR sends TC-UAbort containing "map-refuse" with reject-reason as "invalidDestinationReference". This is independent of the network configuration parameter **mobNetworkIncludeTcapUserInfo**.
- If the incoming request does not contain map-DialogueAS value as "**0.4.0.0.1.1.1.1**" and MAP Phase is 2 or 2+, then RTR shall send TC-UAbort with map-providerAbort and reject-reason as "abnormalDialogue". This is independent of the network configuration parameter **mobNetworkIncludeTcapUserInfo**.

18.11.2 Handling for Outgoing Requests by RTR

The RTR adds the following TCAP User Information in response to outgoing requests if the CdPA network has the parameter **mobNetworkIncludeTcapUserInfo** enabled:

- The TCAP user information "map-open" is included in outgoing requests like MOFSM, SRISM, MTFSM and RSMDS.
- The TCAP user information with map-UserAbortChoice userSpecificReason(0) is included while sending TCAP-U-Abort.

If both LMSI and IMSI are received in the SRISM response, then the RTR prepares MTFSM with TCAP user information "map-open" with "destinationReference" as the received IMSI. This is independent of the parameter **mobNetworkIncludeTcapUserInfo** set.

If the CdPA GT network has user information parameter **mobNetworkIncludeTcapUserInfo** enabled, RTR includes the TCAP User information in outgoing MTFSM. However "destinationReference" is added only if both LMSI and IMSI are present in the corresponding SRISM response.

Note: When the MT modifier rule configured with Prefix SCCP CdPA of SRISM, Strip SCCP CdPA of SRISM or Replace SCCP CdPA of SRISM is applied on the outgoing SRISM request, TCAP user information will be included based on the network determined using the actual recipient present in the request. Modified SCCP CdPA will not be used for the determination of the network.

The RTR does not generate any/extra TCAP user information in the following scenarios:

- When the incoming
  - Message is transparently sent to SMSC as MO.
  - SRISM is transparently forwarded (SRIQ action = ‘Have HLR respond to SMSC directly’).
  - Report SM Delivery Status is transparently forwarded.

  In above cases if TCAP user information was earlier present in the message then RTR transparently forwards it.
- When the network is not known.
- When RTR cannot determine the network, like RTR encounters error while converting the received CgPA in the MOFSM message.

18.12 Modification of the TCAP and MAP Portion of the Incoming Report SM Delivery Status Message

1. The RTR creates a valid outgoing ReportSmDeliveryStatus message for the incoming ReportSmDeliveryStatus message destined to an HLR, as per the MAP Phase configured in Destination network if any of the below conditions return true:

   a. If the MGR GUI configuration option **ReportSmDeliveryStatus GPRS Support Indicator** (**Firewall ➤ MT ➤ Properties**) is set as either ON/OFF.
   b. If the option **Inc. TCAP user info.** is checked in the configured destination network.

   In case of MAP conversion, the responses received from HLR are also converted before sending back to SMSC. For more details refer to the sections *MAP Phase Conversion of Incoming ReportSmDeliveryStatus Requests from SMSC* and *MAP Phase Conversion of Incoming ReportSmDeliveryStatus Response(ACK/NACK) from HLR*.

   Note:

   1. If Japanese MNP is OFF, the destination network is derived from the incoming CdPA GT. If Japanese MNP is ON, the destination network is derived from the recipient address of incoming message.
   2. In case the destination network does not match any configured network, then the MAP phase will be decided according to the value of the semi-static parameter `defaultmapphase`.

2. For incoming Report SM Delivery Status message, the RTR has finer control over including the GPRS support indicator in the outgoing ReportSmDeliveryStatus sent to the HLR on the basis of the configuration option **ReportSmDeliveryStatus GPRS Support Indicator** in the MGR GUI (**Firewall ➤ MT ➤ Properties**). The GPRS support indicator parameter is only supported in MAP phase 2+. The supported values are as follows:

   - Default - the RTR does not modify the GPRS support indicator in the outgoing ReportSmDeliveryStatus message. It would be the same as in the incoming Report SM Delivery Status.
   - OFF - the RTR removes the GPRS support indicator from the message (if present) before sending it to the HLR.

     Also, all the SGSN related outcomes (deliveryOutcomeIndicator, additionalSM-DeliveryOutcome and additionalAbsentSubscriberDiagnosticSM) are removed from the message and the message is converted to the MAP version supported by the destination network.
   - ON - the RTR converts the message to the MAP version supported by the destination network.

     Note: The RTR cannot set the GPRS support indicator in the Report SM Delivery Status to the HLR in this case if the GPRS support indicator is not set in the incoming message:

     - As per 3gpp specification 29.002, GPRS support indicator must be added if both MSC and SGSN delivery outcomes are present in the message. Now if the incoming message has only one delivery outcome then the RTR cannot add the GPRS support indicator. Also, if the incoming message has two delivery outcomes then it will anyways have the GPRS support indicator, otherwise the message will be incorrect.
     - The GPRS support Indicator is only present in MAP Phase 2+. In case the message is converted to lower phase then the GPRS support indicator should not be added.

3. In case the RTR converts the incoming ReportSmDeliveryStatus message according to the destination network MAP Phase and sends it to the HLR, and receives an Abort message due to "Application context name not supported" in response to this outgoing ReportSmDeliveryStatus, the RTR re-sends the outgoing ReportSmDeliveryStatus message one MAP phase version lower than the previous ReportSmDeliveryStatus message. The RTR will re-attempt delivery with decreasing order of map phase 3> 2>1.
4. The RTR transparently forwards the incoming ReportSmDeliveryStatus message if both configuration option **ReportSmDeliveryStatus GPRS Support Indicator** is set as `Default` and **Inc. TCAP user info.** is not checked (i.e. false) in the configured destination network.
5. In case the destination HLR network has TCAP User Info Set, the RTR adds map-open MAP-DialoguePDU in the outgoing ReportSmDeliveryStatus request message converted as per the destination MAP Phase. TCAP user info is included if MAP Phase is either 2 or 2+(3).

   If the incoming SMSC network has TCAP User Info Set, then TCAP user info is added to the Report SM Delivery Status response sent back to SMSC.
6. According to MAP ASN.1 definition, following are the mandatory and optional fields in ReportSmDeliveryStatus message PDU. ReportSmDeliveryStatus message does not exist in map phase 1, the operation is called setMessageWaitingData in case of MAP Phase 1.

   MAP Phase 1 definition:

```
SetMessageWaitingData ::= OPERATION

    PARAMETER SEQUENCE {
        msIsdn  IsdnAddressString,
        serviceCentreAddress AddressString}
    RESULT

    ERRORS {
        UnexpectedDataValue
        UnknownSubscriber,
        MessageWaitingListFull}
```

   MAP Phase 2 definition:

```
ReportSM-DeliveryStatus ::= OPERATION ARGUMENT

    ARGUMENT
        reportSM-DeliveryStatusArg SEQUENCE {
            msisdn ISDN-AddressString,
            serviceCentreAddress AddressString,
            sm-DeliveryOutcome ENUMERATED {
            memoryCapacityExceeded (0),
            absentSubscriber (1),
            successfulTransfer (2)} OPTIONAL, --mandatory in MAP Phase 2

        ... }

    RESULT
        storedMSISDN ISDN-AddressString OPTIONAL

    ERRORS {
        -- dataMissing -- localValue 35,
        -- unexpectedDataValue -- localValue 36,
        -- unknownSubscriber -- localValue 1,
        -- messageWaitingListFull -- localValue 33}
    ::= localValue 47
```

   MAP Phase 2+ definition:

```
reportSM-DeliveryStatus OPERATION  ::=  {
   ARGUMENT     SEQUENCE {
```

```
      msisdn                                    ISDN-AddressString,
      serviceCentreAddress                       AddressString,
      sm-DeliveryOutcome                        ENUMERATED {
         memoryCapacityExceeded    ( 0 ),
         absentSubscriber          ( 1 ),
         successfulTransfer        ( 2 ) },
      absentSubscriberDiagnosticSM              [0] IMPLICIT INTEGER ( 0 .. 255
) OPTIONAL,
      extensionContainer                        [1] IMPLICIT SEQUENCE {
         privateExtensionList   [0] IMPLICIT SEQUENCE  ( SIZE( 1 .. 10 ) ) OF
            SEQUENCE {
               extId      MAP-EXTENSION .&extensionId  ( {
                  ,
                  ...} ) ,
               extType    MAP-EXTENSION .&ExtensionType  ( {
                  ,
                  ...} { @extId   }  )  OPTIONAL} OPTIONAL,
         pcs-Extensions         [1] IMPLICIT SEQUENCE {
            ... } OPTIONAL,
         ... } OPTIONAL,
      ... ,
      gprsSupportIndicator                      [2] IMPLICIT NULL OPTIONAL,
      deliveryOutcomeIndicator                  [3] IMPLICIT NULL OPTIONAL,
      additionalSM-DeliveryOutcome              [4] IMPLICIT ENUMERATED {
         memoryCapacityExceeded    ( 0 ),
         absentSubscriber          ( 1 ),
         successfulTransfer        ( 2 ) } OPTIONAL,
      additionalAbsentSubscriberDiagnosticSM    [5] IMPLICIT INTEGER ( 0 .. 255
) OPTIONAL,
      ip-sm-gw-Indicator                        [6] IMPLICIT NULL OPTIONAL,
      ip-sm-gw-sm-deliveryOutcome               [7] IMPLICIT ENUMERATED {
         memoryCapacityExceeded    ( 0 ),
         absentSubscriber          ( 1 ),
         successfulTransfer        ( 2 ) } OPTIONAL,
      ip-sm-gw-absentSubscriberDiagnosticSM     [8] IMPLICIT INTEGER ( 0 .. 255
) OPTIONAL,
      imsi                                     [9] IMPLICIT OCTET STRING ( SIZE(
 3 .. 8 ) ) OPTIONAL,
      singleAttemptDelivery                     [10] IMPLICIT NULL OPTIONAL,
      correlationID                             [11] IMPLICIT SEQUENCE {
         hlr-id      [0] IMPLICIT OCTET STRING ( SIZE( 3 .. 8 ) ) OPTIONAL,
         sip-uri-A   [1] IMPLICIT OCTET STRING OPTIONAL,
         sip-uri-B   [2] IMPLICIT OCTET STRING} OPTIONAL}
   RESULT     SEQUENCE {
      storedMSISDN         ISDN-AddressString OPTIONAL,
      extensionContainer   SEQUENCE {
         privateExtensionList   [0] IMPLICIT SEQUENCE  ( SIZE( 1 .. 10 ) ) OF
            SEQUENCE {
               extId      MAP-EXTENSION .&extensionId  ( {
                  ,
                  ...} ) ,
               extType    MAP-EXTENSION .&ExtensionType  ( {
                  ,
                  ...} { @extId   }  )  OPTIONAL} OPTIONAL,
         pcs-Extensions         [1] IMPLICIT SEQUENCE {
            ... } OPTIONAL,
         ... } OPTIONAL,
      ... }
   ERRORS     {
      dataMissing |
      unexpectedDataValue |
      unknownSubscriber |
      messageWaitingListFull }
   CODE     local      : 47
   }
```

18.12.1 MAP Phase Conversion of Incoming ReportSmDeliveryStatus Requests from SMSC

The following table contains the details about MAP Phase conversion for ReportSmDeliveryStatus request message.

SMSC MAP Phase Version	HLR MAP Phase Version		
	1	2	3
1	The outgoing PDU will have all parameters present in the incoming PDU. **Note:** The operation is called setMesageWaitingData in case of MAP Phase 1.	The outgoing PDU will have all parameters present in the incoming MAP Phase1 PDU plus the "smDeliveryOutcome" parameter which is a mandatory parameter for MAP Phase 2. The parameter will set to the value "absent subscriber". **Note:** The operation is called reportSM-DeliveryStatus in case of MAP Phase 2.	The outgoing PDU will have all parameters present in the incoming MAP Phase1 PDU plus the "smDeliveryOutcome" parameter which is a mandatory parameter for MAP Phase 3. The parameter will set to the value "absent subscriber". **Note:** The operation is called reportSM-DeliveryStatus in case of MAP Phase 3.
2	The outgoing PDU will have all parameters present in the incoming MAP Phase 2 PDU minus "smDeliveryOutcome" parameter (if present). **Note:** The operation is called setMesageWaitingData in case of MAP Phase 1.	The outgoing PDU will have all parameters present in the incoming MAP Phase 2 PDU.	The outgoing PDU will have all parameters present in the incoming MAP Phase 2 PDU.
3	The outgoing PDU will have only the first 2 parameters from the incoming MAP Phase 3 PDU.	The outgoing PDU will have only the first 3 parameters from the incoming MAP Phase 3 PDU.	• If the configuration option **ReportSmDeliveryStatus GPRS Support Indicator** is ON, then the

SMSC MAP Phase Version	HLR MAP Phase Version		
	1	2	3
	Note: The operation is called setMesageWaitingData in case of MAP Phase 1.		outgoing PDU will have all parameters present in the incoming PDU. • If the configuration option **ReportSmDeliveryStatus GPRS Support Indicator** is OFF, then the outgoing PDU will have parameters present in the incoming PDU minus the GPRS support indicator and all the SGSN related outcomes (deliveryOutcomeIndicator, additionalSM-DeliveryOutcome and additionalAbsentSubscriberDiagnosticSM).

18.12.2 MAP Phase Conversion of Incoming ReportSmDeliveryStatus Response(ACK/NACK) from HLR

The following table contains the details about MAP Phase conversion for incoming ReportSmDeliveryStatus Response message from HLR before sending it to SMSC.

HLR Response MAP Phase Version	SMSC MAP Phase Version		
	1	2	3
1	The outgoing PDU will have all parameters present in the incoming PDU. **Note:** The operation is called setMesageWaitingData in case of MAP Phase 1.	The outgoing PDU will have all parameters present in the incoming PDU. **Note:** The operation is called reportSM-DeliveryStatus in case of MAP Phase 2.	The outgoing PDU will have all parameters present in the incoming PDU. **Note:** The operation is called reportSM-DeliveryStatus in case of MAP Phase 3.
2	• If Error is not `DataMissing`, the outgoing PDU will have all parameters present in the incoming PDU. • If Error is `DataMissing`, the outgoing PDU will have all parameters present in the incoming PDU, except the `DataMissing` error is	The outgoing PDU will have all parameters present in the incoming MAP Phase 2 PDU.	The outgoing PDU will have all parameters present in the incoming PDU.

HLR Response MAP Phase Version	SMSC MAP Phase Version		
	1	2	3
	changed to `UnexpectedDataValue`. **Note:** The operation is called setMesageWaitingData in case of MAP Phase 1.		
3	The outgoing PDU will have all parameters present in the incoming PDU except: • `StoredMSISDN` parameter (if present) and extension Container parameter (if present). • If Error is `DataMissing`, error is changed to `UnexpectedDataValue`. **Note:** The operation is called setMesageWaitingData in case of MAP Phase 1.	The outgoing PDU will have all parameters present in the incoming PDU except the Extension Container parameter (if present)	The outgoing PDU will have all parameters present in the incoming PDU.

18.13 Retrieving Cell-Id Using MAP Any Time Interrogation

For Mobile Originated and Mobile Terminated messages via the CS network, the Originator and Recipient Cell-ID can be determined using a MAP Any Time Interrogation message to the HLR. The originator Cell-ID is stored in the Submit CDR and the Recipient Cell-ID is stored in the Delivery CDR.

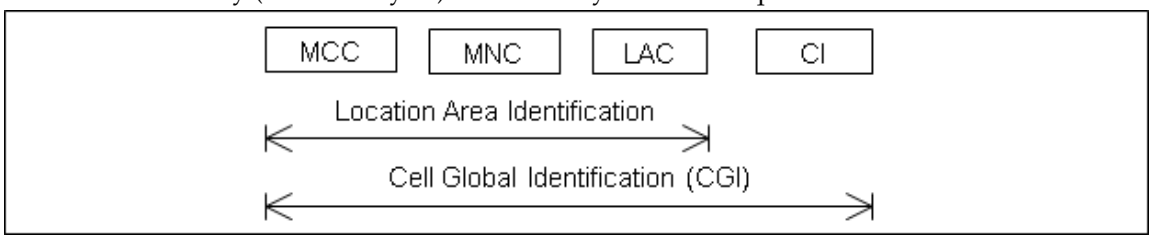
The request for A-Party Cell-ID information will be initiated if configured to do so through the semi-static configuration files before any Routing Rules are processed in the MO leg and the request for the B-Party Cell-ID information, if configured to do so via semi-static configuration files, will be initiated after successful delivery, and optionally after Report SM Delivery Status message. In case of failure to retrieve cell-id, the field will not be included in the corresponding CDR.

There is additional handling for XS-CPY and XS-FWD. CPY and FWD also result in MT delivery.

- In case of CPY related CDRs, MAP ATI for Recipient will be performed on the copied number as well.
- In case of FWD, MAP ATI for Recipient will be performed for the forwarded number. MAP ATI will not be performed for Original Recipient in this case. This information will be stored in Normal Delivery CDR and not forward CDR.

Following is a brief description about Cell-id. Cell-id can be:

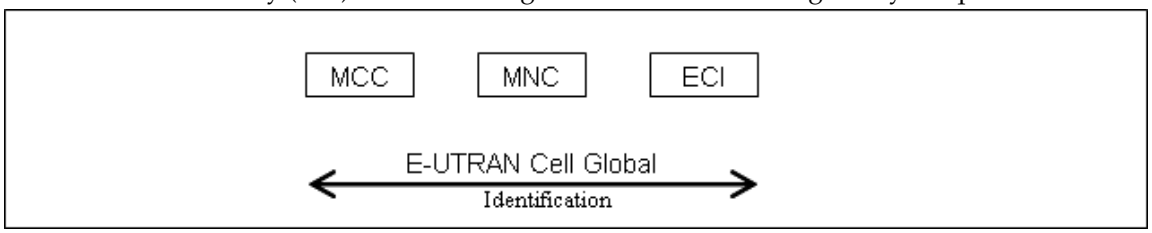
- **LAIFixedLength** - it contains Location Area Identification (total of 5 bytes)
- **CellGlobalIdOrServiceAreaIdFixedLength** - it is concatenation of the Location Area Identification and the Cell Identity (total of 7-bytes). Cell Identity shall be unique within a location area.



For example Cell-id 001-02-3-4 consists of:

- a LAI (001-02-3), which consists of:
  - a PLMN (001-02), which consists of:
    - MCC (001)
    - MNC (02)
- and a LAC (03),
- and a CI (4)

- **E-UTRAN-CGI** - it is composed of the concatenation of the PLMN Identifier (PLMN-Id) and the E-UTRAN Cell Identity (ECI) as shown in figure below and shall be globally unique:



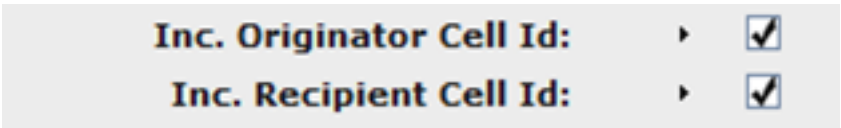
18.13.1 Enabling MAP-ATI

To enable MAP-ATI requests for originator, the parameter *rtrenablemapatifororig* has to be set to `true`. The default value of this parameter is `false`.

To enable MAP-ATI requests for recipient, the parameter *rtrenablemapatiforrecip* has to be set to `always`. The default value of this parameter is `never`. Other supported value is `ownNetwork`; if configured, ATI is sent only for own network (i.e. subscriber MCC/MNC = own mobile country / own network).

Note: MAP-ATI is always performed on MAP version 3, even if SRISM was on MAP version 2 or 3.

To include the Cell-ID information in Submitted and/or Delivered CDR (Supported only for FCDR), the respective fields in the billing profile are required to be enabled.



This functionality requires the **MAP ATI Supported** license. If the license is disabled, the following are non-configurable:

- Semi-static parameters:
  - *rtrenablemapatifororig*
  - *rtrenablemapatiforrecip*
- Billing Profile fields are not visible:
  - Inc. Originator Cell Id
  - Inc. Recipient Cell Id

Note: Even if *rtrenablemapatifororig* is configured as `false`, MAP ATI can still be performed if SRISM for Originator fails with Call Barred or Teleservices not provisioned and the corresponding options `firewallmoactionforspoofingcheckfailureduetocallbarred`, `firewallmoactionforspoofingcheckfailureduetotsvcnotprov` are set to `checkWithMapAti`.

18.13.2 Configuring MAP-ATI Request Parameters

The MAP-ATI requests from RTR are configured using the following parameters:

- *rtrrequestinfobitsformapatifororig* - To configure Requested Information in originator's MAP-ATI request.
- *rtrrequestinfobitsformapatiforrecip* - To configure Requested Information in recipient's MAP-ATI request.
- *rtrmapatitranslationtype* - This parameter is used to configure the value for Translation Type in SCCP CdPA of Outgoing MAP- ATI request towards HLR.

The first two parameters specify a bitstring with values to be requested in the MAP ATI Request (either for Originator or for Recipient) and ATI RequestedInfo is prepared based on the value of these parameters.

Note:

1. RTR will prepare ATI request as per the bits selected by Operator. RTR should ensure that in no way it creates ATI request which is not as per Specification. Hence, RTR would still send MAP-ATI request if any unassigned bit is set.
2. The left-most bit in value represents Bit 0 in the parameter description.

The following table details the bitwise representation:

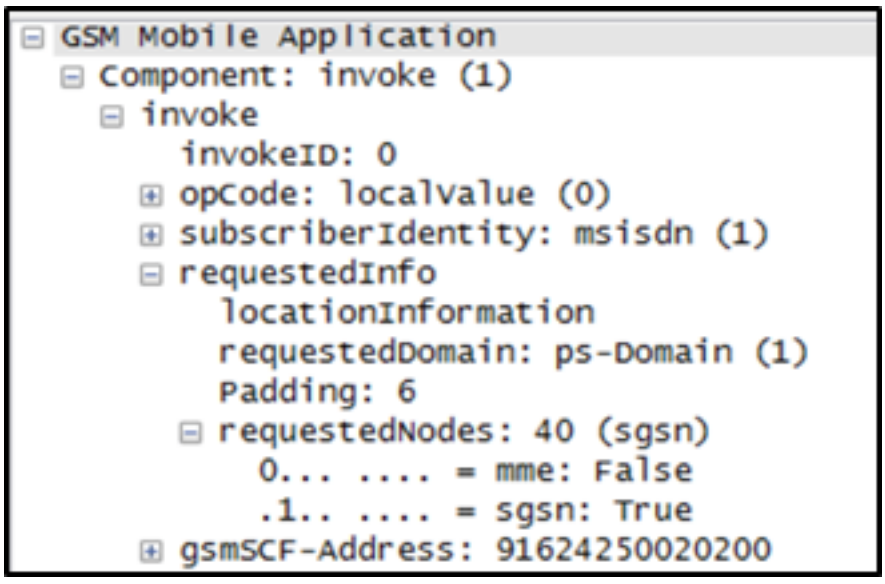
Bit Position	Bit OFF (0)	Bit ON (1)
0	do not request locationInformation	request locationInformation
1	do not request SubscriberState	request SubscriberState
2	reserved for extension container	reserved for extension container
3	do not request currentLocation	request currentLocation
4	do not request requestedDomain	request requestedDomain
5	do not request ms-classmark	request ms-classmark
6	do not request imei	request imei

Bit Position	Bit OFF (0)	Bit ON (1)
7	do not request mnpRequestedInfo	request mnpRequestedInfo
8	do not request tadsData	request tadsData
9	do not request requestedNodes	request requestedNodes
10	do not request servingNodeIndication	request servingNodeIndication
11	do not request locationInformationEPS-Supported	request locationInformationEPS-Supported
12	do not request localTimeZoneRequest	request localTimeZoneRequest
29	sgsn (when requestedNodes bit is ON)	mme (when requestedNodes bit is ON)
30	csDomain (when RequestedDomain bit is ON)	ps-Domain when requestedDomain bit

The default value is '1', which means location information only.

Examples

1. To get only location information only for originator:
   ```
   rtrrequestinfobitsformapatifororig="1"
   ```
2. To get location information and imei for recipient:
   ```
   rtrrequestinfobitsformapatiforrecip="1000001"
   ```
3. To get requested node as sgsn and location information for originator with requestedDomain as 'ps-Domain', the bits 1, 4, 9 and 30 should be ON:
   ```
   rtrrequestinfobitsformapatifororig="10001000010000000000000000000001"
   ```



18.13.2.1 Preparing MAP ATI Request

If configured for originator or recipient, the RTR will create MAP ATI for Originator or Recipient respectively.

- MAP ATI will be created as per ASN.1 structure in 3GPP TS 29.002 V15.3.0, "Mobile Application Part (MAP) specification"
- SCCP CdPA will be Originator/Recipient MSISDN
- RequestedInfo will be prepared as per *rtrrequestinfobitsformapatifororig* for Originator or *rtrrequestinfobitsformapatiforrecip* for Recipient.

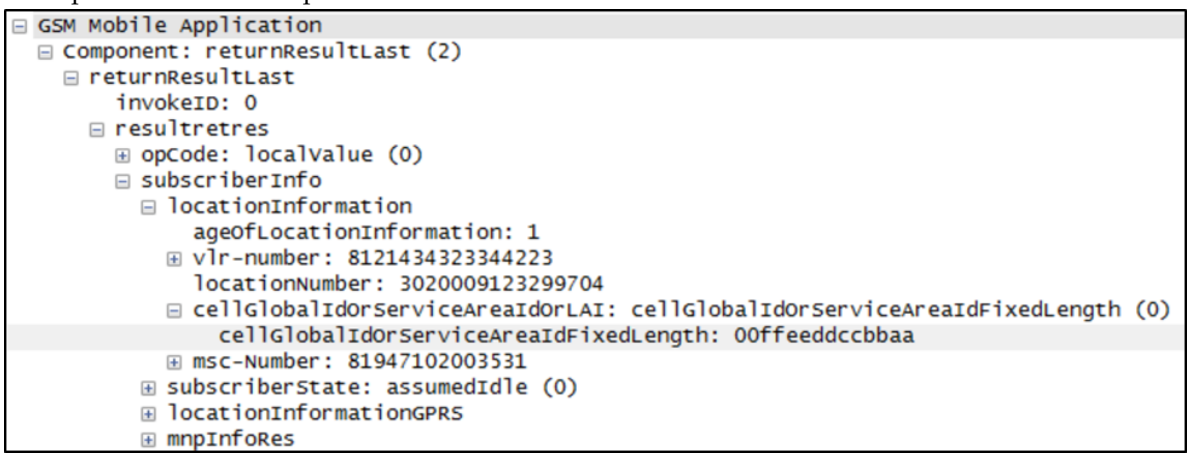
Field	Value
subscriberIdentity	Originator/Recipient Msisdn in international format
RequestedInfo locationInformation [0] NULL OPTIONAL, subscriberState [1] NULL OPTIONAL, currentLocation [3] NULL OPTIONAL, requestedDomain [4] DomainType OPTIONAL, imei [6] NULL OPTIONAL, ms-classmark [5] NULL OPTIONAL, mnpRequestedInfo [7] NULL OPTIONAL, locationInformationEPS-Supported [11] NULL OPTIONAL, t-adsData [8] NULL OPTIONAL, requestedNodes [9] RequestedNodes OPTIONAL, servingNodeIndication [10] NULL OPTIONAL, localTimeZoneRequest [12] NULL OPTIONAL	As per configured in *rtrrequestinfobitsformapatifororig* / *rtrrequestinfobitsformapatiforrecip*
gsmSCF-Address	RTR Virtual GT Address
SCCP CdPA	HLR Address. This will be Originator/Recipient MSISDN SCCP CdPA TT will be as configured in parameter *rtrmapatitranslationtype*
MAP version	Always 3

18.13.3 MAP-ATI Response Handling

The RequetedInfo in MAP-ATI request will be received in the response as the contents of either of the following fields:

- CellGlobalIdOrServiceAreaIdFixedLength
- LAIFixedLength
- E-UTRAN-CGI

Example of MAP-ATI response with **locationInformation**:



Additionally, the RTR maintains the MAP ATI counters. The following counters are maintained:

- Total MAP ATI sent
- Responses received, with separate counters for success, and for the following errors:
  - systemFailure
  - ati-NotAllowed
  - dataMissing
  - unexpectedDataValue
  - unknownSubscriber
  - Timeout
  - TCAP Abort
  - SCCP UDTS

18.13.4 Call Flow Scenarios With MAP ATI

18.13.4.1 MO-MT (ST) Flow

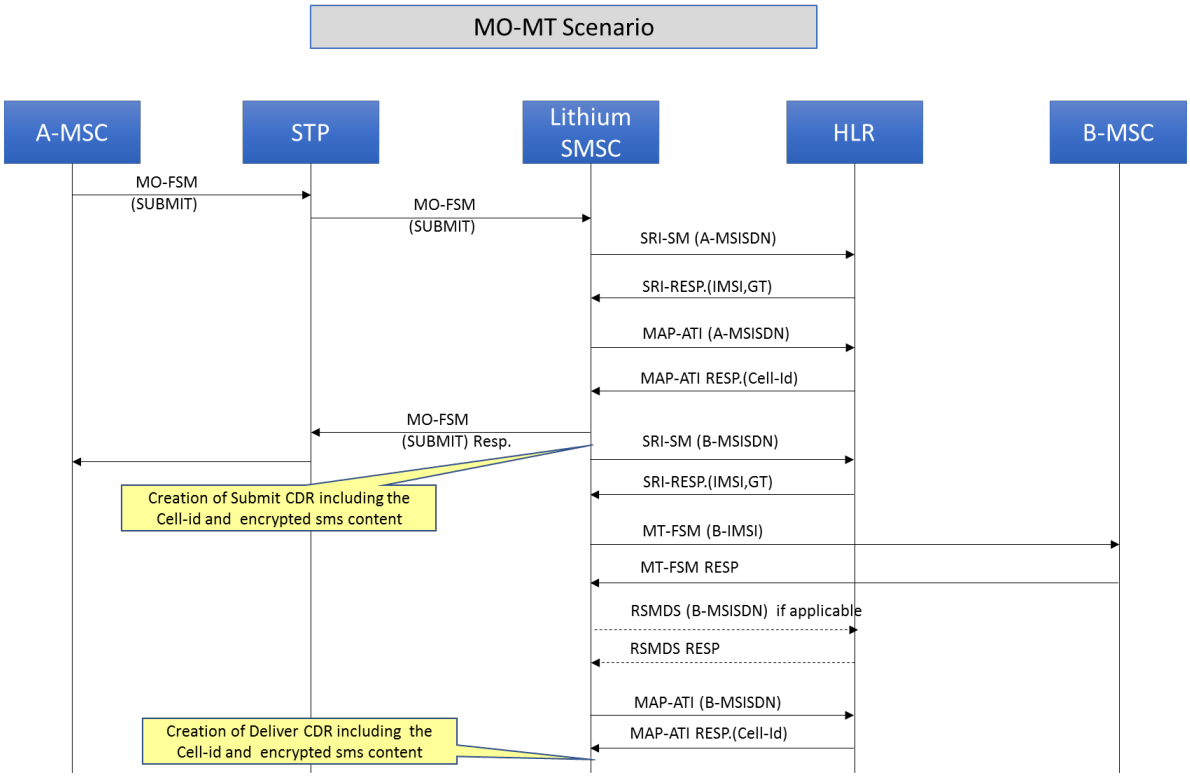


Figure 81: Flow Diagram for MO-MT (ST) scenario

If *rtrenablemapatifororig* is configured as true, the RTR sends MAP ATI after SRI-SM query for originator (if enabled) and before the evaluation of Routing Rules.

If *rtrenablemapatiforrecip* is configured as `always/ownNetwork`, the RTR sends MAP-ATI after MT-FSM success.

18.13.4.2 AO-MT (ST) Flow

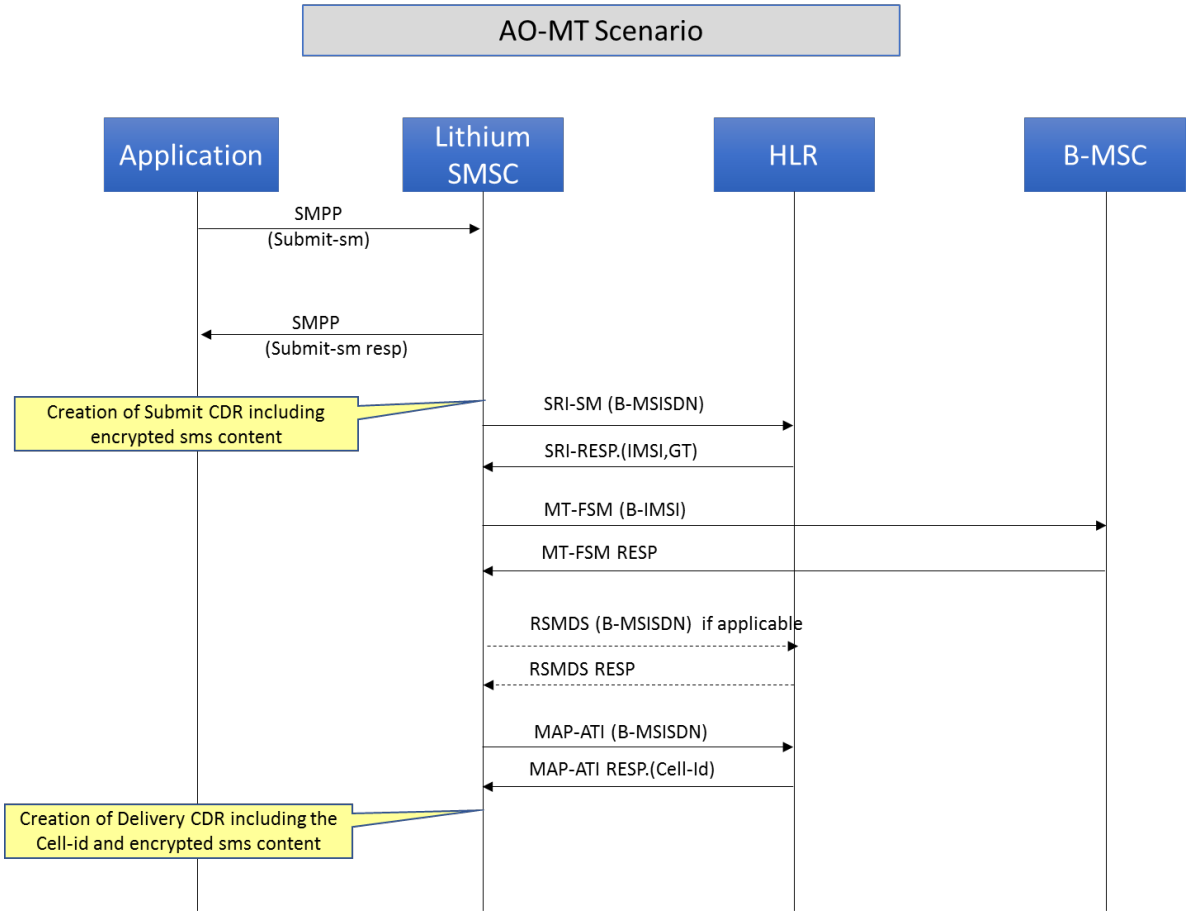


Figure 82: Flow Diagram for AO-MT Scenario

If *rtrenablemapatiforrecip* is configured as `always`/`ownNetwork`, the RTR sends MAP ATI after MT-FSM success.

18.13.4.3 MO-AT (ST) Flow

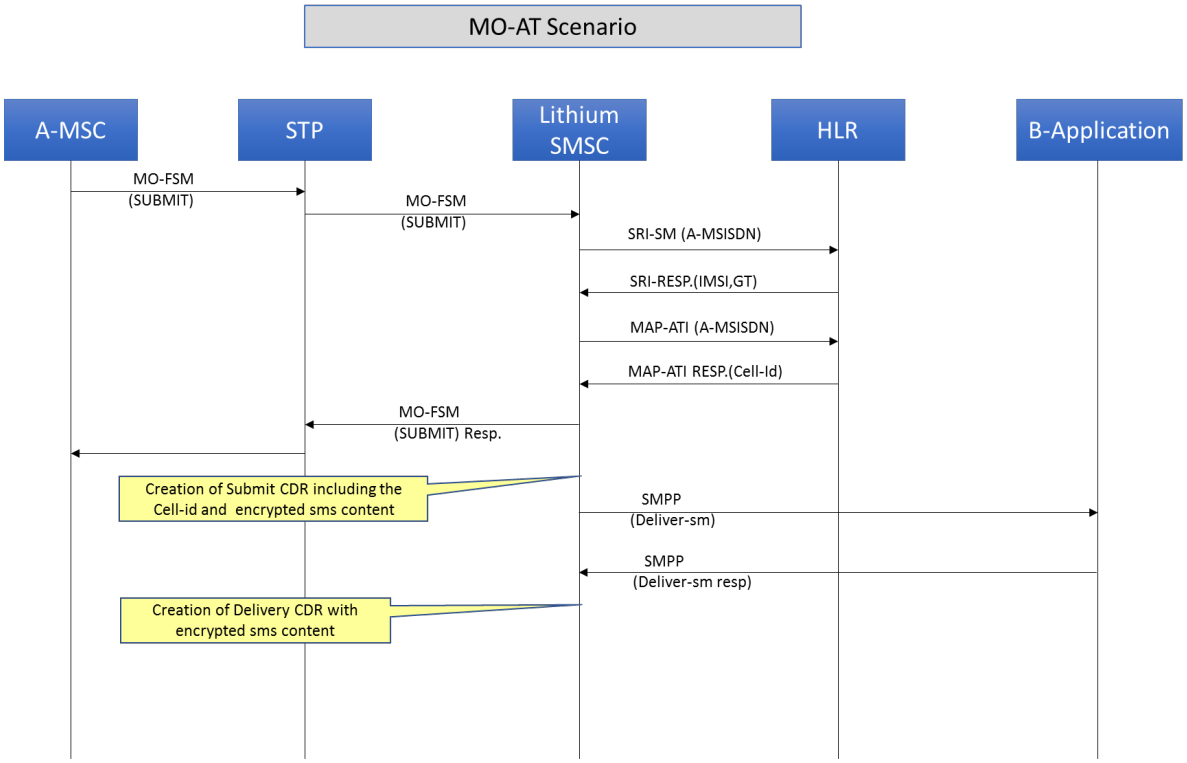


Figure 83: Flow Diagram for MO-AT Scenario

If *rtrenablemapatifororig* is configured as true, the RTR sends MAP ATI after SRI-SM query (if MO spoofing is enabled) and before the evaluation of Routing Rules.

18.13.4.4 MT-MT Home Routing Flow

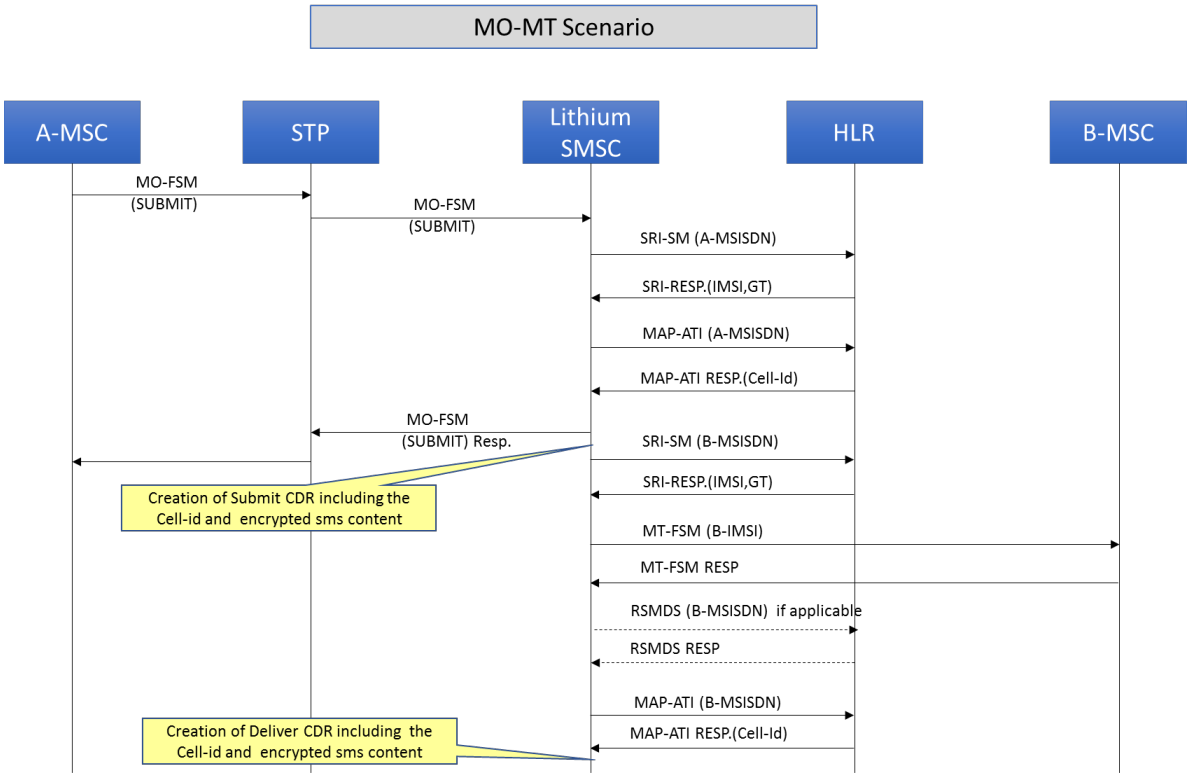


Figure 84: Flow Diagram for MT-MT scenario

If *rtrenablemapatiforrecip* is configured as `always`/`ownNetwork`, the RTR sends MAP-ATI after MT-FSM success.

Chapter 19

Configuration

Topics:

19.1 Introduction

The RTR has a distributed architecture and central configuration management. The RTR configuration has two parts:

- Semi-static configuration that defines fundamental RTR parameters such as SS7 addressing, TCP/IP addressing, and billing properties.
- Dynamic configuration that defines SMS routing parameters such as SMSCs, applications, routing rules, billing profiles, and logging profiles.

Both configuration types are XML-based and are described in this chapter.

19.2 Semi-Static Configuration

The semi-static configuration files are called semi-static because, in general, the parameters do not change frequently. Changing the parameters often affects other network elements or the network connectivity of the RTR. The semi-static configuration files are configured directly in XML.

The RTR semi-static configuration files contain:

- SS7 timers
- SS7 addresses of the RTR (at MTP level and SCCP level)
- SS7 entities such as MTP destinations, routes, linksets, and links
- GTT rules
- Specific parameters for MO routing
- Specific parameters for the Firewall (FWL)
- Specific parameters for CDR generation
- Specific parameters for logging

Note: SS7 connectivity items, mainly MTP related configuration (trunk, link , linkset), are obsolete.

The semi-static configuration consists of two files:

- Host-specific configuration file: Contains parameters for a specific RTR and is located at `/usr/TextPass/etc/<hostname>_config.txt`, where `<hostname>` is the host name of the RTR
- Common configuration file: Contains parameters that are common to all RTRs and is located at `/usr/TextPass/etc/common_config.txt`

Configuration parameters can be placed in either file. In case of a conflict in the settings of a parameter, the host-specific configuration file always takes precedence over the common configuration file.

19.2.1 Configuration Entities

This diagram depicts the entities in the semi-static configuration file.

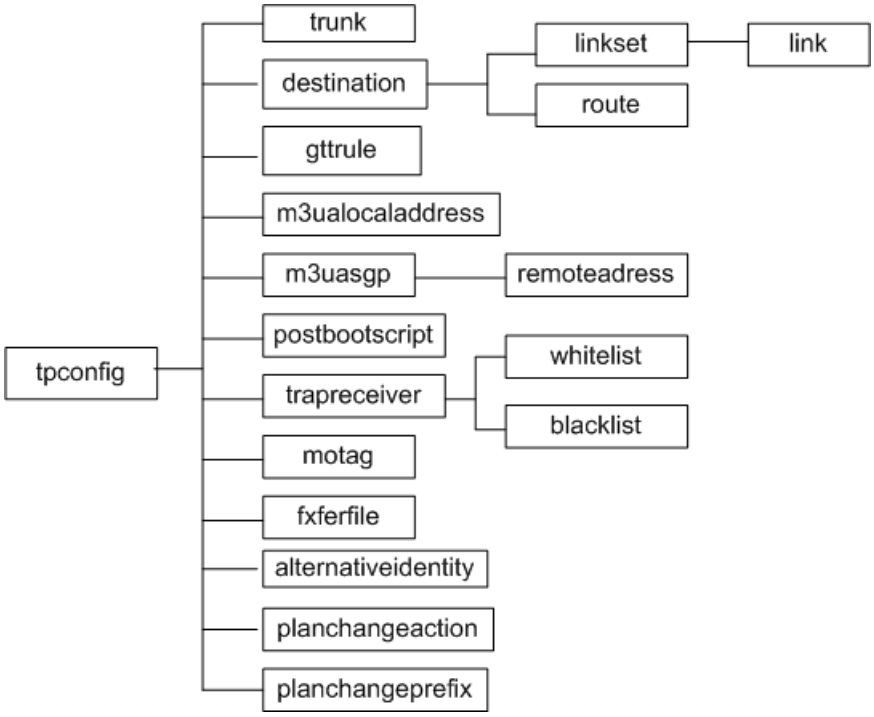


Figure 85: Semi-static configuration file entities

This table describes the entities:

Entity	Instances	Description
tpconfig	1	Top entity of the configuration file. Its attributes specify: • Specific parameters for CDR generation • SS7 timers • SS7 addresses of the RTR (at MTP level and SCCP level) • Specific parameters for MO routing
trunk	0-4	Entity containing configuration details for an E1 trunk.
destination	0-500	Entity containing configuration details for an MTP destination and, optionally, an SCCP STP.
linkset	0-1 (per destination)	Entity containing configuration details for an MTP linkset. A destination entity only has a subordinate linkset entity when the destination is an adjacent.
link	1-16 (per linkset)	Entity containing configuration details for an MTP link.
route	1-32	Entity containing configuration details for an MTP route.
gttrule	0-10000	Entity containing configuration details for an SCCP GTT rule.

Entity	Instances	Description
m3ualocaladdress	0-16	Entity that contains the local IP addresses for M3UA.
m3uasgp	1-256	Entity that contains the configuration details for the remote SGPs.
remoteaddress	1-16	Entity that contains the remote IP addresses for M3UA.
postbootscript	0-8	Entity that contains a UNIX command that will be executed after the RTR has been configured.
trapreceiver	0-8	Entity containing configuration details for a trap receiver.
whitelist	0-50	Entity containing configuration details for a trap whitelist filter.
blacklist	0-50	Entity containing configuration details for a trap blacklist filter.
motag	0-100	Entity containing configuration details for the tags that are scanned within MO messages.
fxferfile	1	Entity containing configuration details for the distribution of the configuration files.
alternativeidentity	1	Entity containing alternative GTs that the RTR will accept in the SCCP CDPA.
planchangeprefix	0-10000	An MSISDN prefix for which a plan change action should be executed.
planchangeaction	0-100	A recipe for changing a MSISDN by a number plan change.

Note: It is not allowed to configure the 'trunk', 'link' and 'linkset' entities if the RTR is licensed for the Japanese SS7 flavour, because in this flavour the RTR supports only SIGTRAN (M3UA) interface with the SS7 network.

19.2.2 tpconfig Entity

This section describes the `tpconfig` attributes.

19.2.2.1 absentsubscribererrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.2 acceptanymodanpiformt

Mandatory/Optional

Optional

Location

Host/Common configuration file

Description

This parameter indicates whether MO messages with recipient numbering plan values other than `isdnTelephony` (1) will be accepted for possible delivery to mobile networks in the following message paths: MO-MT, MO-MT-AT, MO-MT-AO, MO-MT-ST, or MO-ST-MT.

Note: The default recipient address normalization will not be performed in case of a recipient numbering plan value other than `isdnTelephony`. It is recommended to deal with such cases using the *GSM Address Conversion Rules* and/or *Outgoing Address Conversion* features.

Valid Values

- true
- false

Default Value

false

19.2.2.3 actionforatstatusreports

Mandatory/Optional

Optional

Location

Common configuration file

Description

Controls the routing of status reports that terminate in applications.

Valid Values

- route: Delivery of status report to destination
- store: Store in AMS for delivery to destination
- routefallbacktostorage: Single shot delivery of status report to destination. On delivery failure, store status report in AMS

Default

routefallbacktostorage

19.2.2.4 actionforexternalconditionfailuremessages

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action pertaining to the routing of messages that terminate in mobiles and that are sent as result of an external condition that did not satisfy.

Valid Values

- route: Delivery of the messages to destination.
- store: Store in AMS for delivery to destination.
- routefallbacktostorage: Single shot delivery of the messages to destination. On delivery failure, store messages in AMS.

Default

routefallbacktostorage

19.2.2.5 actionformnpcheckfailureduetocallbarred

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to execute when MNP check fails due to earlier "call barred" error.

Valid Values

- pass
- treatasifmnpviolation

Default

treatasifmnpviolation

19.2.2.6 actionformnpcheckfailureduetotsvcnotprov

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to execute when MNP check fails due to earlier "teleservice not provisioned" error.

Valid Values

- pass
- treatasifmnpviolation

Default

treatasifmnpviolation

19.2.2.7 actionformtstatusreports

Mandatory/Optional

Optional

Location

Common configuration file

Description

Controls the routing of status reports that terminate in mobiles.

Valid Values

- route: Delivery of status report to destination.
- store: Store in AMS for delivery to destination.
- routefallbacktostorage: Single shot delivery of status report to destination. On delivery failure, store status report in AMS.

Default

routefallbacktostorage

19.2.2.8 actionforsmcopiestoapplication

Mandatory/Optional

Optional

Location

Common configuration file

Description

Routing action for copies that are sent to an application as AT.

Valid Values

- route: Delivery of copied SM to destination.
- store: Store in AMS for delivery to destination.
- routefallbacktostorage: Single shot delivery of copied SM to destination. On delivery failure, store copied SM in AMS.

Default

routefallbacktostorage

19.2.2.9 actionforsmcopiestomobile

Mandatory/Optional

Optional

Location

Common configuration file

Description

Routing action for copies that are sent to a mobile as MT.

Valid Values

- route: Delivery of copied SM to destination.
- store: Store in AMS for delivery to destination.
- routefallbacktostorage: Single shot delivery of copied SM to destination. On delivery failure, store copied SM in AMS.

Default

routefallbacktostorage

19.2.2.10 adjustprepaidindicatorondeductfailure

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the prepaid-indicator of the Comverse delivery CDR and prepaidBillingState of the CMG delivery CDR should be adjusted from "online-billed" to "hot-billed" if the Diameter deduct operation fails (that is, if the result code is outside the range 2001-2999).

Valid Values

- true
- false

Default

false

19.2.2.11 adjustvalidityperiodinccdr

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicates whether the unit and length of the validity_period field in Comverse CDR records need to be adjusted.

If set to 'true', the validity_period value is represented in minutes with a maximum length of 6 digits. In case the validity_period value in minutes exceeds 6 digits, the CCDR records are populated with '999999'. By default, this property is set to 'false' and the validity_period value is represented in seconds.

Valid Values

- true
- false

Default

false

19.2.2.12 alertreasonindicationfieldinrfsm

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Specifies the choice of the alert reason indication field to be included in the 'Ready For SM' message, which is sent by RTR to the HLR. This parameter is taken into account only when the 'Ready For SM' message is sent over MAP Phase 2+. In case MAP Phase 2 is being used for sending the 'Ready For SM' message, then the RTR ignores this parameter and includes the 'Alert Reason Indicator' field.

Valid Values

- alertReasonIndicator
- additionalAlertReasonIndicator

Default

additionalAlertReasonIndicator

19.2.2.13 aliasforhlrssn

Mandatory/Optional

Optional

Location

Common configuration file

Description

Alias for the HLR Subsystem Number (SSN). The HLR subsystem within the RTR can be addressed through SSN 6 and through this alias.

Valid Values

0 - 255

Default

221

19.2.2.14 aliasformscssn

Mandatory/Optional

Optional

Location

Common configuration file

Description

Alias for MSC Subsystem Number (SSN). The MSC subsystem within the RTR can be addressed through SSN 8 and through this alias.

Valid Values

0 - 255

Default

221

19.2.2.15 aliasforsgsnssn

Mandatory/Optional

Optional

Location

Common configuration file

Description

Alias for SGSN Subsystem Number (SSN). The SGSN subsystem within the RTR can be addressed through SSN 149 and through this alias.

Valid Values

0 - 255

Default

222

19.2.2.16 aliasfortt

Mandatory/Optional

Optional

Location

Common configuration file

Description

Alias for translation type (TT) used in the global title (GT) to address this specific RTR device.

Valid Values

0 - 255

19.2.2.17 allowmofromfriendlysubscribersonly

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the RTR should only allow MO traffic from "friendly" subscribers (own and associated networks) and should reject MO traffic from other operators' subscribers.

Valid Values

- false: All MO messages are accepted, irrespective of the `numberportabilityenabled` and `nationalroamingenabled` settings.
- true: MO messages with an originator MSISDN of a different country are rejected independently of the `numberportabilityenabled` and `nationalroamingenabled` settings.

Default

false

19.2.2.18 alphanumericaddressinorigaddressgsmfieldinfcdr

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether or not an alphanumeric address should be stored in the origAddressGsm field in case of an AO message with an alphanumeric address.

Valid Values

- true (alphanumeric address is placed in origAddressGsm)
- false (short number of the relating application is used for origAddressGsm)

Default

true

19.2.2.19 alternativescselectionforaosmwithdnenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying whether RTR should use an alternative service center selection scheme for an AO/SM with a request for an notification that needs to be delivered on a dialout session.

Valid Values

- true
- false

Default

false

19.2.2.20 alwaysacceptunrecognisedmotag

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies how to handle messages containing unrecognised MO tags in advanced MO tag mode.

Valid Values

- true (messages are always accepted)
- false (messages can only match an MOR rule that relays the message to the SMSC)

Default

false

19.2.2.21 alwaysretrieveoriginatorimsi

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the RTR should always retrieve the originator IMSI before it evaluates the MOR rules.

Valid Values

- true (RTR will retrieve the IMSI before evaluating MOR rules)
- false

Default

false

19.2.2.22 amsmaxresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum time span (in seconds) that the RTR waits for a response from the AMS before it considers the relating message to be timed out. Valid values: 1-3600 (default 5).

19.2.2.23 amsmediatedservicecentretimestampsenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

The RTR internal SM timestamp generation can produce non-unique timestamps when multiple RTRs are in use, as the RTRs do not co-ordinate timestamp generation. The AMS can be used to mediate timestamp generation, resulting in unique timestamps for all RTRs sharing that AMS.

`amsmediatedservicecentretimestampsenabled` is global parameter that enables (id set to `true`) this functionality. The default value is `false.`

Note: Timestamps are accurate to one second and must be unique per originator-recipient pair. Timestamps are incremented into the future when multiple SMs occur in the same second.

Additional Information

`amsmediatedservicecentretimestampsenabled` enables a Service Center Timestamp (SCTS) Query towards the AMS, and whenever the AMS advertises the support for the SCTS Query capability, the RTR will issue such a SCTS query as one of the first actions during its message processing.

If enabled, SCTS Queries will be done for all incoming MO and AO messages.

19.2.2.24 applicationfailureerrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.25 applymtmodifierontpoaforhomeroutedmsg

Mandatory/Optional

Optional

Location

Host/Common configuration file

Description

Indicates whether the MTO modifiers will be used to modify the TP-OA of outgoing MTFSM in home routing scenario. Note that this parameter is not applicable in the case where the SRIQ routing rule action is set to '`Accept and Respond to SMSC immediately`'.

Valid Values

- true
- false

Default Value

false

19.2.2.26 applymtmodifierontpoaforinterceptedmsg

Mandatory/Optional

Optional

Location

Host/Common configuration file

Description

Indicates whether the MTO modifiers will be used to modify the TP-OA of outgoing MTFSM in the intercepted MT scenario. The default value is false, which indicates that the TP-OA in the outgoing MTFSM will not be modified using MTO modifiers in the intercepted MT scenario.

Valid Values

- true
- false

Default Value

false

19.2.2.27 applyoutgoingaconmtdeliverwithorigsn

Mandatory/Optional

Optional

Location

Host/Common configuration file

Description

This parameter indicates whether the outgoing address conversion rule set configured in the MTO rules will be applied on outgoing MT SMS-Deliver messages with originator short number or not. The default value is false, i.e. the outgoing rule set will not be applied on MT SMS-Deliver messages with originator short number.

Valid Values

- true
- false

Default Value

false

19.2.2.28 applyoutgoingrulesetonmtstatusreport

Mandatory/Optional

Optional

Location

Host/Common configuration file

Description

This parameter indicates whether outgoing Rule Set configured in the MTO rules needs to be applied on the outgoing MT Status Report or not. The default value is false, i.e. the outgoing rule set will not be applied on the MT status Report.

Valid Values

- true
- false

Default Value

false

19.2.2.29 atmscformat

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying how the MSC should be specified in an AT-AT or AT Notification. Note that this attribute might be overruled by the application-specific attribute **Format MSC** on the MGR.

Valid Values

- transparent (taken from the corresponding inbound message without modification)
- national
- international

Default

transparent

19.2.2.30 atnotificationvalidityperiod

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Indicates the message Validity Period in seconds, for AT notification messages generated by the RTR.

Valid Values

0 - 360000

Default

0

19.2.2.31 atoriginatorformat

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies how the originator should be specified in an AT-AT or AT Notification message. Note that this attribute might be overruled by the application-specific attribute **Format Originator** on the MGR.

Valid Values

- transparent (taken from the corresponding inbound message without modification)
- national
- international

Default

transparent

19.2.2.32 atrecipientformat

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies how the recipient should be specified in an AT-AT or AT Notification message. Note that this attribute might be overruled by the application-specific attribute **Format Recipient** on the MGR.

Valid Values

- transparent (taken from the corresponding inbound message without modification)
- national
- international

Default

transparent

19.2.2.33 atsmscformat

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying how the SMSC should be specified in an AT-AT or AT Notification. Note that this attribute might be overruled by the application-specific attribute **Format SMSC** on the MGR.

Valid Values

- transparent (taken from the corresponding inbound message without modification)
- national
- international

Default

transparent

19.2.2.34 billingforatatpath

Mandatory/Optional

Optional

Location

Common configuration file

Description

This parameter indicates whether SCDRs should be generated for AT-AT and AT-AT-Store path on successful delivery or not. The default value is false, which means that SCDRs will not be generated. The `billingforatatpath` semi-static value configuration is dependent upon the activation of SS8 SCDRs licence. If the SS8 SCDRs licence is not activated, then `billingforatatpath` semi-static cannot be configured and will contain the default value as false.

Valid Values

- true (generate CDRs)
- false (do not generate CDRs)

Default

false

19.2.2.35 billingforautoreplymessages

Mandatory/Optional

Optional

Location

Common configuration file

Description

Controls whether CDRs are generated for auto reply (ARP) messages. The billing profile for the ARP messages is assigned by the IGMR rules.

Valid Values

- true (generate CDRs)
- false (do not generate CDRs)

Default

false

19.2.2.36 billingforcopiedmessages

Mandatory/Optional

Optional

Location

Common configuration file

Description

Controls whether CDRs are generated for copied messages. The billing profile for the copied messages is assigned by the MTOR rules.

Valid Values

- true (generate CDRs)
- false (do not generate CDRs)

Default

false

19.2.2.37 billingforforwardedmessages

Mandatory/Optional

Optional

Location

Common configuration file

Description

Controls whether CDRs are generated for copied messages. The billing profile for the forwarded messages is assigned by the MTOR rules.

Valid Values

- true (generate CDRs)
- false (do not generate CDRs)

Default

false

19.2.2.38 billingid

Mandatory/Optional

Optional

Location

Host-specific configuration file

Description

Specifies the billing ID, which will replace the %i variable in the billing file name template (configured in the MGR); allows you to set a billing ID per RTR device.

19.2.2.39 billingprofileforexpiredicacherecords

Mandatory/Optional

Optional

Location

Common configuration file

Description

Identifier specifying which active billing profile should be used for final delivery CDRs, generated upon expiry of a record in the Icache. When this attribute is set to the name of an active billing profile, that profile is used to generate the CDR. Otherwise, the RTR evaluates the MO or AO rules (depending on the origin of the SM corresponding to the expired record) in order to determine the billing profile.

Note: This attribute should typically not be used.

Valid Values

A valid billing profile name string

Default

Empty string

19.2.2.40 blockederrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.41 blockifscfnotreachableforcameltrigger

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying whether the RTR should consider a CAMEL trigger as failed when a communications error with SCF occurs. This indicator is only used when ECI application (e.g. PBC) does not specify a Default SMS Handling indicator. When this parameter is not configured, its value defaults to 'false'.

Valid Values

- true
- false

Default

false

19.2.2.42 callbarrederrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.43 cameleventreportsmswithprearrangedend

Mandatory/Optional

Optional

Location

Common configuration file

Description

Option to specify whether TextPass should send the CAMEL EventReportSMS in a TCAP CONTINUE message and assume a pre-arranged END when no FurnishChargingInformation operation is expected in response. The corresponding SNMP attribute in textpass-sms-mib.my is smsPropCamelEventReportSmsWithPrearrangedEnd.

Valid Values

- true
- false

Default

true

19.2.2.44 capphaseforcameltrigger

Mandatory/Optional

Optional

Location

Common configuration file

Description

Default for CAP phase that the RTR is to use for CAMEL trigger. This CAP phase is only used when an ECI application (e.g. PBC) does not specify a Charging Protocol. When this parameter is not configured, its value defaults to 'cap3'.

Valid Values

- cap1
- cap2
- cap3

Default

cap3

19.2.2.45 carrierspecificprefix

Mandatory/Optional

Optional

Location

Common configuration file

Description

Unique Carrier Specific Prefix assigned to the operator in whose network the RTR is deployed.

It is represented as a string of 1 - 4 decimal digits only.

Valid Values

1-9999

Default

Blank string (" ")

19.2.2.46 cdpattforjapanesemnp

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the CdPA Translation Type (TT) value that the RTR will use while initiating a second SRI-SM Request or forwarding a received SRI-SM Request towards another Japanese operator's network. Note that this parameter is applicable only if the `enablejapanesemnp` parameter is set to "true".

Valid Values

0-255

Default

223 (0xDF)

19.2.2.47 commonaddress

Mandatory/Optional

Optional

Location

Common configuration file

Description

E164 address that the RTR should use for the SMSC parameter in MAP operations pertaining to delivery of an MT message. Defaults to the RTR's E164 GT address.

19.2.2.48 considernationalnonhplmntrafficasforeign

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies how to interpret the term "foreign". When foreign is applied in the context of networks, the RTR uses the number ranges defined for the home network(s) to determine whether an address is foreign or local.

Valid Values

- true (any PLMN other than the HPLMN is considered foreign)
- false (foreign refers to the country, and therefore excludes any national PLMN)

Default

false

19.2.2.49 continueonwrongencryptconfig

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Defines what do in case the configuration of the User Data Encryption feature is incorrect. A reason could be a missing key-file or incorrect protection. If this parameter is set to 'true' the entity will continue to start and empty user data will be stored in FCDR, transactional logs (if encrypt user data is enabled) and in event logs which otherwise should have been encrypted. If set to 'false', it is impossible to activate the process. The check itself is only executed if the `licGenEncryptUserData` is enabled.

Valid Values

- true
- false

Default Value

false

19.2.2.50 copiestoapplicationamsqueue

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the AMS queue in which to store copies that are sent to application as AT messages. Set to a number that refers to the queue entity's index in the MGR. Valid values are 0 - 1000. Default is 1.

19.2.2.51 copiestomobileamsqueue

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the AMS queue in which to store copies that are sent to mobile as MT messages. Set to a number that refers to the queue entity's index in the MGR. Valid values are 0 - 1000. Default is 1.

19.2.2.52 copytoapplicationbinarydatasupportenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying whether the Copy to Application (CTA) service will operate upon binary data short messages.

Valid Values

- true
- false

Default

false

19.2.2.53 countrycode

Mandatory/Optional

Mandatory

Location

Common configuration file

Description

Code of the country in which the RTR operates. For example:

- 31: Netherlands
- 32: Belgium
- 33: France
- 44: United Kingdom
- 49: Germany

19.2.2.54 datamissingerrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.55 dateformatofmtreturnmessage

Mandatory/Optional

Optional

Location

Common configuration file

Description

String specifying the format of the Date and Time that are part of the USER DATA of the MT Return Message. The date is the timestamp of the original MO message that was not delivered, causing an internally generated MT Return Message to the originator.

Valid Values

- %y: Year in two digits (04)
- %m: Month in two digits (01 for January, 10 for October)
- %d: Day in two digits (01 for first day of the month)
- %H: Hour in two digits (00 for midnight, 12 for noon)
- %M: Minute in two digits
- %S: Second in two digits
- %-y: Year in two digits (12) or one digit (1) without the leading zero
- %-m: Month in two digits (10 for October) or one digit (1 for January) without the leading zero
- %-d: Day in two digits (10 for tenth day of the month) or one digit (1 for first day of the month) without the leading zero

- %-H: Hour in two digits (12 for noon) or one digit (0 for midnight) without the leading zero
- %-M: Minute in two digits or one digit without the leading zero
- %-S: Second in two digits or one digit without the leading zero

Default

%d.%m.%y %H:%M:%S

19.2.2.56 defaultactionwhennotfoundinmnptable

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the default action to be taken by the RTR for a received MO or AO short message or an incoming SRI-SM Request, in case the IMSI of the recipient subscriber (or the combination of the IMSI and the CdPA prefix received in the SRI-SM) is not found in the MNP table. Note that this parameter is applicable only if the `enablejapanesemnp` parameter is set to "true".

Valid values are `accept`, `forward` and `discard`. If the parameter is set to `forward`, then the RTR will treat it as being equivalent to `accept` and will perform exactly the same processing that it does for `accept`.

Valid Values

- `accept` (0)
- `forward` (1)
- `discard` (2)

Default

`accept` (0)

19.2.2.57 defaultapplicationforatattomsisdn

Mandatory/Optional

Optional

Location

Common configuration file

Description

The application to use if:

- The destination application cannot be derived from the message's B-number, and
- The message's B-number is an MSISDN or alphanumeric

If set to 0, the application associated with the session on which the AT message was received will be the destination application. Default 0.

19.2.2.58 defaultmapphase

Mandatory/Optional

Optional

Location

Common configuration file

Description

The default MAP phase to use if the network is not provisioned in the Mobile Messaging configuration. This is used as the initial MAP phase for dialogues that are initiated toward networks that are not provisioned.

In a FWL configuration in which MT-MT traffic is screened, you may receive MAP phase 2+ SendRoutingInfoForSm or ForwardSm operations that are destined for networks that are not provisioned. You can use this attribute to ensure that instead of always falling back to MAP phase 2, the FWL only falls back to MAP phase 2 if the destination network does not support MAP phase 2+.

Valid Values

- phase1
- phase2
- phase2plus

Default

phase2

19.2.2.59 defaultoperatorabbreviation

Mandatory/Optional

Optional

Location

Common configuration file

Description
Specifies the default abbreviated operator network name to be used for "Service type" field while generating the 3G CDR for MO originating traffic when the abbreviated operator name for the matching network is not configured.

Valid Values

Alphanumeric string of up to 15 characters.

Default

"SB"

19.2.2.60 delayforautoreplytomtmessage

Mandatory/Optional

Optional

Location

Common configuration file

Description

The delay in milliseconds between creating and processing (i.e. delivering or storing) an Auto Reply (ARP) message, generated for an inbound MT message. The delay period starts after a potential delay caused by ARP message regulation (see *maxnumarpspersecond*).

A value of 0 means that the RTR introduces no (extra) delay.

Valid Values

0 - 60000

Default

0

19.2.2.61 delivercdrforsuccessfulaoaoforwarding

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether delivery CDRs should be generated after successful AO-AO or AO-MT-AO submission. Valid values:

- true (default)
- false

19.2.2.62 delivercdrforsuccessfulmoaoforwarding

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether delivery CDRs should be generated after successful MO-AO or MO-MT-AO submission.

Valid Values

- true
- false

Default

false

19.2.2.63 dialoutatstatusreportsamsqueue

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the AMS queue in which to store AT status reports that may only be delivered on dialout sessions. Set to a number that refers to the queue entity's index in the MGR. Default 2.

If many AT status reports must be delivered using dialout, it is strongly recommended to configure a specific AMS queue for this type of status report. The AMS is then able to deliver status reports more quickly.

19.2.2.64 disableoptimisedmoroutingforforeigntraffic

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if optimal routing for foreign MO traffic should be disabled.

Valid Values

- true
- false

Default

false

19.2.2.65 discardoutboundatmsgwhenmaxthroughputiszero

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an outbound AT message or AT notification should be discarded with permanent error if Maximum AT Throughput of the destination application is set to zero (0)..

Valid Values

- true
- false

Default

false

19.2.2.66 dttemplateforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the format for the discharge time to place in a phase 1 status report. The discharge time is assigned when a message is submitted to the RTR.

Valid Values

- %y: Year in two digits (04)
- %m: Month in two digits (01 for January, 10 for October)
- %d: Day in two digits (01 for first day of the month)
- %H: Hour in two digits (00 for midnight, 12 for noon)
- %M: Minute in two digits
- %S: Second in two digits
- %-y: Year in two digits (12) or one digit (1) without the leading zero
- %-m: Month in two digits (10 for October) or one digit (1 for January) without the leading zero
- %-d: Day in two digits (10 for tenth day of the month) or one digit (1 for first day of the month) without the leading zero
- %-H: Hour in two digits (12 for noon) or one digit (0 for midnight) without the leading zero
- %-M: Minute in two digits or one digit without leading zero
- %-S: Second in two digits or one digit without the leading zero

Default

%d.%m.%y %H:%M:%S.

19.2.2.67 ecimscformat

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying how the MSC should be specified in an ECI request.

Note that this attribute might be overruled by the ECI application-specific attribute externalConditionFormatMsc.

Valid Values

transparent, national, international

Default

international

19.2.2.68 ecioriginatorformat

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying how the originator should be specified in an ECI request.

Note that this attribute might be overruled by the ECI application-specific attribute externalConditionFormatOriginator.

Valid Values

transparent, national, international

Default

international

19.2.2.69 ecirecipientformat

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying how the recipient should be specified in an ECI request.

Note that this attribute might be overruled by the ECI application-specific attribute externalConditionFormatRecipient.

Valid Values

transparent, national, international

Default

international

19.2.2.70 ecismscformat

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying how the SMSC should be specified in an ECI request.

Note that this attribute might be overruled by the ECI application-specific attribute externalConditionFormatSmsc.

Valid Values

transparent, national, international

Default

international

19.2.2.71 enableadvancedmotagmode

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether advanced MO tag mode is activated. Advanced MO tag mode features:

- Support for multiple SMSC-like scan tags in a single message.
- Support for scan tag functions with arguments.

In simple MO tag mode, any delimiters to indicate the start or end of an MO tag should be part of the MO tag string. In advanced MO tag mode, delimiters should not be part of the MO tag string. The delimiters are:

- Asterisk (*): Starts a sequence of tags and separates two consecutive tags in a sequence.
- Number sign (#): Terminates a sequence of tags.

Valid Values

- true
- false

Default

false

19.2.2.72 enablealertscrelaying

Mandatory/Optional

Optional

Location

Common configuration file

Description

Enables or disables the AlertSC feature:

- When set to true (default), the RTR will relay any AlertSC that it receives to the network. This functionality requires that a GTT rule matches for the SMSC address (as specified on the MAP layer of the AlertSC). The RTR will relay the AlertSC to the address resulting from the GTT rule. If no GTT rule matches, the RTR will terminate the AlertSC.
- When set to false, the RTR will terminate any AlertSC that it receives.

19.2.2.73 enablebasicthroughputlimithitlogging

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying whether a message should be written to syslog whenever a throughput limit of one of the following entities is being hit:

- AO Routing Rule
- Application
- Application Group
- Service Class
- Service Centre
- SC Node
- SC Termination Point

Please note the following:

- A filter is applied to the log requests for generic events like the 'throughput limit hit' events. The filter can be tuned using the following parameters:
  - genPropGenLogEventInterval
  - genPropGenLogEventCount
  - genPropGenLogLevel

  genPropGenLogEventInterval and genPropGenLogEventCount prevent flooding of the log file by multiple occurrences of the same event within a short time frame. The genPropGenLogLevel parameter should be set to 'warning' or 'error'. Any other value will result in the filter blocking the 'throughput limit exceeded' events.
- Besides the basic logging of 'throughput limit hit' events, a more enhanced type of logging is available. The enhanced type of logging reveals the application causing the 'throughput limit hit'

event. It can be enabled on a per application basis by setting applicationLogLevel equal to 'warning' or 'error'.

Valid Values

- true
- false

Default

false

19.2.2.74 enabledialoutnotificationasamsmessagetype

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the RTR generates AMS store requests with message type dialoutNotification.

Valid Values

- true
- false

Default

false

19.2.2.75 enablegprssupportindicator

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Controls the inclusion of the GPRS Support Indicator in SRISM Request messages with MAP phase 2+.

Valid Values

- true

- false

Default

true

19.2.2.76 enablegprssupportindicatorfordomestichlrqueryonly

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Controls the inclusion of the GPRS Support Indicator in SRISM Request messages to Domestic HLR with MAP phase 2+.

If this parameter is set to `true`, the GPRS Support Indicator is added in SRISM query to Domestic HLR only, for SRI-SM query to International HLR GPRS the Support Indicator will not be present. The GPRS indicator in SRISM Query to Domestic HLR is added based on the parameter `gprssupportindicatorforsrismrequest`.

If this parameter is `true`, then, in case of Japanese MNP with the parameter `action` as **Forward**, the second SRI-SM query will not contain the GPRS Support Indicator.

If the value of this parameter is `false`, the inclusion of the GPRS Support Indicator in SRI-SM will be based on the parameter `gprssupportindicatorforsrismrequest`.

Valid Values

- true
- false

Default

false

19.2.2.77 enablehlrupdates

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the RTR should update the HLR flags.

Valid Values

- true
- false

Default

true

19.2.2.78 enablejapanesemnp

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the enhanced functionality pertaining to Japanese MNP support is enabled on the RTR.

Valid Values

- true
- false

Default

false

19.2.2.79 enablemapphaseoptimisation

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the RTR should use MAP phase 1 when possible. The goal of using MAP phase 1 transactions is to reduce the signalling capacity that is required for a MAP operation. By doing this, the number of possible MAP operations on a link per unit of time increases.

Valid Values

- true
- false

Default

true

19.2.2.80 equipmentnotsmequippederrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.81 equipmentprotocolerrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.82 expectcharginginfoforcameltrigger

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying whether the RTR should expect a FurnishChargingInformation operation from the SCF for the CAMEL trigger issued. This indicator is only used ECI application (e.g. PBC) does not specify a Return Tariff Data indicator. When this parameter is not configured, its value defaults to 'false'.

Valid Values

- true
- false

Default

false

19.2.2.83 extattrforsmbeingforwarded

Mandatory/Optional

Optional

Location

Common configuration file

Description

Index of external attribute that will be set for an SM at the point that a delivery attempt to the forwarded address is initiated. Can be set to a value of 0 - 32. Default value is 0, implying that no external attribute will be set.

19.2.2.84 extattrforsmrequestingconditionalforwarding

Mandatory/Optional

Optional

Location

Common configuration file

Description

Index of external attribute that will be set for an SM when a request to conditionally forward the SM has been received. Can be set to a value of 0 - 32. Default value is 0, implying that no external attribute will be set.

19.2.2.85 extattrforsmrequestingunconditionalforwarding

Mandatory/Optional

Optional

Location

Common configuration file

Description

Index of external attribute that will be set for an SM when a request to unconditionally forward the SM has been received. Can be set to a value of 0 - 32. Default value is 0, implying that no external attribute will be set.

19.2.2.86 externalattributeforpostpaidoriginator

Mandatory/Optional

Optional

Location

Common configuration file

Description

Index of the external attribute that the PBC uses to indicate that the originator is post-paid.

For Comverse CDRs, this is used to compose the prepaid_status field in the CDR and is used for the (optional) alternative indication of the prepaid status in the Sa_options_int_n field.

For CMG CDRs, this is used as a base to compose the ppPser field and the proprietary subscriberStatus and prepaidBillingState fields. Default 0 (no external attribute is defined).

19.2.2.87 externalattributeforpostpaidrecipient

Mandatory/Optional

Optional

Location

Common configuration file

Description

Index of the external attribute that the PBC uses to indicate that the recipient is post-paid.

For Comverse CDRs, this is not used.

For CMG CDRs, this is used as a base to compose the ppPser field. Default 0 (no external attribute is defined).

19.2.2.88 externalattributeforprepaidhotbillingoriginator

Mandatory/Optional

Optional

Location

Common configuration file

Description

Index of the external attribute that the PBC uses to indicate that the originator is prepaid and charged using a hot-billing mechanism (such as Diameter).

For Comverse CDRs, this is used to compose the prepaid_status field in the CDR and is used for the (optional) alternative indication of the prepaid status in the Sa_options_int_n field.

For CMG CDRs, this is used as a base to compose the ppPser field and the proprietary subscriberStatus and prepaidBillingState fields. Default 0 (no external attribute is defined).

19.2.2.89 externalattributeforprepaidhotbillingrecipient

Mandatory/Optional

Optional

Location

Common configuration file

Description

Index of the external attribute that the PBC uses to indicate that the recipient is prepaid and charged using the hot-billing mechanism.

For Comverse CDRs, this is not used.

For CMG CDRs, this is used as a base to compose the ppPser field.

Default 0 (no external attribute is defined).

19.2.2.90 externalattributeforprepaidonlineoriginator

Mandatory/Optional

Optional

Location

Common configuration file

Description

Index of the external attribute that the PBC uses to indicate that the originator is prepaid and charged using an on-line mechanism (such as Diameter).

For Comverse CDRs, this is used to compose the prepaid_status field in the CDR and is used for the (optional) alternative indication of the prepaid status in the Sa_options_int_n field.

For CMG CDRs, this is used as a base to compose the ppPser field and the proprietary subscriberStatus and prepaidBillingState fields.

Default 0 (no external attribute is defined).

19.2.2.91 externalattributeforprepaidonlinerecipient

Mandatory/Optional

Optional

Location

Common configuration file

Description

Index of the external attribute that the PBC uses to indicate that the recipient is prepaid and charged using an online mechanism (such as Diameter).

For Comverse CDRs, this is not used.

For CMG CDRs, this is used as a base to compose the ppPser field.

Default 0 (no external attribute is defined).

19.2.2.92 externalattributeforsmartlimitoriginator

Mandatory/Optional

Optional

Location

Common configuration file

Description

Index of the external attribute that the PBC uses to indicate that the originator is using SmartLimit.

19.2.2.93 externalattributeforsmartlimitrecipient

Mandatory/Optional

Optional

Location

Common configuration file

Description

Index of the external attribute that the PBC uses to indicate that the recipient is using SmartLimit.

19.2.2.94 externalconditionfailuremessagesamsqueue

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the AMS queue in which to store external condition messages. Set to a number that refers to the queue entity's index in the MGR. Default 1

19.2.2.95 externalconditionfailuremessagessentasflashsms

Mandatory/Optional

Optional

Location

Common configuration file

Description

Pertaining to the encoding of messages that terminate in mobiles and that are sent as a result of an external condition that was not satisfied.

Valid Values

- true
- false

Default

false

19.2.2.96 externalconditionmessagesamsqueue

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the AMS queue to store messages that terminate in mobiles and that are sent as result of an external condition that did not satisfy.

Valid Values

1 - 1000

Default

1

19.2.2.97 externalconditionmessagessentasflashsms

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying the encoding of the external condition message (ECM). If set to true, the ECM is sent as a flash SMS.

Valid Values

- true
- false

Default

false

19.2.2.98 facilitynotsupportederrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.99 fallbacktosecdestonpreferredmtdesttimeout

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

This parameter indicates whether retry on secondary destination needs to be performed if MT delivery to preferred MT destination fails due to timeout error.

This parameter is applicable for MAP phase 2+ only. Up until MAP phase 2, the only possible destination of an MT/SM is an MSC. In MAP phase 2+, an MT/SM can be sent to an SGSN as well. In case an (phase 2+) HLR returns both an MSC and an SGSN as possible destinations for an MT/SM, TextPass will try to deliver the SM through the preferred destination. When the attempt to the preferred destination fails, TextPass might retry to deliver the MT/SM through the non-preferred destination. Whether TextPass does the retry on timeout Error is dependent on this parameter. When set as 'false', retry on secondary destination will not occur. By default, this parameter is set to false.

Valid Values

- true
- false

Default Value
false

19.2.2.100 fcdralphanumericformatinconstruct

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying how alphanumeric addresses should be formatted in the MSISDN field of the address construct.

Note that if the message's relation with an application can be established (like in the case of an AO message), `alphanumericaddressinorigaddressgsmfieldinfcdr` allows you to encode the application's short number rather than the alphanumeric address.

Valid Values

- empty: MSISDN field is empty (length 0).
- numeric: decoded as if the address were numeric.
- alphanumeric: decoded as readable string (UTF-8).

Default

numeric

19.2.2.101 fcdrenforceton4andnpi5forshortnumbers

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether TON value 4 (subscriber) and NPI value 5 (private) should be used for short numbers (only applies when the format of the concerned billing field is national or international).

Valid Values

- true
- false

Default

true

19.2.2.102 fcdrmaxdeferperiod

Mandatory/Optional

Optional

Location

Common configuration file

Description

Threshold for maximum value for fcdrDeferPeriod field. If this threshold is exceeded, the maximum value will be put in the billing record.

Valid Values

0 - 8760

Default

8760 (1 year)

19.2.2.103 fcdrmaxvalidityperiod

Mandatory/Optional

Optional

Location

Common configuration file

Description

Threshold for maximum value for fcdrValidityPeriod field. If this threshold is exceeded, the maximum value will be put in the billing record.

Valid Values

0 - 8760

Default

8760 (1 year)

19.2.2.104 fcdrsupportformtmt

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether CDRs must be generated for the MT-MT path when the billing format is FCDR. The CDRs generated are formatted according to a proprietary standard.

Valid Values

- true
- false

Default

false

19.2.2.105 fcdrvsmscid

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value of the `vsmscId` field. When set to -1 (default), the ID is determined based on the last three digits of the SMSC's GT. Otherwise, the specified value is placed into the CDR. Valid for the FCDR format only.

The application specific settings on the MGR (**SMS Applications ➤ Applications ➤ Virtual SMSC Address**) overrules this setting.

Refer to the RTR Billing Manual for a complete description of the interaction of the **Virtual SMSC Address**, `fcdrvsmscid`, and `fcdrvsmscidforaomessages` parameters.

Valid Values

-1 - 999

Default

-1

19.2.2.106 fcdrvsmscidforaomessages

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value of the `vsmscId` field for AO messages. When set to -1 (default), the ID is determined based on the last three (3) digits of the SMSC's GT. Otherwise, the specified value is placed into the FCDR, overruling the `fcdrvsmscid` setting. Valid for the FCDR format only.

The application specific settings on the MGR (**SMS Applications ➤ Applications ➤ Virtual SMSC Address**) overrule this setting.

Refer to the RTR Billing Manual for a complete description of the interaction of the **Virtual SMSC Address**, `fcdrvsmscid`, and `fcdrvsmscidforaomessages` parameters.

Valid Values

-1 - 999

Default

-1

19.2.2.107 firewallacceptnonnumericmtoriginatormsisdn

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the RTR/FWL should accept numeric originator MSISDNs that contain the digits a-f in incoming MT messages.

If this attribute is set to "true", the format of the originator must not be changed by means of an MTO modifier. Doing so will lead to misformatted outgoing MT traffic. This attribute does not affect the handling of alphanumeric MSISDNs.

Valid Values

- false: Non-numeric originator MSISDNs are rejected
- true: Non-numeric originator MSISDNs are allowed

Default

false

19.2.2.108 firewallallowfallbacktosecdest

Mandatory/Optional

Optional

Location

Common configuration file

Description

This parameter indicates if fallback to secondary destination should be performed in Home-Routed scenario. If TRUE, fallback to secondary destination is performed based on the terminating mobile network configuration (mobNetworkPreferredMTDestination, mobNetworkEnableFallbackToSecondaryDestination).

Valid Values

- true
- false

Default

false

19.2.2.109 firewallassumepropertimezonegeneratingbysmsc

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the FWL should assume that the time zone of an inbound MT message is correct, which impacts the time zone that the RTR uses as a base when applying MT modifiers.

Valid Values

- false: Use the time zone of the RTR/FWL as a base
- true: Use the time zone of the message as a base

Default

false

19.2.2.110 firewallcheckmospoofingafterextcondrules

Mandatory/Optional

Optional

Location

Common configuration file

Description

Changes the order in which the FWL performs the MO spoofing check and the MO rule evaluation.

Valid Values

- false: Execute the MO spoofing check first
- true: Evaluate the MOX rules first

Default

false

19.2.2.111 firewallenablemtrtgruleevaluationforsrismresponse

Mandatory/Optional

Optional

Location

Common configuration file

Description

Determines whether SRI-SM responses are subject to MTOR rules.

Valid Values

- false: Only MtForwardSm requests are subject to MTOR rules

- true: MtForwardSm requests and SRI-SM responses are subject to MTOR rules

Default

false

19.2.2.112 firewallenablemultisimservice

Mandatory/Optional

Optional

Location

Common configuration file

Description

Determines whether Nokia Multi-SIM support is enabled.

Valid Values

- false: Multi-SIM support is disabled
- true: Multi-SIM support is enabled

Default

false

19.2.2.113 firewallenablesrismrepublishingfortrustedsmsclist

Mandatory/Optional

Optional

Location

Common configuration file

Description

Enables SRI-SM republishing for SMSCs on the trusted list.

Valid Values

- false: Do not republish SRI-SM requests from trusted SMSCs
- true: Republish SRI-SM requests from SMSCs on the trusted list

Default

false

19.2.2.114 firewallfollowmaplayermmsformtforwarding

Mandatory/Optional

Optional

Location

Common configuration file

Description

Controls how the More-Messages-to-Send (MMS) field of the MAP layer MtForwardSm operation (phase 2 and 2+) should be set in forwarded MT messages:

- false— the 3GPP TS 23.040 layer's TP-MMS field is followed
- true—the value as received at the MAP layer of the inbound operation is reproduced.

For intercepted MT traffic (TCAP CONTINUE messages) this flag is ignored as the outgoing MT/SM only indicates MMS if text insertion causes extra segments.

Valid Values

- false
- true

Default

false

19.2.2.115 firewallmaxintervalbetweensrismandmtfwdsm

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum number of seconds allowed between a SendRoutingInfoForSm (SRI-SM) and an MtForwardSm operation. This value is the lifetime of a correlation record.

In case multiple MtForwardSm messages (correlated to this record) are received within the set timer, the interval gets reset at every MtForwardSm received. If the MtForwardSm arrives at the FWL after the number of seconds specified in this parameter, the correlation record look-up will fail.

Valid Values

1-3600 seconds

Default

60 seconds

19.2.2.116 firewallmnproutingnumberforownnetwork

Mandatory/Optional

Optional

Location

Common configuration file

Description

MNP routing number of the HPLMN, which enables the FWL to identify MSISDNs that have been ported out. This value must start with zero.

19.2.2.117 firewallmoactionfororiginatingaddressspoofing

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when MO spoofing is detected.

Valid Values

- discardwithnoresponse: Discard the message and do not return an acknowledgment to the originator
- discardwithack: Discard the message and return an ACK to the originator
- discardwithnak: Discard the message and return a NACK to the originator
- pass: Allow the Mobile Messaging system to continue processing the message

Default

discardwithnoresponse

19.2.2.118 firewallmoactionforspoofingcheckfailureduetoabsentsubs

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails with an absent subscriber error.

Valid Values

- treatasifspoofing: Treat as spoofing
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.119 firewallmoactionforspoofingcheckfailureduetoabsentsubssm

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails with an absent subscriberSM error.

Valid Values

- treatasifspoofing: Treat as spoofing
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.120 firewallmoactionforspoofingcheckfailureduetocallbarred

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails with a call barred error.

Valid Values

- treatasifspoofing: Treat as spoofing

- checkwithmapati: Check spoofing with MAP-ATI
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.121 firewallmoactionforspoofingcheckfailureduetodatamissing

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails with a data missing error.

Valid Values

- treatasifspoofing: Treat as spoofing
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.122 firewallmoactionforspoofingcheckfailureduetofacnotsupp

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails with a facility not supported error.

Valid Values

- treatasifspoofing: Treat as spoofing
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.123 firewallmoactionforspoofingcheckfailureduetoothererror

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails with an error, other than:

- Call barred error
- Tele-servicenotprovision error
- Unknown subscriber error
- Absent subscriberSM error
- Facilitynotsupported error
- Absent subscriber error
- System failure error
- Data missing error
- Unexpected data value error
- Tcabort error
- Timeout error
- Sccpudts error

Valid Values

- treatasifspoofing: Treat as spoofing
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.124 firewallmoactionforspoofingcheckfailureduetosccpudts

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails due to sccpudts error.

Valid Values

- treatasifspoofing: Treat as spoofing
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.125 firewallmoactionforspoofingcheckfailureduetosystemfailure

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails with a system failure error.

Valid Values

- treatasifspoofing: Treat as spoofing
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.126 firewallmoactionforspoofingcheckfailureduetotcabort

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails with a tcap-abort error.

Valid Values

- treatasifspoofing: Treat as spoofing
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.127 firewallmoactionforspoofingcheckfailureduetotimeout

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails with a timeout error.

Valid Values

- treatasifspoofing: Treat as spoofing
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.128 firewallmoactionforspoofingcheckfailureduetotsvcnotprov

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails with a tele service not provisioned error.

Valid Values

- treatasifspoofing: Treat as spoofing
- checkwithmapati: Check spoofing with MAP-ATI
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.129 firewallmoactionforspoofingcheckfailureduetounexpecdatavalue

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails with an unexpected data-value error.

Valid Values

- treatasifspoofing: Treat as spoofing
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.130 firewallmoactionforspoofingcheckfailureduetounknwnsubs

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Action to be executed when MO spoofing check fails with an unknown subscriber error.

Valid Values

- treatasifspoofing: Treat as spoofing
- pass: Consider the MO spoofing check as successful and let the SM pass.

Default

treatasifspoofing

19.2.2.131 firewallmofwdsmwithspoofingperiod

Mandatory/Optional

Optional

Location

Common configuration file

Description

Period during which the MO spoofing threshold is calculated.

Valid Values

1-86,400 seconds

Default

3600 seconds

19.2.2.132 firewallmofwdsmwithspoofingthreshold

Mandatory/Optional

Optional

Location

Common configuration file

Description

Number of detected MO spoofing attempts within the spoofing period, beyond which the FWL will generate a trap.

Valid Values

0-1,000,000

Default

0 (disable functionality)

19.2.2.133 firewallmospoofingcheckcondition

Mandatory/Optional

Optional

Location

Common configuration file

Description

Determines when the FWL performs the MO spoofing check.

Valid Values

- always: Always check
- whenmscsgsnaddressingsmscongt: Only check when the MSC or SGSN addresses the FWL using GT
- never: Never check

Default

always

19.2.2.134 firewallmospoofingdigits

Mandatory/Optional

Optional

Location

Common configuration file

Description

Number of digits used to compare the MAP layer and SCCP layer MSC/SGSN global title (GT) as part of the MO spoofing check. Digits after this prefix can differ, and spoofing will not be detected. You can override this value per-network using the **Spoofing Check Digits** parameter in the MGR.

Default

4

19.2.2.135 firewallmospoofinghlrqueryceiling

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum number of HLR queries per second that the FWL may issue for MO spoofing checks.

Default

65,535

19.2.2.136 firewallmscsgsnaddressinsuspectsrismresponse

Mandatory/Optional

Optional

Location

Host-specific configuration file

Description

Addresses from which the FWL will randomly select an address to replace the MSC and/or SGSN in a suspect SRI-SM response (to an SMSC). If no addresses are specified, the FWL uses its own GT.

Valid Values

Up to 10 E164 addresses, in international format, separated by spaces.

19.2.2.137 firewallmtactionforconflictingaddress

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when the FWL receives an SRI-SM or MtForwardSm with an SMSC address at the SCCP level that belongs to a different network from the SMSC address at the MAP level.

Valid Values

- blockwithtemporaryerror: Block the message and return a temporary error to the originator
- blockwithpermanenterror: Block the message and return a permanent error to the originator
- blockwithnoresponse: Block the message and do not return an error to the originator
- pass: Allow the Mobile Messaging system to continue processing the message

Default

blockwithnoresponse

19.2.2.138 firewallmtactionformapsmscaddressspoofing

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when the FWL receives an MtForwardSm with an SMSC address on the MAP level that belongs to a different network or country than the SMSC address on the MAP level of the corresponding SRI-SM operation.

Valid Values

- blockwithtemporaryerror: Block the message and return a temporary error to the originator
- blockwithpermanenterror: Block the message and return a permanent error to the originator
- blockwithnoresponse: Block the message and do not return an error to the originator
- pass: Allow the Mobile Messaging system to continue processing the message

Default

blockwithnoresponse

19.2.2.139 firewallmtactionforsccpsmscaddressspoofing

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when the FWL receives an MtForwardSm with an SMSC address on the SCCP level that belongs to a different network or country than the SMSC address on the SCCP level of the corresponding SRI-SM operation.

Valid Values

- blockwithtemporaryerror: Block the message and return a temporary error to the originator
- blockwithpermanenterror: Block the message and return a permanent error to the originator
- blockwithnoresponse: Block the message and do not return an error to the originator
- pass: Allow the Mobile Messaging system to continue processing the message

Default

blockwithnoresponse

19.2.2.140 firewallmtactionforunknownmapaddress

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when the FWL receives an SRI-SM or MtForwardSm with an SMSC address at the MAP level that does not match any configured SMSC.

Valid Vaues

- blockwithtemporaryerror: Block the message and return a temporary error to the originator
- blockwithpermanenterror: Block the message and return a permanent error to the originator
- blockwithnoresponse: Block the message and do not return an error to the originator
- pass: Allow the Mobile Messaging system to continue processing the message

Default

blockwithnoresponse

19.2.2.141 firewallmtactionforunknownsccpaddress

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when the FWL receives an SRI-SM or MtForwardSm with an SMSC address at the SCCP level that does not match any configured SMSC.

Valid Values

- blockwithtemporaryerror: Block the message and return a temporary error to the originator
- blockwithpermanenterror: Block the message and return a permanent error to the originator
- blockwithnoresponse: Block the message and do not return an error to the originator
- pass: Allow the Mobile Messaging system to continue processing the message

Default

blockwithnoresponse

19.2.2.142 firewallmtactionforunsolicitedmtfwdsm

Mandatory/Optional

Optional

Location

Common configuration file

Description

Action to take when the RTR/FWL receives an MtForwardSm that cannot be correlated to a previously received SendRoutingInfoForSm (SRI-SM).

Valid Values

- blockwithtemporaryerror: Block and return a temporary error to the SMSC
- blockwithpermanenterror: Block and return a permanent error to the SMSC
- blockwithnoresponse: Block and do not return a response to the SMSC
- blockwithack: Block and return an ACK to the SMSC

Default

blockwithnoresponse

19.2.2.143 firewallmtfwdsmwithspoofingperiod

Mandatory/Optional

Optional

Location

Common configuration file

Description

Period during which the MT spoofing threshold is calculated.

Valid Values

1-86,400 seconds

Default

3600 seconds

19.2.2.144 firewallmtfwdsmwithspoofingthreshold

Mandatory/Optional

Optional

Location

Common configuration file

Description

Number of detected MT spoofing attempts beyond which the FWL will generate a trap.

Valid Values

0-1,000,000

Default

0 (disables functionality)

19.2.2.145 firewallreportunknownsmscaddressnotifications

Mandatory/Optional

Optional

Location

Common configuration file

Description
Indicator specifying how to report that a SendRoutingForSm or MtForwardSm operation is received with an unknown SCCP or MAP address for the SMSC.

Valid Values

- astrap: Generate SNMP traps.
- aslogmessage: Write warnings to syslog instead.
- ignore

Default

astrap

19.2.2.146 firewallreportunknownsmscaddressnotificationstosyslog

Mandatory/Optional

Optional

Location

Common configuration file

Description
Changes the way the FWL reports a SendRoutingInfoForSm (SRI-SM) or MtForwardSm request containing an unknown SCCP or MAP SMSC address.

Valid Values

- false: Generate SNMP traps

- true: Do not generate SNMP traps; write warnings to syslog instead

Default

false

19.2.2.147 firewallenablesrismrepublishingfortrustedsmsclist

Mandatory/Optional

Optional

Location

Common configuration file

Description

Enables SRI-SM republishing for SMSCs on the trusted list.

Valid Values

- false: Do not republish SRI-SM requests from trusted SMSCs
- true: Republish SRI-SM requests from SMSCs on the trusted list

Default

false

19.2.2.148 firewallmofwdsmsccpcdpagtaiwhitelist

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list of SMSC GTs that identify MoForwardSm operations that are destined for specific SMSCs. Only MoForwardSm operations with SCCP CDPAs that are in this list will be evaluated by the MO rules.

19.2.2.149 firewallmosmtrustedoriginatorlist[1..16]

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list (created in the MGR) containing MSISDNs that should be matched against the originator MSISDN in the MoForwardSm operation. If there is a match, the MO message is considered to be trusted.

The attribute must be specified as `firewallmosmtrustedoriginatorlist#`, where # is a number between 1 and 16.

Valid Values

Each list can contain up to 10,000 addresses.

19.2.2.150 firewallmospoofingsrismhlrgtwhitelist

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list (created in the MGR) containing MSISDNs that should be matched against the HLR GT address received in the **SendRoutingInfoForSm** (SRI-SM) operation which was issued for the MO spoofing check. If there is a match, the MO spoofing check is considered to be successfully passed.

If this parameter is not configured, then, by default, it is considered to be an empty string and hence the RTR/FWL does not attempt to match any list of MSISDNs against the HLR GT address received.

19.2.2.151 firewallmospoofingsrismmscorsgsnwhitelist1

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a first list (created in the MGR) containing MSISDNs that should be matched against the MSC or SGSN in the SendRoutingInfoForSm (SRI-SM) operation that was issued for the MO spoofing check. If there is a match, the MO spoofing check is considered to be successfully passed.

19.2.2.152 firewallmospoofingsrismmscorsgsnwhitelist2

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a second list (created in the MGR) containing MSISDNs that should be matched against the MSC or SGSN in the SendRoutingInfoForSm (SRI-SM) operation that was issued for the MO spoofing check. If there is a match, the MO spoofing check is considered to be successfully passed.

19.2.2.153 firewallmospoofingsrismorigimsiwhitelist

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list (created in the MGR) containing IMSIs that should be matched against the Originator IMSI received in the **SendRoutingInfoForSm** (SRI-SM) operation which was issued for the MO spoofing check. If there is a match, the MO spoofing check is considered to be successfully passed.

If this parameter is not configured, then, by default, it is considered to be an empty string and hence the RTR/FWL does not attempt to match any list of IMSIs against the Originator IMSI received.

19.2.2.154 firewallrepublishsrismcdpasetsameasinitialsrism

Mandatory/Optional

Optional

Location

Common configuration file

Description

Changes the RTR/FWL's SCCP address modification for republished SendRoutingInfoForSm (SRI-SM) requests.

Valid Values

- false: Set the CDPA equal to the CDPA of the response to the original SRI-SM request

- true: Set the CDPA equal to the GT of the MSISDN to be queried

Default

false

19.2.2.155 firewallrepublishsrismnetworks

Mandatory/Optional

Optional

Location

Common configuration file

Description
List of networks to which SRI-SM republishing applies. When `firewallrepublishsrismnetworks` is assigned a value, the FWL assumes that republishing applies to all SRI-SM requests that are classified as suspect. For suspect SRI-SM requests, republishing is done whenever the network (as associated with the IMSI) is equal to one of the specified networks.

Valid Values

List of up to 10 networks in the format:

1. Two-letter country code (according to ISO 3166)
2. A hyphen
3. The name of a network defined in the MGR

For example:

```
nl-kpn,nl-vodafone
```

19.2.2.156 firewalltrustedsmsclist

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list containing the GTs of SMSCs for which the FWL should skip the MT spoofing check.

19.2.2.157 firewallusecommonaddressinsuspectmtforwardsm

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if the SMSC address at the MAP layer of suspect MtForwardSm requests should be replaced with the common address of the RTR/FWL.

Valid Values

- false: Do not replace the SMSC address
- true: Replace the SMSC address with the value specified in the commonaddress attribute

Default

false

19.2.2.158 firewallusehlraddressassccpcgpainsuspectsrismresponse

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if the SCCP CGPA in a suspect SendRoutingInfoForSm (SRI-SM) response (to an SMSC) should be replaced with the GT of the HLR.

Valid Values

- false: Use the GT of the RTR
- true: Use the GT of the HLR

Default

false

19.2.2.159 firewallussdrequestforretrievingmultisimstatus

Mandatory/Optional

Optional

Location

Common configuration file

Description

String to use in the USSD request that checks if an MSISDN is subscribed to the Nokia multi-SIM service.

Default

*137#

19.2.2.160 firewallussdresponseformultisimstatusdisabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

String that the HLR includes in the USSD response, indicating that an MSISDN is not subscribed to the Nokia multi-SIM service.

Default

NOT SUCCESSFUL

19.2.2.161 forcestatusreportfordroppedmomessage

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether a phase 1 status report should be generated if an MO message:

- Was accepted
- Was later dropped
- Did not request a form of status report itself

Only applies to MO-MT routing with no fallback destination.

Valid Values

- true
- false

Default

false

19.2.2.162 gtaddressinfo

Mandatory/Optional

Mandatory

Location

Host-specific configuration file (if SS7 is in use)

Description

Fifteen-digit address digit string used in the specific GT of a RTR.

19.2.2.163 gtindicator

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Global title indicator used in the specific GT of an RTR. Valid values: 0-4 (default 0).

19.2.2.164 gtnationalusebit

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Specifies the value of national use bit used in the specific GT of a RTR.

Valid Values

- true
- false

Default

false

19.2.2.165 gtnatureofaddressind

Mandatory/Optional

Optional

Location

Host-specific or Common configuration filee

Description

Type of address indicator used in the specific GT of an RTR.

Valid Values

- unknown
- subscribernumber
- reservedfornationaluse
- nationalsignificantnumber
- internationalnumber

Default

internationalnumber

19.2.2.166 gttranslationtype

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Translation type used in the specific GT of an RTR. The translation type is only non-zero in exceptional cases, such as routing an MO message to an SMSC to conserve the MSC address. Valid values: 0-255.

19.2.2.167 havemscsgsnavailableforat

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicates whether or not the MSC/SGSN address of an MO/SM shall be made available to applications when MO-AT routing is applied. The actual availability will depend on whether or not the application protocol supports relaying this information.

Valid Values

- true
- false

Default

true

19.2.2.168 hlrqueryforrecipientbeforeapproval

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the HLR query for the recipient is done before or after the evaluation of the MO external condition (MOX) rules.

Valid Values

- true (query precedes rule evaluation)
- false (rule evaluation precedes query)

Default

false

19.2.2.169 hlrqueryforrecipientofaobeforeapproval

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the HLR query for the recipient is done before or after the evaluation of the AO external condition (AOX) rules.

Valid Values

- true (query precedes rule evaluation)
- false (query depends on the routing path; only attempted if the recipient number is an MSISDN)

Default

false

19.2.2.170 hlrqueryforrecipientofigmbeforeapproval

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying that a HLR query for the recipient shall be done before the evaluation of the external condition rules for internally generated messages (IGMX rules). When set to 'false', the HLR query for the recipient may be done later during the IGM processing, depending on the selected routing path.

An HLR query is only attempted if the recipient number has been recognized as an MSISDN.

Valid Values

- true
- false

Default

false

19.2.2.171 hubmaxresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum time (in seconds) that the RTR waits for a response from the HUB before it considers the relating message as timed out. Default 15.

19.2.2.172 ignoreemptymotaginadvancedmode

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the RTR should ignore an empty MO scan tag (indicated by a pound sign at the beginning of the message). This attribute only has an effect when the RTR is operating in advanced MO tag mode.

Valid Values

- true: Ignore the empty MO scan tag
- false: Strip the empty MO scan tag from the message

Default

false

19.2.2.173 ignorepermanentfailureofhlrqueryforrecipient

Mandatory/Optional

Optional

Location

Common configuration file

Description

Determines the RTR's behavior if the HLR query for a recipient IMSI that is performed before MOX rule evalutation results in a permanent error:

- true: The RTR will ignore the permanent error. To prevent MT delivery retries for a message with a permanent HLR query error, you should configure the MO rules such that no message with a permanent HLR query error is routed to a fallback to MT. Typically, such messages should be routed to an application or be rejected.
- false (default): The RTR will NACK the MO message.

19.2.2.174 illegalequipmenterrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.175 illegalsubscribererrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.176 includeconcatenatedmsginfoinccdr

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicates whether RTR should include information related to concatenated message segments, i.e. the message reference number, the total number of segments and the segment sequence number, in the generated Comverse CDR records or not. If set to TRUE, and if the message is not concatenated or is a notification message, then only zero (0) values will be filled in the CCDR for the above fields since no actual concatenated message information is available. Default value is FALSE, in which case RTR will not include concatenated message segment related information in CCDR records.

Valid Values

- true
- false

Default

false

19.2.2.177 includemscaddrinmofwdsmtosmsc

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies when the MSC address shoud be included in the CGPA of the MoForwardSm operation toward the SMSC.

Valid Values

- never: Never include the MSC address
- always: Always include the MSC address
- foreignonly: Only include the MSC address when the MSC is located in another country

Default

never

19.2.2.178 includepcincallingpartyaddress

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the point code should be included in the calling party address of MSUs that this device sends.

Valid Values

- true
- false

Default

false

19.2.2.179 includeuserdatainnotificationrequest

Mandatory/Optional

Optional

Location

Common configuration file

Description

This parameter indicates whether user data of the original message will be included while sending the notification request to HUB or not. When this parameter is set to true, Then the user data of the original message will be included in the MXP message while sending the notification request to the HUB component. If this parameter is set to false, then user data of original message will not include in the MXP message.

Valid Values

- true
- false

Default

false

19.2.2.180 interceptfilelocation

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

This parameter indicates the location where RTR will write the intercept files. By default it is an empty string (`""`), if not configured in the semi-static file. The path cannot be empty if the parameter is provided in the semi-static file. The RTR will not create the intercept file location directory. It must be created during the intercept file generation setup, with file owner as `textpassdmf` user, group as `textpass` and permissions as 730. Execute permissions to group (`textpass`) on every parent directory of intercept directory must be given.

Valid Value
String of 255 characters

Default

Empty string

19.2.2.181 internationalprefix

Mandatory/Optional

Optional

Location

Common configuration file

Description

International prefix as used in country in which the RTR operates. Default 00.

19.2.2.182 invalidsmeaddresserrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.183 ipaddress

Mandatory/Optional

Optional

Location

Host-specific configuration file

Description

IP address of the server.

19.2.2.184 lcdrrouterid

Mandatory/Optional

Optional

Location

Common configuration file

Description

Unique ID for RTR that is used in the generation of the Call Reference field.

Valid Values

0 - 31

Default

0

19.2.2.185 linkutilisationthreshold1

Mandatory/Optional

Optional

Location

Common configuration file

Description

Percentage used to generate traps about the Rx or Tx line usage. Value should be less than threshold 2. Valid values: 0-100 (default 0, meaning no traps will be generated).

19.2.2.186 linkutilisationthreshold2

Mandatory/Optional

Optional

Location

Common configuration file

Description

Percentage used to generate traps about the Rx or Tx line usage. Value should be less than threshold 3. Valid values: 0-100 (default 0, meaning no traps will be generated).

19.2.2.187 linkutilisationthreshold3

Mandatory/Optional

Optional

Location

Common configuration file

Description

Percentage used to generate traps about the Rx or Tx line usage. Value should be greater than threshold 2 and less than threshold 4. Valid values: 0-100 (default 0, meaning no traps will be generated).

19.2.2.188 linkutilisationthreshold4

Mandatory/Optional

Optional

Location

Common configuration file

Description

Percentage used to generate traps about the Rx or Tx line usage. Value should be greater than threshold 3 and less than threshold 5. Valid values: 0-100 (default 40; if 0, no traps will be generated).

19.2.2.189 linkutilisationthreshold5

Mandatory/Optional

Optional

Location

Common configuration file

Description

Percentage used to generate traps about the Rx or Tx line usage. Value should be greater than threshold 4. Valid values: 0-100 (default 80; if 0, no traps will be generated).

19.2.2.190 localmscaddressincameltrigger

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

E164 address that the RTR should use for the MSC parameter in CAMEL operations that are issued for non-MO/SMs. When this address is not configured, the RTR uses the E164 address that is defined for its GT.

Valid Values

E164 Address (0 - 15 character string)

Default

None

19.2.2.191 localsmscaddressincameltrigger

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

E164 address that the RTR should use for the SMSC parameter in CAMEL operations that are issued for non-MO/SMs. When this address is not configured, the RTR uses the E164 address as set for *commonaddress*.

Valid Values

E164 Address (0 - 15 character string)

Default

None

19.2.2.192 logtransparentuserdatalevel

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the cases in which user data should be shown in log files.

Valid Values

- never
- always
- protocolviolationsonly
- encryptalways

Default is determined by license.

19.2.2.193 lowestmapphasetosupportimsiinmofwdsm

Mandatory/Optional

Optional

Location

Common configuration file

Description

Lowest MAP phase for which the SMSCs support passing the IMSI in an MoForwardSm operation.

Valid Values

- phase1
- phase2
- phase2plus

Default

phase2plus

19.2.2.194 m3uaaspidentifier

Mandatory/Optional

Optional

Location

Common configuration file

Description

ASP identifier assigned to the RTR device for the M3UA protocol. Default 0.

19.2.2.195 m3uanetworkappearance

Mandatory/Optional

Optional

Location

Common configuration file

Description

Network appearance for the M3UA protocol. Default 0.

19.2.2.196 m3uaroutingcontextforpointcode

Mandatory/Optional

Optional

Location

Common configuration file

Description

Routing context assigned to specific point code of an RTR for the M3UA protocol. Default 0.

19.2.2.197 m3uaroutingcontextforvirtualpointcode

Mandatory/Optional

Optional

Location

Common configuration file

Description

Routing context assigned to virtual point code of an RTR for the M3UA protocol. Default 1.

19.2.2.198 matchmoroutingrulesfordestinationapplication

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the RTR should check the destination application parameter of the MOR rules before sending a message to be evaluated by MOX rules. If an MOR rule will change the destination application of a message, the RTR uses the new destination when it sends the message to the MOX rules for evaluation. After MOX evaluation, the MOR rules evaluate the message to determine the routing action.

This functionality enables the MOX rules to use the modified destination for EC application evaluation when a message is an MO-AT path (with the exception of the MO-MT-AT path).

Note: The destination application can again be changed during MOX rule evaluation, if one of the external attributes that the EC application returns to the RTR indicates that the destination should change.

Valid Values

- false: Do not check the destination application before MOX evaluation
- true: Check the destination application before MOX evaluation and change it if necessary

This functionality should be used with care. It will increase the processing power that the RTR requires. When it is in use, the destination application will provide application-related parameters, such as the destination application short number and/or the terminating application charging units, to the evaluation of the MOX rules.

Default

false

19.2.2.199 maxlengthforshortnumber

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum length for short numbers, which are used to address applications. Valid values: 3-6 (default is 5).

19.2.2.200 maxnumarpspersecond

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum number of Auto Reply (ARP) messages that can be processed per second. If the number of ARP requests per second exceeds this threshold, processing of ARP messages is delayed (regulated).

Valid Values

1 - 2147483647

Default

100

19.2.2.201 maxnumberofdestinationtps

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum number of Service Center Termination Points that can be configured as the set of destinations for delivering an outbound AO message. The set contains one Primary Termination Point while the others are Fallback Termination Points. Delivery attempts of an outbound AO message are made

towards each of the destination Termination Points starting with the Primary one, till the message is successfully delivered or all the Termination Points in the set are exhausted.

By default the maximum number of destination Termination Points is set to 4.

Valid Values

1 - 250

Default

4

19.2.2.202 maxnumconcurrentcopytransactions

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum number of concurrent copy transactions; copying of messages is refused if the number of pending copy transactions meets this threshold. Default is 1000. Maximum is 99,999,999.

19.2.2.203 maxnumcopiespersecond

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum number of copies that can be made per second; if this threshold is exceeded, copying is delayed. Default is 100. Maximum is 2,147,483,647.

19.2.2.204 maxnumpendingarps

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum number of Auto Reply (ARP) messages pending to be processed. The generation of an ARP message is refused when the number of pending ARP messages reaches this threshold.

ARP messages are 'pending' while queued due to traffic shaping (see *maxnumarpspersecond*), or due to a delay (see *delayforautoreplytomtmessage*).

A value of 0 turns the generation of ARP messages off.

Valid Values

0 - 99999999

Default

1000

19.2.2.205 maxretriesforexternalconditionmessages

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum number of times that the RTR retries delivery for MT external condition messages. Default is 0.

19.2.2.206 maxstatusreportretries

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum number of times that the RTR retries delivery for MT status reports. Default is 0.

19.2.2.207 maxstorerequestspersecond

Mandatory/Optional

Optional

Location

Common configuration file

Description

The maximum number of Store Request messages that a (set of) RTR(s) may send per second to a (set of) AMS(s). Setting this threshold helps preventing the RTR(s) from flooding AMSs with messages to be stored. All RTRs should be set to the same value.

Note: This attribute is set to the maximum allowed value by default, which is 2147483647. In a future release this attribute will be removed.

The `maxstorerequestspersecond` attribute is used on the RTR to determine the maximum number of requests to store an SM (or status report) in *any* available AMS for a *single* RTR. That number is achieved by dividing the provisioned `maxstorerequestspersecond` value by the number of RTR nodes detected to be "active" by TNL (+ 1 for the RTR's own instance). Each RTR limits the number of store requests per second at that number.

Example: Assume that there are 2 RTRs and 2 AMSs, and that this attribute is set to 500. Then, each of the two RTRs is restricted to distribute 250 SMs per second over the two AMSs. If one AMS goes down, each RTR will send all 250 SMs to the remaining AMS.

Valid Values

1 - 2147483647 store request messages per second

Default

2147483647 (equivalent to no limitation)

19.2.2.208 memorycapacityexceedederrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.209 messagekeyweightsformsisdndestination

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the weights for computing a key for a message for which the destination is an MSISDN, specifically for a load distribution algorithm. Default is 1000,100,10,1'.

19.2.2.210 messagekeyweightsforshortnumberdestination

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the weights for computing a key for a message for which the destination is a short number, specifically for a load distribution algorithm. Default is 1000,100,10,1'.

19.2.2.211 mnpNetworkInfo

Mandatory/Optional

Mandatory

Location

Common/Host configuration file

Description
Specifies the destination network associated with this entry. A value of 0 means that the network is not configured. This parameter can be set to non-zero index only if MNP Action is set as Forward.

Valid Values

0..1000

Default Value

0

19.2.2.212 mobilecountrycode

Mandatory/Optional

Mandatory

Location

Common configuration file

Description

Mobile country code of the mobile network in which the RTR operates.

19.2.2.213 mobilenetworkcode

Mandatory/Optional

Mandatory

Location

Common configuration file

Description

Mobile network code of the mobile network in which the RTR operates.

19.2.2.214 modiscarderror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Error that the RTR uses to discard an MO message, which occurs if one of the following is true:

- The applicable MOR rule has a discard action
- No MOR rule matches the message
- No MOR rule can be applied (for example, due to throughput regulation)

Valid Values

- unknownsubscriber
- absentsubscriber
- systemfailure
- facilitynotsupported
- memorycapacityexceeded
- equipmentprotocolerror
- equipmentnotsmequipped
- unknownservicecentre
- sccongestion
- invalidcmeaddress
- subscribernotscsubscriber

Default

systemfailure

19.2.2.215 moresponseafterhlrquery

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the RTR should send a response to an MO message after it has completed the HLR query to obtain recipient details. The response depends on the HLR query result:

- Permanent error: Response is a NACK.
- Success or temporary error: Response is an ACK.

A usage scenario for this attribute is when an operator requires that MO messages to unknown recipients be rejected. Valid values:

- true
- false (default)

19.2.2.216 moroutingaddimsiifretrieved

Mandatory/Optional

Optional

Location

Common configuration file

Description

This attribute influences the inclusion of IMSI in outgoing MO based on incoming MO, for optimised MO routing and transparent MO routing to unknown SMSCs. This option is used to configure whether or not the RTR adds the IMSI to a MAP Phase 2+ MO/SM that is forwarded using optimised or transparent routing, if it is retrieved from a HLR and is not present in the original MO/SM.

This option is provided to offer compatibility with previous versions of this product. If set to 'true' then this provides compatibility with previous versions of this product. If set to 'false' then `TextPass` will not add the originator IMSI, thus removing a reason to create a segmented outgoing MO/SM out of an unsegmented incoming MO/SM.

Valid Values

- true
- false

Default

true

19.2.2.217 motagcasesensitive

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifes whether the MO tags that trigger specific functions (e.g. phase 1 status report) are case sensitive.

Valid Values

- true
- false

Default

true

19.2.2.218 mtforwardsmabsentsubscribererror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an "absent subscriber" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.219 mtforwardsmapplspecificerror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "Application specific" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.220 mtforwardsmcannotreplaceshortmsg

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "Can Not Replace Short Message" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.221 mtforwardsmdatamissingerror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "data missing" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

permanent

19.2.2.222 mtforwardsmequipmentnotsmequippederror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "not short message equipped" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.223 mtforwardsmequipmentprotocolerror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an "equipment protocol" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.224 mtforwardsmequipunspecifiederrorcause

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "Unspecified error cause" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.225 mtforwardsmerrorinms

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "Error in MS" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.226 mtforwardsmfacilitynotsupportederror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "facility not supported" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.227 mtforwardsmillegalequipmenterror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an "illegal equipment" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

permanent

19.2.2.228 mtforwardsmillegalsubscribererror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an "illegal subscriber" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

permanent

19.2.2.229 mtforwardsmimsidetach

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "Imsi Detached" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.230 mtforwardsminvalidsmeaddresserror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an "invalid SME" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.231 mtforwardsmmemorycapacityexceedederror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "memory exceeded" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.232 mtforwardsmmsgclassnotsupported

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "Message Class Not Supported" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.233 mtforwardsmnopagingresp

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "No Paging" Response in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.234 mtforwardsmnoresponseviaipsmgw

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "No Response Via IPSMGW" on a SIP Terminating operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.235 mtforwardsmnosmstoragecapabilityinsim

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "No SMS Storage Capability in (U) SIM" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.236 mtforwardsmroamrestrict

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "Roaming Restriction" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.237 mtforwardsmsccpaborted

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an "SCCP unit data service" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.238 mtforwardsmshortmsgtype0notsupported

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "Short Message Type 0 Not Supported" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.239 mtforwardsmsimappltoolkitbusy

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "(U)SIM Application Toolkit Busy" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.240 mtforwardsmsimdatadownloaderror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "(U)SIM Data Download Error" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.241 mtforwardsmsimstoragefull

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "(U) SIM Storage full" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.242 mtforwardsmsubscriberbusyformtsmserror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "subscriber busy for MT SMS" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.243 mtforwardsmsystemfailureerror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "system" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.244 mtforwardsmtcapaborted

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "TCAP abort" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.245 mtforwardsmtimeout

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a timeout on an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.246 mtforwardsmtpdunotsupported

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "TPDU not supported" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.247 mtforwardsmuederegistered

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "UE Deregistered" on a SIP Terminating operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.248 mtforwardsmunexpecteddatavalueerror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an "UnexpectedDataValue" error in an MtForwardSm operation is considered a temporary or permanent error.

An "UnexpectedDataValue" error is a generic error that can be reported for MO, MT, and SRI-SM messages when there is some malformatting in the message. The MAP specification defines which error codes are applicable. In case repetitive occurrences of "UnexpectedDataValue" errors are received, contact NewNet support for further investigation of these errors.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.249 mtforwardsmunidentifiedsubscribererror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an "unidentified subscriber" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.250 mtforwardsmunspecifieddatacodingscheme

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "Unspecified TP-DCS" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.251 mtforwardsmunspecifiedprotocolid

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "Unspecified TP-PID" error in an MtForwardSm operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.252 mtfsmnopagingresptimeout

Mandatory/Optional

Optional

Location

Common configuration file

Description

Option to specify the timeout duration (in seconds) for determining if a MTFSM NACK with Absent Subscriber error indicates a 'No Paging Response' or not.

The corresponding SNMP attribute in `textpass-sms-mib.my` is `smsPropMtFsmNoPagingResponseTimeout`.

Valid values: 1-255.

Default value: 9

19.2.2.253 mtmtuseuniquescts

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if the MT-MT routine path shall use unique timestamp to replace the original SCTS received in the inbound MT ForwardSM. The unique timestamp is created by the RTR to distinguish multiple inbound MT SMs with the same recipient.

The generated unique timestamp can refer to the time in the future. This timestamp is used in FCDR formatted billing, logging and outbound MT ForwardSM if the parameter is set to true.

Valid values:

- true
- false

Default value:

false

19.2.2.254 mtnotificationvalidityperiod

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Indicates the message Validity Period in seconds, for MT notification messages generated by the RTR.

Valid Values

0 - 360000

Default

0

19.2.2.255 mtoriginatorformatfordomestictraffic

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying how the originator should be specified in an MT/SM that is sent to a recipient of the same country as the one in which the Mobile Messaging RTR has been installed. Default is that recipient is taken from the MO/SM or AO/SM without any modification.

Valid Values

- transparent
- national
- international

Default

Taken from the MO/SM or AO/SM

19.2.2.256 mtoriginatorformatformtmtdomestictraffic

Mandatory/Optional

Optional

Location

Host/Common configuration file

Description

Indicator specifying how the originator should be specified in an MT/SM for an MT-MT scenario that is sent to a recipient of the same country as the one in which the Mobile Messaging RTR has been installed. Note that this parameter is not applicable in the case where the SRIQ routing rule action is set to '`Accept and Respond to SMSC immediately`'."

Valid Values

- transparent
- national
- international

Default

transparent

19.2.2.257 mtp2timer1

Mandatory/Optional

Optional

Location

Common configuration file

Description

"Alignment ready" timer, expressed in units of 100 milliseconds. Valid values: 40-50 seconds (default 50).

19.2.2.258 mtp2timer2

Mandatory/Optional

Optional

Location

Common configuration file

Description

"Not aligned" timer, expressed in units of 100 milliseconds. Valid values: 5-150 seconds (default 150).

19.2.2.259 mtp2timer3

Mandatory/Optional

Optional

Location

Common configuration file

Description

"Aligned" timer, expressed in units of 100 milliseconds. Valid values: 1-2 seconds (default 1.5).

19.2.2.260 mtp2timer4emergency

Mandatory/Optional

Optional

Location

Common configuration file

Description

"Emergency proving" timer, expressed in units of 100 milliseconds. Valid values: 0.4-0.6 seconds (default 0.6).

19.2.2.261 mtp2timer4normal

Mandatory/Optional

Optional

Location

Common configuration file

Description

"Normal proving period" timer, expressed in units of 100 milliseconds. Valid values: 7.5-9.5 seconds (default 9).

19.2.2.262 mtp2timer5

Mandatory/Optional

Optional

Location

Common configuration file

Description

"Sending SIB" timer, expressed in units of 100 milliseconds. Valid values: 0.08-0.12 seconds (default 0.1).

19.2.2.263 mtp2timer6

Mandatory/Optional

Optional

Location

Common configuration file

Description

"Remote congestion" timer, expressed in units of 100 milliseconds. Valid values: 3-6 seconds (default 6).

19.2.2.264 mtp2timer7

Mandatory/Optional

Optional

Location

Common configuration file

Description

"Excessive delay of acknowledgement" timer, expressed in units of 100 milliseconds. Valid values: 0.5-2 seconds (default 2).

19.2.2.265 mtp3mgmttimer10

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer waiting to repeat signalling route set test messages, expressed in units of 100 milliseconds.Default 45 seconds.

19.2.2.266 mtp3mgmttimer15

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer waiting to start a signalling route set congestion test, expressed in units of 100 milliseconds. Default 3 seconds.

19.2.2.267 mtp3mgmttimer16

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer waiting for route set congestion status update, expressed in units of 100 milliseconds. Default 2 seconds.

19.2.2.268 mtp3mgmttimer17

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer defining delay to avoid oscillation of initial alignment and link restart, expressed in units of 100 milliseconds. Default 1 second.

19.2.2.269 mtp3mgmttimer19

Mandatory/Optional

Optional

Location

Common configuration file

Description

Supervision timer during MTP restart to avoid constant exchange of TFP, TFR, and TRA messages, expressed in units of 100 milliseconds. Default 67 seconds.

19.2.2.270 mtp3mgmttimer2

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer waiting for change-over acknowledgement, expressed in units of 100 milliseconds. Default 1.4 seconds.

19.2.2.271 mtp3mgmttimer20

Mandatory/Optional

Optional

Location

Common configuration file

Description

Overall MTP restart timer at the signalling point whose MTP restarts, expressed in units of 100 milliseconds. Default 59 seconds.

19.2.2.272 mtp3mgmttimer21

Mandatory/Optional

Optional

Location

Common configuration file

Description

Overall MTP restart timer at a signalling point adjacent to one whose MTP restarts, expressed in units of 100 milliseconds. Default 63 seconds.

19.2.2.273 mtp3mgmttimer8

Mandatory/Optional

Optional

Location

Common configuration file

Description

Transfer prohibited inhibition timer, expressed in units of 100 milliseconds. Default 1.2 seconds.

19.2.2.274 mtp3testtimer1

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer defining maximum time allowed between test request message (an SLTM) and its response (an SLTA), expressed in units of 100 milliseconds. Default 8 seconds.

19.2.2.275 mtp3testtimer2

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer defining the duration of the interval at which test request messages are sent, expressed in units of 100 milliseconds. Default 60 seconds.

19.2.2.276 mtpermanentdiscarderrorforhlr

Mandatory/Optional

Optional

Location

Common configuration file

Description

Error that the RTR uses to permanently discard an incoming MAP SRI-SM request for a MT message issued by an SMSC.

Valid values:

- unknownsubscriber (default)
- absentsubscriber
- systemfailure
- facilitynotsupported
- memorycapacityexceeded
- equipmentprotocolerror
- unknownservicecentre
- sccongestion
- invalidcmeaddress
- subscribernotscsubscriber

19.2.2.277 mtpermanentdiscarderrorformscorsgsn

Mandatory/Optional

Optional

Location

Common configuration file

Description

Error that the RTR uses to permanently discard an incoming MAP MT-ForwardSM request for a MT message issued by an SMSC.

Valid Values

- unidentifiedsubscriber (default)
- absentsubscribersm
- systemfailure
- facilitynotsupported
- memorycapacityexceeded
- equipmentprotocolerror
- equipmentnotsmequipped
- subscriberbusyformtsms
- illegalsubscriber
- illegalequipment

19.2.2.278 mtstatusreportsamsqueue

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the AMS queue in which to store MT status reports. Set to a number that refers to the queue entity's index in the MGR. Default 1.

19.2.2.279 mttemporarydiscarderrorforhlr

Mandatory/Optional

Optional

Location

Common configuration file

Description

Error that the RTR uses to temporarily discard an incoming MAP SRI-SM request for a MT message issued by an SMSC.

Valid values:

- unknownsubscriber
- absentsubscriber (default)
- systemfailure
- facilitynotsupported
- memorycapacityexceeded
- equipmentprotocolerror

- unknownservicecentre
- sccongestion
- invalidcmeaddress
- subscribernotscsubscriber

19.2.2.280 mttemporarydiscarderrorformscorsgsn

Mandatory/Optional

Optional

Location

Common configuration file

Description

Error that the RTR uses to temporarily discard an incoming MAP MT-ForwardSM request for a MT message issued by an SMSC.

Valid Values

- unidentifiedsubscriber
- absentsubscribersm (default)
- systemfailure
- facilitynotsupported
- memorycapacityexceeded
- equipmentprotocolerror
- equipmentnotsmequipped
- subscriberbusyformtsms
- illegalsubscriber
- illegalequipment

19.2.2.281 nationalprefix

Mandatory/Optional

Optional

Location

Common configuration file

Description

National (trunk) prefix used in country in which the RTR operates. Default 0.

19.2.2.282 nationalroamingenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the operator's network is used by other operators in the same country. If this is not the case, the RTR can optimise MNP checks to determine whether incoming MO messages are from the operator's own subscribers.

Valid Values

- false: MO messages from own network MSCs are passed, MO messages from other operators of the same country are blocked.
- true **or** if the MO message comes from a different country, the RTR starts considering the originator IMSI:
  - If the IMSI is known, the RTR rejects messages with invalid IMSIs or IMSIs that are not from own network. Only own ("friendly") IMSIs are passed.
  - If the IMSI is not known, the RTR tries to retrieve it by means of an SRI-SM. If the SRI-SM fails, the MO will be rejected, except for the errors "call barred" and "teleservice not provisioned", for which the message can be accepted if so configured. Refer to:
    - `actionformnpcheckfailureduetocallbarred`
    - `actionformnpcheckfailureduetotsvcnotprov`

Default

false

19.2.2.283 ncdrexchangeid

Mandatory/Optional

Optional

Location

Common configuration file

Description

Address to be used for the Exchange Id field in the header and tail and for smsCentre file in the body of the Nokia CDR (NCDR) block. By default, this address is equal to the specific GT address.

Valid Values

E164 address

Default

Equal to the specific GT address.

19.2.2.284 networkdiscoverymulticastaddress

Mandatory/Optional

Optional

Location

Common configuration file

Description

Multicast address used for network discovery; can only be changed when the device's administrative state is inactive.

19.2.2.285 networkdiscoverynetworkaddress

Mandatory/Optional

Optional

Location

Common configuration file

Description

Network address used for network discovery; can only be changed when the device's administrative state is inactive.

19.2.2.286 networkdiscoverynetworkmask

Mandatory/Optional

Optional

Location

Common configuration file

Description

Network mask used for network discovery; can only be changed when the device's administrative state is inactive.

19.2.2.287 networkindicator

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the type of SS7 network.

Valid Values

- 0 (international)
- 1 (spare; international use only)
- 2 (national)
- 3 (reserved for national use)

Default

2

19.2.2.288 numberportabilityenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether MNP is implemented in the operator;s country.

Valid Values

- false: The RTR does not care about the `nationalroamingenabled` setting, but only looks at the originator MSISDN (accept own MSISDN and reject foreign MSISDN).
- true: The RTR looks at the `nationalroamingenabled` setting.

Default

false

19.2.2.289 operatorabbrevationforunknownnetworks

Mandatory/Optional

Optional

Location

Common configuration file

Description
Specifies the default abbreviated network name to be used for "Service type" field while generating the 3G CDR for MO originating traffic when the originating GT address of the message do not match any of the configured network.

Valid Values

Alphanumeric string of up to 15 characters.

Default

"OP"

19.2.2.290 optimisedmorouting

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether optimised MO routing is enabled. In optimised MO routing, the RTR relays the TCAP dialogue from the MSC to the SMSC. In conventional MO routing, the RTR sets up a new TCAP dialogue toward the SMSC.

Valid Values

- true (optimised routing)
- false (conventional routing)

Default

false

19.2.2.291 optimisedmtdelivery

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether optimised MT delivery is enabled. In optimised MT delivery, the RTR considers a message to be undeliverable when the HLR indicates that the MS is unavailable. In conventional MT delivery, the RTR ignores the HLR's indication of whether the MS can receive more messages.

Valid Values

- true (optimised delivery)
- false (conventional delivery)

Default

true

19.2.2.292 outboundextcondrulesenabledforigsm

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying whether outbound (MT) external condition rules are applied to internally generated messages (for example, copy and forward messages).

Valid Values

- true
- false

Default

false

19.2.2.293 overridebufferednotificationrequestforaoaomessages

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the request for a buffered notification of an AO-AO message should be modified.

Valid Values

- -1: Do not change the value of the buffered notification request
- 0: Force the buffered notification request to off
- 1: Force the buffered notification request to on

This global modifier is only intended for use in combination with a PBC-based transaction database for generating final delivery CDRs on the AO-AO path. It should not be used for any other purpose; instead, rule-based AO modifiers should be used. This modifier must not be used at the same time as rule-based AO modifiers that affect the notification request bits.

Default

-1

19.2.2.294 overridedeliverynotificationrequestforaoaomessages

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the request for a delivery notification of an AO-AO message should be modified.

Valid Values

- -1: No modification
- 0: Off
- 1: On

This global modifier is only intended for use in combination with a PBC-based transaction database for generating final delivery CDRs on the AO-AO path. It should not be used for any other purpose; instead, rule-based AO modifiers should be used. This modifier must not be used at the same time as rule-based AO modifiers that affect the notification request bits.

Default

-1

19.2.2.295 overridenondeliverynotificationrequestforaoaomessages

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the request for a non-delivery notification of an AO-AO message should be modified.

- -1: No modification (default)
- 0: Off
- 1: On

This global modifier is only intended for use in combination with a PBC-based transaction database for generating final delivery CDRs on the AO-AO path. It should not be used for any other purpose; instead, rule-based AO modifiers should be used. This modifier must not be used at the same time as rule-based AO modifiers that affect the notification request bits.

19.2.2.296 overridenotificationtypeformoaomessages

Mandatory/Optional

Optional

Location

Common configuration file

Description

String of three characters (0 or 1) that specifies which notification types should be requested when an MO message is forwarded to an SMSC as AO.

If any notification type is set to 1, the value received in the MO message is ignored. Otherwise, if the MO message requests a status report, then delivery and non-delivery notifications are requested. Format:

- First character: Notification of successful delivery
- Second character: Notification of a failed delivery
- Third character: Buffered notification

Default 110 (delivery and non-delivery notifications requested).

19.2.2.297 pairedunicodecharlist

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description
Specifies paired unicode characters that should not be split between consecutive segments of a concatenated message.

Valid Values
A sequence of hexadecimal values separated by semicolons (';'). The values should be encoded in UTF-16 format. The string must end with ';' if it is not empty.

Default

002320E3;003120E3;003220E3;003320E3;003420E3;003520E3;003620E3;003720E3;003820E3;003920E3;003020E3;

19.2.2.298 pcssnroutingwhenincludingmscaddrinmofwdsmtosmsc

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if the SCCP CGPA routing indicator should be set to PC/SSN when the MSC address is included in the CGPA of the MoForwardSm operation toward the SMSC.

Valid Values

- false: Do not set the routing indicator to PC/SSN
- true: Set the routing indicator to PC/SSN

Default

false

19.2.2.299 phase1bufferedstatusreportenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether phase 1 status reports with status buffered are generated.

Valid Values

- true
- false

Default

false

19.2.2.300 phase1statusreportoverrules

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies which status report overrules when both a phase 1 and a phase 2/2+ status report are requested for an MO message.

Valid Values

- true (phase 1 overrules)
- false (phrase 2/2+ overrules)

Default

false

19.2.2.301 phase1statusreporttemplateforbufferedstatus

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the format of the phase 1 status report that is sent to the message originator, that has been buffered for delivery at a later time.

Valid Values

- $(SCTS): Service centre timestamp
- $(DISCHARGE_TIME): Discharge time
- $(DESTINATION): Address of the message recipient

Default

"**STATUS** Buffered. Message to $(DESTINATION) sent at $(SCTS)".

19.2.2.302 phase1statusreporttemplatefordeletedstatus

Mandatory/Optional

Optional

Location

Common configuration file

Description

String specifying the format of a phase 1 status report that is sent to the originator of a message that has been deleted before it could be delivered to the recipient of the message. Same valid values as the template for buffered status.

Default

"**STATUS** Deleted. Message to $(DESTINATION) sent at $(SCTS)".

19.2.2.303 phase1statusreporttemplatefordiscardedstatus

Mandatory/Optional

Optional

Location

Common configuration file

Description

String specifying the format of a phase 1 status report that is sent to the originator of a message that has been discarded before it could be delivered to the recipient of the message. Same valid values as the template for buffered status.

Default

"**STATUS** Discarded. Message to $(DESTINATION) sent at $(SCTS)".

19.2.2.304 phase1statusreporttemplateforexpiredstatus

Mandatory/Optional

Optional

Location

Common configuration file

Description

String specifying the format of a phase 1 status report that is sent to the originator of a message that has expired before it could be delivered to the recipient of the message. Same valid values as the template for buffered status.

Default

"**STATUS** Expired. Message to $(DESTINATION) sent at $(SCTS)".

19.2.2.305 phase1statusreporttemplateforfailedstatus

Mandatory/Optional

Optional

Location

Common configuration file

Description

String specifying the format of a phase 1 status report that is sent to the originator of a message that could be delivered to the recipient of the message. Same valid values as the template for buffered status.

Default

"**STATUS** Failed. Message to $(DESTINATION) sent at $(SCTS)".

19.2.2.306 phase1statusreporttemplateforsucceededstatus

Mandatory/Optional

Optional

Location

Common configuration file

Description

String specifying the format of a phase 1 status report that is sent to the originator of a message that has been successfully delivered to the recipient of the message. Same valid values as the template for buffered status.

Default

"**STATUS** Delivered. Message to $(DESTINATION) sent at $(SCTS)".

19.2.2.307 phase2bufferedstatusreportenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether phase 2 status reports with status pending are generated.

Valid Values

- true
- false

Default

false

19.2.2.308 phase2statusreporttpstatusbuffered

Mandatory/Optional

Optional

Location

Common configuration file

Description

Value for the TP-STATUS field of a phase 2 status report when the report indicates that the original message was buffered. Valid values: 0-255. Default 0x30.

19.2.2.309 phase2statusreporttpstatusdeleted

Mandatory/Optional

Optional

Location

Common configuration file

Description

Value for the TP-STATUS field of a phase 2 status report when the report indicates that the original message was deleted. Valid values: 0-255. Default 0x48.

19.2.2.310 phase2statusreporttpstatusdiscarded

Mandatory/Optional

Optional

Location

Common configuration file

Description

Value for the TP-STATUS field of a phase 2 status report when the report indicates that the original message was discarded. Valid values: 0-255. Default 0x70.

19.2.2.311 phase2statusreporttpstatusexpired

Mandatory/Optional

Optional

Location

Common configuration file

Description

Value for the TP-STATUS field of a phase 2 status report when the report indicates that the original message expired. Valid values: 0-255. Default 0x46.

19.2.2.312 phase2statusreporttpstatusfailed

Mandatory/Optional

Optional

Location

Common configuration file

Description

Value for the TP-STATUS field of a phase 2 status report when the report indicates that the original message failed. Valid values: 0-255. Default 0x70.

19.2.2.313 phase2statusreporttpstatussucceeded

Mandatory/Optional

Optional

Location

Common configuration file

Description

Value for the TP-STATUS field of a phase 2 status report when the report indicates that the original message succeeded. Valid values: 0-255. Default 0x00.

19.2.2.314 pointcode

Mandatory/Optional

Mandatory

Location

Host-specific configuration file

Description

Specific point code of an RTR (used to address a particular RTR). Valid formats:

- Decimal (for example, 2232)
- x.y.z, where x is the area, y is the cluster, and z is the member (for example, 7.124.6)

Valid ranges:

- Decimal
  - ANSI 65536-16777215
  - ITU-T 0-16383
  - Japanese SS7 0 - 65535
- Area
  - ANSI 1-255
  - ITU-T 0-7
  - Japanese SS7 0-31
- Cluster
  - ANSI 0-255
  - ITU-T 0-255
  - Japanese SS7 0-15
- Member
  - ANSI 0-255

- ITU-T 0-7
- Japanese SS7 0-127

19.2.2.315 preferredmtdestination

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the preferred destination for MT traffic (only applies to MAP phase 2).

Before phase 2, the only possible destination for an MT message was an MSC. In MAP phase 2+, an MT message can be sent to an SGSN, as well.

If a phase 2+ HLR returns an MSC and an SGSN as possible destinations, the RTR will try to deliver the message to the preferred destination. If this attempt fails, the RTR can retry the delivery to the non-preferred destination; this depends on the type of delivery failure that the preferred destination reported.

Valid Values

- msc
- sgsn

Default

msc

19.2.2.316 preservenationalorigton

Mandatory/Optional

Optional

Location

Host/Common configuration file

Description

If this parameter is true, it indicates that when the received TON/NPI of Originator is 2/1 and the normalized MSISDN does not start with an E164 country code and the configured MTO modifier Originator format is national with TON/NPI as 0/1, then the incoming TON/NPI will be used in the TP-OA of the outgoing MTFSM. To disable this behavior, set the parameter as false.

Valid Values

- true
- false

Default

true

19.2.2.317 processpriority

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the priority of the the RTR process started.

Valid values:

- critical
- high
- normal (default)
- low

19.2.2.318 pseudoterminatingmscaddress

Mandatory/Optional

Mandatory

Location

Common configuration file

Description

E164 address that Router will use to fake a Terminating MSC Address for messages terminating to IMS network. The MSC Address will be used in billing records. The E164 address should be specified in international format without the international prefix. Value will not show up if not set.

19.2.2.319 pseudoterminatingmscpointcode

Mandatory/Optional

Mandatory

Location

Common configuration file

Description

Point code of MSC and formatted as commonly done in ITU-T. The RTR is using it to fake Terminating MSC point code. Note that this point code can be changed/viewed by this object as well as the smsPropPseudoTerminatingMscPointCodeString object. Value will not show up if not set.

19.2.2.320 pseudoterminatingmscpointcodestring

Mandatory/Optional

Mandatory

Location

Common configuration file

Description

Point code of MSC and formatted as commonly done in ASNI. The RTR is using it to fake Terminating MSC point code. Note that this point code can be changed/viewed by this object as well as the `smsPropPseudoTerminatingMscPointCode` object. Value will show as `not set` if not set. Setting it to this value is also the way to unset it.

19.2.2.321 queueforincomingattraffic

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the AMS queue to which all incoming AT traffic will be routed. The AMS is responsible for delivering the messages to the application. Default 0 (no messages are routed to the AMS).

19.2.2.322 regularatstatusreportsamsqueue

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the AMS queue in which to store AT status reports that may be delivered on sessions established by the application. Set to a number that refers to the queue entity's index in the MGR.

Valid Values

1 - 1000

Default

2

19.2.2.323 relaymterrortosmscforhomeroutedmessages

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the MTFSM error code that TextPass receives while trying to deliver a home-routed MT message will be relayed transparently to the SMSC or not.

Note that this parameter is applicable only in the case where the SRIQ routing rule action is set to 'Accept and Respond to SMSC immediately'.

By default it is set to 'false', in which case the MTFSM error code will not be relayed to the SMSC in the above scenario; instead the parameters `mttemporarydiscarderrorformscorsgsn` and `mtpermanentdiscarderrorformscorsgsn` will determine the error code which will be returned back to the SMSC, depending upon whether a temporary error or a permanent error is encountered.

Valid Values

- true
- false

Default

false

19.2.2.324 repstsaddgprssupportindicatorifbothmscsgsnpresent

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

If true, then GPRS Support Indicator is added in Report SM Delivery Status message only when SRISM response contained both MSC and SGSN addresses. If the value of this parameter is false, then in all Report SM Delivery Status message GPRS Support Indicator will be present.

Valid Values

- true
- false

Default

false

19.2.2.325 requiress7connectivity

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the RTR may only change to the operating state when it has established connectivity to the SS7 network.

Valid Values

- true
- false

Default

true

19.2.2.326 resetsequencenumberofbillingprofileupondestroy

Mandatory/Optional

Optional

Location

Common configuration file

Description

Boolean specifying whether destroying a billing profile should imply a reset of the associated sequence number in the permanent storage that the RTR maintains for billing profile sequence numbers.

The sequence number that is maintained for a billing profile is (optionally) used in the names of the CDR files that are generated for the billing profile.

Resetting the billing profile sequence number is required to ensure that a newly added billing profile that is mapped to a table index that has been used before has a properly initialized sequence number (rather than the sequence number of the billing profile that was mapped to the same table index before). The value 'false' is typically used when a billing profile is temporary removed. Not resetting the sequence number will then ensure that the sequence number after removal will commence from the value before the removal.

Valid Values

- true
- false

Default

true

19.2.2.327 resetsequencenumberofloggingprofileupondestroy

Mandatory/Optional

Optional

Location

Common configuration file

Description

Boolean specifying whether destroying a logging profile should imply a reset of the associated sequence number in the permanent storage that the RTR maintains for logging profile sequence numbers.

The sequence number that is maintained for a logging profile is (optionally) used in the names of the CDR files that are generated for the logging profile.

Resetting the logging profile sequence number is required to ensure that a newly added logging profile that is mapped to a table index that has been used before has a properly initialized sequence number (rather than the sequence number of the logging profile that was mapped to the same table index before). The value 'false' is typically used when a logging profile is temporary removed. Not resetting the sequence number will then ensure that the sequence number after removal will commence from the value before the removal.

Valid Values

- true
- false

Default

true

19.2.2.328 restrictcopyingtoownsubscriberbase

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying whether the copying should only be done when the destination belongs to Home PLMN (HPLMN). Valid values:

- true (default)
- false

Enabling copying outside the HPLMN opens up the possibility of copy loops. As a result of copy loops, the RTR (and even the whole HPLMN) may become inoperable. As such, it strongly discouraged to enable copying outside the HPLMN.

19.2.2.329 restrictforwardingtoownsubscriberbase

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying whether the forwarding should only be done when the destination of the forwarding belongs to Home PLMN (HPLMN). Valid values:

- true (default)
- false

Enabling forwarding outside the HPLMN opens up the possibility of forward loops. As a result of forward loops, the RTR (and even the whole HPLMN) may become inoperable. As such, it strongly discouraged to enable forwardingoutside the HPLMN.

19.2.2.330 retryintervalforexternalconditionmessages

Mandatory/Optional

Optional

Location

Common configuration file

Description

Interval between two consecutive retries for an MT external condition message. The interval is expressed in number of seconds. Default 60 seconds.

19.2.2.331 returnmessagemaxuserdatalength

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

The User Data (original message) variable should have a maximum configurable length (x), after which the content should be truncated to x minus 3, with 3 periods added, i.e., with x = 25, 'Hi, this message is too long for a notification' should become 'Hi, this message is to...'. If the DCS of the return message is GSM7, the maximum length is 160. If the DCS of the return message is UCS2, the maximum length will be 70.

Valid Values

3 to 160

Default

12

19.2.2.332 rtrcreatemtmtcdrforerrorscenarios

Mandatory/Optional

Optional

Location

Host-specific or common configuration file

Description

This parameter allows the creation of the MT-MT home-routing 3G CDRs in case of error scenarios. When this parameter is set to true, the RTR will support the creation of 3G CDRs in the MT-MT home-routing flow when the message is temporary/permanent/blocked/discarded due to routing or external condition rules, or due to the MT spoofing scenarios or a received network error.

Note: This parameter is designed for 3G CDR. It may be enabled for the other CDR formats like FCDR, ECDR and LCDR. The behavior of enabling the parameter for CDR format other than the 3G CDR is undefined.

Valid Values

- true
- false

Default

false (0)

19.2.2.333 rtrdcscharcodingconversion

Mandatory/Optional

Mandatory

Location

Common configuration file

Description

This parameter indicates how the coding conversion, the custom character set conversion and the conversion from Data Coding to TP-DCS or vice-versa must be performed for inbound AO scenarios and MO AT scenarios.

Valid Values

- transparent: The transparent behavior of the data coding scheme, coding and character set conversion.
- japan: Japanese network specific behavior of the data coding scheme, coding and character set conversion.
- gsm23038: Behavior as per 3gpp specification will be followed. (This option is part of a future scope, and is currently not supported).

Default

transparent (0)

19.2.2.334 rtrdefaultrecipimsiforfcdr

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

This parameter indicates the default recipient IMSI for FCDR if the actual B-IMSI is not available.

For example, B-IMSI is not available in case SRI-SM request for recipient will be skipped or failed.

Valid Values
5-15 digit number

Default

Empty string

19.2.2.335 rtrenablemapatifororig

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

This parameter indicates whether an MAP Any Time Interrogation (MAP ATI) request should be performed on originator.

Note: Even if this parameter is false, MAP ATI still can happen if:

- SRISM for Originator failed with Call Barred or AbsentSubscriberSM error with 'MS purged for GPRS' diagnostic and `firewallmoactionforspoofingcheckfailureduetocallbarred` is set to `checkWithMapAti`.
- SRISM for Originator failed with Teleservices not provisioned and `firewallmoactionforspoofingcheckfailureduetotsvcnotprov` is set to `checkWithMapAti` .

Valid Values

- false
- true

Default Value

false

19.2.2.336 rtrenablemapatiforrecip

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

This parameter indicates whether an MAP Any Time Interrogation (MAP ATI) request should be performed on Recipient.

Note: MAP ATI will be performed only if the MT Delivery is successful.

Valid Values

- never: Never perform MAP ATI for recipient
- ownNetwork: Only for own network (subscriber MCC/MNC = own mobile country / own network)
- always: Always perform MAP ATI for recipient

Default Value

never

19.2.2.337 rtrimsmttimeout

Mandatory/Optional

Mandatory

Location

Common configuration file

Description

Timeout for MT deliveries to the IMS domain (in seconds).

The default value is 600.

Valid range: 1 to 3900.

Note: This value must be greater than the timeout for MT deliveries (parameter `iiwmtimsmaxresponsetime`) configured on the IIW.

19.2.2.338 rtrincludepcinmofwdsmtosmsc

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Specifies whether the Point Code should be included in the SCCP calling party address of the MO Forward SM sent towards the SMSC. When this parameter is `true`, the RTR will include its own specific point code in the SCCP Calling party address.

Note: This parameter will only be applicable when the incoming MO Forward SM does not contain the point code in the SCCP calling party address and the semi-static parameter *pcssnroutingwhenincludingmscaddrinmofwdsmtosmsc* is also set to `true`.

Valid Values

- true
- false

Default Value

false

19.2.2.339 rtrinsertsubmitreportinmofsmresponse

Mandatory/Optional

Mandatory

Location

Common/Host configuration file

Description
This parameter governs the inclusion of SMS Submit Report and Opcode in MO-FSM ack/nack. If this parameter is true and the incoming MO-FSM request MAP Phase version is 3, then SMS Submit Report and Opcode will be inserted in the MO-FSM_ack and MO-FSM_nack response.

Valid Values

- true
- false

Default

false

19.2.2.340 rtrinterceptfilenametemplate

Mandatory/Optional

Optional

Location

Common configuration file

Description

This parameter indicates the intercept file pattern, used to write the files to intercept directory. They are string specifying the format for the name of the intercept file. The following format specifiers are supported:

- %Y - year specified in four digits (e.g. 2004)
- %y - year specified in two digits (e.g. 04)
- %m - month specified in two digits (e.g. 01 for Jan, 10 for Oct)
- %d - day specified in two digits (e.g. 01 for 1st day of month, 31 for last day of month)

- %H - hour specified in two digits (e.g. 00 for midnight, 12 for noon)
- %M - minute specified in two digits
- %S - second specified in two digits
- %h - hostname
- %U - UID of the user from which RTR process is running
- %1 - a one-digit sequence number
- %2 - a two-digit sequence number
- %3 - a three-digit sequence number
- %4 - a four-digit sequence number
- %5 - a five-digit sequence number
- %6 - a six-digit sequence number
- %7 - a seven-digit sequence number
- %8 - a eight-digit sequence number

For example: `intercept_%h_%U_%Y%m%d_%H%M%S_%3.dat`

The default value is an empty string (""), if not configured in the semi-static file. The path can't be empty if the parameter is provided in the semi-static file. If this option is not set the RTR will not generate intercept files at the location configured against parameter *interceptfilelocation*.

Valid Value
String of 255 characters

Default

Empty string

19.2.2.341 rtrmapatitranslationtype

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

Value for Translation Type in SCCP CdPA of Outgoing MAP ATI request towards HLR.

Default Value

The default for ITU-T is 0, whilst 10 is used as a default for ANSI.

19.2.2.342 rtrmaxinterceptfileduration

Mandatory/Optional

Optional

Location

Common configuration file

Description
This parameter indicates the max time duration after which the intercept file will be closed and moved to location specified in the parameter *interceptfilelocation*.The value is provided in seconds.

Valid Value
10-900

Default

60

19.2.2.343 rtrmaxuserdatalengthfortcapsegmentation

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

This parameter indicates that TCAP segmentation will be performed if MTFSM user data length in bytes is equal to or greater than value of this parameter for unknown terminating network. In case of matching terminating network, the minimum of this parameter and **MTFSM Max User Data Length for TCAP Segmentation** present in the configured network (**Environment ➤ Networks**) is taken for TCAP segmentation.

If the value is 0, then TCAP segmentation is always performed irrespective of the terminating network configuration. The default value is 141 which means TCAP segmentation for unknown networks is not performed based on user data length in bytes.

Valid Values

0-141

Default

141

19.2.2.344 rtrrequestinfobitsformapatifororig

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

This parameter specifies a bitstring with values to be requested in the MAP ATI Request for Originator. The ATI RequestedInfo parameter is prepared based on this parameter.

Note:

1. The RTR will prepare the ATI request according to the bits selected by the operator. The RTR should ensure that in no way it creates an ATI request which is not as per specification.
2. In this `rtrrequestinfobitsformapatifororig` field the left-most bit is referred to as 'Bit 0'.

   Example 1: set parameter `rtrrequestinfobitsformapatifororig="1000000"`

   Here, the **leftmost-bit is '1'**,which represents the **locationinformation** field.

   It means this field is requested in map-Ati request.

   Example 2: set parameter `rtrrequestinfobitsformapatifororig="0111111"`

   Here, the **leftmost-bit is '0'**,which represents the **locationinformation** field.

   It means this field is not requested in map-Ati request.

Valid Values

The bitwise representation has the following meaning:

- Bit 0
  - if ON, request LocationInformation
  - if OFF, do not request locationInformation
- Bit 1
  - if ON, request SubscriberState
  - if OFF, do not request SubscriberState
- Bit 2
  - if ON, reserved for extension container
  - if OFF, reserved for extension container
- Bit 3
  - if ON, request currentLocation
  - if OFF, do not request currentLocation
- Bit 4
  - if ON, request requestedDomain
  - if OFF, do not request requestedDomain
- Bit 5
  - if ON, request ms-classmark

  - if OFF, do not request ms-classmark
- Bit 6
  - if ON, request imei
  - if OFF, do not request imei
- Bit 7
  - if ON, request mnpRequestedInfo
  - if OFF, do not request mnpRequestedInfo
- Bit 8
  - if ON, Request t-adsData
  - if OFF, do not request t-adsData
- Bit 9
  - if ON, request requestedNodes
  - if OFF, do not request requestedNodes
- Bit 10
  - if ON, request servingNodeIndication
  - if OFF, do not request servingNodeIndication
- Bit 11
  - if ON, request locationInformationEPS-Supported
  - if OFF, do not request locationInformationEPS-Supported
- Bit 12
  - if ON, request localTimeZoneRequest
  - if OFF, do not request localTimeZoneRequest
- Bit 29 - This bit is only meaningful if requestedNodes is ON
  - if ON, mme (when requestedNodes bit is ON)
  - if OFF, sgsn (when requestedNodes bit is ON)
- Bit 30 - This bit is only meaningful if requestedDomain is ON
  - if ON, ps-Domain (when requestedDomain bit is ON)
  - if OFF, csDomain (when RequestedDomain bit is ON)

Default Value

1 - it means location information only.

19.2.2.345 rtrrequestinfobitsformapatiforrecip

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

This parameter specifies a bitstring with values to be requested in the MAP ATI Request for Recipient. The ATI RequestedInfo parameter is prepared based on this parameter.

Note:

1. The RTR will prepare the ATI request according to the bits selected by the operator. The RTR should ensure that in no way it creates an ATI request which is not as per specification.
2. In this `rtrrequestinfobitsformapatiforrecip` field the left-most bit is referred to as 'Bit 0'.

   Example 1: set parameter `rtrrequestinfobitsformapatiforrecip="1000000"`

   Here, the **leftmost-bit is '1'**,which represents the **locationinformation** field.

   It means this field is requested in map-Ati request.

   Example 2: set parameter `rtrrequestinfobitsformapatiforrecip="0111111"`

   Here, the **leftmost-bit is '0'**,which represents the **locationinformation** field.

   It means this field is not requested in map-Ati request.

Valid Values

The bitwise representation has the following meaning:

- Bit 0
  - if ON, request LocationInformation
  - if OFF, do not request locationInformation
- Bit 1
  - if ON, request SubscriberState
  - if OFF, do not request SubscriberState
- Bit 2
  - if ON, reserved for extension container
  - if OFF, reserved for extension container
- Bit 3
  - if ON, request currentLocation
  - if OFF, do not request currentLocation
- Bit 4
  - if ON, request requestedDomain
  - if OFF, do not request requestedDomain
- Bit 5
  - if ON, request ms-classmark

- if OFF, do not request ms-classmark

- Bit 6
  - if ON, request imei
  - if OFF, do not request imei
- Bit 7
  - if ON, request mnpRequestedInfo
  - if OFF, do not request mnpRequestedInfo
- Bit 8
  - if ON, Request t-adsData
  - if OFF, do not request t-adsData
- Bit 9
  - if ON, request requestedNodes
  - if OFF, do not request requestedNodes
- Bit 10
  - if ON, request servingNodeIndication
  - if OFF, do not request servingNodeIndication
- Bit 11
  - if ON, request locationInformationEPS-Supported
  - if OFF, do not request locationInformationEPS-Supported
- Bit 12
  - if ON, request localTimeZoneRequest
  - if OFF, do not request localTimeZoneRequest
- Bit 29 - This bit is only meaningful if requestedNodes is ON
  - if ON, mme (when requestedNodes bit is ON)
  - if OFF, sgsn (when requestedNodes bit is ON)
- Bit 30 - This bit is only meaningful if requestedDomain is ON
  - if ON, ps-Domain (when requestedDomain bit is ON)
  - if OFF, csDomain (when RequestedDomain bit is ON)

Default Value

1 - it means location information only.

19.2.2.346 rtrsetownnetandownctyforpcroutedmofsm

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

This parameter indicates whether for a PC Routed MOFSM with CgPA RI = SSN, the MSC country code and network should be determined using SCCP CgPA GTA address or set to the RTR's own country and network.

If set to false, the CgPA GTA Address will be used to determine the MSC country and network.

If set to true, the MSC country and network are assumed to be same as the RTR's own country and network.

Valid Values

- true
- false

Default Value

true

19.2.2.347 rtrskipsrismforunconditionalforwarding

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

This parameter indicates whether the SMSC shall skip the SRI-SM operation for original recipient and forward the message to the provisioned forward address for unconditional XS-FWD services.

In case this parameter value is false, the SRI-SM operation for original recipient is performed.

Valid Values

- true
- false

Default

false

19.2.2.348 rtrusedefaulttranslationtypeformoforwarding

Mandatory/Optional

Optional

Location

Common configuration file

Description
Option whether RTR uses the default translation type for forwarding of MO messages when no output translation type is specified by a GTT rule. Note that the default translation type is 0 for ITU/Japanese SS7 networks or 10 for ANSI networks. If the value is false, the actual translation type is used for forwarding of MO messages.

Valid Values

- true
- false

Default

true

19.2.2.349 rtruseprenormalizedtypeofnumberforroutingcondition

Mandatory/Optional

Optional

Location

Common configuration file

Description

Option whether RTR uses the pre-normalized type of number (TON) for the routing conditions. If the value is false, the normalized value is used.

Valid Values

- true
- false

Default Value

true

19.2.2.350 rtrusetransaddrforabbreviatednumberforfcdr

Mandatory/Optional

Optional

Location

Host/Common configuration file

Description

This parameter indicates whether the SMSC shall use the translated address for the abbreviated numbers in the FCDR fields origAddress and origAddressGSM. If true, SMSC uses the translated address. Otherwise, the untranslated address is used.

For Notification FCDR, the orglOrigAddress and orglOrigAddressGSM fields will be updated for the translated address for the abbreviated numbers.

Valid Values

- true
- false

Default Value

false

19.2.2.351 runtextpassprocess

Mandatory/Optional

Mandatory (for running the RTR)

Location

Host-specific configuration file

Description

Specifies if the RTR process should be started. Should be "true" for running the RTR.

Valid Values

- true
- false

19.2.2.352 sccpabortederrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.353 sccpdiscardudtwithownaddressincgpa

Mandatory/Optional

Optional

Location

Common configuration file

Description

Boolean specifying whether UDTs with own address in SCCP CGPA will be discarded. Default is 'true'.

19.2.2.354 sccpmaxpdulengthfortcapsegmentation

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Specifies the maximum number of bytes in a SCCP UDT PDU, beyond which TCAP-layer segmentation is applied. Note that a UDT PDU comprises of the SCCP header fields including the Called and Calling Party Addresses (which are of variable lengths), and the TCAP data field with a maximum allowed length of 255 bytes for ITU-T/Japanese SS7 or 252 bytes for ANSI.

In case an outgoing MO-FSM or MT-FSM message contains a SCCP PDU having length greater than the configured value of this parameter, or if it contains a TCAP data field having length greater than the maximum allowed value (see above), then RTR applies TCAP-layer segmentation on that outgoing message.

Note:

1. Once TCAP-layer segmentation is applied on a message, the resulting PDUs will not be subjected to the segmentation check again, irrespective of their lengths. Hence, the actual length of a SCCP PDU containing a segmented TCAP data field *may be* greater than the configured value of this parameter.
2. It is recommended not to set this parameter to a value higher than the default, for each SS7 flavour mentioned above.

Valid Values

0-268

Default

- 268 for ITU-T

- 266 for Japanese SS7
- 265 for ANSI

19.2.2.355 sccpoptimisedaddressing

Mandatory/Optional

Optional

Location

Host specific or common configuration file

Description

When the `sccpAlwaysUsePcSsnAddressing` object is set to 'true', this parameter has no effect.

This parameter is applicable only when the `sccpAlwaysUsePcSsnAddressing` object is set to 'false'.

When `sccpoptimisedaddressing` is set to 'true', which is the default, the SCCP calling party address in the UDT's output by TextPass depends on the routing indicator of the SCCP called party address.

- If this indicator is set to PC/SSN, TextPass will specify a routing indicator of PC/SSN for the SCCP calling party address of the SCCP calling party address. Furthermore, it will not include a GT address in the SCCP calling party address.
- When the indicator is GT or when optimised addressing is disabled, TextPass will use an SCCP calling party address as specified by the objects that make up the SCCP address of TextPass.

Valid Values

- true
- false

Default

true

19.2.2.356 sccppointcoderoutingfunctionsformofsm

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

This parameter indicates whether for a PC routed MO-FSM with CgPA RI = SSN, the SCCP CgPA GT address included in the MO-FSM Response or not.

If set to true then in the MO-FSM Response:

- MTP OPC is set to the RTR actual point code.
- SCCP CgPA RI is GT, GTA is set as RTR's specific GT.
- SCCP CdPA is same as SCCP CgPA of incoming MOFSM.
- MTP DPC is set to either MTP OPC or SCCP PC of the incoming MO-FSM based.

Note: If this parameter is set to true then parameters configuration of `sccpOptimisedAddressing` and `sccpAlwaysUsePcSsnAddressing` will not work. If set to false, then its configuration will work as per defined.

Valid Values

- true
- false

Default
false

19.2.2.357 sccptimerstatinfo

Mandatory/Optional

Optional

Location

Common configuration file

Description

Delay between requests for subsystem status information. Default 10 seconds.

19.2.2.358 sctstemplateforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the format for the service centre timestamp that is placed in a phase 1 status report. The service centre status report is assigned when a message is submitted to the RTR.

Valid Values

- %y: Year in two digits (04)
- %m: Month in two digits (01 for January, 10 for October)
- %d: Day in two digits (01 for first day of the month)
- %H: Hour in two digits (00 for midnight, 12 for noon)

- %M: Minute in two digits
- %S: Second in two digits
- %-y: Year in two digits (12) or one digit (1) without the leading zero
- %-m: Month in two digits (10 for October) or one digit (1 for January) without the leading zero
- %-d: Day in two digits (10 for tenth day of the month) or one digit (1 for first day of the month) without the leading zero
- %-H: Hour in two digits (12 for noon) or one digit (0 for midnight) without the leading zero
- %-M: Minute in two digits or one digit without the leading zero
- %-S: Second in two digits or one digit without the leading zero

Default

%d.%m.%y %H:%M:%S.

19.2.2.359 sendrfsmonsipregistration

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Specifies if RTR should send a 'Ready For SM' message to the HLR when the IPSM-GW indicates the RTR that the UE has performed a new registration. If set to true, RTR will first try to obtain the IMSI of the concerned subscriber by sending a SRI-SM Request. Upon receiving an IMSI, RTR will include the same in a 'Ready For SM' message that will be sent to the HLR. If set to false, or if an IMSI is not returned by the HLR, then RTR will not send a 'Ready For SM' message to the HLR.

Valid Values

- true
- false

Default

false

19.2.2.360 sendroutinginfoformsderegistered

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "MS DeRegistered Error" message on a SRI-SM operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.361 sendroutinginfoformspurged

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "MS Purged Error" message on a SRI-SM operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.362 sendroutinginfoforsmabsentsubscribererror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an "absent subscriber" error on a SRI-SM operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.363 sendroutinginfoforsmcallbarrederror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "call barred" error on a SRI-SM operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.364 sendroutinginfoforsmdatamissingerror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "data missing" error on a SRI-SM operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.365 sendroutinginfoforsmfacilitynotsupportederror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "facility not supported" error on a SRI-SM operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.366 sendroutinginfoforsmsccpaborted

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an "SCCP unit data service" message on a SRI-SM operation is considered a temporary or permanent error.

Valid Values

- temporary(0)

- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.367 sendroutinginfoforsmsystemfailureerror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "system failure" message on a SRI-SM operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.368 sendroutinginfoforsmtcapaborted

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "TCAP abort" message on a SRI-SM operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.369 sendroutinginfoforsmteleservicenotprovisionederror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a "teleservice not provisioned" message on a SRI-SM operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

permanent

19.2.2.370 sendroutinginfoforsmtimeout

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if a timeout on a SRI-SM operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.371 sendroutinginfoforsmunexpecteddatavalueerror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an "UnexpectedDataValue" message on a SRI-SM operation is considered a temporary or permanent error.

An "UnexpectedDataValue" error is a generic error that can be reported for MO, MT, and SRI-SM messages when there is some malformatting in the message. The MAP specification defines which error codes are applicable. In case repetitive occurrences of "UnexpectedDataValue" errors are received, contact NewNet support for further investigation of these errors.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

temporary

19.2.2.372 sendroutinginfoforsmunknownsubscribererror

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies if an "unknown subscriber" message on a SRI-SM operation is considered a temporary or permanent error.

Valid Values

- temporary(0)
- permanent(1) or permanentforrecipient(1)
- permanentformessage(2)

Default Value

permanent

19.2.2.373 servicekeyincameltrigger

Mandatory/Optional

Optional

Location

Common configuration file

Description

Value that the RTR should use for the Service Key parameter in CAMEL operations that are issued when an ECI application (e.g. PBC) does not provide a Service Key. When this parameter is not configured, the value defaults to 0.

Valid Values

0 - 0xffffffff

Default

0

19.2.2.374 setmwdfornopagingresponse

Mandatory/Optional

Optional

Location

Common configuration file

Description

Option to specify whether RTR should send a Report SM Delivery Status message to the HLR to set the MWD, in case it encounters an 'Absent Subscriber' error for a MT delivery attempt with the reason being 'No Paging Response'.

The corresponding SNMP attribute in `textpass-sms-mib.my` is `wsmsPropSetMwdForNoPagingError`.

Valid values:

- true (default)
- false

19.2.2.375 setsmdeliverynotintendedinhlrquerybeforerfsm

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Specifies whether RTR should include the optional parameter 'SM Delivery Not Intended' in the SRI-SM Request that it sends to the HLR upon receiving a SIP registration indication from the IPSM-GW. The purpose of this SRI-SM Request is to obtain the concerned subscriber's IMSI, which is required while sending the subsequent 'Ready For SM' message to the HLR.

If MAP Phase 2 is being used for sending the SRI-SM Request, then RTR ignores this parameter and does not include 'SM Delivery Not Intended' parameter.

Valid Values

- true
- false

Default

false

19.2.2.376 setsmdeliverynotintendedinorighlrquery

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Specifies whether RTR should include the optional parameter 'SM Delivery Not Intended' while sending an Originator HLR query for a MO message (for the purpose of MNP check or MO spoofing check). If MAP Phase 1 or Phase 2 is being used for sending the SRI-SM Request, then RTR ignores this parameter and does not include 'SM Delivery Not Intended'.

Valid Values

- true
- false

Default

false

19.2.2.377 sigencodingmismatchbehavior

Mandatory/Optional

Optional

Location

Common configuration file

Description

When a signature is provided for a message and the signature encoding varies from the message encoding, the RTR must choose whether to drop the signature or to try to convert the encoding. On conversion, any unknown characters will be replaced by a single question mark (`"?"`).

Valid Values

- drop
- convert

Default

convert

19.2.2.378 sigshortrecipientbehavior

Mandatory/Optional

Optional

Location

Common configuration file

Description

Defines the behavior when a signature is provided for a message for which the recipient is a short number. The signature can either be added or omitted.

Valid Values

- omitSignature
- addSignature

Default

omitSignature

19.2.2.379 simdownloadprocessingforconditionalforwarding

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying how short messages with a protocol ID equal to value for SIM Data Download (127) should be processed in case of conditional forwarding.

Note: This indicator specifies the behaviour when the delivery attempt to the original recipient has failed and the message needs to be forwarded to the forwarded address.

Possible values:

- pass
- blockwithtemporaryerror
- blockwithpermanenterror
- blockwithack (default)

19.2.2.380 simdownloadprocessingforunconditionalforwarding

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying how short messages with a protocol ID equal to value for SIM Data Download (127) should be processed in case of unconditional forwarding. Valid values:

- pass
- blockwithtemporaryerror
- blockwithpermanenterror
- blockwithack (default)

19.2.2.381 sipsmsbarringaction

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying the nature of SMS barring action that the RTR takes based on the result of the HSS query for messages originated from/to the SIP network. SMS barring functionality is supported for the short messages received by the IPSM-GW through:

- TRANSPORT LEVEL Interworking for SIPO messages.
- TRANSPORT and SERVICE LEVEL interworking for SIPT messages.

The default value is "noBarring", which implies that the RTR will not perform any HSS query for the purpose of SMS barring, and will not take any barring action.

Valid Values

- noBarring(0)
- sipoBarring(1)
- siptBarring(2)
- sipoSiptBarring(3)

Default

noBarring(0)

19.2.2.382 sipsmsbarringonerrorresponse

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the message should be barred by the RTR, when an error other than timeout and call barred is received from the HSS, in response to the query that was made for checking the SMS barring status. If set to false, the RTR will not take any barring action and will allow normal processing of the message upon receiving an error response from the HSS.

Valid Values

- true
- false

Default

false

19.2.2.383 sipsmsbarringonresponsetimeout

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether the message should be barred by the RTR in case a timeout occurs while waiting for a response to the HSS query, which was made for checking the SMS barring status. The above scenario may occur either due to the HSS response not being received by the IIW in time, or due to a timeout on the internal MIP interface before the IIW can send a response back to the RTR. If set to false, the RTR will not take any barring action and will allow normal processing of the message upon encountering a timeout while waiting for a response to the HSS query.

Valid Values

- true
- false

Default

false

19.2.2.384 smscaddressforhlroperations

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

E164 address that the RTR should use for the SMSC parameter in MAP operations to HLR. Default is the value of commonaddress or, if that attribute is not set, the RTR GT.

19.2.2.385 smscaddressformultisimhlrredirectionbypass

Mandatory/Optional

Optional

Location

Common configuration file

Description

SMSC address (0-15 digits) that the RTR will use in all SendRoutingInfoForSm and ReportSmDeliveryStatus communications between the RTR and HLR for AO-MT messages that are originated by an application with the **Multi SIM HLR Redirection Bypass** option selected. This attribute should be used in the common confguration file, not the host-specific file.

19.2.2.386 smschavenumberportabilitycheck

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether SMSCs have an MNP check.

Valid Values

- false: The RTR performs the MNP check (if allowmofromfriendlysubscribersonly is set to "true")
- true: The RTR does not check the originator when incoming MO traffic is routed to an SMSC

Default

false

19.2.2.387 snmpproplistenaddresstype

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

This parameter indicates whether SNMP Listener type is IPv4 only or Dual-stack.

Valid Values

- ipv4
- dual

Default Value

ipv4

19.2.2.388 srismfallbackonmsderegistered

Mandatory/Optional

Optional

Location

Common configuration file

Description

Option to specify whether RTR should attempt a fallback SRISM request in case the original SRISM request returned a NACK with MS Deregistered error.

Note: This parameter is relevant only if the option to send fallback SRISM requests is enabled through MGR ('Network' configuration).

Valid values:

- true
- false (default)

19.2.2.389 srismfallbackonmspurged

Mandatory/Optional

Optional

Location

Common configuration file

Description

Option to specify whether RTR should attempt a fallback SRISM request in case the original SRISM request returned a NACK with MS Purged error.

Note: This parameter is relevant only if the option to send fallback SRISM requests is enabled through MGR ('Network' configuration).

Valid values:

- true
- false (default)

19.2.2.390 sscfn1

Mandatory/Optional

Optional

Location

Common configuration file

Description

The number of PDUs sent during normal proving. Default 1000.

19.2.2.391 sscftimer1

Mandatory/Optional

Optional

Location

Common configuration file

Description

Time between the link release action and the next link re-establish action during alignment, expressed in milliseconds. Default 5 seconds.

19.2.2.392 sscftimer2

Mandatory/Optional

Optional

Location

Common configuration file

Description

Total time SSCF will attempt alignment, expressed in milliseconds. Default 120 seconds.

19.2.2.393 sscftimer3

Mandatory/Optional

Optional

Location

Common configuration file

Description

Time between proving PDUs, expressed in milliseconds. Default 100 milliseconds.

19.2.2.394 sscopmaxcc

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum value for the state variable VT (CC), corresponding to the maximum number of transmissions of a BGN, END, ER, or RS PDU. Default 4.

19.2.2.395 sscopmaxpd

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum acceptable value for the state variable VT(PD) before sending a POLL PDU and resetting VT(PD) to 0. This parameter is an upper limit for counter VT(PD) that sends a POLL PDU after every (MaxPD) SD PDUs. Default 500.

19.2.2.396 sscoptimercc

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer_CC, expressed in milliseconds. Default 200 milliseconds.

19.2.2.397 sscoptimeridle

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer_IDLE, expressed in milliseconds. Default 100 milliseconds.

19.2.2.398 sscoptimerkeepalive

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer_KEEP-ALIVE, expressed in milliseconds. Default 100 milliseconds.

19.2.2.399 sscoptimernoresponse

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer_NO-RESPONSE, expressed in milliseconds. Default 1500 milliseconds.

19.2.2.400 sscoptimerpoll

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer_POLL, expressed in milliseconds. Default 100 milliseconds.

19.2.2.401 ssiqueriesenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying whether Service Subscription Information (SSI) queries will be attempted. Valid values are:

- true
- false

The default value follows the value of the *Subscriber Subscription Info* license setting.

19.2.2.402 statusreportenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies whether GSM status reports should be enabled.

Valid Values

- true
- false

Default

false

19.2.2.403 statusreportprocessingforconditionalforwarding

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying how status reports should be processed in case of conditional forwarding.

Note: This indicator specifies the behaviour when the delivery attempt to the original recipient has failed and the status report needs to be forwarded to the forwarded address.

Valid values:

- pass
- blockwithtemporaryerror
- blockwithpermanenterror
- blockwithack (default)

19.2.2.404 statusreportprocessingforunconditionalforwarding

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying how status reports should be processed in case of unconditional forwarding.

Valid Values

- pass
- blockwithtemporaryerror
- blockwithpermanenterror
- blockwithack

Default

blockwithack

19.2.2.405 statusreportretryinterval

Mandatory/Optional

Optional

Location

Common configuration file

Description

Interval between two consecutive retries for an MT status report, expressed in seconds. Default 60.

19.2.2.406 storagefailureerrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.407 strippaddingfromgsm0340address

Mandatory/Optional

Optional

Location

Common configuration file

Description

Attribute to indicate whether a `0xf` nibble is allowed to indicate an odd number of digits in a GSM 03.40 address.

In other words, if the RTR receives a non-alphanumeric number with an even number of nibbles and with a terminal nibble of `0xf`, this nibble will be stripped and the address will be adjusted to represent an odd number of decimal digits.

Valid Values

- false
- true

Default

false

19.2.2.408 subscriberbusyformterrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description
Error string specifying that an SM has failed to be delivered due to a subscriber busy for MT/SM error. Setting this error string only makes sense when `mtforwardsmsubscriberbusyformtsmserror` is set to '`permanentforrecipient`' or '`permanentformessage`'.

Valid Values

Max. 160 character string.

Default Value

```
Subscriber busy for MT/SM (code 31)
```

19.2.2.409 systemfailureerrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.410 tcapabortederrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.411 tcapmaxapplicationguardtime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer defining maximum time span allowed between receiving Invoke and response from higher layer for Invoke. Expressed in units of seconds.

If the time taken to respond on the message is longer than this timeout value:

1. A syslog warning will be generated.
2. The counter `tcapApplicationGuardTimerExpiredCounter` will be incremented.

Note: On expiry of the Application Guard timer, the message is not discarded or failed.

Valid Values

1 - 100 (value in seconds)

Default

30 seconds

19.2.2.412 tcapmaxlongresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer for long MAP operations defining maximum time span allowed between a TCAP request message (TC-BEGIN, TC-CONTINUE) and a TCAP response (TC-END, TC-CONTINUE), expressed in seconds. This timer applies to the MAP MtForwardSm operation.

The value of this timer will be applicable when:

1. No network is configured for the recipient or
2. Value of the **MTFSM max response time** field for the recipient network is configured to 0 (default value).

Valid Values

1 - 100 seconds

Default

30 seconds

19.2.2.413 tcapmaxnegotiationestablishresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer defining maximum time span allowed between a TC-Begin sent by RTR without component to initiate a Dialogue and subsequent TC-Continue received without component on the same TCAP session, expressed in units of seconds.

Valid Values

1 - 100 (value in seconds)

Default

5 seconds

19.2.2.414 tcapmaxnextmessagewaitingresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer defining maximum time span allowed between a TC-CONTINUE sent and subsequent TC-Continue received on the same TCAP session, expressed in units of seconds. This timer is applicable only for the scenario where RTR is a TCAP transaction receiver.

Valid Values

1 - 100 (value in seconds)

Default

5 seconds

19.2.2.415 tcapmaxreportsmresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer for Report SM Delivery Status operation defining maximum time span allowed between a 'Report SM delivery status' request from the RTR and its response, expressed in units of seconds.

The default value is 0, which indicates that the system-wide timer value *tcapmaxresponsetime* will be used.

Valid Values

0 - 100 (value in seconds)

Default

0 seconds

19.2.2.416 tcapmaxresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer for regular MAP operations defining maximum time span allowed between a TCAP request message (TC-BEGIN, TC-CONTINUE) and a TCAP response (TC-END, TC-CONTINUE), expressed in seconds. This timer applies to any MAP operation other than MtForwardSm.

If the following timers are configured with a non-zero value, then they override the `tcapmaxreponsetime` value:

1. *tcapmaxsrismresponsetime*
2. *tcapmaxreportsmresponsetime*

Note: If the value of the semi-static parameter *tcapmaxresponsetime* is changed from its default value of 5 seconds, consider changing the values of the semi-static parameters *tcapmaxnegotiationestablishresponsetime* and *tcapmaxnextmessagewaitingresponsetime* as well.

Valid Values

1 - 100 (value in seconds)

Default

5 seconds

19.2.2.417 tcapmaxsrismresponsetime

Mandatory/Optional

Optional

Location

Common configuration file

Description

Timer for SRISM operation defining the maximum time span allowed between a SRISM Request from the RTR and its Response. This value is expressed in seconds.

The default value is 0, which indicates that the system-wide timer value *tcapmaxresponsetime* will be used.

Valid Values

0 - 100 (value in seconds)

Default

0 seconds

19.2.2.418 tcaprandomidgeneration

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies which algorithm will be used for generating the TCAP originating transaction id. If the value is true, a random value of the TCAP transaction id will be generated, else incremental value of TCAP transaction id will be generated.

Valid Values

- False: incremental value of TCAP transaction id will be generated
- True: random value of the TCAP transaction id will be generated

Default

False

19.2.2.419 tcaprelaytccontinueonvpc

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies how the FWL should handle a TC-CONTINUE that it receives on a VPC (only supported for an ITU-T SS7 stack)

Valid Values

- false: Pass TC-CONTINUE to the MAP layer for further processing
- true: Derive the TC-CONTINUE destination
  - If the destination is the FWL, the FWL treats the TC-CONTINUE as if it were received on that PC
  - If the destination is another firewall, the FWL relays the TC-CONTINUE to that firewall (if an MTP destination exists for it)

Default

false

19.2.2.420 teleservicenotprovisionederrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.421 throughputcontrolmaxdelay

Mandatory/Optional

Optional

Location

Common configuration file

Description

Maximum delay between receiving an AO message from an application and returning the ACK to the application. The throughput control mechanism takes this threshold into account. When this mechanism detects that the delay as result of throughput control exceeds the threshold, the message is NACKed. Default 3 seconds.

19.2.2.422 timeouterrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.423 ttusedfororiginatorimsiretrieval

Mandatory/Optional

Optional

Location

Common configuration file

Description

The Translation Type (TT) value to be used in the SCCP Called Party Address of the SRI-SM operation that retrieves the originator IMSI.

Valid Values

0 - 255

Default

- 0 for ITU-T
- 0 for Japanese SS7
- 14 for ANSI

19.2.2.424 ttwhenincludingmscaddrinmofwdsmtosmsc

Mandatory/Optional

Optional

Location

Common configuration file

Description

Value for the TT when the MSC address is included in the SCCP CGPA of an MoForwardSm operation toward an SMSC.

Default

- 0 for ITU-T
- 0 for Japanese SS7
- 14 for ANSI

19.2.2.425 unexpecteddatavalueerrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.426 unidentifiedsubscribererrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.427 unknownsubscribererrorstringforphase1statusreport

Mandatory/Optional

Optional

Location

Common configuration file

Description

String returned in error message for corresponding error.

19.2.2.428 useaddressformattingforatnotifications

Mandatory/Optional

Optional

Location

Common configuration file

Description

For AT Notifications, generated or non-transparently AT-AT forwarded by the RTR, this attribute specifies if the address format specified for originator, recipient, MSC and SMSC by the application (or the corresponding system-wide setting) shall be considered or not.

Note: UCP 57 and UCP 58 messages are not affected by the setting of this attribute.

When enabled ("true"), the following attributes will be used to determine the formatting of the addresses in an AT notification.

Application settings configured through the MGR (**SMS Applications ➤ Applications**):

- **Format Originator**
- **Format Recipient**
- **Format MSC**
- **Format SMSC**

or, the system-wide attributes configured in the common configuration file:

- `atoriginatorformat`
- `atrecipientformat`
- `atmscformat`
- `atsmscformat`

When disabled ("false"), address formatting configuration mentioned above (application setting configuration and system-wide attributes) do not affect the format of the addresses in the notification message.

For example, when disabled ("false"), '**Format Originator**' and '`atoriginatorformat`' do not affect the format of the originator address in the notification message.

Valid Values

- true
- false

Default

false

19.2.2.429 useapplicationccdrgroupid

Mandatory/Optional

Optional

Location

Host-specific configuration file

Description
Indicates whether to use the **CCDR Group ID** configured for an application on the MGR while generating Comverse CDR records corresponding to messages originated from or destined to the application. If set to 'true', then the CCDR Group ID configured for the application will be used while generating the relevant CCDR records.

Valid Values

- true
- false

Default

false

19.2.2.430 useincomingservicecentreaddressfordelivery

Mandatory/Optional

Optional

Location

Common configuration file

Description

This attribute specifies whether to use the Service Center address of incoming messages in the corresponding outgoing MTForwardSm and Status-Report messages. This applies to both phase 1 status reports and regular phase 2+ status reports.

If a VSMSC address is used, this attribute has no effect.

If the SMSC address is supposed to be modified by an MTO Modifier, that modification takes precedence over this setting.

Valid Values

- true
- false

Default

false

19.2.2.431 usemapaddressformocdpa

Mandatory/Optional

Optional

Location

Common configuration file

Description

When set to true, the SCCP called party address of MOForwardSM messages towards the SMSC is taken from the MAP layer SMSC address rather than from the configured SCCP address of the selected SMSC entry.

Valid Values

- true
- false

Default

false

19.2.2.432 virtualpointcode

Mandatory/Optional

Mandatory

Location

Common configuration file

Description

Virtual point code of a RTR, used to address a group of RTRs. See `pointcode`.

19.2.2.433 whitelistofaorecipientforhlrquerybeforeapproval

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list with conditions that should be matched with the recipient MSISDN of an inbound AO message. If a list is specified and the corresponding list is provisioned, the `hlrqueryforrecipientofaobeforeapproval` attribute is ignored. If there is a match, the RTR issues an HLR query before evaluating the AOX rules. If a list is not specified or the specified list does not match a provisioned list, the RTR uses the `hlrqueryforrecipientofaobeforeapproval` attribute, independent of the AO message's recipient address.

19.2.2.434 whitelistofigmrecipientforhlrquerybeforeapproval

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list with conditions that should be matched with the recipient MSISDN of an Internally Generated Message (IGM).

If a name is specified, and the corresponding list is provisioned, the setting of *hlrqueryforrecipientofigmbeforeapproval* is ignored. If there is a match, the RTR will issue an HLR query before evaluating the external condition rules for internally generated messages (IGMX rules).

If a name is not specified (default) or does not match with a provisioned condition list, *hlrqueryforrecipientofigmbeforeapproval* is used to control the behavior of the RTR, independent of the IGM's recipient address.

Valid Values

String (0-31 characters)

Default

None

19.2.2.435 whitelistofmomscforspoofchecksuppression

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list of MSC GTs that should be matched against the originator of an MO message. If there is match, the FWL does not perform an MO spoofing check for the message.

19.2.2.436 whitelistofmorecipientforhlrquerybeforeapproval

Mandatory/Optional

Optional

Location

Common configuration file

Description

Name of a list with conditions that should be matched with the recipient MSISDN of an inbound MO message. If a list is specified and the corresponding list is provisioned, `hlrqueryforrecipientbeforeapproval` is ignored. If there is a match, the RTR issues an HLR query before evaluating the MOX rules. If a list is not specified or the specified list does not match a provisioned list, the RTR uses `hlrqueryforrecipientbeforeapproval`, independent of the MO message's recipient address.

19.2.2.437 x121countrycode

Mandatory/Optional

Optional

Location

Common configuration file

Description
X.121 country code for country in which the RTR operates.

Valid Values

X.121 address

Default

204

19.2.2.438 x121nationalprefix

Mandatory/Optional

Optional

Location

Common configuration file

Description

X.121 national prefix as used in country in which the RTR operates. Typically equal to 0.

Valid Values

X.121 address

Default

0

19.2.2.439 rtrdefaultdomainselection

Mandatory/Optional

Optional

Location

Common configuration file

Description

Default domain selection for messages originating from SS7 network, if domain is not received from ECI app or configured in MTOR.

Valid Values

- legacy
- imsdomain
- imsthenss7domain
- ss7domain

Default

legacy

19.2.2.440 rtranytimemodificationonhssfailureenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying whether TextPass should send the deactivate modification instruction for IPSM-GW in a anyTimeModification message to the HLR upon HSS failure. The default value is false.

Valid Values

- true
- false

Default

false

19.2.2.441 rtranytimemodificationonsipfailureenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicator specifying whether TextPass should send the deactivate modification instruction for IPSM-GW in a anyTimeModification message to the HLR upon SIP failure. The default value is false.

Valid Values

- true
- false

Default

false

19.2.2.442 rtrdeliverconcatmessagetorcs

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicates whether RTR shall force SS7 delivery of concatenated messages regardless of whether recipient domain in RCS or deliver concatenated messages to RCS if recipient domain is RCS. Default value is false.

Valid Values

- true
- false

Default

false

19.2.2.443 rtr4gdeliverymode

Mandatory/Optional

Optional

Location

Common configuration file

Description

Indicates whether RTR shall deliver messages to 4G network via Transport Level Interworking (SMSoIP) or via Service Level Interworking (currently RCS). Default value is SMSoIP.

Valid Values

- smsoip
- rcs

Default

smsoip

19.2.2.444 rtrdefaultdomainfor4goriginatedmessage

Mandatory/Optional

Optional

Location

Common configuration file

Description

Default domain selection for messages originating from 4G network, if domain is not received from ECI app or configured in MTOR. Default value is legacy Note: This parameter is applicable only for messages received from 4G network. For messages originated from SS7 network, smsMtoPropDefaultDomainSelection will be applicable..

Valid Values

- legacy
- ss7Domain

Default

legacy

19.2.2.445 rtrsipauthenticationtokena

Mandatory/Optional

Optional

Location

Common configuration file

Description

When receiving a SIP originated message in transport mode per MESSAGE method the IIW will communicate an extra MXP field to the RTR. This MXP field will contain the word 'Route:' followed by the contents of all SIP Route header fields in the SIP message, separated by commas.

If rtrsipauthenticationtokena case-insensitively matches a part of the collated Route: header, the Router will reject the SIP message with an SS7 negative acknowledgement, Facility Not Supported.

Valid Values

- An ASCII string
- The empty string (it never matches)

Default

The empty string

19.2.2.446 rtrsipauthenticationtokenb

Mandatory/Optional

Optional

Location

Common configuration file

Description

When receiving a SIP originated message in transport mode per MESSAGE method the IIW will communicate an extra MXP field to the RTR. This MXP field will contain the word 'Route:' followed by the contents of all SIP Route header fields in the SIP message, separated by commas.

If rtrsipauthenticationtokenb case-insensitively matches a part of the collated Route: header, the Router will reject the SIP message with an SS7 negative acknowledgement, Facility Not Supported.

Valid Values

- An ASCII string
- The empty string (it never matches)

Default

The empty string

19.2.2.447 snmppropalarmownipaddress

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

The IPv4 address of the TextPass node. If set, this address will be used as source address for sending SNMP traps. This parameter is used to populate Trap Agent address for IPv4/IPv6 address. If this parameter is not set, then the IPv4 address of first network interface is used to populate Trap Agent Address in SNMP Traps.

Valid Value
IPv4 address

Default

Empty string

19.2.2.448 snmppropalarmownipv6address

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

The IPv6 address or hostname of the TextPass node. If set, this address will be used as source address for sending SNMP traps.

Valid Values

IPv6 address or hostname(maximum length can be of 255 characters)

Default

Empty string

19.2.2.449 snmpproplistenaddresstype

Mandatory/Optional

Optional

Location

Common/Host configuration file

Description

This parameter indicates whether SNMP Listener type is IPv4 only or Dual-stack.

Valid Values

ipv4 or dual

Default

ipv4

19.2.3 destination Entity

This section describes the `destination` attributes.

Located in the host-specific or common configuration file.

19.2.3.1 name

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Name of the MTP destination.

19.2.3.2 type

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Type of MTP destination.

Valid Values

- stp
- msc
- hlr
- smsc
- relay
- monitoredsmsc

19.2.3.3 pointcode

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Point code of the MTP destination. Valid formats:

- Decimal (for example, 2232)
- x.y.z, where x is the area, y is the cluster, and z is the member (for example, 7.124.6)

Valid ranges:

- Decimal
  - ANSI 65536-16777215
  - ITU-T 0-16383
  - Japanese SS7 0 - 65535
- Area
  - ANSI 1-255
  - ITU-T 0-7
  - Japanese SS7 0-31
- Cluster
  - ANSI 0-255
  - ITU-T 0-255
  - Japanese SS7 0-15
- Member
  - ANSI 0-255
  - ITU-T 0-7

- Japanese SS7 0-127

19.2.3.4 throughput

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Maximum throughput (in MSUs per second) for the destination, excluding MSUs for MTP management and MTP testing and maintenance.

19.2.3.5 stppriorirty

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Priority of the STP. The RTR will always select the STP with the highest priority. Only applies if the `type` is "stp".

19.2.3.6 stpthroughput

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Maximum throughput (in UDTs and UDTSs per second) for the STP, excluding the UDTs for SCCP management. Only applies if the `type` is "stp".

19.2.3.7 stpweight

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Weight of the STP. When more than one STP of the highest priority are available, the RTR will perform load sharing based on the STPs' weight. The higher the weight, the higher the load. Only applies if the `type` is "stp".

19.2.4 route Entity

This section describes the `route` attributes. This is a subordinate of the `destination` entity.

Located in the host-specific or common configuration file.

19.2.4.1 m3uasgp

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Name of M3UA SGP (signalling gateway process) entity. This attribute is mutually exclusive with the `linkset` and `m3uaas` attributes.

19.2.4.2 m3uaas

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Name of M3UA AS (Application Server) entity that the route uses. Only modify-able if the entry's administrative state is 'inactive'. This attribute is mutually exclusive with the `linkset` and `m3uasgp` attributes.

19.2.4.3 priority

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Priority of the route. The RTR will always select the route with highest priority.

19.2.4.4 throughput

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Maximum throughput (in MSUs per second) for the route, excluding the MSUs for MTP management and MTP testing and maintenance.

19.2.4.5 weight

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Weight of the route. When more than one route of the highest priority are available, the RTR will perform load sharing based on the routes' weight. The higher the weight, the higher the load.

19.2.5 m3ualocaladdress Entity

This section describes the `m3ualocaladdress` attributes.

Located in the host-specific configuration file.

19.2.5.1 spec

Mandatory/Optional

Mandatory

Location

Host-specific configuration file

Description

Specifies the local IP address for M3UA.

19.2.6 remoteaddress Entity

This section describes the `remoteaddress` attributes. This is a subordinate of the `m3uasgp` and `m3uaasp` entities.

Located in the host-specific or common configuration file.

19.2.6.1 spec

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

When configured as part of `m3uasgp`, it specifies the IP address of the remote M3UA SGP.

When configured as part of `m3uaasp`, it specifies the IP address of the remote M3UA ASP .

19.2.7 m3uasgp Entity

This section describes the `m3uasgp` attributes.

Located in the host-specific or common configuration file.

19.2.7.1 name

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Name of the M3UA SGP (signalling gateway process).

19.2.7.2 fillinaspidentifierfield

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Specifies whether the ASP identifier should be specified in messages toward M3UA SGP.

Valid Values

- true
- false

Default

true

19.2.7.3 fillinnetworkappearancefield

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Boolean specifying whether network appearance should be specified in messages towards M3UA SGP.

Valid Values

- true
- false

Default

false

19.2.7.4 fillinroutingcontextfield

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Boolean specifying whether routing context should be specified in messages towards M3UA SGP.

Valid Values

- true
- false

Default

true

19.2.7.5 trafficmodefield

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Traffic mode that will be advertised to the SGP.

Valid Values

- unconfigured (no `trafficmode` field will be included in the request to the SGP)
- override
- loadshare
- broadcast

Default

unconfigured

19.2.7.6 useforpointcode

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Specifies whether M3UA SGP is used for traffic from/to the specific point code of the RTR.

Valid Values

- true
- false

Default

true

19.2.7.7 useforvirtualpointcode

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Specifies M3UA SGP is used for traffic to the virtual point code of the RTR.

Valid Values

- true
- false

Default

true

19.2.7.8 sctplocalport

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

SCTP port used on the RTR end for SCTP association with M3UA SGP. Valid values: 0-65535 (default 2905).

19.2.7.9 sctplocalsendport

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Local SCTP port for the outgoing SCTP association that the RTR maintains with the remote M3UA SGP. Valid values: 0-65535 (default 0; port is chosen by the system).

19.2.7.10 sctpmaxinboundpdusize

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Maximum PDU size for messages from M3UA SGP. Valid values: 0-8108 (default 1500).

19.2.7.11 sctpmaxoutboundpdusize

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Maximum PDU size for messages toward M3UA SGP. Valid values: 0-8108 (default 1500).

19.2.7.12 sctpremoteport

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

SCTP port used on the M3UA SGP end for SCTP association with M3UA SGP. Valid values: 0-65535 (default 2905).

19.2.7.13 sctpremotesendport

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Remote SCTP port for the incoming SCTP association that the RTR maintains with the remote M3UA SGP. Valid values: 0-65535 (default 0).

19.2.7.14 sctptimerheartbeat

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for SCTP heartbeat timer, expressed in milliseconds. Valid values: 100-30000 (default 1000).

19.2.7.15 initiatingstartupenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies that the RTR should initiate the start of SCTP association.

Valid Values

- true
- false

Default

true

19.2.7.16 sctpmaxallowedinboundstreams

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Maximum allowed number of inbound streams on SCTP association with M3UA SGP. Valid values: 1-255 (default 255).

19.2.7.17 sctpmaxassociationretransmits

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for SCTP parameter that governs the maximum number of retransmits for an association. Valid values: 5-65535 (default 20).

19.2.7.18 sctpmaxconnectattempts

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for SCTP parameter that governs how many times connect attempts are made and thus how many SCTP INIT messages are sent. Valid values: 8-65535 (default 8).

19.2.7.19 sctpmaxpathretransmits

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for SCTP parameter that governs the maximum number of retransmits for a path. Valid values: 5-65535 (default 15).

19.2.7.20 sctpmaxretransmittimeout

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for SCTP timer RTO.max, expressed in milliseconds. Valid values: 1000-30000 (default 2000).

19.2.7.21 sctppreferredoutboundstreams

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Preferred number of outbound streams on SCTP association with M3UA SGP. Valid values: 1-255 (default 2).

19.2.7.22 sctprecvbuffer

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Requested size of the local recv buffer (in bytes). Valid values: 0-2147483647 (default 0, use the operating system default). The operating system may have a maximum size, which cannot be exceeded without changing system-wide settings.

19.2.7.23 sctprecvlowat

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Requested low water mark of the local receive buffer (in bytes). This value must be lower than the receive buffer size. Usually a value between 10% and 25% is recommended. Valid values: 0-2147483647 (default 0, use the operating system default).

19.2.7.24 sctpsendbuffer

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Requested size of the local send buffer in bytes. Valid values: 0-2147483647 (default 0, use the operating system default). The operating system may have a maximum size, which cannot be exceeded without changing system-wide settings.

19.2.7.25 sctpsendlowat

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Requested low water mark of the local send buffer (in bytes).This value must be lower than the send buffer size. Usually a value between 10% and 25% is recommended. Valid values: 0-2147483647 (default 0, use the operating system default).

19.2.7.26 sctpnodelay

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Specifies the setting of the NO DELAY flag and enables or disables the Nagle algorithm. The Nagle algorithm may reduce the network load on high-latency, low-throughput connections by delaying and bundling small messages into one network packet. The messages are only delayed until the acknowledgement of the previous packet is received (or until a full packet can be sent). Disabling the Nagle algorithm may reduce latency, at the expense of an increased network load. However, disabling the Nagle algorithm does not guarantee that no bundling is performed.

Valid Values

- true (do not use Nagle algorithm)
- false (use Nagle algorithm)

Default

false

19.2.7.27 sctpsackdelay

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

The SCTP SACK delay ranges from 0 to 3000 (default 0, use the operating system default). Whenever possible, the system default settings should be used (that is, this attribute should be absent).

19.2.8 m3uaas Entity

This section describes the remote M3UA Application Server attributes.

Located in the host-specific or common configuration file.

19.2.8.1 name

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Name of the M3UA AS (application server).

19.2.8.2 routingcontext

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Routing context associated with remote M3UA AS.

Valid Values

0..4294967295

Default Value

0

19.2.9 m3uaasp Entity

This section describes the m3uaasp attributes. This is a subordinate of the m3uaas entity. For each m3uaas entity there can be up to 16 m3uaasp entities.

Located in the host-specific or common configuration file.

19.2.9.1 name

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Name of the M3UA ASP (application server process).

19.2.9.2 fillinnetworkappearancefield

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Boolean specifying whether the RTR includes network appearance in messages towards an M3UA ASP.

When it is set to 'true', the field is always specified. When it is set to 'false', the field is never specified.

Valid Values

- true
- false

Default Value

false

19.2.9.3 sctplocalport

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
SCTP port used on the RTR end for SCTP association with remote M3UA ASP.

Valid Values
0 - 65535

Default Value

2905

19.2.9.4 sctpremoteport

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
SCTP port used on the remote M3UA ASP end for SCTP association with M3UA SGP.

Valid Values
0 - 65535

Default Value

2905

19.2.9.5 sctpmaxoutboundpdusize

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Maximum outbound PDU size for the SCTP association that RTR maintains with the remote M3UA ASP.

Valid Values
0 - 8108

Default Value

1500

19.2.9.6 sctpmaxinboundpdusize

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Maximum inbound PDU size for the SCTP association that RTR maintains with the remote M3UA ASP.

Valid Values
0 - 8108

Default Value

1500

19.2.9.7 sctptimerheartbeat

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Value for SCTP heartbeat timer, expressed in milliseconds.

Valid Values
100 - 30000

Default Value

1000

19.2.9.8 initiatingstartupenabled

Mandatory/Optional

Optional

Location

Common configuration file

Description
Specifies whether RTR should initiate establishment of SCTP association. When set to 'true', RTR actively tries to establish the association by sending out INIT chunks and responding with INIT ACK chunks when receiving INIT chunks. When set to 'false', RTR has a passive role, meaning that it will only respond to inbound INIT chunks.

Valid Values

- true
- false

Default Value

false

19.2.9.9 sctpmaxretransmittimeout

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Value for SCTP timer RTO.max, expressed in milliseconds.

Valid Values
1000 - 30000

Default Value

2000

19.2.9.10 sctpmaxpathretransmits

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Value for SCTP parameter that governs the maximum number of retransmits for a path.

Valid Values
5 - 65535

Default Value

15

19.2.9.11 sctpmaxassociationretransmits

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Value for SCTP parameter that governs the maximum number of retransmits (Association.Max.Retrans) for an association.

Valid Values
5 - 65535

Default Value

20

19.2.9.12 sctpmaxconnectattempts

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Value for SCTP parameter that governs how many times connect attempts are made and thus how many SCTP INIT messages are sent (Max.Init.Retransmits).

Valid Values
8 - 65535

Default Value

8

19.2.9.13 sctpmaxallowedinboundstreams

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Maximum allowed number of inbound streams on SCTP association with remote M3UA ASP.

Valid Values
1 - 255

Default Value

255

19.2.9.14 sctppreferredoutboundstreams

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Preferred number of outbound streams on SCTP association with remote M3UA ASP.

Valid Values
1 - 255

Default Value

2

19.2.9.15 sctpsackdelay

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description
Time (in ms) to wait before acknowledging SCTP DATA chunks. Whenever possible, the system default settings should be used (that is, this attribute should be absent). A value of 0 (default) means use the system default, which tends to be 200ms.

Valid Values
0 - 3000

Default Value

0

19.2.10 gttrule Entity

This section describes the `gttrule` attributes.

Located in the host-specific or common configuration file.

19.2.10.1 inputgtaddressinfo

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Value that should match the global title address information in the input.

Valid Values

- In case of an exact-matching rule, one or more digits.
- In case of a wildcard rule, zero or more digits followed by an asterisk.

19.2.10.2 inputgtnatureofaddressind

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value that should match the nature of address indicator in the input.

Valid Values

- unknown
- subscribernumber
- reservedfornationaluse
- nationalsignificantnumber
- internationalnumber

Default

internationalnumber

19.2.10.3 inputgtnumberingplan

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value that should match the Numbering Plan in the input. If not specified, any Numbering Plan value satisfies.

Valid Values

- unknown
- isdnTelephone
- generic
- data

- telex
- maritime
- landMobile
- isdnMobile
- private

19.2.10.4 inputgttranslationtype

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value that should match the translation type in the input. Valid values: 0-255

19.2.10.5 inputsubsystemnumber

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value that should match the subsystem number in the input. Valid values: 0-255

19.2.10.6 outputgtaddressinfo

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for global title address information that is specified in output when rule matches. For example, if `inputgtaddressinfo` is 31653*, `outputgtaddressinfo` is 0653*, and the global title address information in the input is 31653131313, then the global title address info in the output will be 0653131313.

For wildcard rules, the value can be zero or more digits followed by an asterisk. The value for global title address information in the output will then specify the digits within `outputgtaddressinfo`, followed by the digits in the input that are caught by the asterisk in `inputgtaddressinfo`.

19.2.10.7 outputgtindicator

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for global title indicator that is specified in output when rule matches. If outputroutingindicator is "gt", the valid values are 4(for ITU-T and Japanese SS7 systems) and 2 (for ANSI systems). Otherwise, 0 and 4 are valid values for ITU-T/Japanese SS7 (default 4), and 0 and 2 are valid values for ANSI (default 2).

19.2.10.8 outputgtnatureofaddressind

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for nature of address indicator that is specified in output when rule matches This attribute only applies when outputgtindicator is 4.

Valid Values

- unknown
- subscriberNumber
- reservedForNationalUse
- nationalSignificantNumber
- internationalNumber

19.2.10.9 outputgtnumberingplan

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for Numbering Plan that is specified in output when rule matches. If not specified, defaults to value as set in input.

Valid Values

- unknown
- isdnTelephone
- generic
- data
- telex
- maritime
- landMobile
- isdnMobile
- private

19.2.10.10 outputgttranslationtype

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for translation type that is specified in output when rule matches. This attribute only applies when `outputgtindicator` is 4.

19.2.10.11 outputloadshareset

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Name of the load share set of output MTP destinations. An outgoing UDT is sent to one of the MTP destinations in the load share set, as specified for the load share set member. The MTP destination is selected by load sharing mechanism.

Note that this attribute is mutually exclusive to both *outputmtpdestination* and *outputpointcode* attributes.

19.2.10.12 outputmtpdestination

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Name of MTP destination to which UDT is sent. By default, UDT is sent to the STPs.

Note that this attribute and the *outputloadshareset* attribute are mutually exclusive.

19.2.10.13 outputnationalusebit

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Specifies the value for national use bit that is specified in output when rule matches.

Valid Values

- true
- false

Default

false

19.2.10.14 outputpointcode

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for point code that is specified in output when rule matches. For SRI-SM to HLR traffic, please use *outputmtpdestination*. If not specified, point code is not included in output.

Note that this attribute and the *outputloadshareset* attribute are mutually exclusive.

Valid formats:

- Decimal (for example, 2232)
- `x.y.z`, where `x` is the area, `y` is the cluster, and `z` is the member (for example, 7.124.6)

Valid ranges:

- Decimal: ANSI 65536-16777215, ITU-T 0-16383, and Japanese SS7 0 - 65535
- Area: ANSI 1-255, ITU-T 0-7, and Japanese SS7 0-31
- Cluster: ANSI 0-255, ITU-T 0-255, and Japanese SS7 0-15
- Member: ANSI 0-255, ITU-T 0-7, and Japanese SS7 0-127

19.2.10.15 outputroutingindicator

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for routing indicator that is specified in output when rule matches.

Valid Values

- gt (route on global title)
- ssn (route on subsystem number)

Default

gt

19.2.10.16 outputsubsystemnumber

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

Value for subsystem number that is specified in output when rule matches. Valid values: 0-255.

19.2.11 trapreceiver Entity

This section describes the `trapreceiver` attributes.

Located in the host-specific or common configuration file.

19.2.11.1 ipaddress

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

IP address (IPv4 or IPv6) or Hostname of the trap receiver.

19.2.11.2 udpport

Mandatory/Optional

Optional

Location

Host-specific or Common configuration file

Description

UDP port on the trap receiver to which traps are sent.

19.2.12 whitelist Entity

This section describes the `whitelist` attributes. This is a subordinate of the `trapreceiver` entity.

Located in the host-specific or common configuration file.

19.2.12.1 whitelistindex1

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Index of entry in table containing information of alarm stations. This index is actually a reference to the related alarm station. Its value its equal to the index of the alarm station entry.

19.2.12.2 whitelistindex2

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Index of entry in table containing info of whitelist items.

19.2.12.3 whitelistsubsystem

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Object identifier for the subsystem on whitelist entry.

19.2.12.4 whitelisttype

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Type of trap inside the subsystem.

19.2.13 blacklist Entity

This section describes the `blacklist` attributes. This is a subordinate of the `trapreceiver` entity.

Located in the host-specific or common configuration file.

19.2.13.1 blacklistindex1

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Index of entry in table containing information of alarm stations. This index is actually a reference to the related alarm station. Its value its equal to the index of the alarm station entry.

19.2.13.2 blacklistindex2

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Index of entry in table containing info of blacklist items.

19.2.13.3 blacklistsubsystem

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Object identifier for the subsystem on blacklist entry.

19.2.13.4 blacklisttype

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

Type of trap inside the subsystem.

19.2.14 postbootscript Entity

This section describes the `postbootscript` attributes.

Located in the host-specific or common configuration file.

19.2.14.1 command

Mandatory/Optional

Mandatory

Location

Host-specific or Common configuration file

Description

A UNIX command.

19.2.15 ascii2gsm Entity

This section describes the `ascii2gsm` attributes.

Located in the common configuration file.

19.2.15.1 gsmcode

Mandatory/Optional

Mandatory

Location

Common configuration file

Description

Seven-bit number coded in hex (for example, 41 equals "A").

19.2.15.2 gsmtable

Mandatory/Optional

Optional

Location

Common configuration file

Description

Valid Values

- default
- extended

Default

default

19.2.15.3 asciicode

Mandatory/Optional

Mandatory

Location

Common configuration file

Description

A seven-bit hex number for `gsm2ascii7` or eight-bit hex number for `gsm2ascii8` and `ascii2gsm`, coded in hex (for example, 30 equals "0").

19.2.16 motag Entity

This section describes the `motag` attributes.

Located in the common configuration file.

19.2.16.1 string

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the string for a tag in an MO message that triggers a specific function.

19.2.16.2 function

Mandatory/Optional

Optional

Location

Common configuration file

Description

Specifies the function that is triggered by a tag in an MO message. Supported functions:

- phase1statusreport
- deferreddeliveryrelativehours
- deferreddelivery (deprecated)

Note: "deferreddelivery" function is now deprecated. Instead of "deferreddelivery", use "deferreddeliveryrelativehours".

19.2.17 fxferfile Entity

This section describes the `whitelist` attributes.

Located in the host-specific configuration file.

19.2.17.1 localpath

Mandatory/Optional

Mandatory

Location

Host-specific configuration file

Description

Path to the common semi-static configuration file on the local node (i.e. current node).

19.2.17.2 serverpath

Mandatory/Optional

Mandatory

Location

Host-specific configuration file

Description

Path to the common semi-static configuration file on the server node (i.e. OAM node).

19.2.17.3 validate

Mandatory/Optional

Optional

Location

Host-specific configuration file

Description

Ensures that the tp_fclient tool will validate the configuration file it receives from the tp_fserver tool. This attribute should only be used to validate `common_config.txt` (not `MGRData.xml.gz`). Sample syntax:

```
validate="/usr/TextPass/bin/tp_config --validatecommonconfig SERVERFILE"
```

SERVERFILE is not a placeholder. The `common_config.txt` file must be referenced with this word (case-sensitive).

19.2.18 alternativeidentity Entity

This section describes the `alternativeidentity` attributes.

Located in the host-specific or common configuration file.

19.2.18.1 gt

Mandatory/Optional

Mandatory

Location

Host-specific configuration file

Description

A string of 1 to 20 digits representing an alternative GT for the RTR to use. Up to 10 instances of `alternativeidentity` are allowed.

19.2.19 planchangeaction Entity

This section describes the `planchangeaction` attributes. Up to 100 such entities are supported. See *Numbering Plan Change Support* for a description and example of how to use this entity.

Location: Common configuration file.

19.2.19.1 name

Mandatory/Optional

Mandatory

Description

Unique name of the action. Non-unique values are rejected.

Valid Values

A string of 1 to 31 UTF-8 bytes.

Default
N/A

19.2.19.2 minlength

Mandatory/Optional

Optional

Description

Condition on the minimum number of digits in the input (normalized) address.

Valid Values

0 - 38

Default

0

19.2.19.3 maxlength

Mandatory/Optional

Optional

Description

Condition on the maximum number of digits in the input (normalized) address.

Valid Values

0 - 38

Default

38

19.2.19.4 strip

Mandatory/Optional

Optional

Description

Number of digits to strip off the start of the input (normalized) address, when the action is applied and prefix replacement should take place.

Valid Values

0 - 38

Default

0

19.2.19.5 prefix

Mandatory/Optional

Optional

Description

String of digits, which are supposed to be prefixed to the stripped (normalized) address during prefix replacement.

Valid Values

ASCII-encoded string of 0 to 38 decimal digits.

Default

(empty string)

19.2.20 planchangeprefix Entity

This section describes the `planchangeprefix` attributes. Up to 10000 such entities are supported. See *Numbering Plan Change Support* for a description and example on how to use this entity.

Location: Common configuration file.

19.2.20.1 digits

Mandatory/Optional

Mandatory

Description

Unique prefix that the input (normalized) address should best-match in order to apply the corresponding action (if any). Best-matching means that the longest matching provisioned prefix will match. Non-unique values are rejected.

Default

N/A

19.2.20.2 action

Mandatory/Optional

Optional

Description

The `name` of the `planchangeaction` entity that should be applied when this `planchangeprefix` matches.

Values

string of 1 to 31 UTF-8 bytes, which refers to one of the provisioned actions.

Default
When not specified, no action will be applied if this prefix matches, and the input (normalized) address remains unchanged.

19.2.21 sccploadshareset Entity

This section describes the sccploadshareset attributes. Upto 5000 such entities are supported.

See *SCCP Load Balancing* for a description and example on how to use this entity.

Location: Host-specific or Common configuration file.

19.2.21.1 name

Mandatory/Optional

Mandatory

Location: Host-specific or Common configuration file

Description

Name of the load share set that is used to uniquely identify it. Non-unique values are rejected.

Valid Values

Any non-empty string of alphanumeric characters, underscore ('_') and hyphen ('-') with a maximum length of 31 characters.

19.2.22 member Entity

This section describes the member attributes. This is a subordinate of the sccploadshareset entity. This attribute defines an individual member of an SCCP load share set.

Location: Host-specific or Common configuration file.

19.2.22.1 mtpdestination

Mandatory/Optional

Mandatory

Description

The name of MTP destination to which UDT is sent when the member is selected by the load sharing mechanism.

Valid Values

Pre-configured name of a destination entity.

19.2.22.2 subsystemnumber

Mandatory/Optional

Optional

Description

Value of Subsystem Number corresponding to the MTP destination that is used for sending UDT when the member is selected by the load sharing mechanism. Note that this attribute should be either specified or omitted for all the members belonging to a single load share set; however the value may be same or different for each member.

Valid Values

0-255.

19.2.22.3 priority

Mandatory/Optional

Optional

Description

Priority of the load share set member. TextPass device will always select the member having the highest priority within a load share set.

Valid Values

0-7

Default

0

19.2.22.4 weight

Mandatory/Optional

Optional

Description

Weight of the load share set member. When more than one member having the highest priority value are available in a load share set, the TextPass device will perform load sharing among those members based on the ratio of their respective weights. The higher the weight, the higher the load.

Valid Values

1-100

Default

1

19.3 Network Discovery Configuration

To enable communication between RTRs, HUBs, AMSs, and IIWs, network discovery must be configured with the following `tpconfig` attributes in `common_config.txt`:

- `networkdiscoverymulticastaddress`
- `networkdiscoverynetworkaddress`
- `networkdiscoverynetworkmask`

These values may only be changed when the `deviceAdminState` of the device in question is "inactive".

NewNet Mobile Messaging nodes use network discovery to notify each other of their presence in the network. All nodes send out heartbeats via UDP multicast to inform other nodes of their presence. These heartbeats contain the necessary parameters to set up the communication channels between the nodes. The default heartbeat interval is 5 seconds.

All components are aware of each other's presence. The communication channels are set up only between specific components: HUB-HUB, HUB-RTR, AMS-AMS, RTR-AMS, IIW-IIW, and RTR-IIW.

Because the IP TTL is 1, all NewNet Mobile Messaging nodes should be on the same subnet for network discovery to work.

For troubleshooting purposes, use `tp_walk networkDiscoveryTable` to see all discovered nodes/products.

19.4 SCTP Multi-Homing

SCTP multi-homing is used to ensure a fail over from one interface to another in case the interface carrying traffic goes down. SCTP multi-homing allows an end-to-end check to the remote node.

The default configuration is two interfaces for short messages and two interfaces for billing file transfer, `ssh`, SNMP etc. Mobile Messaging software asks the operating system (OS) to open SCTP associations. One association contains two paths in this case (this means two IP interfaces per node can be used to send short messages to a given remote node). The OS uses SCTP multi-homing to set up the SCTP paths. Only one path at a time will have actual short message (traffic) on it, and is called 'primary'. The decision to use the secondary path in case the primary path goes down is made on OS level. Mobile Messaging software is not aware about this change.

An IP address is considered 'active' for SCTP multi-homing when SCTP heartbeat (time for SCTP heartbeats is configurable on OS level) receives an SCTP heartbeat ACK. All IP addresses can be active, but only one interface should handle traffic at any time.

Configuration

When configuring multiple M3UA local addresses (`m3ualocaladdress`), it is required to configure the same number of M3UA remote addresses (`remoteaddress`). If a different number of M3UA local and remote addresses are specified, the RTR will not accept it and `tp_config --validateonly` will give a warning message.

Example

This is a sample portion of a host-specific configuration file that simulates the use of multi-homing with two local M3UA addresses and two remote M3UA addresses.

```
<!-- SIGTRAN configuration, M3UA ASP role -->
<m3ualocaladdress spec="10.0.0.9"/>
<m3ualocaladdress spec="10.0.0.10"/>

<m3uasgp name="sgp1"
      useforvirtualpointcode="false"
      sctplocalport="2906"
      sctpremoteport="2906"
    >
  <remoteaddress spec="10.1.3.3"/>
  <remoteaddress spec="10.1.3.103"/>
</m3uasgp>

<!-- or use some experimental options -->
<m3uasgp name="sgp2"
      sctplocalport="2906"
      sctpremoteport="2906"
      sctplocalsendport="2907"
      sctpsendbuffer="1024000"
      sctpsendlowat="102400"
      sctprecvbuffer="1024000"
      sctprecvlowat="102400"
      sctpnodelay="true"
    >
  <remoteaddress spec="10.1.3.4"/>
  <remoteaddress spec="10.1.3.104"/>
</m3uasgp>
```

19.5 Parameters for M3UA ASP Configuration

To support SIGTRAN, the following optional SCTP parameters are present in the XML configuration file:

- `sctplocalsendport="2907"`
- `sctpsendbuffer="1024000"`
- `sctpsendlowat="102400"`
- `sctprecvbuffer="1024000"`
- `sctprecvlowat="102400"`
- `sctpnodelay="true"`

The following table describes the SCTP parameters.

Parameter	M/O	Description
m3uasgpsctplocalsendport	M	Local SCTP port for the outgoing SCTP association that the RTR maintains with the remote M3UA SGP. Default is 0, which means chosen by the system.

Parameter	M/O	Description
m3uasgpsctpsendbuffer	M	Requested size of the local send buffer in bytes. The default value is 0, which means to use the OS default. Note that the OS may have a maximum size, which can not be exceeded without changing system wide settings.
m3uasgpsctpsendlowat	M	Requested low water mark of the local send buffer in bytes. The default value is 0, which means to use the OS default. This value has to be lower than the send buffer size. Usually a value between 10% and 25% is recommended.
m3uasgpsctprecvbuffer	M	Requested size of the local recv buffer in bytes. The default value is 0, which means to use the OS default. Note that the OS may have a maximum size, which can not be exceeded without changing system wide settings.
m3uasgpsctprecvlowat	M	Requested low water mark of the local receive buffer in bytes. The default value is 0, which means to use the OS default. This value has to be lower than the receive buffer size. Usually a value between 10% and 25% is recommended.
m3uasgpsctpnodelay	M	Requested setting of the NO DELAY flag. Setting this flags disables the Nagle algorithm. The Nagle algorithm may reduce the network load on high latency low throughput connections by delaying and bundling small messages into one network packet. The messages are only delayed until the acknowledgement of the previous packet is received (or until a full packet can be send). Disabling the Nagle algorithm may reduce latency slightly on high latency low throughput connections, at the expense of an increased network load. However, disabling the Nagle algorithm is no guarantee that no bundling is performed. The default is false, which means to use the Nagle algorithm.

19.6 Parameters for M3UA SGP Configuration

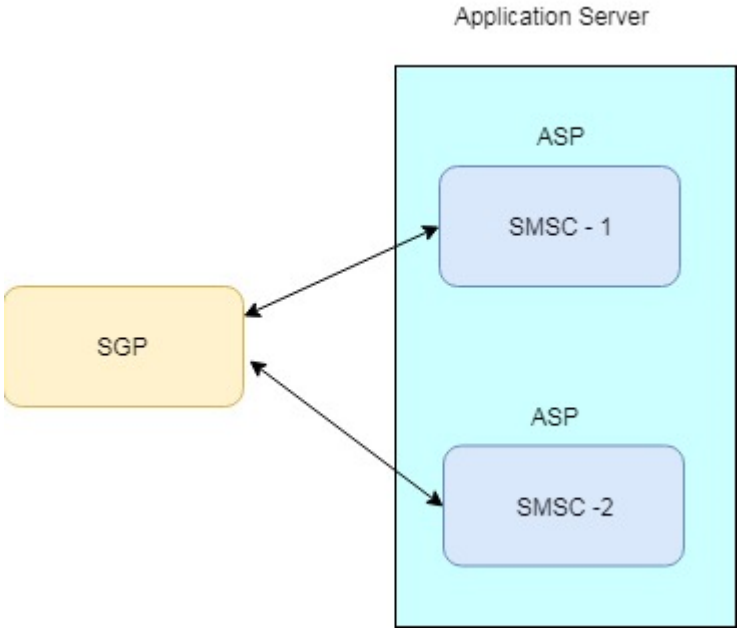
The following table describes the SCTP parameters used for the M3UA SGP configuration. The RTR acts as an SGP with the `m3uaasp` and `m3uaasp` entities.

Parameter	M/O	Description
sctplocalport	O	Local SCTP port for the SCTP association that TextPass maintains with the remote M3UA ASP.
sctpremoteport	O	Remote SCTP port for the SCTP association that TextPass maintains with the remote M3UA ASP.
sctpmaxoutboundpdusize	O	Maximum outbound PDU size for the SCTP association that TextPass maintains with the remote M3UA ASP.
sctpmaxinboundpdusize	O	Maximum inbound PDU size for the SCTP association that TextPass maintains with the remote M3UA ASP.
sctptimerheartbeat	O	SCTP heartbeat interval for the SCTP association that TextPass maintains with the remote M3UA ASP, expressed in units of milliseconds.
sctpmaxretransmittimeout	O	Maximum value of the dynamic retransmit timer (RTO.max) for the SCTP association that TextPass maintains with the remote M3UA ASP, expressed in units of milliseconds.
sctpmaxpathretransmits	O	Maximum number of path retries (Path.Max.Retrans) for the SCTP association that TextPass maintains with the remote M3UA ASP.
sctpmaxassociationretransmits	O	Maximum number of association retries (Association.Max.Retrans) for the SCTP association that TextPass maintains with the remote M3UA ASP.
sctpmaxconnectattempts	O	Maximum number of connect attempts (Max.Init.Retransmits) for the SCTP association that TextPass maintains with the remote M3UA ASP.
sctpmaxallowedinboundstreams	O	Maximum number of inbound streams that TextPass allows for the SCTP association that TextPass maintains with the remote M3UA ASP.
sctppreferredoutboundstreams	O	Number of outbound streams that TextPass prefers for the SCTP association that TextPass maintains with the remote M3UA ASP.
sctpsackdelay	O	Time (in ms) to wait before acknowledging SCTP DATA chunks. A value of 0 (default) means use the system default, which tends to be 200ms. This setting only has an effect for newly created SCTP associations, and only when running on RHEL.

19.7 M3UA SGP Configuration

The RTR, acting as SGP, can be connected to multiple ASPs (Application Server Processes). The AS (Application Server) contains a set of one or more unique Application Server Processes. Within one Application Server, there can be up to 16 application signaling processes. The router load balances the signaling traffic over ASP.

The figure below gives a sample configuration where the RTR, acting as SGP, has SCTP association with two ASPs that are part of one Application Server.

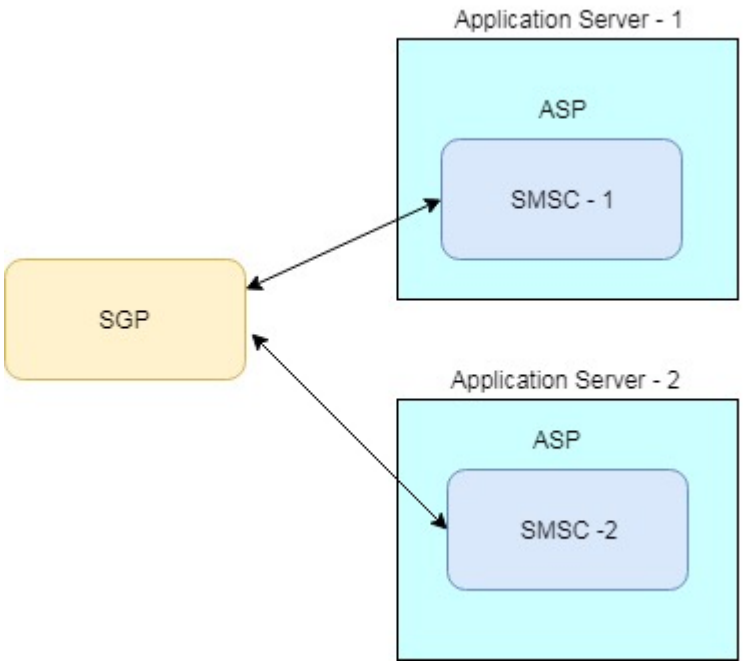


Sample M3UA SGP configuration for above application server:

```
<m3ualocaladdress spec="172.16.133.71"/>
<m3ualocaladdress spec="172.16.134.71"/>

<m3uaasp name="SMSC-1"
        sctplocalport="5739"
        sctpremoteport="5738"
        fillinnetworkappearancefield="false"
        sctpmaxoutboundpdusize="2048"
        sctpmaxinboundpdusize="2048"
        sctptimerheartbeat="30000"
        sctpmaxretransmittimeout="1000"
        sctpmaxpathretransmits="5"
        sctpmaxassociationretransmits="10"
        sctpmaxconnectattempts ="10"
        sctpmaxallowedinboundstreams ="2"
        sctppreferredoutboundstreams = "2"
        initiatingstartupenabled = "false"
        sctpsackdelay="0"
      >
     <!-- Use multiple IP addresses for SCTP multi-homing -->
       <remoteaddress spec="172.16.133.187"/>
```

```
      <remoteaddress spec="172.16.134.187"/>
   </m3uaasp>


<m3uaasp name="SMSC-2"
       sctplocalport="5739"
       sctpremoteport="5738"

       fillinnetworkappearancefield="false"
       sctpmaxoutboundpdusize="2048"
       sctpmaxinboundpdusize="2048"
       sctptimerheartbeat="30000"
       sctpmaxretransmittimeout="1000"
       sctpmaxpathretransmits="5"
       sctpmaxassociationretransmits="10"
       sctpmaxconnectattempts ="10"
       sctpmaxallowedinboundstreams ="2"
       sctppreferredoutboundstreams = "2"
       initiatingstartupenabled = "false"
       sctpsackdelay="0"
     >
       <remoteaddress spec="172.16.133.185"/>
       <remoteaddress spec="172.16.134.185"/>
   </m3uaasp>

   <m3uaas name="smsc_vp"  routingcontext="0" >
      <instance asp="SMSC-1"/>
      <instance asp="SMSC-2"/>
   </m3uaas>

  <destination name="SMSC" type="smsc" pointcode="5391">
       <route m3uaas="smsc_vp"/>
  </destination>
```

The figure below gives a sample network diagram where RTR, acting as SGP, has SCTP associations with two Application Servers. Each Application Server has one ASP.



Sample M3UA SGP configuration for above network diagram:

```
<m3ualocaladdress spec="172.16.133.71"/>
<m3ualocaladdress spec="172.16.134.71"/>

<m3uaasp name="SMSC-1"
        sctplocalport="5739"
        sctpremoteport="5738"
        fillinnetworkappearancefield="false"
        sctpmaxoutboundpdusize="2048"
        sctpmaxinboundpdusize="2048"
        sctptimerheartbeat="30000"
        sctpmaxretransmittimeout="1000"
        sctpmaxpathretransmits="5"
        sctpmaxassociationretransmits="10"
        sctpmaxconnectattempts ="10"
        sctpmaxallowedinboundstreams ="2"
        sctppreferredoutboundstreams = "2"
        initiatingstartupenabled = "false"
        sctpsackdelay="0"
     >
     <!-- Use multiple IP addresses for SCTP multi-homing -->
       <remoteaddress spec="172.16.133.187"/>
       <remoteaddress spec="172.16.134.187"/>
    </m3uaasp>


<m3uaasp name="SMSC-2"
        sctplocalport="5739"
        sctpremoteport="5738"

        fillinnetworkappearancefield="false"
        sctpmaxoutboundpdusize="2048"
        sctpmaxinboundpdusize="2048"
        sctptimerheartbeat="30000"
        sctpmaxretransmittimeout="1000"
        sctpmaxpathretransmits="5"
        sctpmaxassociationretransmits="10"
        sctpmaxconnectattempts ="10"
        sctpmaxallowedinboundstreams ="2"
        sctppreferredoutboundstreams = "2"
        initiatingstartupenabled = "false"
        sctpsackdelay="0"
      >
        <remoteaddress spec="172.16.133.185"/>
        <remoteaddress spec="172.16.134.185"/>
    </m3uaasp>

    <m3uaas
        name="smsc_vp1"
        routingcontext="0"
    >
       <instance asp="SMSC-1"/>
   </m3uaas>

  <destination name="SMSC1" type="smsc" pointcode="5391">
        <route m3uaas="smsc_vp1"/>
  </destination>

    <m3uaas
        name="smsc_vp2"
        routingcontext="1"
```

```
   >
      <instance asp="SMSC-2"/>
   </m3uaas>

<destination name="SMSC2" type="smsc" pointcode="5392">
      <route m3uaas="smsc_vp2"/>
</destination>
```

19.8 Activating Configuration Files

To activate the configuration files, execute the following command at the command prompt of each RTR:

```
tp_config [<specific file> [<common file>]]
```

If you do not specify the configuration files in the command, `tp_config` uses both of them.

Note:

- Executing `tp_config` restarts the RTR, which is service-affecting. Therefore, it is recommended that the configuration files be activated during low-traffic hours.
- The `tp_start` command-line tool, which starts the RTR, automatically executes `tp_config`.

19.9 Configuration File Distribution

The `tp_fclient` tool manages the replication of XML configuration data files from a server. `tp_fclient` enables a client system to subscribe to all changed XML configuration data files that the MGR on the assigned server produces.

The `tp_fserver` tool manages the replication of XML configuration data files from a server. `tp_fserver` enables a server system to interact with clients.

For more information about `tp_fclient` and `tp_fserver`, refer to the Tools Operator Manual.

tp_fclient Configuration

To configure the `tp_fclient` tool:

1. To enable the `tp_start` tool to start the `tp_fclient` tool, add the following line to the host-specific configuration file (located in `usr/TextPass/etc`):
   ```
   runtpfclientprocess="true"
   ```
2. Remove any instances of `tp_fclient` as `postbootscript` command in the host-specific configuration file. For example:
   ```
   <postbootscript command="/usr/TextPass/bin/tp_fclient a.b.c.d"/>
   <postbootscript command="/usr/TextPass/bin/tp_fclient --continuous a.b.c.d &amp;amp;"/>
   ```
3. In the `/etc/hosts` file, add the host name (or alias) of the MGR node.

When `tp_start` starts multiple applications at the same time, it will always start the `tp_fclient` process first. `tp_start` will first invoke `tp_fclient` without the `--continuous` option, which will cause `tp_fclient` to retrieve files once unconditionally. `tp_start` will start `tp_fclient`

subsequently without the `--continuous` option, which will cause `tp_fclient` to retrieve files only when a change occurs.

Note: The files in `/usr/local/apache/mBalance/TPManager/data` that are replicated by the file transfer utilities must be owned by the user textpass that starts the scripts. If not, an error will occur and the script will abort.

Starting and Stopping tp_fclient

The `tp_fclient` tool can also be started and stopped independently:

```
$ tp_start --tp_fclient
$ tp_stop --tp_fclient
```

19.10 Dynamic Configuration

The dynamic configuration is called dynamic because, in general, the parameters change frequently. The parameters are related to the RTR's routing behaviour. The dynamic configuration is configured in the MGR, which is a Web interface.

The dynamic RTR configuration contains:

- RTR devices
- Countries
- Networks
- Applications
- SMSCs
- Routing rules
- Modifiers
- Counting rules
- Billing profiles
- Logging profiles

Refer to the MGR Operator Manual for information about the dynamic configuration.

The below two application configuration parameters are used in RTR to overwrite the TON/NPI settings of recipient address for outbound SMPP messages. These settings are application specific. The actual Recipient's Number does not change based on these settings, only the TON/NPI fields are overwritten.

19.10.1 applicationoutboundsmppaddresston

Mandatory/Optional

Optional

Location

MGR

Description

Type-of-number value to be used by the RTR to overwrite the TON in the recipient address for the outbound SMPP messages. This parameter is not applicable for the alphanumeric address.

By default, this parameter is set to `noChange` (`-1`).

19.10.2 applicationoutboundsmppaddressnpi

Mandatory/Optional

Optional

Location

MGR

Description

Numbering-plan-identification value to be used by the RTR to overwrite the NPI in the recipient address for the outbound SMPP messages. This parameter is not applicable for the alphanumeric address.

By default, this parameter is set to `noChange` (`-1`).

Chapter 20

Security

Topics:

20.1 Introduction

This chapter describes an overview of the security aspects of the NewNet Mobile Messaging system.

20.2 Controlling System Access

Access to NewNet Mobile Messaging system is controlled using the available security mechanisms. Refer to the RedHat Enterprise documentation.

20.3 User Groups and Password Privileges

All MGR users belong to a user group. There are three default user groups:

- Administrator
- Super user
- Customer support

Refer to the MGR Operator Manual for more information about user groups and information about the MGR's user password security policy.

20.4 Authenticating Applications

Authentication of application access to RTRs is controlled by using UCP 60 session management (i.e. short number and password) and SMPP bind operations.

NewNet Mobile Messaging systems are assumed to operate in a network environment that is secured by means of firewalls and corresponding adequate security measures.

Note: Only administrators can specify the NewNet Mobile Messaging password policy for application passwords.

20.5 Detecting and Reporting Security Violations

Access to log files or audit files and other system resources on NewNet Mobile Messaging systems is controlled using the available security mechanisms. Refer to the RedHat Enterprise documentation.

Chapter 21

Software License

Topics:

21.1 Introduction

Some NewNet Mobile Messaging software components are licensed features, which means that the appropriate software licenses need to be purchased before the corresponding functionality can be used.

21.2 Licensed Items

The following RTR items are licensed:

Licensed Item	Possible Values	M/O
E1 connections	1 - 16	O
Links	1 - 4096	O
HSL link	• True • False	M
SMPP access[1]	• True • False	O
UCP access[1]	• True • False	O
CIMD2 access[1]	• True • False	O
OIS access	• True • False	O
SS7 ITU-T	• True • False	M
SS7 ANSI	• True • False	M
SS7 China	• True • False	M

Licensed Item	Possible Values	M/O
SS7 Japan	• True • False	M
Map GSM	• True • False	M
TDMA IS136	• True • False	M
CDMA IS95	• True • False	M
Sigtran SUA	• True • False	M
Sigtran M3UA	• True • False	M
Sigtran Ethernet	• True • False	M
Maximum throughput[2]	1 - 9999	M
Commercial throughput[2]	1 - 9999	M
Camel maximum throughput[2]	1 - 9999	O
Camel commercial throughput[2]	1 - 9999	O
CDR SS8	• True • False	O
CDR CMG	• True • False	O
CDR Logica	• True • False	O
CDR Sema	• True • False	O

Licensed Item	Possible Values	M/O
CDR Nokia	• True • False	O
CDR Ericsson	• True • False	O
CDR Comverse	• True • False	O
CDR Huawei	• True • False	O
CDR Comverse 3G	• True • False	O
Routing path MO-MO[3]	• True • False	O
Routing path MT-MT[3]	• True • False	O
Routing path MO-AT[3]	• True • False	O
Routing path AO-MT[3]	• True • False	O
Routing path AO-MT-AO[3]	• True • False	O
Routing path MO-MT-MO[3]	• True • False	O
Routing path MO-MT[3]	• True • False	O
Routing path MO-Discard[3]	• True • False	O

Licensed Item	Possible Values	M/O
Routing path MT-Discard[3]	• True • False	O
MO and MT SCCP Conditions	• True • False	O
External condition interface (ECI)	• True • False	O
Check IMSI	• True • False	O
Statistics entities MO	• True • False	O
Statistics entities MT	• True • False	O
Statistics MO counting rules	• True • False	O
Statistics MT counting rules	• True • False	O
Routing path MO-MT-AT[3]	• True • False	O
Routing path AO-AO[3]	• True • False	O
Routing path AT-AT[3]	• True • False	O
Routing path AT-AO[3]	• True • False	O
Advanced External Condition Interface	• True • False	O

Licensed Item	Possible Values	M/O
Firewall logging support	• True • False	O
Additional Firewall statistics	• True • False	O
Anti-MO spoofing	• True • False	O
Anti-MT spoofing	• True • False	O
Logging transparent user data level	• Always • Protocol violations only • Never	O
Routing path AO-AO-AO[3]	• True • False	O
Routing path AO-AT[3]	• True • False	O
Routing path AO-Discard[3]	• True • False	O
Routing path AT-Discard[3]	• True • False	O
Standard statistics	• True • False	O
Additional statistics	• True • False	O
Extended application support	• True • False	O
Camel Phase 2 ECI	• True	O

Licensed Item	Possible Values	M/O
	• False	
Camel Phase 3 ECI	• True • False	O
Text Insert ECI	• True • False	O
Copy ECI	• True • False	O
Forward ECI	• True • False	O
Routing path MO-MT-Store[3]	• True • False	O
Routing path MO-AT-Store[3]	• True • False	O
Routing path AO-MT-Store[3]	• True • False	O
Routing path MO-Store[3]	• True • False	O
Routing path AO-Store[3]	• True • False	O
Routing path Store-MT[3]	• True • False	O
Routing path Store-AT[3]	• True • False	O
Routing path MO-MT-AO[3]	• True • False	O

Licensed Item	Possible Values	M/O
Routing path MO-AO[3]	• True • False	O
Routing path MO-MO 3G[3]	• True • False	O
Routing path MT-MT 3G[3]	• True • False	O
Routing path Store-AO[3]	• True • False	O
Routing path AT-Store[3]	• True • False	O
MO scan tags	• True • False	O
Home Routing	• True • False	O
HLR Proxy	• True • False	O
Subscriber Subscription Information (SSI)	• True • False	O
Configured nodes for adjusted LL	0 - 64	O
Reject on adjusted throughput breach	• True • False	O
Service messages	• True • False	O
Hide user data in events	• True: User data (message content) will be masked with Xs in event logs (user data length will not be affected)	O

Licensed Item	Possible Values	M/O
	• False: User data will appear in event logs	
Routing path MT-AT[3]	• True • False	O
Routing path MT-AO[3]	• True • False	O
Routing path MT-Store[3]	• True • False	O
J-Interface	• True • False	O
Domain Selection	• True • False	O
TP-OA SMSC Address Match	• True • False	O
SMSoIP Delivery	• True • False	O
RCS Delivery	• True • False	O
SCCP Loadsharing	• True • False	O
Enable Message Template	• True • False	O

Notes:

1. At least one application protocol must be licensed when a routing path containing AT or AO is licensed
2. The maximum allowed throughput is also determined by the SS7 interface type and the type of routing paths used.
3. At least one routing path must be licensed, otherwise no messages can be routed.

4. For starting the RTR in ITU-T SS7 mode, the "SS7 ITU-T" license item must be set to "True" (i.e. enabled).
5. For starting the RTR in ANSI SS7 mode, the "SS7 ITU-T" license item must be set to "False" (i.e. disabled) and the "SS7 ANSI" license item must be set to "True".
6. For starting the RTR in Japanese SS7 mode, both "SS7 ITU-T" and "SS7 ANSI" license items must be set to "False" and the "SS7 Japan" license item must be set to "True".
7. When the RTR is licensed for Japanese SS7 mode, the "Sigtran M3UA" license item must also be set to "True"; otherwise the RTR would not be able to interface with the SS7 network.

21.2.1 Multi-Instance License

Multiple instances feature allows you to run multiple RTR (up to 10 instances) on the same node. Multi-instance license should be enabled for NMM user to run one additional instance of RTR. To run one additional instance of RTR from newly created NMM user (using script `tp_manage_user`), instance license for newly create user id (operating system user identifier) should be enabled in license file.

21.3 License Behaviour

21.3.1 Permanent versus Temporary Licenses

Licenses may be either temporary (e.g. only valid for one month) or perpetual. Typically licenses for test systems are temporary and licenses for production systems are perpetual. For temporary licenses, the start and end dates are contained in the license files, and the software will generate traps to alert the user to the fact that the license is about to expire (see *License Warnings*). License files are valid until 23:59 on the end date.

21.3.2 Activation versus Regular License Files

For an initial (clean) software installation, both an activation file and a regular license file are required. These should be placed in the `/var/TextPass/etc` directory. Subsequent license files with incremental license numbers (previous license + 1) will be accepted by the system without an activation file, provided that the previous license has not expired.

21.3.3 Throughput License

The RTR license has both a system-specific and a site-wide throughput component. The total throughput capacity is distributed over the available RTRs within one site as defined below.

The throughput licenses for each single RTR consist of the following defined license limits:

- Commercial License Limit (CLL)—Maximum allowed throughput in short messages per second (SM/s) as commercially agreed (the purchased license). Exceeding this limit will result in "license exceeded" SNMP traps. The counter

  "licTotalMessagesOverLicenseLimit" shows the total number of transactions over CLL since the system boots up.

- Adjusted Commercial License Limit (ACLL)—Has a dynamic value. As long as all systems of a redundant configuration are functional, their respective ACLL has the same value as the CLL. If one of the systems experiences an outage, the remaining systems' ACLL is adapted so that the sum of all ACLLs is the same as before the outage.

  Note: The Adjusted Commercial License limit (ACLL) is only enabled when the number of nodes for Adjusted License Limit (ALL) is different. This setting is created during license creation and cannot be altered later. The value of ACLL can be seen in the license file behind the item: "Configured Nodes for Adjusted LL" in the TPR/RTR section.

- Technical License Limit (TLL)—Maximum possible throughput of the RTR in SM/s. Exceeding this limit is not possible, and messages beyond this limit will not be serviced (rejected). This technical license limit is always equal to or greater than the commercial limit (CLL). Exceeding this limit will result in “license exceeded” SNMP traps. The counter "licTotalMessagesRejected" shows the total number of transactions rejected due to TLL since the system boots up.

Contact your Account Manager immediately if a throughput license upgrade is required.

21.3.3.1 Messages Counted in Throughput License

Only incoming messages are counted with regard to the throughput license. Note that incoming notifications (AT) or incoming status reports (MT), too, are counted as one incoming message in the license. The diagram depicts the relevant entities and messages for throughput license counting. All messages entering the RTR on the dotted line are counted.

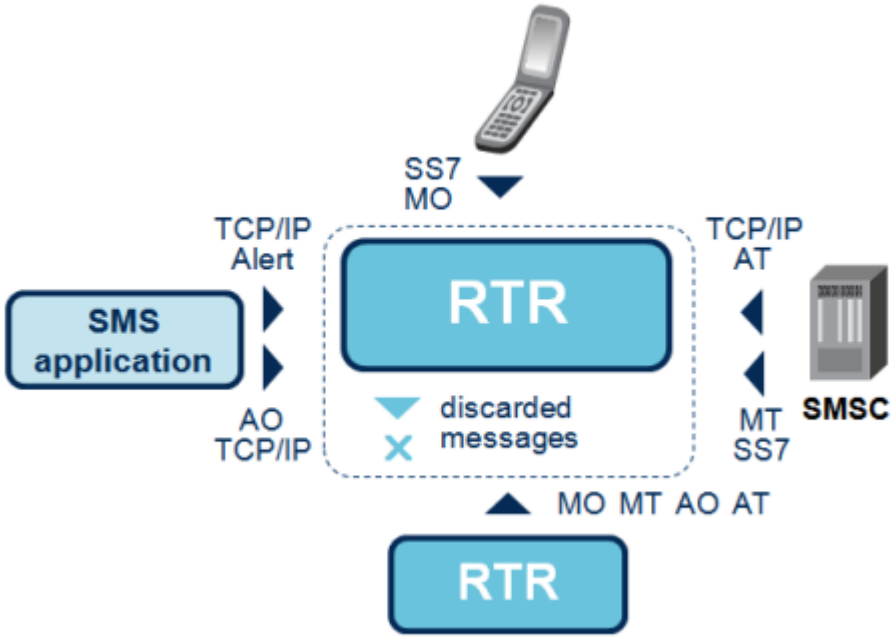


Figure 86: Messages counted in license

21.3.4 Grace Period

If one of the system identification items to which the license is tied (host ID, Ethernet MAC address, zone name or signalling card number) changes because of hardware maintenance, the license will

enter a grace period of 7 days. Contact NewNet Support to obtain a license for the new system identification within this 7-day period.

It is possible to retain the host ID of servers when the system motherboard is replaced. Ask your hardware repair technician to keep the host ID chip or card from the original systems and install them on the new servers.

21.4 Checking Your License

To view the current license values, execute the following command at the command prompt:

```
tp_system [system]
```

Where `[system]` is the IP address or host name of the RTR.

The following is a sample of the output of the `tp_system` tool.

```
Identification:
    TextPass/SMS R04.11.04.00
    TextPass Sigtran-Only
    Linux build

Uptime:
    0 days 01h:51m:46s

License key:
XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX

License information:
    License version 23
    License number TST-93814
    Hardware ID 287567c3
    SS7 Board No dummy
    Ext Serial No SGH509XRXJ
    Instance Serial No 200
    License exceeds in 2096 hours
    License exceeds at Sun Mar 10 00:00:00 2019
    License issue number 17
    Hide User Data in Events disabled
    VmWare Support disabled
    Core Count 0
    Encrypt User Data disabled
    4 E1/T1 trunks
    64 SS.7 links
    HSL support enabled
    SS7/ITU-T module enabled
    SS7/ANSI module disabled
    SS7/China module disabled
    GSM/MAP module enabled
    TDMA/IS136 module disabled
    CDMA/IS95 module disabled
    SIGTRAN/SUA module disabled
    SIGTRAN/M3UA module enabled
    Ethernet for SIGTRAN support enabled
    SMPP access enabled
    UCP access enabled
    CIMD2 access enabled
    OIS access disabled
    10000 transactions/sec granted
    10000 transactions/sec according license
    0 configured nodes of site
```

```
    1 available nodes of site
    10000 adjusted transactions/sec
    Reject messages on breach of transactions/sec enabled
    Send service message to HQ enabled
    10000 Camel transactions/sec granted
    10000 Camel transactions/sec according license
    CDR/CMG module enabled
    CDR/Logica module enabled
    CDR/SEMA module enabled
    CDR/Nokia module enabled
    CDR/Ericsson module enabled
    CDR/Comverse module enabled
    CDR/SS8 module enabled
    CDR/Huawei module enabled
    Routing path MO-MO enabled
    Routing path MO-AT enabled
    Routing path MO-MT enabled
    Routing path MO-MT-MO enabled
    Routing path MO-MT-AT enabled
    Routing path MO-Discard enabled
    Routing path MT-MT enabled
    Routing path MT-Discard enabled
    Routing path AO-MT enabled
    Routing path AO-MT-AO enabled
    Routing path AO-AO-AO enabled
    Routing path AO-AT enabled
    Routing path AO-Discard enabled
    Routing path AT-Discard enabled
    Routing path MO-MT-ST enabled
    Routing path MO-AT-ST enabled
    Routing path AO-MT-ST enabled
    Routing path MO-ST    enabled
    Routing path AO-ST    enabled
    Routing path SO-MT    enabled
    Routing path SO-AT    enabled
    Routing path SO-AO    enabled
    Routing path MO-MT-AO enabled
    Routing path MO-AO    enabled
    Routing path 3G MO-MO enabled
    Routing path MT-MT 3G enabled
    Routing path AT-ST    enabled
    Routing path MT-AT    enabled
    Routing path MT-AO    enabled
    Routing path MT-ST    enabled
    External condition interface enabled
    Advanced External condition interface enabled
    Check IMSI enabled
    Entity-based MO statistics enabled
    Entity-based MT statistics enabled
    Rule-based MO statistics enabled
    Rule-based MT statistics enabled
    Firewall logging support enabled
    Firewall additional statisstics enabled
    Firewall anti MO spoofing enabled
    Firewall anti MT spoofing enabled
    Firewall Transparent User Data Level always
    Standard statistics          enabled
    Additional statistics        enabled
    Extended Application support enabled
    ECI Camel phase2 support     enabled
    ECI Camel phase3 support     enabled
    MO Scan Tags support        enabled
    Home Routing support        enabled
    Hlr Proxy                   disabled
    Subscriber Subscription Info enabled
```

```
    MO and Mt SCCP Conditions   enabled
    J-Interface                 enabled
    Domain Selection            enabled
    RCS Delivery                enabled
    SMSoIP Delivery             enabled
    TP-OA SMSC Address Match    enabled
    SCCP Loadsharing            disabled
    SS7/Japan module            disabled
    CDR/Comverse 3G module      enabled
    Enable Message Template     enabled
    MAP ATI Supported           enabled

Alarm stations:
    127.0.0.1:11173
```

If multi-instance license is enabled for user id `200` (`'textpass'`) in the license file, then `tp_system` will display the instance user id as shown below:

```
        Instance Serial No 200
```

21.5 Activating a New License

A new license key is required to activate new services or adapt connectivity or performance settings. Please contact your NewNet account manager to obtain a new license key.

To activate a new license key:

1. Place a valid RTR license file in the `TextPass/etc` directory.
2. At the command prompt, execute the following command (this is usually not service affecting):

   ```
   tp_system --texpass --read_licensekey [system]
   ```

   Where `[system]` is the IP address or host name of the RTR.

Note: Also ensure that a valid license is placed and activated on the MGR node as well.

It is not required to restart the RTR when activating a new license; however, you should always restart the Manager if the license affects functionality, to ensure that the correct functionality will appear in the interface.

To verify the new license, execute the following command:

```
tp_system --textpass --show_licensekey [system]
```

Where `[system]` is the IP address or host name of the RTR.

If the RTR is started without a valid license, RTR initialisation will fail after a series of errors. After this, a valid license can be activated.

21.6 License Warnings

The following license-related SNMP traps are available:

- `attemptToExceedLicensedThroughput`—Warns when the Commercial License Limit (CLL) is exceeded.

- `attemptToExceedNumOfLicensedTrunks`—Warns when more than the allowed number of SS7 E1 trunks are configured.
- `attemptToExceedNumOfLicensedLinks`—Warns when more than the allowed number of SS7 links are configured.
- `attemptToUseNonLicencedFeature`—Warns when an attempt to use an unlicensed feature is made.

The following SNMP traps warn when the license limits are approaching:

- `licenseWillExpire`—The temporary license will expire in the given number of hours.
- `licenseExpired`—The validity period of the license has expired.

The traps are generated at these intervals:

- `licenseWillExpire`—Before it expires, 14 days in advance
- `licenseWillExpire`—7 days in advance
- `licenseWillExpire`—3 days in advance
- `licenseWillExpire`—1 day in advance
- `licenseExpired`—At the moment it expires and then every hour until fixed

To adapt the license in a timely manner and avoid expiry, these traps should be properly handled by the Network Management System.

Chapter 22

System Management

Topics:

22.1 Introduction

This chapter describes the command-line tools available to assist in determining the status of the system or locating the cause of the problem, if any.

22.2 Stopping the System

The RTR is designed to run unattended and almost maintenance-free for normal operation. If the RTR process needs to be stopped, execute the following command at the command prompt of the RTR node:

```
tp_stop --textpass
```

This command will gracefully shut down the RTR and stop the RTR process and the watchdog process.

22.3 Starting the System

To start the RTR process, execute the following command at the command prompt of the RTR node:

```
tp_start --textpass
```

This command will start the RTR and the watchdog process.

During initialisation, the RTR process uses the `tp_config` tool to load the configuration.

When the RTR node restarts after an unplanned outage (such as a power failure), the RTR process is restarted automatically and resumes service.

As an alternative to using the `tp_start` tool, the RTR can be rebooted, after which it will automatically restart.

22.4 Watchdog Process

The watchdog process and the Mobile Messaging component process communicate via Unix signals.

The watchdog process expects contact from the Mobile Messaging component process every second. If the component process does not contact the watchdog for six seconds, the watchdog stops and restarts the component process.

If a signal is missed, the watchdog writes the following message in the syslog:

```
Missing health signal, missed <number of signals> signals, allowed <max number of
missed signals>
```

If the watchdog stops the component process, it writes the following messages:

```
Missed <number of signals> health signals: trying to cleanly abort process <process
 ID>
Application killed (<process ID>), waiting <number of seconds> seconds before
restarting
```

When the watchdog attempts to restart the component process, it writes the following message:

```
Application restarted, number of unsuccessfully restarts <number of restarts>,
application was running for <number of seconds> seconds
```

If the component process dies or is stopped by the watchdog three times within 30 minutes, the watchdog stops attempting to restart the process and writes the following message:

```
Application terminated, too many restarts within predefined interval
```

To monitor the `syslog`, execute:

```
# tail -f /var/log/messages
```

22.5 System Verification

22.5.1 Basic System Verification

For basic verification of the RTR status, execute the following command at the command prompt:

```
tp_system [system]
```

Where `[system]` is a resolvable host name or the IP address of the RTR. The response contains the time that the RTR process has been running. If there is no response, the specified system cannot be reached or the RTR is not running correctly.

To verify the SS7 links connected to the RTR, execute the following command at the command prompt:

```
ss7_link [system]
```

Where `[system]` is a resolvable host name or the IP address of the RTR. The response contains the time that the RTR process has been running. If there is no response, the specified system cannot be reached or the RTR is not running correctly.

For more information about command-line tools, refer to the Tools Operator Manual.

22.5.2 Advanced System Verification

For more detailed information about the RTR system, use the `tp_walk` command-line tool (as user textpass) to retrieve information about specific RTR counters. Useful attribute groups for RTR verification are:

Group	Description
smsCounters	Total SMS counters, summarized per result category
moRtgRuleTable	Properties of MOR rules
moCntRuleTable	Properties of MOC rules
applicationTable	Properties of applications
smscTable	Properties of SMSCs
mtpLink	Properties of MTP links; individual attributes for RTR verification are `mtpLinkRxUtilisation` and `mtpLinkTxUtilisation`

For more information about `tp_walk`, refer to the Tools Operator Manual.

Additional RTR troubleshooting methods are investigation of core files and analysis of XML configuration data files.

22.6 SS7 Tracing

You can create SS7 trace filters to capture SS7 data and send it to a configured trace receiver. RTR uses external application `tshark` to apply filters on incoming/outgoing SS7 traffic.

The trace receiver is a command-line tool (`tp_trace_receiver`); refer to the Tools Operator Manual for more information about its configuration and usage.

22.6.1 Creating Trace Filters

To create a trace filter:

1. In the left navigation bar, select **Tracing ➤ SS7 Trace Filter**.
   The Trace Filters tab appears.
2. Click **Add New**.
   A new SS7 Trace Filters tab appears.
3. Enter a unique name for the trace filter in the **Name** box (maximum 31 characters).
4. Optionally enter a description of the trace filter in the **Description** box.
5. In the **Server IP** box, enter the IP address of the server to which to send the traces from this filter.
6. In the **Server Port** box, enter the UDP port of the server to which to send the traces from this filter.
7. In the **Filter Expression** box, enter the Filter Expression for the Trace filter (maximum 2048 character including whitespace). Filter Expression should be understood by `tshark` (Refer to *http://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html*).

   Note: Using filter expression would have an effect on memory usage and long running traces with filter expression are not recommended. If filter expression is not configured, then all incoming/outgoing SS7 PDUs will be sent to the trace receiver server unfiltered.
8. In the **Memory Usage** box, enter the Maximum amount of memory in Megabytes allowed to use by filtering application, from 512 to 4096 (4 GB). Default value is 1024 MB. Memory parameter is applicable only if **Filter Expression** is specified. In case `tshark` process memory usage exceeds the configured value then the `tshark` process will get restarted.
9. In the **Linkset** box, enter list of linkset names to trace (maximum 16 linksets). If this field is left blank then all linksets specified in the corresponding RTR node's host configuration file will be traced. Linkset-based tracing capability is supported only for SS7 (MTP3) links, not for SIGTRAN (M3UA) links. Multiple linksets can be specified separated by the new-line character.
10. Click **Save**.
    The MGR creates the filter and closes the tab.
11. Activate the trace filter.

    Note:

    1. You must activate SS7 trace filters for them to begin collecting data.
    2. Maximum 10 SS7 trace filters can be configured in a domain on MGR.

3. Only one SS7 trace filter can be active in a domain at a time.
4. You must de-activate SS7 trace filter before deleting any SS7 trace filter.

22.6.2 Tshark Memory Usage And Throughput

The memory usage of the `tshark` process depends on the following three factors:

1. Complexity of filter expression.
2. Duration for which trace filter process is continuously running
3. Throughput rate at which SS7 PDUs are received and filtered

Running trace filters with filter expression continuously for long time is not recommended as it significantly increases the memory usage of `tshark` process. The maximum amount of memory allowed to be used by the filtering application (`tshark`) can be configured as mentioned above. When `tshark` process memory usage exceeds the configured value, `tshark` process exits and RTR is informed about the status ('exited') of `tshark` process. Accordingly, RTR restarts `tshark` process for applying the filter expression again. During the time-interval between the exit and subsequent restart of `tshark` process, incoming/outgoing SS7 PDUs will not be traced.

SS7 tracing functionality is capable of supporting a maximum throughput rate of 3000 PDUs/sec. for filtering by the `tshark` application.

The following table provides typical figures for the no. of SS7 PDUs sent to `tshark` for filtering during the processing flow of a single message (received by the RTR), w.r.t. some commonly used routing paths.

Note that the actual number of SS7 PDUs to be filtered per incoming message may be different from the figures given below for some of the routing paths, depending on special configuration or routing action (e.g. Early SRI-SM, Originator IMSI retrieval, fallback to Store or external SMSC etc.).

Routing Path	**No. of SS7 PDUs sent to tshark (per message)**
MO-MT (FDA without fallback)	6
MT-MT (Home Routing)	6
AO-MT (FDA without fallback)	4
MO-AT	2

22.6.3 Filter Expression

RTR uses external application `tshark` to apply filters on incoming/outgoing SS7 traffic and send filtered PDUs to trace receiver. You must specify filter expression which can be understood by `tshark` application. `tshark` provides a simple but powerful display filter language that allows you to build quite complex filter expressions. You can compare values in packets as well as combine expressions into more specific expressions. The following sections provide more information on doing this.

22.6.3.1 Comparing Values

You can build display filters that compare values using a number of different comparison operators.

Note: You can use same filter expression which can be used on WireShark GUI.

English	Symbol	Description and example
eq	==	ip.src==192.168.210.10
ne	!=	ip.src!=192.168.210.10
gt	>	frame.len > 10
lt	<	frame.len < 128
ge	>=	frame.len ge 0x100
le	<=	frame.len <= 0x20

In addition, all protocol fields are typed. The following table provides a list of the types and example of how to express them.

Unsigned integer (8-bit, 16-bit, 24-bit, 32-bit) Signed integer (8-bit, 16-bit, 24-bit, 32-bit)	You can express integers in decimal, octal, or hexadecimal. The following display filters are equivalent: ip.len le 1500 ip.len le 02734 ip.len le 0x436
Boolean	A boolean field is present in the protocol decode only if its value is true. For example, **tcp.flags.syn** is present, and thus true, only if the SYN flag is present in a TCP segment header. Thus the filter expression **tcp.flags.syn** will select only those packets for which this flag exists, that is, TCP segments where the segment header contains the SYN flag. Similarly, to find source-routed token ring packets, use a filter expression of **tr.sr**.
IPv4 address	ip.addr == 192.168.0.1 Classless InterDomain Routing (CIDR) notation can be used to test if an IPv4 address is in a certain subnet. For example, this display filter will find all packets in the 129.111 Class-B network: ip.addr == 129.111.0.0/16
String (text)	http.request.uri == "http://www.newnetmobility.com/"

22.6.3.2 Combining Expressions

You can combine filter expressions in Wireshark using the logical operators shown in table below:

English	Symbol	Description and example
and	&&	**Logical AND** ip.src==10.0.0.5 and tcp.flags.fin

English	Symbol	Description and example
or	||	**Logical OR** ip.scr==10.0.0.5 or ip.src==192.1.1.1
xor	^^	**Logical XOR** tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == 0.6.29
not	!	**Logical NOT** not llc
[...]		**Substring Operator** Wireshark allows you to select subsequences of a sequence in rather elaborate ways. After a label you can place a pair of brackets [] containing a comma separated list of range specifiers. eth.src[0:3] == 00:00:83 The example above uses the n:m format to specify a single range. In this case n is the beginning offset and m is the length of the range being specified. eth.src[1-2] == 00:83 The example above uses the n-m format to specify a single range. In this case n is the beginning offset and m is the ending offset. eth.src[:4] == 00:00:83:00 The example above uses the :m format, which takes everything from the beginning of a sequence to offset m. It is equivalent to 0:m eth.src[4:] == 20:20 The example above uses the n: format, which takes everything from offset n to the end of the sequence. eth.src[2] == 83 The example above uses the n format to specify a single range. In this case the element in the sequence at offset n is selected. This is equivalent to n:1. eth.src[0:3,1-2,:4,4:,2] == 00:00:83:00:83:00:00:83:00:20:20:83 Wireshark allows you to string together single ranges in a comma separated list to form compound ranges as shown above.

22.6.3.3 List of Supported Display Filters

RTR uses `tshark` version 1.6.14 for applying filters. `tshark` supports a wide range of display filters. For detailed list of display filters, refer to *http://www.wireshark.org/docs/dfref/*.

Refer to *http://www.wireshark.org/docs/dfref/g/gsm_map.html* for display filters supported on GSM MAP protocol.

22.7 Command-Line Tools for Troubleshooting

The following command-line tools are available for troubleshooting purposes:

Tool	Description
m3ua_link	Allows you to: • Show the status of the M3UA link • Enable or disable the M3UA SGP admin state • Display the information fields for all the peer SGPs, along with the M3UA SGP information • Enable or disable the M3UA ASP admin state • Display the information of all configured ASPs in multi-instance mode.
ss7_link	Allows you to: • Show the status of the link (including error conditions) • Receive and displaying all traps related to the link • Enable or disable the link
tp_event	Allows you to decode an event log file created by an event log profile.
tp_fcdr tp_lcdr tp_ecdr tp_ncdr tp_ccdr tp_scdr tp_3g_cdr	Allow you to decode and view CDR files of all supported types.
tp_log	Allows you to decode a log file created by a log profile.
tp_manage_user	Allows you to manage users in a multi-instance setup.
tp_status	Provides the operational state and uptime of components.
tp_system	Allows you to: • View software and hardware information • Activate licenses • Boot the system • Enable and disable subscriptions to the trap service
tp_trace_receiver	Receives trace data from components and writes it to a PCAP file.

Tool	Description
tp_walk	Provides the real-time value of any SNMP attribute.
tp_walkall	Provides the real-time value of all SNMP attributes.

22.8 Commands for Troubleshooting

The following operating system tools are available for troubleshooting:

Tool	Description
`gcore`	Generates a core file
`hostid`	Provides the host ID of the system (required for a license)
`ifconfig`	Provides an overview of the IP configuration
`netstat`	Provides an overview of IP network statistics
`ping`	An IP diagnostic command
`top`	Shows statistics about active processes
`ps`	Provides information about processes
`sar`	Provides performance data
`tcpdump`	Trace network traffic on TCP/IP level

Refer to the Red Hat Enterprise Linux documentation at *http://www.redhat.com/docs/*.

Chapter 23

Service Center Time Stamps

Topics:

This chapter briefly describes the implications of unique service center timestamps in the mobile messaging system.

23.1 Service Center Time Stamps

RTR nodes can create unique Service Center Time Stamps (SCTSs) for a certain recipient MSISDN. SCTSs cannot have the same timestamp assigned to two messages to the same recipient processed during the same second, so SCTSs sent within a single second are assigned a timestamp one second into the future to the second message. A record is kept for remembering that the next second has also been used, and any new message to the same recipient processed before the latest used timestamp will create an SCTS one second further into the future.

In most cases, several RTR nodes process messages at the same time, and with load balancing over all RTR nodes, messages cannot be routed for the same recipient to the same RTR node. As such, a RTR node cannot guarantee unique SCTSs across all RTR nodes. In order to achieve SCTS uniqueness, the RTR provides the option to offload the SCTS generation to available AMS nodes. All RTR nodes use the same algorithm to ensure that all SCTS requests for the same recipient are sent to the same AMS node, producing the desired unique timestamps.

In order to enable the AMS-based SCTS generation, the

```
amsmediatedservicecentertimestampsenable
```

attribute should be set to "true" in the common configuration file. Otherwise, SCTS generation will be performed on the RTR node as described above.

Chapter 24

Intercept Files

Topics:

24.1 Introduction

Intercept files are generated by the RTR. They are used by the Direct Message Filter (DMF) component. The DMF provides the near real-time reporting on specific monitored MSISDNs, with the minimum amount of required manual interaction by the operator staff.

The RTR is in the path of all the messages. The RTR creates an intercept file at the time of Submit, Expired, Deleted, Blocked and Delivery (success/failed) CDR generation.

24.2 Configuring Intercept Files

1. Intercept file location directory:

   The RTR creates intercept files in the location on local file system mentioned by the semi-static parameter *interceptfilelocation*.

   The RTR does not create the intercept files location directory. It must be created during the intercept file generation setup with the file owner as `textpassdmf` user, group as `textpass` and permissions as `730`. The user `textpass` will not have read permission, so it will not be able to check the intercept files. Execute permissions to group (`textpass`) on every parent directory of intercept directory must be given.

   To store the intercept file while they are created, the RTR creates a `processing` directory with permission as `730` in the intercept directory.

2. Intercept file name template:

   The RTR generates intercept files with names based on the template defined by the semi-static parameter *rtrinterceptfilenametemplate*. This parameter is a format string that specifies the name of the intercept file in the intercept directory.

   To set *rtrinterceptfilenametemplate*, one must first set *interceptfilelocation* with a location having proper permissions. If this parameter is not set, the RTR will not generate intercept files at the specified intercept directory location. The RTR creates intercept files with permission `222`.

   Use the following case-sensitive variables to construct the intercept file name template:

Variable	Description
%Y	Year formatted with four digits (for example, 2008)
%y	Year formatted with two digits (for example, 08)
%m	Month formatted with two digits (for example, 01 for January and 10 for October)
%d	Day formatted with two digits (for example, 01 for the first day of May and 31 for the last day of May)
%H	Hour in 24-hour time format

Variable	Description
%M	Minutes
%S	Seconds
%h	Host name
%U	UID (operating system user identifier) of the user from which RTR process is running
%1	One-digit sequence number
%2	Two-digit sequence number
%3	Three-digit sequence number
%4	Four-digit sequence number
%5	Five-digit sequence number
%6	Six-digit sequence number
%7	Seven-digit sequence number
%8	Eight-digit sequence number

For example: `intercept_%h_%Y%m%d_%H%M%S_%3.dat`, results in the following files for the user `textpass`:

`intercept_southhost_20080830_023145_111.dat`

3. Maximum intercept file duration:

   The semi-static parameter *rtrmaxinterceptfileduration* indicates the maximum duration after which the intercept file is closed from the `processing` directory and moved to the location specified by the parameter *interceptfilelocation*. The default value of this parameter is 60 seconds.

24.3 Intercept File Record

1. Intercept file record are created as per the FCDR ASN.1 definition. Please refer to the RTR Billing Manual for the details of FCDR ASN1 definition.
2. The `origType` and `destType` fields are included in FCDR.asn1.
   a. These fields are not part of CDRs.
   b. These are logged only in case of intercept file records.
   c. The `tp_fcdr` utility can decode these 2 fields if they are present.
3. Intercept file records have addresses in International format.
4. FCDR asn.1 has a lot of fields. Not all the fields are applicable or available for every message. All the fields which are applicable and available for the message are stored in Intercept record.

   For example, for an AO from a short number, **Originator IMSI** and **Originator MSC** are not available, so these fields are not stored in the intercept record.
5. Intercept File record will have User Data if it is enabled in License as for CDR.

6. Below are the values of the FCDR ASN.1 fields that are taken while creating intercept record:
   a. Use SMPP SAR info is false
   b. Use Short Number as Originator for AO is true
   c. Address Information Includes MSISDN Utf8 is true
   d. Use AO for consolidation for AO AT is false
   e. Max validity period is 8760 hours (1 year)
   f. Alphanumeric addresses are decoded as if the address were numeric in the MSISDN field of the address construct
   g. In case of an AO message with an alphanumeric address, the alphanumeric address is populated in the `untranslOrigAddressGSM` field.
   h. Max defer period is 8760 hours (1 year)
   i. TON value 4 (subscriber) and NPI value 5 (private) are used for short numbers
   j. VSMSC ID is determined based on the last 3 digits of the SMSC's GT
   k. Max intercept file size is 1024 * 1024 bytes
   l. Not Delivered Status is rejected
   m. Mt Failed Status is failed

   For detailed information about the above-mentioned fields, refer to the section 4.2 Formatted Call Detail Record (FCDR) of RTR Billing Manual.
7. Notifications are not stored in Intercept files.
8. For direct delivery flows like AO-MT, MO-MT, MO-MT-ST (with MT success in FDA), one intercept record is created at the time of submission and another at the time of Delivery (success).
9. For Store related scenario's like MO-ST-MT, AO-ST-MT etc., one submit intercept record is created for Store part and another for Store to Delivery(success/failed)/Deleted/Expired part.
10. Only 1 submission intercept record is generated in all the flow. Please do not confuse this with flows such as MO-MO or AO-AO. In these flows, 2 submission intercept records are generated, one for submission of incoming MO/AO message and other for the outgoing MO/AO message getting sent to an SMSC.
11. In case of MO/SIPO-MT/SIPT fallback to storage scenario, submit intercept record is generated when message is received by RTR. No intermediate submit record is generated when message falls back to Store in case of FDA failure. Also, the RTR will not generate the intercept record with the 'failed' status when the FDA gets failed.
12. Each delivery attempt from AMS is recorded in intercept record.
13. In case of MO-MT failed or AO-AT failed scenario, only 1 failed intercept record is generated. In these cases, the submit intercept record is only generated if there is an MO/AO positive submit ack.
14. In submission record, the `destType` field is not included for terminating MT/SIPT scenarios. At the time of submission in case of MT/SIPT terminating scenario, the RTR is not aware whether the message is destined for an SS7 or IMS domain, hence this field is not populated.
15. Traps are generated if there is a failure in the creation or writing of the intercept file.

24.4 Intercept File Record Fields

Field	Description
amsStatus	AMS Status of the message. Possible values: • unknown(0): AMS is not involved • temp(1): AMS attempt resulted in temporary error • perm(2): AMS attempt resulted in permanent error • delivered(3): AMS attempt resulted in successful delivery.
aser	Additional services. Meaningful bits: • Bit 7: Notification requested • Bit 29: Single-shot indication
billId	Billing ID; only present if originator is an LA and the message was submitted as UCP51 with a non-empty billing field.
callingLineId	Calling line ID: • In case of MO, contains MSISDN of originator • In case of AO, TON is 4, NPI is 5
callingLineIdGSM	Calling line ID, formatted according to 3GPP TS 23.040: • In case of MO, contains MSISDN of originator (formatted according to 3GPP TS 23.040) • In case of AO, TON is 4, NPI is 5
chargeInfo	Proprietary NewNet native Diameter field (only applies when PBC is in use with the Diameter protocol); see AVP 12 in the description of the NewNet native Diameter dialect for more information.
cimdPriority	Proprietary field indicating CIMD priority (1-9). This only applies to AO messages submitted by a CIMD application. Value 0 indicates that the service description field was not present in the message.
cimdServiceDescription	Proprietary field indicating CIMD service description (0-99). This only applies to AO messages submitted by a CIMD application. Value 0 indicates that the service description field was not present in the message.
cimdTariffClass	Proprietary field indicating CIMD tariff class (0-99). This only applies to AO messages submitted by a CIMD application. Value 0 indicates that the tariff class was not present in the message.
cmReferenceNr	Reference number (0-255) that is constant for each piece of a concatenated message (only present in case of a concatenated message).

Field	Description
Consolidation	The intercept record format allows for a single value to be recorded as the consolidation field only (applies to AO-AT traffic). If a message is routed from one application to another, two different values may be applicable to the same message. This is only present if originator or recipient is an LA. If not specified, the field is set to the LA's short number and: • Encoded if short number is no longer than 5 digits • Pre-pended with zeroes if number is shorter than 5 digits (for example, 4000 becomes 04000)
currentSegment	Sequence number (0-255) that indicates sequence of pieces in a concatenated message (only present in case of a concatenated message).
deferIndicator	Deferred delivery request indicator.
deferPeriod	Period of deferred delivery request.
deliveryAttempts	Number of delivery attempts before generating the CDR for a processed message.
destPointCode	Point code of the destination MSC or SGSN (only present if routing on the point code and if recipient is a mobile).
destType	This field specifies Message Termination MO, AO, SIPO, MT, AT, SIPT
dgtiAddress	Address of the destination MSC or SGSN (only present if routing on the global title and if recipient is a mobile).
dgtiAddressGSM	Address of the destination MSC or SGSN (only present if routing on the global title and if recipient is a mobile), formatted according to 3GPP TS 23.040.
externalAttributes	Proprietary field indicating external attributes set by the EC application (only applies when an EC application has CDR-specific set or reset attributes in the response).
furnishChargingInfo	Proprietary CAMEL field (0-9999). Note that this field can be empty (blank string), and only CDRs containing a non-empty field qualify for refunding.
genericUrgencyLevel	Always 1 (normal).
intlMobileSubId	Recipient's IMSI (value is only available if the RTR performed an SRI-SM for the recipient address).
Lang	Always 0.
mesgReplyPath	Possible values: • Message is a reply path (1) • Message is a reply path response (2) • Message is neither (field will not be present)

Field	Description
messageReference	Unique message ID (unique across CDRs).
Mser	Requested services. Meaningful bits: • Bit 0: No default validity period for SM • Bit 3: Generate delivery notification • Bit 4: Generate non-delivery notification • Bit 7: Priority message
notifAddress	Address to which notification was sent (only present if notif indicator is included).
notifAddressGSM	Address to which notification was sent (only present if notif indicator is included), formatted according to 3GPP TS 23.040.
notifIndicator	Possible values: • 0: Notification or status report was not generated for this message • 1: Notification or status report was generated For AO-MT traffic, this field is only set if the message included a notification request and if **Allow Notification** option in **SMS Applications ➤ Applications** is selected.
Nser	New services. Meaningful bits: • Bit 2: Replace PID supplied • Bit 5: Originator is an LA • Bit 6: Recipient is an LA
ogtiAddress	Address of the first MSC in the routing path (only present if routing on the global title).
ogtiAddressGSM	Address of the first MSC in the routing path (only present if routing on the global title), formatted according to 3GPP TS 23.040.
origAddress	Originator address.
origAddressGSM	Originator address, formatted according to 3GPP TS 23.040. Refer to Originator Address Fields for more information.
originatorApplicationChargingUnits	Number of units used when charging messages sent by the application.
originatorSsi	Originator SSI service names that are applicable to the message, in CSV format.
origIntlMobileSubId	Originator's IMSI
origLASN	Originating application short number in decimal notation.
origMsgID	message_id returned to the message originator on submission (SMPP only).

Field	Description
origPointCode	Point code of the first MSC in the routing path.
origType	This field specifies Message Originator MO, AO, SIPO, MT, AT, SIPT , IGM
portNumber	Connect port of the LA; listen port on the HUB (only present if originator or recipient is an LA).
ppPser	Indicates if originator is a prepaid subscriber (only applies when PBC is in use; not included for AO traffic). The RTR sets bit 0 (orig-pp) to: • 0: Originator is post-paid • 1: Originator is prepaid
prepaidBillingState	Proprietary field indicating billing state of the originator (only applies when PBC is in use). Possible values: • H: Prepaid, hot-billing • N: Post-paid • O: Prepaid, online-charged If the *adjustprepaidindicatorondeductfailure* attribute in the RTR configuration file is set to true, online-charged will be changed to hot-billed.
prepaidBillingStateOfRecipient	Proprietary field indicating billing state of the recipient (only applies when PBC is in use). Possible values: • H: Prepaid, hot-billing • N: Post-paid • O: Prepaid, online-charged If the *adjustprepaidindicatorondeductfailure* attribute in the RTR configuration file is set to true, online-charged will be changed to hot-billed.
prepaidResultCode	Proprietary field indicating Diameter result code (only applies when PBC is in use with the Diameter protocol).
prioIndicator	Priority delivery request indicator.
recipAddress	Recipient address.
recipAddressGSM	Recipient address, formatted according to 3GPP TS 23.040.
recipientRoutingNumber	Proprietary field indicating routing number used in the SCCP called party address for operations toward the HLR when MNP is in use.
recipientSsi	Recipient SSI service names that are applicable to the message, in CSV format.
recipLASN	Recipient large account short number in decimal notation.

Field	Description
segmentsTotal	Total number (0-255) that indicates the total number of pieces in a concatenated message (only present in case of a concatenated message).
serviceType	service_type provided by the message originator (SMPP only).
signaturePresent	Indicates whether an SMS signature is present. Possible values: • 0: Signature is not present • 1: Signature is present This only applies when XS-SIG is in use.
smeReference	• For GSM-submitted messages, the TP-MR provided by the message originator • For non-GSM-submitted messages, always 0
smsContentDcs	Indicates the encoding used in the smsContents field: • DEFAULT: ISO Latin 1 ISO-8859-1, used for messages with GSM 7-bit default alphabet encoding • DATA: Binary data • UCS2: UCS2 encoding
smsContents	Content of the user data, encoded according to smsContentDcs. Note: For Mobile-Terminated messages matching an MTOR rule that specifies an MT Character (Translation) Map, the 'SMS Content' field would reflect the un-translated user data, i.e. the data just before the MT character translation was applied.
smscPresentationAddress	Proprietary field indicating MAP presentation address of the SMSC that send the MT message (only applies to the MT-MT routing path). Controls the inclusion of the following parameters in the SMSC address: • TON • NPI • MSISDN • PID
smscPresentationAddressGSM	Proprietary field indicating MAP presentation address of the SMSC that send the MT message (only applies to the MT-MT routing path), formatted according to 3GPP TS 23.040.
ss8LastFailureReason	Proprietary field indicating the last failure reason. Possible values: • No failure reason available (0) • Unknown subscriber (1) • Unidentified subscriber (5) • Illegal subscriber (9) • Teleservice not provisioned (11) • Illegal equipment (12)

Field	Description
	• Call barred (13) • Facility not supported (21) • Absent subscriber (27) • Subscriber busy for MT SMS (31) • Message waiting list full (33) • System failure (34) • Data missing (35) • Unexpected data value (36) • Memory capacity exceeded (50) • Equipment protocol error (51) • Equipment not SM equipped (52) • Internal system failure (80) • HLR timed out (86) • MSC timeout (87) • TCAP abort received (101)

Status	Message status. Possible values:
	• Delivered (0): RTR sent the message to the application
	• Configurable value: Message was discarded while sending a positive acknowledgement toward the originator
	• A value of submitted (4) means that the RTR applied an always ACK rule or has routed the message to the SMSC; a value of expired (1) means that the MO-AT routing failed
	• A value of failed (5) is used only in case there is a delivery failure while trying to send a copied/forwarded message to the mail server, via the HUB and the EMG
	• A value of rejected (9) is used only in case there is a discard message when one of the following routing rule actions or external condition rule failure actions has been applied:
	  • Discard with Nack
	  • Discard with no response
	  • Discard with Permanent Error

submitDate	Date the message was submitted to the RTR (format YYMMDD).
submitTime	Time the message was submitted to the RTR (format HHMMSS). Note that this field contains the potentially adjusted submission time as described in the RTR Operator Manual chapter on Service Center Time Stamps. As such, the value of this field, as well as the submitDate field, should not be used to determine the arrival time of the message, rather, the orglSubmitTime/orglSubmitDate should be included in the intercept records and used instead. Since submitTime/submitDate fields are made unique by increasing the value, submitTime / submitDate could exceed the orglSubmitTime/ orglSubmitDate, the terminTime/ terminDate,

Field	Description
	and the CDR file time/ date. For inbound MT and outbound MT, the submitTime is the timestamp received from SMSC. If mtmtuseuniquescts is set to true, the RTR generates a unique timestamp for MT-MT home-routed case (i.e. submitTime/submitDate fields are made unique by increasing the value). This unique timestamp may represent the time in the future. For routing paths other than MT-MT (e.g. MT-AO, MT-AT, MT-Store-MT) this parameter value is a RTR generated unique timestamp if mtmtuseuniquescts is true and a SMSC timestamp if set to false.
subscriberStatus	Proprietary field indicating subscriber status (only applies when PBC is in use). Possible values: • Prepaid with credit below threshold (1) • Post-paid (2) • Prepaid with credit above threshold (3) • Cost control post-paid (4) • Cost control prepaid (5) • Cost control with no account (6) • Convergente (7)
subscriberStatusOfRecipient	Proprietary field indicating recipient's subscriber status (only applies when PBC is in use). Possible values: • Prepaid with credit below threshold (1) • Post-paid (2) • Prepaid with credit above threshold (3) • Cost control post-paid (4) • Cost control prepaid (5) • Cost control with no account (6) • Convergente (7)
terminatorApplicationChargingUnits	Number of units used when charging messages sent to the application.
terminDate	Date the RTR delivered or deleted the message (format YYMMDD).
terminTime	Time the RTR delivered or deleted the message (format HHMMSS).
tpDCS	• For GSM-submitted messages, TP-DCS provided by the message originator • For SMPP-submitted messages, data_coding provided by the message originator • Always 0 when message is not GSM- or SMPP-submitted
transparentPid	• In case of MO, contains PID of recipient address, as provided by originator

Field	Description
	• In case of AO or UCP51, contains contents of RPID • In case of AO, empty RPID, or other submit operation, contains 0
untranslOrigAddress	Source address, as received before any modification or normalization.
untranslOrigAddressGSM	Source address, as received before any modification or normalization, formatted according to 3GPP TS 23.040.
untranslRecipAddress	Destination address, as received before any modification or normalization.
untranslRecipAddressGSM	Destination address, as received before any modification or normalization, formatted according to 3GPP TS 23.040.
validityPeriod	Message validity period.
vsmscId	Last three digits of the service center that was originally addressed. Refer to Virtual SMSC Fields for more information.
vsmscType	Whether Virtual SMSC (VSMSC) is associated with an LA.
Xser	Extra services. Meaningful bits: • Bit 15: Reject duplicates
xsMessageType	Proprietary field indicating the message type: • forwardedMessage (0) • copiedMessage (1) • copyToApplication (2) • autoReply (3) • copyToEmail (4) • forwardToEmail (5) This only applies when XS-CPY, XS-FWD and/or XS-ARP are in use.
xsTieBillingId	Proprietary field indicating XS-TIE billing ID (only applies when XS-TIE is in use).

24.5 Sample Intercept File

The following sample intercept file contains a submit and delivery intercept record for single SIPO-MT flow:

```
File: intercept_log_2019190207135050KVM722001.dat, CDR: 1

          30 80 a0 25  80 01 01 81  01 01 82 01  00 83 0c 34  39 31 37 32
          30 34 39 30  30 30 31 84  0c 34 39 31  37 32 30 34  39 30 30 30
          31 81 07 91  94 71 02 94  00 10 a2 25  80 01 01 81  01 01 82 01
```

```
          00 83 0c 38  35 35 32 30  31 32 33 34  35 36 37 84  0c 38 35 35
          32 30 31 32  33 34 35 36  37 83 07 91  58 25 10 32  54 76 84 03
          13 02 07 85  03 0d 32 34  86 01 04 87  03 13 02 07  88 03 0d 32
          34 89 02 00  a0 8a 01 00  ab 06 80 01  18 81 01 00  8c 01 00 8e
          01 00 91 02  02 9a 92 01  02 b6 25 80  01 01 81 01  01 82 01 00
          83 0c 34 39  31 37 32 30  30 30 30 30  31 31 84 0c  34 39 31 37
          32 30 30 30  30 30 31 31  97 07 91 94  71 02 00 00  11 98 02 06
          10 99 03 13  02 07 9a 03  0d 32 34 9b  01 00 be 25  80 01 01 81
          01 01 82 01  00 83 0c 34  39 31 37 32  30 34 39 30  30 30 31 84
          0c 34 39 31  37 32 30 34  39 30 30 30  31 9f 1f 07  91 94 71 02
          94 00 10 9f  22 05 00 00  00 00 00 9f  23 03 00 00  00 9f 24 05
          00 00 00 00  00 9f 25 03  00 00 00 9f  28 01 00 9f  2a 05 00 00
          00 00 00 9f  2f 02 00 9b  9f 30 07 44  45 46 41 55  4c 54 9f 31
          81 a0 6c 6f  6d 70 6b 64  67 61 7a 63  6a 71 6a 6f  6a 6f 6d 65
          70 65 6f 68  77 76 76 78  70 6f 65 72  72 67 63 76  65 6c 6a 76
          64 67 65 6d  6a 6e 6e 6a  6e 64 6e 70  74 6f 69 75  70 67 72 6f
          75 78 78 62  75 78 71 65  68 65 68 76  6e 61 66 61  6a 71 6e 6f
          64 76 61 61  6a 71 61 71  78 6a 73 6b  7a 70 63 66  75 77 74 61
          74 6b 6a 66  65 62 64 65  75 62 75 70  6b 66 65 70  69 70 7a 6a
          65 68 62 64  61 78 79 71  79 71 62 6a  64 63 66 63  61 79 78 78
          77 64 65 62  71 74 63 65  63 64 61 74  79 61 71 63  6c 69 61 78
          74 6e 9f 46  0e 10 ac 48  85 00 00 5c  5c 29 ac e9  4c f5 00 9f
          4a 0a 30 30  30 30 30 30  30 30 30 31  9f 52 01 00  bf 53 17 80
          01 01 81 01  01 82 01 00  83 0c 34 39  31 37 32 30  34 39 30 30
          30 31 9f 54  07 91 94 71  02 94 00 10  bf 55 17 80  01 01 81 01
          01 82 01 00  83 0c 38 35  35 32 30 31  32 33 34 35  36 37 9f 56
          07 91 58 25  10 32 54 76  9f 58 01 00  9f 59 01 01  9f 83 5b 34
          33 47 50 50  2d 45 2d 55  54 52 41 4e  2d 46 44 44  3b 75 74 72
          61 6e 2d 63  65 6c 6c 2d  69 64 2d 33  67 70 70 3d  32 36 32 30
          39 36 65 61  31 30 30 31  34 31 30 34  9f 83 5c 78  49 45 45 45
          2d 45 2d 55  54 52 41 4e  2d 46 44 44  3b 75 74 72  61 6e 2d 63
          65 6c 6c 2d  69 64 2d 33  67 70 70 3d  32 36 32 30  32 61 63 35
          30 30 62 32  39 63 30 33  33 33 33 33  33 33 33 33  33 33 33 33
          33 33 33 33  33 33 33 33  33 33 33 33  33 33 33 33  33 31 31 31
          31 31 31 31  31 31 31 31  31 31 31 31  31 31 31 32  32 32 32 32
          32 32 32 32  32 32 34 34  34 34 34 34  34 34 34 31  9f 83 5d 78
          33 47 50 50  2d 45 2d 55  54 52 41 4e  2d 46 44 44  3b 63 65 6c
          6c 2d 74 69  6d 65 3d 32  30 31 36 2d  30 37 2d 31  32 54 31 35
          3a 31 35 3a  34 37 5a 3b  72 65 67 2d  74 69 6d 65  3d 32 30 31
          36 2d 30 37  2d 31 32 54  31 35 3a 31  35 3a 34 37  5a 3b 75 74
          72 61 6e 2d  63 65 6c 6c  2d 69 64 2d  33 67 70 70  3d 32 36 32
          30 32 61 63  35 30 30 61  31 31 31 30  35 35 35 35  35 35 35 31
          9f 83 5f 01  00 9f 83 66  00 9f 83 6a  01 00 9f 83  71 05 00 00
          00 00 00 9f  83 75 01 03  9f 83 77 01  00 00 00

30 80            CallDetailedRecord = {
a0 25              origAddress = {
80 01 01             ton = international(1)
81 01 01             npi = telephone(1)
82 01 00             pid = 0
83 0c 34 39 31 37 32 30 34 39 30 30 30 31
                     msisdn = '491720490001'
84 0c 34 39 31 37 32 30 34 39 30 30 30 31
                     msisdnUTF8 = '491720490001'
                     }
81 07 91 94 71 02 94 00 10
                     origAddressGSM = 'international/telephone 491720490001'
a2 25                recipAddress = {
80 01 01             ton = international(1)
81 01 01             npi = telephone(1)
82 01 00             pid = 0
83 0c 38 35 35 32 30 31 32 33 34 35 36 37
                     msisdn = '855201234567'
84 0c 38 35 35 32 30 31 32 33 34 35 36 37
                     msisdnUTF8 = '855201234567'
```

```
                    }
83 07 91 58 25 10 32 54 76
                    recipAddressGSM = 'international/telephone 855201234567'
84 03 13 02 07
                    submitDate = 7-Feb-2019
85 03 0d 32 34
                    submitTime = 13:50:52
86 01 04            status = submitted(4)
87 03 13 02 07
                    terminDate = 7-Feb-2019
88 03 0d 32 34
                    terminTime = 13:50:52
89 02 00 a0         lengthOfMessage = 160
8a 01 00            prioIndicator = false(0)
ab 06               validityPeriod = {
80 01 18              hours = 24
81 01 00              minutes = 0
                    }
8c 01 00            deferIndicator = false(0)
8e 01 00            notifIndicator = false(0)
91 02 02 9a         vsmscId = 666
92 01 02            vsmscType = public(2)
b6 25               ogtiAddress = {
80 01 01              ton = international(1)
81 01 01              npi = telephone(1)
82 01 00              pid = 0
83 0c 34 39 31 37 32 30 30 30 30 30 31 31
                      msisdn = '491720000011'
84 0c 34 39 31 37 32 30 30 30 30 30 31 31
                      msisdnUTF8 = '491720000011'
                    }
97 07 91 94 71 02 00 00 11
                    ogtiAddressGSM = 'international/telephone 491720000011'
98 02 06 10         origPointCode = 1552
99 03 13 02 07
                    orglSubmitDate = 7-Feb-2019
9a 03 0d 32 34
                    orglSubmitTime = 13:50:52
9b 01 00            transparentPid = 0
be 25               callingLineId = {
80 01 01              ton = international(1)
81 01 01              npi = telephone(1)
82 01 00              pid = 0
83 0c 34 39 31 37 32 30 34 39 30 30 30 31
                      msisdn = '491720490001'
84 0c 34 39 31 37 32 30 34 39 30 30 30 31
                      msisdnUTF8 = '491720490001'
                    }
9f 1f 07 91 94 71 02 94 00 10
                    callingLineIdGSM = 'international/telephone 491720490001'
9f 22 05 00 00 00 00 00
                    aser =  {
                      swinq(0) = false(0)
                      swdel(1) = false(0)
                      notifreq(7) = false(0)
                      notifalw(8) = false(0)
                      usrnotif(9) = false(0)
                      lradreq(10) = false(0)
                      ackdel(26) = false(0)
                      ackman(27) = false(0)
                      singleshot(29) = false(0)
                    }
9f 23 03 00 00 00
                    mser =  {
                      svp(0) = false(0)
```

```
                      sdd(2) = false(0)
                      nde(3) = false(0)
                      nnd(4) = false(0)
                      nbu(5) = false(0)
                      pri(7) = false(0)
                      unsol(8) = false(0)
                      lrad(9) = false(0)
                    }
9f 24 05 00 00 00 00 00
                    nser =  {
                      mrep(2) = false(0)
                      deleted(3) = false(0)
                      replaced(4) = false(0)
                      lao(5) = false(0)
                      lar(6) = false(0)
                      fwad(7) = false(0)
                      fwad-cond(8) = false(0)
                      user-data-header(24) = false(0)
                      del-by-operator(28) = false(0)
                    }
9f 25 03 00 00 00
                    xser =  {
                      inqdel(4) = false(0)
                      swnotif(8) = false(0)
                      dl(9) = false(0)
                      rejdupl(15) = false(0)
                    }
9f 28 01 00         lang = 0
9f 2a 05 00 00 00 00 00
                    ppPser =  {
                      orig-pp(0) = false(0)
                      recip-pp(1) = false(0)
                      orig-blocked(2) = false(0)
                      recip-blocked(3) = false(0)
                      prim(4) = false(0)
                      charge-recip(5) = false(0)
                      free(6) = false(0)
                      during-jam(7) = false(0)
                      applied-pmgt(8) = false(0)
                    }
9f 2f 02 00 9b
                    smeReference = 155
9f 30 07 44 45 46 41 55 4c 54
                    smsContentDcs = 'DEFAULT'
9f 31 a0 6c 6f 6d 70 6b 64 67 61 7a 63 6a 71 6a 6f 6a 6f 6d 65 70 65 6f 68 77 76 76
 78 70 6f 65 72 72 67 63 76 65 6c 6a 76 64 67 65 6d 6a 6e 6e 6a 6e 64 6e 70 74 6f
69 75 70 67 72 6f 75 78 78 62 75 78 71 65 68 65 68 76 6e 61 66 61 6a 71 6e 6f 64 76
 61 61 6a 71 61 71 78 6a 73 6b 7a 70 63 66 75 77 74 61 74 6b 6a 66 65 62 64 65 75
62 75 70 6b 66 65 70 69 70 7a 6a 65 68 62 64 61 78 79 71 79 71 62 6a 64 63 66 63 61
 79 78 78 77 64 65 62 71 74 63 65 63 64 61 74 79 61 71 63 6c 69 61 78 74 6e
                    smsContents =
'lompkdgazcjqjojomepeohwvvxpoerrgcveljvdgemjnnjndnptoiupgrouxxbuxqehehvnafajqnodvaajqaqxjskzpcfuwtatkjfebdeubupkfepipzjehbdaxyqyqbjdcfcayxxwdebqtcecdatyaqcliaxtn'
9f 46 0e 10 ac 48 85 00 00 5c 5c 29 ac e9 4c f5 00
                    messageReference = 10-ac-48-85-00-00-5c-5c-29-ac-e9-4c-f5-00
9f 4a 0a 30 30 30 30 30 30 30 30 30 31
                    origMsgID = '0000000001'
9f 52 01 00         deliveryAttempts = 0
bf 53 17            untranslOrigAddress = {
80 01 01              ton = international(1)
81 01 01              npi = telephone(1)
82 01 00              pid = 0
83 0c 34 39 31 37 32 30 34 39 30 30 30 31
                      msisdn = '491720490001'
                    }
9f 54 07 91 94 71 02 94 00 10
```

```
                    untranslOrigAddressGSM = 'international/telephone 491720490001'
bf 55 17            untranslRecipAddress = {
80 01 01              ton = international(1)
81 01 01              npi = telephone(1)
82 01 00              pid = 0
83 0c 38 35 35 32 30 31 32 33 34 35 36 37
                      msisdn = '855201234567'
                    }
9f 56 07 91 58 25 10 32 54 76
                   untranslRecipAddressGSM = 'international/telephone 855201234567'
9f 58 01 00         tpDCS = 0
9f 59 01 01         genericUrgencyLevel = normal(1)
9f 83 5b 34 33 47 50 50 2d 45 2d 55 54 52 41 4e 2d 46 44 44 3b 75 74 72 61 6e 2d 63
 65 6c 6c 2d 69 64 2d 33 67 70 70 3d 32 36 32 30 39 36 65 61 31 30 30 31 34 31 30
34
                    originatorPaniUE =
3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=262096ea10014104
9f 83 5c 78 49 45 45 45 2d 45 2d 55 54 52 41 4e 2d 46 44 44 3b 75 74 72 61 6e 2d 63
 65 6c 6c 2d 69 64 2d 33 67 70 70 3d 32 36 32 30 32 61 63 35 30 30 62 32 39 63 30
33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33
 33 33 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 32 32 32 32 32 32 32
32 32 32 32 34 34 34 34 34 34 34 34 34 31
                    originatorPaniNP =
IEEE-E-UTRAN-FDD;utran-cell-id-3gpp=2620ac500b29c033333333333333333333333333331111111111111111112222222222244444444411
9f 83 5d 78 33 47 50 50 2d 45 2d 55 54 52 41 4e 2d 46 44 44 3b 63 65 6c 6c 2d 74 69
 6d 65 3d 32 30 31 36 2d 30 37 2d 31 32 54 31 35 3a 31 35 3a 34 37 5a 3b 72 65 67
2d 74 69 6d 65 3d 32 30 31 36 2d 30 37 2d 31 32 54 31 35 3a 31 35 3a 34 37 5a 3b 75
 74 72 61 6e 2d 63 65 6c 6c 2d 69 64 2d 33 67 70 70 3d 32 36 32 30 32 61 63 35 30
30 61 31 31 31 30 35 35 35 35 35 35 35 31
                    originatorPcni =
3GPP-E-UTRAN-FDD;cell-time=2016-07-12T15:15:47Z;reg-time=2016-07-12T15:15:47Z;utran-cell-id-3gpp=2620ac500a111055555551
9f 83 5f 01 00
                    signaturePresent = false(0)
9f 83 66 00         furnishChargingInfo = ''
9f 83 6a 01 00
                    ss8LastFailureReason = noFailureReasonAvailable(0)
9f 83 71 05 00 00 00 00 00
                    externalAttributes =  {
                      attribute-1(0) = false(0)
                      attribute-2(1) = false(0)
                      attribute-3(2) = false(0)
                      attribute-4(3) = false(0)
                      attribute-5(4) = false(0)
                      attribute-6(5) = false(0)
                      attribute-7(6) = false(0)
                      attribute-8(7) = false(0)
                      attribute-9(8) = false(0)
                      attribute-10(9) = false(0)
                      attribute-11(10) = false(0)
                      attribute-12(11) = false(0)
                      attribute-13(12) = false(0)
                      attribute-14(13) = false(0)
                      attribute-15(14) = false(0)
                      attribute-16(15) = false(0)
                      attribute-17(16) = false(0)
                      attribute-18(17) = false(0)
                      attribute-19(18) = false(0)
                      attribute-20(19) = false(0)
                      attribute-21(20) = false(0)
                      attribute-22(21) = false(0)
                      attribute-23(22) = false(0)
                      attribute-24(23) = false(0)
                      attribute-25(24) = false(0)
                      attribute-26(25) = false(0)
                      attribute-27(26) = false(0)
```

```
                    attribute-28(27) = false(0)
                    attribute-29(28) = false(0)
                    attribute-30(29) = false(0)
                    attribute-31(30) = false(0)
                    attribute-32(31) = false(0)
                  }
9f 83 75 01 03
                  origType = SIPO(3)
9f 83 77 01 00
                  amsStatus = Unknown(0)
00 00           }


File: intercept_log_2019190207135050KVM722001.dat, CDR: 2

          30 80 a0 25  80 01 01 81  01 01 82 01  00 83 0c 34  39 31 37 32
          30 34 39 30  30 30 31 84  0c 34 39 31  37 32 30 34  39 30 30 30
          31 81 07 91  94 71 02 94  00 10 a2 25  80 01 01 81  01 01 82 01
          00 83 0c 38  35 35 32 30  31 32 33 34  35 36 37 84  0c 38 35 35
          32 30 31 32  33 34 35 36  37 83 07 91  58 25 10 32  54 76 84 03
          13 02 07 85  03 0d 32 34  86 01 00 87  03 13 02 07  88 03 0d 32
          36 89 02 00  a0 8a 01 00  ab 06 80 01  18 81 01 00  8c 01 00 8e
          01 00 91 02  02 9a 92 01  02 b3 25 80  01 01 81 01  01 82 01 00
          83 0c 34 39  39 37 33 33  33 33 33 33  33 33 84 0c  34 39 39 37
          33 33 33 33  33 33 33 33  94 07 91 94  79 33 33 33  33 b6 25 80
          01 01 81 01  01 82 01 00  83 0c 34 39  31 37 32 30  30 30 30 30
          31 31 84 0c  34 39 31 37  32 30 30 30  30 30 31 31  97 07 91 94
          71 02 00 00  11 98 02 06  10 99 03 13  02 07 9a 03  0d 32 34 9b
          01 00 9d 08  54 06 02 21  43 65 07 f0  be 25 80 01  01 81 01 01
          82 01 00 83  0c 34 39 31  37 32 30 34  39 30 30 30  31 84 0c 34
          39 31 37 32  30 34 39 30  30 30 31 9f  1f 07 91 94  71 02 94 00
          10 9f 22 05  00 00 00 00  00 9f 23 03  00 00 00 9f  24 05 00 00
          00 00 00 9f  25 03 00 00  00 9f 28 01  00 9f 2a 05  00 00 00 00
          00 9f 2f 02  00 9b 9f 30  07 44 45 46  41 55 4c 54  9f 31 81 a0
          6c 6f 6d 70  6b 64 67 61  7a 63 6a 71  6a 6f 6a 6f  6d 65 70 65
          6f 68 77 76  76 78 70 6f  65 72 72 67  63 76 65 6c  6a 76 64 67
          65 6d 6a 6e  6e 6a 6e 64  6e 70 74 6f  69 75 70 67  72 6f 75 78
          78 62 75 78  71 65 68 65  68 76 6e 61  66 61 6a 71  6e 6f 64 76
          61 61 6a 71  61 71 78 6a  73 6b 7a 70  63 66 75 77  74 61 74 6b
          6a 66 65 62  64 65 75 62  75 70 6b 66  65 70 69 70  7a 6a 65 68
          62 64 61 78  79 71 79 71  62 6a 64 63  66 63 61 79  78 78 77 64
          65 62 71 74  63 65 63 64  61 74 79 61  71 63 6c 69  61 78 74 6e
          9f 46 0e 10  ac 48 85 00  00 5c 5c 29  ac e9 4c f5  00 9f 4a 0a
          30 30 30 30  30 30 30 30  30 31 9f 52  01 01 bf 53  17 80 01 01
          81 01 01 82  01 00 83 0c  34 39 31 37  32 30 34 39  30 30 30 31
          9f 54 07 91  94 71 02 94  00 10 bf 55  17 80 01 01  81 01 01 82
          01 00 83 0c  38 35 35 32  30 31 32 33  34 35 36 37  9f 56 07 91
          58 25 10 32  54 76 9f 58  01 00 9f 59  01 01 9f 83  5b 34 33 47
          50 50 2d 45  2d 55 54 52  41 4e 2d 46  44 44 3b 75  74 72 61 6e
          2d 63 65 6c  6c 2d 69 64  2d 33 67 70  70 3d 32 36  32 30 39 36
          65 61 31 30  30 31 34 31  30 34 9f 83  5c 78 49 45  45 45 2d 45
          2d 55 54 52  41 4e 2d 46  44 44 3b 75  74 72 61 6e  2d 63 65 6c
          6c 2d 69 64  2d 33 67 70  70 3d 32 36  32 30 32 61  63 35 30 30
          62 32 39 63  30 33 33 33  33 33 33 33  33 33 33 33  33 33 33 33
          33 33 33 33  33 33 33 33  33 33 33 33  33 33 33 31  31 31 31 31
          31 31 31 31  31 31 31 31  31 31 31 31  31 32 32 32  32 32 32 32
          32 32 32 32  34 34 34 34  34 34 34 34  34 31 9f 83  5d 78 33 47
          50 50 2d 45  2d 55 54 52  41 4e 2d 46  44 44 3b 63  65 6c 6c 2d
          74 69 6d 65  3d 32 30 31  36 2d 30 37  2d 31 32 54  31 35 3a 31
          35 3a 34 37  5a 3b 72 65  67 2d 74 69  6d 65 3d 32  30 31 36 2d
          30 37 2d 31  32 54 31 35  3a 31 35 3a  34 37 5a 3b  75 74 72 61
          6e 2d 63 65  6c 6c 2d 69  64 2d 33 67  70 70 3d 32  36 32 30 32
          61 63 35 30  30 61 31 31  31 30 35 35  35 35 35 35  35 31 9f 83
          5f 01 00 9f  83 66 00 9f  83 6a 01 00  9f 83 71 05  00 00 00 00
          00 9f 83 75  01 03 9f 83  76 01 04 9f  83 77 01 03  00 00
```

```
30 80            CallDetailedRecord = {
a0 25              origAddress = {
80 01 01             ton = international(1)
81 01 01             npi = telephone(1)
82 01 00             pid = 0
83 0c 34 39 31 37 32 30 34 39 30 30 30 31
                     msisdn = '491720490001'
84 0c 34 39 31 37 32 30 34 39 30 30 30 31
                     msisdnUTF8 = '491720490001'
                   }
81 07 91 94 71 02 94 00 10
                   origAddressGSM = 'international/telephone 491720490001'
a2 25              recipAddress = {
80 01 01             ton = international(1)
81 01 01             npi = telephone(1)
82 01 00             pid = 0
83 0c 38 35 35 32 30 31 32 33 34 35 36 37
                     msisdn = '855201234567'
84 0c 38 35 35 32 30 31 32 33 34 35 36 37
                     msisdnUTF8 = '855201234567'
                   }
83 07 91 58 25 10 32 54 76
                   recipAddressGSM = 'international/telephone 855201234567'
84 03 13 02 07
                   submitDate = 7-Feb-2019
85 03 0d 32 34
                   submitTime = 13:50:52
86 01 00           status = delivered(0)
87 03 13 02 07
                   terminDate = 7-Feb-2019
88 03 0d 32 36
                   terminTime = 13:50:54
89 02 00 a0        lengthOfMessage = 160
8a 01 00           prioIndicator = false(0)
ab 06              validityPeriod = {
80 01 18             hours = 24
81 01 00             minutes = 0
                   }
8c 01 00           deferIndicator = false(0)
8e 01 00           notifIndicator = false(0)
91 02 02 9a        vsmscId = 666
92 01 02           vsmscType = public(2)
b3 25              dgtiAddress = {
80 01 01             ton = international(1)
81 01 01             npi = telephone(1)
82 01 00             pid = 0
83 0c 34 39 39 37 33 33 33 33 33 33 33
                     msisdn = '499733333333'
84 0c 34 39 39 37 33 33 33 33 33 33 33
                     msisdnUTF8 = '499733333333'
                   }
94 07 91 94 79 33 33 33 33
                   dgtiAddressGSM = 'international/telephone 499733333333'
b6 25              ogtiAddress = {
80 01 01             ton = international(1)
81 01 01             npi = telephone(1)
82 01 00             pid = 0
83 0c 34 39 31 37 32 30 30 30 30 30 31 31
                     msisdn = '491720000011'
84 0c 34 39 31 37 32 30 30 30 30 30 31 31
                     msisdnUTF8 = '491720000011'
                   }
97 07 91 94 71 02 00 00 11
                   ogtiAddressGSM = 'international/telephone 491720000011'
```

```
98 02 06 10        origPointCode = 1552
99 03 13 02 07
                   orglSubmitDate = 7-Feb-2019
9a 03 0d 32 34
                   orglSubmitTime = 13:50:52
9b 01 00           transparentPid = 0
9d 08 54 06 02 21 43 65 07 f0
                   intlMobileSubId = 456-02-0123456700
be 25              callingLineId = {
80 01 01             ton = international(1)
81 01 01             npi = telephone(1)
82 01 00             pid = 0
83 0c 34 39 31 37 32 30 34 39 30 30 30 31
                     msisdn = '491720490001'
84 0c 34 39 31 37 32 30 34 39 30 30 30 31
                     msisdnUTF8 = '491720490001'
                   }
9f 1f 07 91 94 71 02 94 00 10
                   callingLineIdGSM = 'international/telephone 491720490001'
9f 22 05 00 00 00 00 00
                   aser =  {
                     swinq(0) = false(0)
                     swdel(1) = false(0)
                     notifreq(7) = false(0)
                     notifalw(8) = false(0)
                     usrnotif(9) = false(0)
                     lradreq(10) = false(0)
                     ackdel(26) = false(0)
                     ackman(27) = false(0)
                     singleshot(29) = false(0)
                   }
9f 23 03 00 00 00
                   mser =  {
                     svp(0) = false(0)
                     sdd(2) = false(0)
                     nde(3) = false(0)
                     nnd(4) = false(0)
                     nbu(5) = false(0)
                     pri(7) = false(0)
                     unsol(8) = false(0)
                     lrad(9) = false(0)
                   }
9f 24 05 00 00 00 00 00
                   nser =  {
                     mrep(2) = false(0)
                     deleted(3) = false(0)
                     replaced(4) = false(0)
                     lao(5) = false(0)
                     lar(6) = false(0)
                     fwad(7) = false(0)
                     fwad-cond(8) = false(0)
                     user-data-header(24) = false(0)
                     del-by-operator(28) = false(0)
                   }
9f 25 03 00 00 00
                   xser =  {
                     inqdel(4) = false(0)
                     swnotif(8) = false(0)
                     dl(9) = false(0)
                     rejdupl(15) = false(0)
                   }
9f 28 01 00        lang = 0
9f 2a 05 00 00 00 00 00
                   ppPser =  {
                     orig-pp(0) = false(0)
```

```
                        recip-pp(1) = false(0)
                        orig-blocked(2) = false(0)
                        recip-blocked(3) = false(0)
                        prim(4) = false(0)
                        charge-recip(5) = false(0)
                        free(6) = false(0)
                        during-jam(7) = false(0)
                        applied-pmgt(8) = false(0)
                      }
9f 2f 02 00 9b
                      smeReference = 155
9f 30 07 44 45 46 41 55 4c 54
                      smsContentDcs = 'DEFAULT'
9f 31 a0 6c 6f 6d 70 6b 64 67 61 7a 63 6a 71 6a 6f 6a 6f 6d 65 70 65 6f 68 77 76 76
 78 70 6f 65 72 72 67 63 76 65 6c 6a 76 64 67 65 6d 6a 6e 6e 6a 6e 64 6e 70 74 6f
69 75 70 67 72 6f 75 78 78 62 75 78 71 65 68 65 68 76 6e 61 66 61 6a 71 6e 6f 64 76
 61 61 6a 71 61 71 78 6a 73 6b 7a 70 63 66 75 77 74 61 74 6b 6a 66 65 62 64 65 75
62 75 70 6b 66 65 70 69 70 7a 6a 65 68 62 64 61 78 79 71 79 71 62 6a 64 63 66 63 61
 79 78 78 77 64 65 62 71 74 63 65 63 64 61 74 79 61 71 63 6c 69 61 78 74 6e
                      smsContents =
'lompkdgazcjqjojomepeohwvvxpoerrgcveljvdgemjnnjndnptoiupgrouxxbuxqehehvnafajqnodvaajqaqxjskzpcfuwtatkjfebdeubupkfepipzjehbdaxyqyqbjdcfcayxxwdebqtcecdatyaqcliaxtn'
9f 46 0e 10 ac 48 85 00 00 5c 5c 29 ac e9 4c f5 00
                      messageReference = 10-ac-48-85-00-00-5c-5c-29-ac-e9-4c-f5-00
9f 4a 0a 30 30 30 30 30 30 30 30 30 31
                      origMsgID = '0000000001'
9f 52 01 01           deliveryAttempts = 1
bf 53 17              untranslOrigAddress = {
80 01 01                ton = international(1)
81 01 01                npi = telephone(1)
82 01 00                pid = 0
83 0c 34 39 31 37 32 30 34 39 30 30 30 31
                        msisdn = '491720490001'
                      }
9f 54 07 91 94 71 02 94 00 10
                      untranslOrigAddressGSM = 'international/telephone 491720490001'
bf 55 17              untranslRecipAddress = {
80 01 01                ton = international(1)
81 01 01                npi = telephone(1)
82 01 00                pid = 0
83 0c 38 35 35 32 30 31 32 33 34 35 36 37
                        msisdn = '855201234567'
                      }
9f 56 07 91 58 25 10 32 54 76
                     untranslRecipAddressGSM = 'international/telephone 855201234567'
9f 58 01 00           tpDCS = 0
9f 59 01 01           genericUrgencyLevel = normal(1)
9f 83 5b 34 33 47 50 50 2d 45 2d 55 54 52 41 4e 2d 46 44 44 3b 75 74 72 61 6e 2d 63
 65 6c 6c 2d 69 64 2d 33 67 70 70 3d 32 36 32 30 39 36 65 61 31 30 30 31 34 31 30
34
                      originatorPaniUE =
3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=262096ea10014104
9f 83 5c 78 49 45 45 45 2d 45 2d 55 54 52 41 4e 2d 46 44 44 3b 75 74 72 61 6e 2d 63
 65 6c 6c 2d 69 64 2d 33 67 70 70 3d 32 36 32 30 32 61 63 35 30 30 62 32 39 63 30
33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33
 33 33 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 31 32 32 32 32 32 32 32
32 32 32 32 34 34 34 34 34 34 34 34 34 31
                      originatorPaniNP =
IEEE-E-UTRAN-FDD;utran-cell-id-3gpp=26202ac500b29c0333333333333333333333333333333111111111111111111222222222224444444441
9f 83 5d 78 33 47 50 50 2d 45 2d 55 54 52 41 4e 2d 46 44 44 3b 63 65 6c 6c 2d 74 69
 6d 65 3d 32 30 31 36 2d 30 37 2d 31 32 54 31 35 3a 31 35 3a 34 37 5a 3b 72 65 67
2d 74 69 6d 65 3d 32 30 31 36 2d 30 37 2d 31 32 54 31 35 3a 31 35 3a 34 37 5a 3b 75
 74 72 61 6e 2d 63 65 6c 6c 2d 69 64 2d 33 67 70 70 3d 32 36 32 30 32 61 63 35 30
30 61 31 31 31 30 35 35 35 35 35 35 35 31
                      originatorPcni =
3GPP-E-UTRAN-FDD;cell-time=2016-07-12T15:15:47Z;reg-time=2016-07-12T15:15:47Z;utran-cell-id-3gpp=26202ac500a111055555551
```

```
9f 83 5f 01 00
                    signaturePresent = false(0)
9f 83 66 00         furnishChargingInfo = ''
9f 83 6a 01 00
                    ss8LastFailureReason = noFailureReasonAvailable(0)
9f 83 71 05 00 00 00 00 00
                    externalAttributes =  {
                      attribute-1(0) = false(0)
                      attribute-2(1) = false(0)
                      attribute-3(2) = false(0)
                      attribute-4(3) = false(0)
                      attribute-5(4) = false(0)
                      attribute-6(5) = false(0)
                      attribute-7(6) = false(0)
                      attribute-8(7) = false(0)
                      attribute-9(8) = false(0)
                      attribute-10(9) = false(0)
                      attribute-11(10) = false(0)
                      attribute-12(11) = false(0)
                      attribute-13(12) = false(0)
                      attribute-14(13) = false(0)
                      attribute-15(14) = false(0)
                      attribute-16(15) = false(0)
                      attribute-17(16) = false(0)
                      attribute-18(17) = false(0)
                      attribute-19(18) = false(0)
                      attribute-20(19) = false(0)
                      attribute-21(20) = false(0)
                      attribute-22(21) = false(0)
                      attribute-23(22) = false(0)
                      attribute-24(23) = false(0)
                      attribute-25(24) = false(0)
                      attribute-26(25) = false(0)
                      attribute-27(26) = false(0)
                      attribute-28(27) = false(0)
                      attribute-29(28) = false(0)
                      attribute-30(29) = false(0)
                      attribute-31(30) = false(0)
                      attribute-32(31) = false(0)
                    }
9f 83 75 01 03
                    origType = SIPO(3)
9f 83 76 01 04
                    destType = MT(4)
9f 83 77 01 03
                    amsStatus = Delivered(3)
00 00             }
```

Appendix A

Log Record ASN.1 Data Types

Topics:

A.1 Log Record ASN.1 Data Types

The following sample intercept file contains a submit and delivery intercept record for single SIPO-MT flow:

```
-- ------------------------------------------------------------------------
--
--   (c) Copyright 2004-2015 NewNet
--
--   This software is proprietary to and embodies the confidential technology
--   of NewNet. Possession, use, duplication or dissemination of the
--   software and media is authorized only pursuant to a valid written license
--   from NewNet.
--
-- ------------------------------------------------------------------------
-- $Id: logging.asn1,v 1.79 2015/07/09 11:29:13 opaliwal Exp $
-- ------------------------------------------------------------------------

LOGGING DEFINITIONS IMPLICIT TAGS ::=
BEGIN

--- Following construct defines all possible log records.

InboundMessage ::=  --snacc isPdu:"TRUE"
CHOICE {
    -- Following are log records that will be generated when the log format is
    -- equal to 'asn1Extended'

    trustedMoFwdSm                                  [APPLICATION 0] IMPLICIT
TrustedMoFwdSm,
    suspectMoFwdSm                                  [APPLICATION 1] IMPLICIT
SuspectMoFwdSm,
    trustedSriSm                                    [APPLICATION 2] IMPLICIT
TrustedSriSm,
    suspectSriSm                                    [APPLICATION 3] IMPLICIT
SuspectSriSm,
    trustedMtFwdSm                                  [APPLICATION 4] IMPLICIT
TrustedMtFwdSm,
    suspectMtFwdSm                                  [APPLICATION 5] IMPLICIT
SuspectMtFwdSm,

    -- event                                          [APPLICATION 30] IMPLICIT
 Event,

    -- Following are log records that will be generated when the log format is
    -- equal to 'asn1ExtendedWithCountryAndNetworkInfo'

    trustedMoFwdSmWithCountryAndNetworkInfo         [APPLICATION 100] IMPLICIT
MoFwdSmWithCountryAndNetworkInfo,
    suspectMoFwdSmWithCountryAndNetworkInfo         [APPLICATION 101] IMPLICIT
MoFwdSmWithCountryAndNetworkInfo,

    trustedSriSmWithCountryAndNetworkInfo           [APPLICATION 102] IMPLICIT
TrustedSriSmWithCountryAndNetworkInfo,
    suspectSriSmWithCountryAndNetworkInfo           [APPLICATION 103] IMPLICIT
SuspectSriSmWithCountryAndNetworkInfo,
    trustedMtFwdSmWithCountryAndNetworkInfo         [APPLICATION 104] IMPLICIT
TrustedMtFwdSmWithCountryAndNetworkInfo,
    suspectMtFwdSmWithCountryAndNetworkInfo         [APPLICATION 105] IMPLICIT
SuspectMtFwdSmWithCountryAndNetworkInfo,
   -- trustedCdmaMoFwdSmWithCountryAndNetworkInfo      [APPLICATION 106] IMPLICIT
```

```
 TrustedCdmaMoFwdSmWithCountryAndNetworkInfo,
    receivedSubmitSmWithCountryAndNetworkInfo          [APPLICATION 116] IMPLICIT
ReceivedSubmitSmWithCountryAndNetworkInfo,
    receivedDeliverSmWithCountryAndNetworkInfo         [APPLICATION 117] IMPLICIT
ReceivedDeliverSmWithCountryAndNetworkInfo,
    receivedNotificationWithCountryAndNetworkInfo      [APPLICATION 118] IMPLICIT
ReceivedNotificationWithCountryAndNetworkInfo,

    extCondMessageWithCountryAndNetworkInfo            [APPLICATION 131] IMPLICIT
EventWithCountryAndNetworkInfo,
    amsDeliveryAttemptForAoMtWithCountryAndNetworkInfo [APPLICATION 132] IMPLICIT
EventWithCountryAndNetworkInfo,
    amsDeliveryAttemptForMoMtWithCountryAndNetworkInfo [APPLICATION 133] IMPLICIT
EventWithCountryAndNetworkInfo,
    amsDeliveryAttemptForMoAtWithCountryAndNetworkInfo [APPLICATION 134] IMPLICIT
EventWithCountryAndNetworkInfo,
    amsDeliveryAttemptForAoAtWithCountryAndNetworkInfo [APPLICATION 135] IMPLICIT
EventWithCountryAndNetworkInfo,
   -- Note: The AoAt log record is also used for logging AT-Store-AT messages coming
 out of the AMS.

    amsTerminateWithCountryAndNetworkInfo              [APPLICATION 136] IMPLICIT
EventWithCountryAndNetworkInfo,
    notifEventWithCountryAndNetworkInfo                [APPLICATION 137] IMPLICIT
EventWithCountryAndNetworkInfo,
    copyForwardEventWithCountryAndNetworkInfo          [APPLICATION 138] IMPLICIT
EventWithCountryAndNetworkInfo,
    msCommandWithCountryAndNetworkInfo                 [APPLICATION 139] IMPLICIT
CommandWithCountryAndNetworkInfo,

    -- Note: Registration log record is also used for De-Registration of UE
    imsRegistrationWithCountryAndNetworkInfo           [APPLICATION 140] IMPLICIT
RegistrationWithCountryAndNetworkInfo
}




-- Following record is generated for an inbound MO-ForwardSM operation
-- that is considered to be trusted.

TrustedMoFwdSm ::= SEQUENCE {
    timestamp                  [0] IMPLICIT GeneralizedTime,
    routingAction              [1] IMPLICIT MoFwdSmRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'discardWithAck',
    -- 'discardWithNak', or 'discardWithNoResponse'.
    -- responseInfo is included otherwise.
    rejectInfo                 [2] IMPLICIT SEQUENCE {
        rejectCause                [0] IMPLICIT RejectCause,
        moRoutingRule              [1] IMPLICIT NameString OPTIONAL,
        moExtConditionRule         [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo               [3] IMPLICIT SEQUENCE {
        submissionResult             [0] IMPLICIT MoFwdSmSubmissionResult,
        moRoutingRule              [1] IMPLICIT NameString
    } OPTIONAL,
    -- sccpCgPaOfFirstSegment and sccpCdPaOfFirstSegment are only included when
    -- the MO-ForwardSM has been received in a segmented TCAP dialogue.
    sccpCgPaOfFirstSegment     [6] IMPLICIT SccpAddress OPTIONAL,
    sccpCdPaOfFirstSegment     [7] IMPLICIT SccpAddress OPTIONAL,
    sccpCgPa                   [8] IMPLICIT SccpAddress,
```

```
    sccpCdPa                    [9] IMPLICIT SccpAddress,
    mapSmsc                    [12] IMPLICIT GsmAddress OPTIONAL,
    mapMsisdn                  [13] IMPLICIT GsmAddress OPTIONAL,
    mapImsi                    [14] IMPLICIT Imsi OPTIONAL,
    -- smsSubmit and smsCommand are mutually exclusive.
    smsSubmit                  [15] IMPLICIT SEQUENCE {
        smsServices                 [0] IMPLICIT SmsSubmitServices,
        smsMessageReference         [1] IMPLICIT MessageReference,
        smsRecipient                [2] IMPLICIT GsmAddress,
        smsProtocolId               [3] IMPLICIT ProtocolId,
        smsDataCodingScheme         [4] IMPLICIT DataCodingScheme,
        smsValidityPeriod           [5] IMPLICIT GeneralizedTime OPTIONAL,
        smsUserDataHeader           [6] IMPLICIT UserDataHeader OPTIONAL,
        smsUserData                 [7] IMPLICIT UserData
    } OPTIONAL,
    smsCommand                 [16] IMPLICIT SEQUENCE {
        smsServices                 [0] IMPLICIT SmsCommandServices,
        smsMessageReference         [1] IMPLICIT MessageReference,
        smsProtocolId               [2] IMPLICIT ProtocolId,
        smsCommandType              [3] IMPLICIT CommandType,
        smsMessageNumber            [4] IMPLICIT MessageNumber,
        smsRecipient                [5] IMPLICIT GsmAddress,
        smsCommandData              [6] IMPLICIT CommandData
    } OPTIONAL,
   originatingPointCode         [19] IMPLICIT PointCode OPTIONAL
}

-- Following record is generated for an inbound MO-ForwardSM operation
-- that is considered to be suspect.

SuspectMoFwdSm ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    routingAction               [1] IMPLICIT MoFwdSmRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'discardWithAck',
    -- 'discardWithNak', or 'discardWithNoResponse'.
    -- responseInfo is included otherwise.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        moRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        moExtConditionRule          [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        submissionResult            [0] IMPLICIT MoFwdSmSubmissionResult,
        moRoutingRule               [1] IMPLICIT NameString
    } OPTIONAL,
    ignoredRejectCauses         [4] IMPLICIT IgnoredRejectCauses,
    -- sccpCgPaOfFirstSegment and sccpCdPaOfFirstSegment are only included when
    -- the MO-ForwardSM has been received in a segmented TCAP dialogue.
    sccpCgPaOfFirstSegment      [6] IMPLICIT SccpAddress OPTIONAL,
    sccpCdPaOfFirstSegment      [7] IMPLICIT SccpAddress OPTIONAL,
    sccpCgPa                    [8] IMPLICIT SccpAddress,
    sccpCdPa                    [9] IMPLICIT SccpAddress,
    mapSmsc                    [12] IMPLICIT GsmAddress OPTIONAL,
    mapMsisdn                  [13] IMPLICIT GsmAddress OPTIONAL,
    mapImsi                    [14] IMPLICIT Imsi OPTIONAL,
    -- smsSubmit and smsCommand are mutually exclusive.
    smsSubmit                  [15] IMPLICIT SEQUENCE {
        smsServices                 [0] IMPLICIT SmsSubmitServices,
        smsMessageReference         [1] IMPLICIT MessageReference,
        smsRecipient                [2] IMPLICIT GsmAddress,
        smsProtocolId               [3] IMPLICIT ProtocolId,
        smsDataCodingScheme         [4] IMPLICIT DataCodingScheme,
        smsValidityPeriod           [5] IMPLICIT GeneralizedTime OPTIONAL,
        smsUserDataHeader           [6] IMPLICIT UserDataHeader OPTIONAL,
```

```
        smsUserData                 [7] IMPLICIT UserData
    } OPTIONAL,
    smsCommand                  [16] IMPLICIT SEQUENCE {
        smsServices                 [0] IMPLICIT SmsCommandServices,
        smsMessageReference         [1] IMPLICIT MessageReference,
        smsProtocolId               [2] IMPLICIT ProtocolId,
        smsCommandType              [3] IMPLICIT CommandType,
        smsMessageNumber            [4] IMPLICIT MessageNumber,
        smsRecipient                [5] IMPLICIT GsmAddress,
        smsCommandData              [6] IMPLICIT CommandData
    } OPTIONAL,
   originatingPointCode         [19] IMPLICIT PointCode OPTIONAL,
    -- infoFromHlr comprises information pertaining to the originator of the
    -- MO-ForwardSM
    infoFromHlr                 [30] IMPLICIT SEQUENCE {
        mapImsi                     [0] IMPLICIT Imsi OPTIONAL,
        mapMsc                      [1] IMPLICIT GsmAddress OPTIONAL,
        mapSgsn                     [2] IMPLICIT GsmAddress OPTIONAL
    } OPTIONAL
}

-- Following record is generated for an inbound SendRoutingInfoForSM operation
-- that is considered to be trusted.

TrustedSriSm ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    routingAction               [1] IMPLICIT SriSmRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'blockWithTemporaryError',
    -- 'blockWithPermanentError', 'blockWithNoResponse', or 'blockWithAck'.
    -- responseInfo is included otherwise.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtExtConditionRule          [2] IMPLICIT NameString OPTIONAL,
        sriqRoutingRule             [3] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        queryResult                 [0] SriSmQueryResult,
        mapImsi                     [1] Imsi OPTIONAL,
        mapLmsi                     [2] Lmsi OPTIONAL,
        mapMsc                      [3] GsmAddress OPTIONAL,
        mapSgsn                     [4] GsmAddress OPTIONAL,
        mtRoutingRule               [6] IMPLICIT NameString OPTIONAL,
        sriqRoutingRule             [7] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    sccpCgPa                    [8] SccpAddress,
    sccpCdPa                    [9] SccpAddress,
    mapSmsc                     [12] GsmAddress,
    mapMsisdn                   [13] GsmAddress
}

-- Following record is generated for an inbound SendRoutingInfoForSM operation
-- that is considered to be suspect.

SuspectSriSm ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    routingAction               [1] IMPLICIT SriSmRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'discardWithAck',
    -- 'discardWithNak', or 'discardWithNoResponse'.
    -- responseInfo is included otherwise.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
```

```
        mtExtConditionRule          [2] IMPLICIT NameString OPTIONAL,
        sriqRoutingRule             [3] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        queryResult                 [0] IMPLICIT SriSmQueryResult,
        mapImsi                     [1] IMPLICIT Imsi OPTIONAL,
        mapLmsi                     [2] IMPLICIT Lmsi OPTIONAL,
        mapMsc                      [3] IMPLICIT GsmAddress OPTIONAL,
        mapSgsn                     [4] IMPLICIT GsmAddress OPTIONAL,
        scrambledImsi               [5] IMPLICIT Imsi OPTIONAL,
        mtRoutingRule               [6] IMPLICIT NameString OPTIONAL,
        sriqRoutingRule             [7] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    ignoredRejectCauses         [4] IMPLICIT IgnoredRejectCauses,
    sccpCgPa                    [8] IMPLICIT SccpAddress,
    sccpCdPa                    [9] IMPLICIT SccpAddress,
    mapSmsc                     [12] IMPLICIT GsmAddress,
    mapMsisdn                   [13] IMPLICIT GsmAddress
}

-- Following record is generated for an inbound MT-ForwardSM operation
-- that is considered to be trusted.

TrustedMtFwdSm ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    routingAction               [1] IMPLICIT MtFwdSmRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'discardWithAck',
    -- 'discardWithNak', or 'discardWithNoResponse'.
    -- responseInfo is included otherwise.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtExtConditionRule          [2] IMPLICIT NameString OPTIONAL,
        mtiRoutingRule              [3] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        deliveryResult              [0] IMPLICIT MtFwdSmDeliveryResult,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtiRoutingRule              [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    -- sccpCgPaOfFirstSegment and sccpCdPaOfFirstSegment are only included when
    -- the MT-ForwardSM has been received in a segmented TCAP dialogue.
    sccpCgPaOfFirstSegment      [6] IMPLICIT SccpAddress OPTIONAL,
    sccpCdPaOfFirstSegment      [7] IMPLICIT SccpAddress OPTIONAL,
    sccpCgPa                    [8] IMPLICIT SccpAddress,
    sccpCdPa                    [9] IMPLICIT SccpAddress,
    mapSmsc                     [12] IMPLICIT GsmAddress OPTIONAL,
    mapImsi                     [13] IMPLICIT Imsi OPTIONAL,
    mapLmsi                     [14] IMPLICIT Lmsi OPTIONAL,
    smsDeliver                  [15] IMPLICIT SEQUENCE {
        smsServices                 [0] IMPLICIT SmsDeliverServices,
        smsOriginator               [1] IMPLICIT GsmAddress,
        smsProtocolId               [2] IMPLICIT ProtocolId,
        smsDataCodingScheme         [3] IMPLICIT DataCodingScheme,
        smsScTimestamp              [4] IMPLICIT GeneralizedTime,
        smsUserDataHeader           [5] IMPLICIT UserDataHeader OPTIONAL,
        smsUserData                 [6] IMPLICIT UserData
    } OPTIONAL,
    statusReport                [16] IMPLICIT SEQUENCE {
        smsServices                 [0] IMPLICIT StatusReportServices,
        smsMessageReference         [1] IMPLICIT MessageReference,
        smsRecipient                [2] IMPLICIT GsmAddress,
        smsScTimestamp              [3] IMPLICIT GeneralizedTime,
        smsDischargeTime            [4] IMPLICIT GeneralizedTime,
```

```
        smsStatus                   [5] IMPLICIT Status
    } OPTIONAL,
    correlatedSriSm             [30] IMPLICIT SEQUENCE {
        sccpCgPa                    [0] IMPLICIT SccpAddress OPTIONAL,
        mapSmsc                     [1] IMPLICIT GsmAddress OPTIONAL,
        mapMsisdn                   [2] IMPLICIT GsmAddress,
        mapImsi                     [3] IMPLICIT Imsi,
        mapLmsi                     [4] IMPLICIT Lmsi OPTIONAL,
        mapMsc                      [5] IMPLICIT GsmAddress OPTIONAL,
        mapSgsn                     [6] IMPLICIT GsmAddress OPTIONAL
    } OPTIONAL,
    outboundMt                  [21] IMPLICIT OutboundMt OPTIONAL
}

-- Following record is generated for an inbound MT-ForwardSM operation
-- that is considered to be suspect.

SuspectMtFwdSm ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    routingAction               [1] IMPLICIT MtFwdSmRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'discardWithAck',
    -- 'discardWithNak', or 'discardWithNoResponse'.
    -- responseInfo is included otherwise.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtExtConditionRule          [2] IMPLICIT NameString OPTIONAL,
        mtiRoutingRule              [3] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        deliveryResult              [0] IMPLICIT MtFwdSmDeliveryResult,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtiRoutingRule              [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    ignoredRejectCauses         [4] IMPLICIT IgnoredRejectCauses,
    -- sccpCgPaOfFirstSegment and sccpCdPaOfFirstSegment are only included when
    -- the MT-ForwardSM has been received in a segmented TCAP dialogue.
    sccpCgPaOfFirstSegment      [6] IMPLICIT SccpAddress OPTIONAL,
    sccpCdPaOfFirstSegment      [7] IMPLICIT SccpAddress OPTIONAL,
    sccpCgPa                    [8] IMPLICIT SccpAddress,
    sccpCdPa                    [9] IMPLICIT SccpAddress,
    mapSmsc                     [12] IMPLICIT GsmAddress OPTIONAL,
    mapImsi                     [13] IMPLICIT Imsi OPTIONAL,
    -- smsDeliver and statusReport are mutually exclusive.
    smsDeliver                  [15] IMPLICIT SEQUENCE {
        smsServices                 [0] IMPLICIT SmsDeliverServices,
        smsOriginator               [1] IMPLICIT GsmAddress,
        smsProtocolId               [2] IMPLICIT ProtocolId,
        smsDataCodingScheme         [3] IMPLICIT DataCodingScheme,
        smsScTimestamp              [4] IMPLICIT GeneralizedTime,
        smsUserDataHeader           [5] IMPLICIT UserDataHeader OPTIONAL,
        smsUserData                 [6] IMPLICIT UserData
    } OPTIONAL,
    statusReport                [16] IMPLICIT SEQUENCE {
        smsServices                 [0] IMPLICIT StatusReportServices,
        smsMessageReference         [1] IMPLICIT MessageReference,
        smsRecipient                [2] IMPLICIT GsmAddress,
        smsScTimestamp              [3] IMPLICIT GeneralizedTime,
        smsDischargeTime            [4] IMPLICIT GeneralizedTime,
        smsStatus                   [5] IMPLICIT Status
    } OPTIONAL,
    correlatedSriSm             [30] IMPLICIT SEQUENCE {
        sccpCgPa                    [0] IMPLICIT SccpAddress OPTIONAL,
        mapSmsc                     [1] IMPLICIT GsmAddress OPTIONAL,
```

```
        mapMsisdn                   [2] IMPLICIT GsmAddress,
        mapImsi                     [3] IMPLICIT Imsi,
        mapLmsi                     [4] IMPLICIT Lmsi OPTIONAL,
        mapMsc                      [5] IMPLICIT GsmAddress OPTIONAL,
        mapSgsn                     [6] IMPLICIT GsmAddress OPTIONAL
    } OPTIONAL
}

HssQuery ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime OPTIONAL,
    routingAction               [1] IMPLICIT SriSmRoutingAction OPTIONAL,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'blockWithTemporaryError',
    -- 'blockWithPermanentError', 'blockWithNoResponse', or 'blockWithAck'.
    -- responseInfo is included otherwise.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtExtConditionRule          [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    -- userDataAnswer
    shPullResponseInfo          [3] IMPLICIT SEQUENCE {
        queryResult                 [0] IMPLICIT SriSmQueryResult,
        resultCode                  [1] IMPLICIT DiameterShResultCode OPTIONAL,
        experimentalResult          [2] IMPLICIT DiameterShResultCode OPTIONAL,
        imsUserState                [3] IMPLICIT ImsUserState OPTIONAL,
        scscfName                   [4] IMPLICIT SipUrl OPTIONAL,
        hssRule                     [5] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    -- imsPublicUserIdentity, imsPublicServiceIdentity Url, now MSISDN
    userIdentity                [13] IMPLICIT GsmAddressInfo OPTIONAL,
    iiw                         [60] IMPLICIT IiwId OPTIONAL
}

-- Following record is generated for an inbound MO-ForwardSM operation
-- that is considered to be trusted, suspect, or a status report.

MoFwdSmWithCountryAndNetworkInfo ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    routingAction               [1] IMPLICIT MoFwdSmRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'discardWithAck',
    -- 'discardWithNak', or 'discardWithNoResponse'.
    -- responseInfo is included otherwise.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        moRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        moExtConditionRule          [2] IMPLICIT NameString OPTIONAL,
        mnpViolation                [3] IMPLICIT MnpViolation OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        submissionResult              [0] IMPLICIT MoFwdSmSubmissionResult,
        moRoutingRule               [1] IMPLICIT NameString
    } OPTIONAL,
    ignoredRejectCauses         [4] IMPLICIT IgnoredRejectCauses OPTIONAL,
    -- sccpCgPaOfFirstSegment and sccpCdPaOfFirstSegment are only included when
    -- the MO-ForwardSM has been received in a segmented TCAP dialogue.
    sccpCgPaOfFirstSegment      [6] IMPLICIT SccpAddressInfo OPTIONAL,
    sccpCdPaOfFirstSegment      [7] IMPLICIT SccpAddressInfo OPTIONAL,
    sccpCgPa                    [8] IMPLICIT SccpAddressInfo,
    sccpCdPa                    [9] IMPLICIT SccpAddressInfo,
    mapSmsc                     [12] IMPLICIT GsmAddressInfo OPTIONAL,
    mapMsisdn                   [13] IMPLICIT GsmAddressInfo OPTIONAL,
    mapImsi                     [14] IMPLICIT ImsiInfo OPTIONAL,
    -- smsSubmit and smsCommand are mutually exclusive.
```

```
    smsSubmit                   [15] IMPLICIT SEQUENCE {
        smsServices                  [0] IMPLICIT SmsSubmitServices,
        smsMessageReference          [1] IMPLICIT MessageReference,
        smsRecipient                 [2] IMPLICIT GsmAddressInfo,
        smsProtocolId                [3] IMPLICIT ProtocolId,
        smsDataCodingScheme          [4] IMPLICIT DataCodingScheme,
        smsValidityPeriod            [5] IMPLICIT GeneralizedTime OPTIONAL,
        smsUserDataHeader            [6] IMPLICIT UserDataHeader OPTIONAL,
        smsUserData                  [7] IMPLICIT UserData
    } OPTIONAL,
    smsCommand                  [16] IMPLICIT SEQUENCE {
        smsServices                  [0] IMPLICIT SmsCommandServices,
        smsMessageReference          [1] IMPLICIT MessageReference,
        smsProtocolId                [2] IMPLICIT ProtocolId,
        smsCommandType               [3] IMPLICIT CommandType,
        smsMessageNumber             [4] IMPLICIT MessageNumber,
        smsRecipient                 [5] IMPLICIT GsmAddressInfo,
        smsCommandData               [6] IMPLICIT CommandData
    } OPTIONAL,
    originatingPointCode        [19] IMPLICIT PointCode OPTIONAL,
    outboundMo                  [20] IMPLICIT OutboundMo OPTIONAL,
    outboundMt                  [21] IMPLICIT OutboundMt OPTIONAL,
    outboundAo                  [22] IMPLICIT OutboundAo OPTIONAL,
    outboundAt                  [23] IMPLICIT OutboundAt OPTIONAL,
    storage                     [24] IMPLICIT StorageInfo OPTIONAL,
    -- infoFromHlr comprises information pertaining to the originator of the
    -- MO-ForwardSM
    infoFromHlr                 [30] IMPLICIT SEQUENCE {
        mapImsi                      [0] IMPLICIT ImsiInfo,
        mapMsc                       [1] IMPLICIT GsmAddressInfo OPTIONAL,
        mapSgsn                      [2] IMPLICIT GsmAddressInfo OPTIONAL
    } OPTIONAL,
    recipientRoutingNumber      [33] IMPLICIT RoutingNumber OPTIONAL,
    ecResponseData              [34] IMPLICIT SEQUENCE OF EcResponseData OPTIONAL,
    ssiInfo                     [50] IMPLICIT SsiServiceInfo OPTIONAL,
    --2184
    hssQuery                    [60] IMPLICIT HssQuery OPTIONAL,
    outboundSip                 [61] IMPLICIT OutboundSip OPTIONAL,
    originalIiw                 [62] IMPLICIT IiwId OPTIONAL
}


-- Following record is generated for an inbound SendRoutingInfoForSM operation
-- that is considered to be trusted.

TrustedSriSmWithCountryAndNetworkInfo ::= SEQUENCE {
    timestamp                   [0] GeneralizedTime,
    routingAction               [1] SriSmRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'discardWithAck',
    -- 'discardWithNak', or 'discardWithNoResponse'.
    -- responseInfo is included otherwise.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                  [0] IMPLICIT RejectCause,
        mtRoutingRule                [1] NameString OPTIONAL,
        mtExtConditionRule           [2] NameString OPTIONAL,
        sriqRoutingRule              [3] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        queryResult                  [0] SriSmQueryResult,
        mapImsi                      [1] ImsiInfo OPTIONAL,
        mapLmsi                      [2] Lmsi OPTIONAL,
        mapMsc                       [3] GsmAddressInfo OPTIONAL,
        mapSgsn                      [4] GsmAddressInfo OPTIONAL,
        mtRoutingRule                [6] IMPLICIT NameString OPTIONAL,
```

```
        sriqRoutingRule             [7] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    sccpCgPa                    [8] SccpAddressInfo,
    sccpCdPa                    [9] SccpAddressInfo,
    mapSmsc                     [12] GsmAddressInfo,
    mapMsisdn                   [13] GsmAddressInfo,
    ecResponseData              [34] IMPLICIT SEQUENCE OF EcResponseData OPTIONAL,
    mtRoutingRuleSkipped        [49] IMPLICIT NameString OPTIONAL,
    ssiInfo                     [50] IMPLICIT SsiServiceInfo OPTIONAL,
    --2184
    hssQuery                    [60] IMPLICIT HssQuery OPTIONAL
}

-- Following record is generated for an inbound SendRoutingInfoForSM operation
-- that is considered to be suspect.

SuspectSriSmWithCountryAndNetworkInfo ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    routingAction               [1] IMPLICIT SriSmRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'discardWithAck',
    -- 'discardWithNak', or 'discardWithNoResponse'.
    -- responseInfo is included otherwise.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtExtConditionRule          [2] IMPLICIT NameString OPTIONAL,
        sriqRoutingRule             [3] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        queryResult                 [0] IMPLICIT SriSmQueryResult,
        mapImsi                     [1] IMPLICIT ImsiInfo OPTIONAL,
        mapLmsi                     [2] IMPLICIT Lmsi OPTIONAL,
        mapMsc                      [3] IMPLICIT GsmAddressInfo OPTIONAL,
        mapSgsn                     [4] IMPLICIT GsmAddressInfo OPTIONAL,
        scrambledImsi               [5] IMPLICIT ImsiInfo OPTIONAL,
        mtRoutingRule               [6] IMPLICIT NameString OPTIONAL,
        sriqRoutingRule             [7] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    ignoredRejectCauses         [4] IMPLICIT IgnoredRejectCauses,
    sccpCgPa                    [8] IMPLICIT SccpAddressInfo,
    sccpCdPa                    [9] IMPLICIT SccpAddressInfo,
    mapSmsc                     [12] IMPLICIT GsmAddressInfo,
    mapMsisdn                   [13] IMPLICIT GsmAddressInfo,
    ecResponseData              [34] IMPLICIT SEQUENCE OF EcResponseData OPTIONAL,
    mtRoutingRuleSkipped        [49] IMPLICIT NameString OPTIONAL,
    ssiInfo                     [50] IMPLICIT SsiServiceInfo OPTIONAL,
    --2184
    hssQuery                    [60] IMPLICIT HssQuery OPTIONAL
}

-- Following record is generated for an inbound MT-ForwardSM operation
-- that is considered to be trusted.

TrustedMtFwdSmWithCountryAndNetworkInfo ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    routingAction               [1] IMPLICIT MtFwdSmRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'discardWithAck',
    -- 'discardWithNak', or 'discardWithNoResponse'.
    -- responseInfo is included otherwise.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtExtConditionRule          [2] IMPLICIT NameString OPTIONAL,
```

```
        mtiRoutingRule              [3] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        deliveryResult              [0] IMPLICIT MtFwdSmDeliveryResult,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtiRoutingRule              [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    -- sccpCgPaOfFirstSegment and sccpCdPaOfFirstSegment are only included when
    -- the MT-ForwardSM has been received in a segmented TCAP dialogue.
    sccpCgPaOfFirstSegment      [6] IMPLICIT SccpAddressInfo OPTIONAL,
    sccpCdPaOfFirstSegment      [7] IMPLICIT SccpAddressInfo OPTIONAL,
    sccpCgPa                    [8] IMPLICIT SccpAddressInfo,
    sccpCdPa                    [9] IMPLICIT SccpAddressInfo,
    mapSmsc                     [12] IMPLICIT GsmAddressInfo OPTIONAL,
    mapImsi                     [13] IMPLICIT ImsiInfo OPTIONAL,
    mapLmsi                     [14] IMPLICIT Lmsi OPTIONAL,
    smsDeliver                  [15] IMPLICIT SEQUENCE {
        smsServices                 [0] IMPLICIT SmsDeliverServices,
        smsOriginator               [1] IMPLICIT GsmAddressInfo,
        smsProtocolId               [2] IMPLICIT ProtocolId,
        smsDataCodingScheme         [3] IMPLICIT DataCodingScheme,
        smsScTimestamp              [4] IMPLICIT GeneralizedTime,
        smsUserDataHeader           [5] IMPLICIT UserDataHeader OPTIONAL,
        smsUserData                 [6] IMPLICIT UserData
    } OPTIONAL,
    statusReport                [16] IMPLICIT SEQUENCE {
        smsServices                 [0] IMPLICIT StatusReportServices,
        smsMessageReference         [1] IMPLICIT MessageReference,
        smsRecipient                [2] IMPLICIT GsmAddressInfo,
        smsScTimestamp              [3] IMPLICIT GeneralizedTime,
        smsDischargeTime            [4] IMPLICIT GeneralizedTime,
        smsStatus                   [5] IMPLICIT Status
    } OPTIONAL,
    correlatedSriSm             [30] IMPLICIT SEQUENCE {
        sccpCgPa                    [0] IMPLICIT SccpAddressInfo OPTIONAL,
        mapSmsc                     [1] IMPLICIT GsmAddressInfo OPTIONAL,
        mapMsisdn                   [2] IMPLICIT GsmAddressInfo,
        mapImsi                     [3] IMPLICIT ImsiInfo,
        mapLmsi                     [4] IMPLICIT Lmsi OPTIONAL,
        mapMsc                      [5] IMPLICIT GsmAddressInfo OPTIONAL,
        mapSgsn                     [6] IMPLICIT GsmAddressInfo OPTIONAL
    }  OPTIONAL,
    --BG19606-19607
    outboundMt                  [21] IMPLICIT OutboundMt OPTIONAL,
    ecResponseData              [34] IMPLICIT SEQUENCE OF EcResponseData OPTIONAL,
    mtRoutingRuleSkipped        [49] IMPLICIT NameString OPTIONAL,
    ssiInfo                     [50] IMPLICIT SsiServiceInfo OPTIONAL,
    --2184
    hssQuery                    [60] IMPLICIT HssQuery OPTIONAL,
    outboundSip                 [61] IMPLICIT OutboundSip OPTIONAL
}

-- Following record is generated for an inbound MT-ForwardSM operation
-- that is considered to be suspect.

SuspectMtFwdSmWithCountryAndNetworkInfo ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    routingAction               [1] IMPLICIT MtFwdSmRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'discardWithAck',
    -- 'discardWithNak', or 'discardWithNoResponse'.
    -- responseInfo is included otherwise.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
```

```
        mtExtConditionRule          [2] IMPLICIT NameString OPTIONAL,
        mtiRoutingRule              [3] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        deliveryResult              [0] IMPLICIT MtFwdSmDeliveryResult,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtiRoutingRule              [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    ignoredRejectCauses         [4] IMPLICIT IgnoredRejectCauses,
    -- sccpCgPaOfFirstSegment and sccpCdPaOfFirstSegment are only included when
    -- the MT-ForwardSM has been received in a segmented TCAP dialogue.
    sccpCgPaOfFirstSegment      [6] IMPLICIT SccpAddressInfo OPTIONAL,
    sccpCdPaOfFirstSegment      [7] IMPLICIT SccpAddressInfo OPTIONAL,
    sccpCgPa                    [8] IMPLICIT SccpAddressInfo,
    sccpCdPa                    [9] IMPLICIT SccpAddressInfo,
    mapSmsc                     [12] IMPLICIT GsmAddressInfo OPTIONAL,
    mapImsi                     [13] IMPLICIT ImsiInfo OPTIONAL,
    -- smsDeliver and statusReport are mutually exclusive.
    smsDeliver                  [15] IMPLICIT SEQUENCE {
        smsServices                 [0] IMPLICIT SmsDeliverServices,
        smsOriginator               [1] IMPLICIT GsmAddressInfo,
        smsProtocolId               [2] IMPLICIT ProtocolId,
        smsDataCodingScheme         [3] IMPLICIT DataCodingScheme,
        smsScTimestamp              [4] IMPLICIT GeneralizedTime,
        smsUserDataHeader           [5] IMPLICIT UserDataHeader OPTIONAL,
        smsUserData                 [6] IMPLICIT UserData
    } OPTIONAL,
    statusReport                [16] IMPLICIT SEQUENCE {
        smsServices                 [0] IMPLICIT StatusReportServices,
        smsMessageReference         [1] IMPLICIT MessageReference,
        smsRecipient                [2] IMPLICIT GsmAddressInfo,
        smsScTimestamp              [3] IMPLICIT GeneralizedTime,
        smsDischargeTime            [4] IMPLICIT GeneralizedTime,
        smsStatus                   [5] IMPLICIT Status
    } OPTIONAL,
    correlatedSriSm             [30] IMPLICIT SEQUENCE {
        sccpCgPa                    [0] IMPLICIT SccpAddressInfo OPTIONAL,
        mapSmsc                     [1] IMPLICIT GsmAddressInfo OPTIONAL,
        mapMsisdn                   [2] IMPLICIT GsmAddressInfo,
        mapImsi                     [3] IMPLICIT ImsiInfo,
        mapLmsi                     [4] IMPLICIT Lmsi OPTIONAL,
        mapMsc                      [5] IMPLICIT GsmAddressInfo OPTIONAL,
        mapSgsn                     [6] IMPLICIT GsmAddressInfo OPTIONAL
    }  OPTIONAL,
    ecResponseData              [34] IMPLICIT SEQUENCE OF EcResponseData OPTIONAL,
    mtRoutingRuleSkipped        [49] IMPLICIT NameString OPTIONAL,
    ssiInfo                     [50] IMPLICIT SsiServiceInfo OPTIONAL,
    --2184
    hssQuery                    [60] IMPLICIT HssQuery OPTIONAL,
    outboundSip                 [61] IMPLICIT OutboundSip OPTIONAL
}

-- Following record is generated when an AO/SM has been received from an
-- application.

ReceivedSubmitSmWithCountryAndNetworkInfo ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    routingAction               [1] IMPLICIT AoRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    -- rejectInfo is included when the action is 'discardWithAck' or
    -- 'discardWithNak'.
    -- responseInfo is included otherwise.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        aoRoutingRule               [1] IMPLICIT NameString OPTIONAL,
```

```
        aoExtConditionRule          [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        submissionResult            [0] IMPLICIT AoSubmissionResult,
        routingErrorCode            [1] IMPLICIT ErrorCode OPTIONAL,
        aoRoutingRule               [2] IMPLICIT NameString,
        serviceCentreTimestamp      [3] IMPLICIT GeneralizedTime OPTIONAL
    } OPTIONAL,
    applicationName             [17] IMPLICIT NameString,
    applicationShortNumber      [18] IMPLICIT GsmAddress,
    messageFields               [19] IMPLICIT SEQUENCE {
        -- originatorAddress and alphanumericOriginator are mutually
        -- exclusive
        -- recipientAddress and alphanumericRecipient are mutually
        -- exclusive
        originatorAddress           [2] GsmAddressInfo OPTIONAL,
        recipientAddress            [4] GsmAddressInfo OPTIONAL,
        dataCodingScheme            [5] DataCodingScheme OPTIONAL,
        protocolIdentifier          [6] ProtocolId OPTIONAL,
        notificationType            [7] NotificationType,
        userData                    [10] UserData,
        userDataHeader              [11] UserDataHeader OPTIONAL,
        moreMessagesToSend          [12] BOOLEAN OPTIONAL,
        priority                    [13] Priority,
        replyPathIndicator          [14] BOOLEAN OPTIONAL,
        deferredDeliveryTime        [17] GeneralizedTime OPTIONAL,
        validityPeriod              [18] GeneralizedTime OPTIONAL,
        singleShotIndicator         [19] BOOLEAN,
        billingIdentifier           [20] BillingId OPTIONAL,
        tariffClass                 [25] TariffClass OPTIONAL,
        serviceDescription          [26] ServiceDescription OPTIONAL,
        alphanumericOriginator      [30] AlphanumericAddress OPTIONAL,
        alphanumericRecipient       [31] AlphanumericAddress OPTIONAL,
        portNumber                  [34] PortNumber OPTIONAL,
        sourcePort                  [46] PortNumber OPTIONAL,
        destinationPort             [47] PortNumber OPTIONAL,
        endToEndAckRequest          [50] EndToEndAckRequest OPTIONAL,
        endToEndMessageType         [52] EndToEndMessageType OPTIONAL,
        messageReference            [53] MessageReference OPTIONAL,
        privacy                     [54] Privacy OPTIONAL,
        numberOfMessages            [55] NumberOfMessages OPTIONAL,
        language                    [56] Language OPTIONAL,
        payloadType                 [63] PayloadType OPTIONAL,
        sourceSubAddress            [67] SubAddress OPTIONAL,
        destSubAddress              [68] SubAddress OPTIONAL,
        userResponseCode            [69] UserResponseCode OPTIONAL,
        displayTime                 [70] DisplayTime OPTIONAL,
        callbackNumbers             [71] SEQUENCE OF CallbackNumber OPTIONAL,
        msValidityIndicator         [72] MsValidityIndicator OPTIONAL,
        msValidityPeriod            [73] MsValidityPeriod OPTIONAL,
        alertOnMessageDelivery      [74] AlertOnMessageDelivery OPTIONAL,
        smsSignal                   [75] SmsSignal OPTIONAL,
        sourceBearerType            [76] BearerType OPTIONAL,
        destBearerType              [77] BearerType OPTIONAL,
        smDefaultMsgId              [78] SmDefaultMessageId OPTIONAL,
        sourceNetworkType           [79] NetworkType OPTIONAL,
        destNetworkType             [80] NetworkType OPTIONAL
    },
    outboundMt                  [21] IMPLICIT OutboundMt OPTIONAL,
    outboundAo                  [22] IMPLICIT OutboundAo OPTIONAL,
    outboundAt                  [23] IMPLICIT OutboundAt OPTIONAL,
    storage                     [24] IMPLICIT StorageInfo OPTIONAL,
    recipientRoutingNumber      [33] IMPLICIT RoutingNumber OPTIONAL,
    ecResponseData              [34] IMPLICIT SEQUENCE OF EcResponseData OPTIONAL,
    originalMessageFields       [46] OriginalMessageFields OPTIONAL,
```

```
    ssiInfo                     [50] IMPLICIT SsiServiceInfo OPTIONAL,
    --2184
    hssQuery                    [60] IMPLICIT HssQuery OPTIONAL,
    outboundSip                 [61] IMPLICIT OutboundSip OPTIONAL
}

-- Following record is generated when an AT/SM has been received from an SMSC.

ReceivedDeliverSmWithCountryAndNetworkInfo ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    routingAction               [1] IMPLICIT AtiRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        atRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        atExtConditionRule          [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        deliveryResult              [0] IMPLICIT AtDeliveryResult,
        routingErrorCode            [1] IMPLICIT ErrorCode OPTIONAL,
        atRoutingRule               [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    applicationName             [17] IMPLICIT NameString,
    applicationShortNumber      [18] IMPLICIT GsmAddress,
    messageFields               [19] IMPLICIT SEQUENCE {
        -- recipientAddress and alphanumericRecipient are mutually
        -- exclusive
        originatorAddress           [2] GsmAddressInfo,
        recipientAddress            [4] GsmAddressInfo OPTIONAL,
        dataCodingScheme            [5] DataCodingScheme,
        protocolIdentifier          [6] ProtocolId,
        userData                    [10] UserData,
        userDataHeader              [11] UserDataHeader OPTIONAL,
        moreMessagesToSend          [12] BOOLEAN,
        priority                    [13] Priority OPTIONAL,
        replyPathIndicator          [14] BOOLEAN,
        serviceCentreTimestamp      [21] GeneralizedTime OPTIONAL,
        originatedImsi              [27] ImsiInfo OPTIONAL,
        originatedMscAddress        [28] GsmAddressInfo OPTIONAL,
        alphanumericOriginator      [30] AlphanumericAddress OPTIONAL,
        alphanumericRecipient       [31] AlphanumericAddress OPTIONAL,
        portNumber                  [34] PortNumber OPTIONAL,
        sourcePort                  [46] PortNumber OPTIONAL,
        destinationPort             [47] PortNumber OPTIONAL,
        endToEndAckRequest          [50] EndToEndAckRequest OPTIONAL,
        endToEndMessageType         [52] EndToEndMessageType OPTIONAL,
        messageReference            [53] MessageReference OPTIONAL,
        privacy                     [54] Privacy OPTIONAL,
        numberOfMessages            [55] NumberOfMessages OPTIONAL,
        language                    [56] Language OPTIONAL,
        payloadType                 [63] PayloadType OPTIONAL,
        sourceSubAddress            [67] SubAddress OPTIONAL,
        destSubAddress              [68] SubAddress OPTIONAL,
        userResponseCode            [69] UserResponseCode OPTIONAL,
        displayTime                 [70] DisplayTime OPTIONAL,
        callbackNumbers             [71] SEQUENCE OF CallbackNumber OPTIONAL,
        msValidityIndicator         [72] MsValidityIndicator OPTIONAL,
        msValidityPeriod            [73] MsValidityPeriod OPTIONAL,
        alertOnMessageDelivery      [74] AlertOnMessageDelivery OPTIONAL,
        smsSignal                   [75] SmsSignal OPTIONAL,
        sourceBearerType            [76] BearerType OPTIONAL,
        destBearerType              [77] BearerType OPTIONAL,
        smDefaultMsgId              [78] SmDefaultMessageId OPTIONAL,
        sourceNetworkType           [79] NetworkType OPTIONAL,
        destNetworkType             [80] NetworkType OPTIONAL
```

```
    },
    outboundAo                  [22] IMPLICIT OutboundAo OPTIONAL,
    outboundAt                  [23] IMPLICIT OutboundAt OPTIONAL,
    storage                     [24] IMPLICIT StorageInfo OPTIONAL,
    ecResponseData              [34] IMPLICIT SEQUENCE OF EcResponseData OPTIONAL,
    -- insideRejectInfo and insideResponseInfo are mutually exclusive.
    originalMessageFields       [46] OriginalMessageFields OPTIONAL,
    insideRejectInfo            [47] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        atiRoutingRule              [1] IMPLICIT NameString OPTIONAL,
        atiExtConditionRule         [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    insideResponseInfo          [48] IMPLICIT SEQUENCE {
        deliveryResult              [0] IMPLICIT AtDeliveryResult,
        routingErrorCode            [1] IMPLICIT ErrorCode OPTIONAL,
        atiRoutingRule              [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    ssiInfo                     [50] IMPLICIT SsiServiceInfo OPTIONAL
}

EventWithCountryAndNetworkInfo ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    applicationName             [17] IMPLICIT NameString OPTIONAL,
    applicationShortNumber      [18] IMPLICIT GsmAddress OPTIONAL,
   messageFields               [19] IMPLICIT MessageFields,
    outboundMt                  [21] IMPLICIT OutboundMt OPTIONAL,
    outboundAt                  [23] IMPLICIT OutboundAt OPTIONAL,
    moreMessagesToSend          [25] IMPLICIT BOOLEAN OPTIONAL,
    numberOfPreviousAttempts    [26] IMPLICIT INTEGER OPTIONAL,
    serviceCentreTimestamp      [27] IMPLICIT GeneralizedTime,
    messageIdentifier           [28] IMPLICIT AmsMessageId OPTIONAL,
    isNotificationMessage       [36] IMPLICIT BOOLEAN OPTIONAL,
    unConditionalForward        [37] IMPLICIT BOOLEAN OPTIONAL,
-- The follow field is the internal event for diagnostics:
    event                       [38] IMPLICIT Event OPTIONAL,
    ssiInfo                     [50] IMPLICIT SsiServiceInfo OPTIONAL,
    --2184
    hssQuery                    [60] IMPLICIT HssQuery OPTIONAL,
    outboundSip                 [61] IMPLICIT OutboundSip OPTIONAL,
    atNotificationInfo          [62] IMPLICIT SEQUENCE {
       deliveryResult              [0] IMPLICIT AtDeliveryResult,
       routingErrorCode            [1] IMPLICIT ErrorCode OPTIONAL
    } OPTIONAL,
    mtStatusReportInfo          [63] IMPLICIT SEQUENCE {
       deliveryResult              [0] IMPLICIT MtFwdSmDeliveryResult
    } OPTIONAL,
   destEmailAddr             [65] IMPLICIT VisibleString (SIZE (1..2600)) OPTIONAL
}

CommandWithCountryAndNetworkInfo ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime OPTIONAL,
    applicationName             [17] IMPLICIT NameString OPTIONAL,
    applicationShortNumber      [18] IMPLICIT GsmAddress OPTIONAL,
    messageFields               [19] IMPLICIT MessageFields OPTIONAL,
    moreMessagesToSend          [25] IMPLICIT BOOLEAN OPTIONAL,
    serviceCentreTimestamp      [27] IMPLICIT GeneralizedTime OPTIONAL,
    messageIdentifier           [28] IMPLICIT AmsMessageId OPTIONAL,
-- The follow field is the internal event for diagnostics:
    event                       [38] IMPLICIT Event OPTIONAL,
    msgCommand                  [39] IMPLICIT MsgCommand OPTIONAL,
    smResult                    [40] IMPLICIT ModifyResult OPTIONAL,
    cmdOriginatorAddress        [41] IMPLICIT GsmAddressInfo OPTIONAL,
    cmdAlphanumericOriginator   [42] IMPLICIT AlphanumericAddress OPTIONAL,
    cmdRecipientAddress         [43] IMPLICIT GsmAddressInfo OPTIONAL,
    foundCount                  [44] IMPLICIT INTEGER OPTIONAL,
```

```
    cancelMode                  [45] IMPLICIT CancelMode OPTIONAL
}

RegistrationWithCountryAndNetworkInfo ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    originalIiw                 [62] IMPLICIT IiwId OPTIONAL,
    registrationInfo            [63] IMPLICIT SEQUENCE {
        registrationType           [0] RegistrationType,
        expireValue                [1] ExpireValue,
        recipientAddress           [4] GsmAddressInfo
    },
    atmRequestResult            [64] IMPLICIT AtmRequestResult
}

MessageFields ::= SEQUENCE {
    -- originatorAddress and alphanumericOriginator are mutually exclusive
    -- recipientAddress and alphanumericRecipient are mutually exclusive
    protocol                    [0] Protocol OPTIONAL,
    originatorAddress           [2] GsmAddressInfo OPTIONAL,
    recipientAddress            [4] GsmAddressInfo OPTIONAL,
    dataCodingScheme            [5] DataCodingScheme OPTIONAL,
    protocolIdentifier          [6] ProtocolId OPTIONAL,
    notificationType            [7] NotificationType OPTIONAL,
    userData                    [10] UserData OPTIONAL,
    userDataHeader              [11] UserDataHeader OPTIONAL,
-- For reasons of backward compatibility this field is present in the parent
    moreMessagesToSend          [12] BOOLEAN OPTIONAL,
    priority                    [13] Priority OPTIONAL,
    replyPathIndicator          [14] BOOLEAN OPTIONAL,
    deferredDeliveryTime        [17] GeneralizedTime OPTIONAL,
    validityPeriod              [18] GeneralizedTime OPTIONAL,
    singleShotIndicator         [19] BOOLEAN OPTIONAL,
    billingIdentifier           [20] BillingId OPTIONAL,
    deliveryStatus              [22] DeliveryStatus OPTIONAL,
    errorCode                   [23] ErrorCode OPTIONAL,
    tariffClass                 [25] TariffClass OPTIONAL,
    serviceDescription          [26] ServiceDescription OPTIONAL,
    originatedImsi              [27] ImsiInfo OPTIONAL,
    originatedMscAddress        [28] GsmAddressInfo OPTIONAL,
    serviceCentreAddress        [29] GsmAddressInfo OPTIONAL,
    alphanumericOriginator      [30] AlphanumericAddress OPTIONAL,
    alphanumericRecipient       [31] AlphanumericAddress OPTIONAL,
    gsmStatusReportType         [32] GsmStatusReportType OPTIONAL,
    originatingPointCode        [33] PointCode OPTIONAL,
    portNumber                  [34] PortNumber OPTIONAL,
    gsmMessageReference         [40] MessageReference OPTIONAL,

    sourcePort                  [46] PortNumber OPTIONAL,
    destinationPort             [47] PortNumber OPTIONAL,
    endToEndAckRequest          [50] EndToEndAckRequest OPTIONAL,
    endToEndMessageType         [52] EndToEndMessageType OPTIONAL,
    messageReference            [53] MessageReference OPTIONAL,
    privacy                     [54] Privacy OPTIONAL,
    numberOfMessages            [55] NumberOfMessages OPTIONAL,
    language                    [56] Language OPTIONAL,
    payloadType                 [63] PayloadType OPTIONAL,
    sourceSubAddress            [67] SubAddress OPTIONAL,
    destSubAddress              [68] SubAddress OPTIONAL,
    userResponseCode            [69] UserResponseCode OPTIONAL,
    displayTime                 [70] DisplayTime OPTIONAL,
    callbackNumbers             [71] SEQUENCE OF CallbackNumber OPTIONAL,
    msValidityIndicator         [72] MsValidityIndicator OPTIONAL,
    msValidityPeriod            [73] MsValidityPeriod OPTIONAL,
    alertOnMessageDelivery      [74] AlertOnMessageDelivery OPTIONAL,
    smsSignal                   [75] SmsSignal OPTIONAL,
```

```
    sourceBearerType            [76] BearerType OPTIONAL,
    destBearerType              [77] BearerType OPTIONAL,
    smDefaultMsgId              [78] SmDefaultMessageId OPTIONAL,
    sourceNetworkType           [79] NetworkType OPTIONAL,
    destNetworkType             [80] NetworkType OPTIONAL,
    xsMessageType               [82] XsMessageTypeInfo OPTIONAL
}

OriginalMessageFields ::= SEQUENCE {
-- Fields here should exactly match those in MessageFields by their tag values
    originatorAddress           [2] GsmAddressInfo OPTIONAL,
    recipientAddress            [4] GsmAddressInfo OPTIONAL
}

-- Following record is generated when an notification for an AO/SM has been
-- received from an SMSC.

ReceivedNotificationWithCountryAndNetworkInfo ::= SEQUENCE {
    timestamp                   [0] IMPLICIT GeneralizedTime,
    routingAction               [1] IMPLICIT AtiRoutingAction,
    -- rejectInfo and responseInfo are mutually exclusive.
    rejectInfo                  [2] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        atRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        atExtConditionRule          [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    responseInfo                [3] IMPLICIT SEQUENCE {
        deliveryResult              [0] IMPLICIT AtDeliveryResult,
        routingErrorCode            [1] IMPLICIT ErrorCode OPTIONAL,
        atRoutingRule               [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    applicationName             [17] IMPLICIT NameString,
    applicationShortNumber      [18] IMPLICIT GsmAddress,
    messageFields               [19] IMPLICIT SEQUENCE {
        -- recipientAddress and alphanumericRecipient are mutually
        -- exclusive
        originatorAddress           [2] GsmAddressInfo,
        recipientAddress            [4] GsmAddressInfo OPTIONAL,
        moreMessagesToSend          [12] BOOLEAN,
        priority                    [13] Priority OPTIONAL,
        serviceCentreTimestamp      [21] GeneralizedTime OPTIONAL,
        deliveryStatus              [22] DeliveryStatus,
        errorCode                   [23] ErrorCode OPTIONAL,
        deliveryTimestamp           [24] GeneralizedTime OPTIONAL,
        alphanumericOriginator      [30] AlphanumericAddress OPTIONAL,
        alphanumericRecipient       [31] AlphanumericAddress OPTIONAL,
        portNumber                  [34] PortNumber OPTIONAL,
        sourcePort                  [46] PortNumber OPTIONAL,
        destinationPort             [47] PortNumber OPTIONAL,
        endToEndAckRequest          [50] EndToEndAckRequest OPTIONAL,
        endToEndMessageType         [52] EndToEndMessageType OPTIONAL,
        messageReference            [53] MessageReference OPTIONAL,
        privacy                     [54] Privacy OPTIONAL,
        numberOfMessages            [55] NumberOfMessages OPTIONAL,
        language                    [56] Language OPTIONAL,
        payloadType                 [63] PayloadType OPTIONAL,
        sourceSubAddress            [67] SubAddress OPTIONAL,
        destSubAddress              [68] SubAddress OPTIONAL,
        userResponseCode            [69] UserResponseCode OPTIONAL,
        displayTime                 [70] DisplayTime OPTIONAL,
        callbackNumbers             [71] SEQUENCE OF CallbackNumber OPTIONAL,
        msValidityIndicator         [72] MsValidityIndicator OPTIONAL,
        msValidityPeriod            [73] MsValidityPeriod OPTIONAL,
        alertOnMessageDelivery      [74] AlertOnMessageDelivery OPTIONAL,
        smsSignal                   [75] SmsSignal OPTIONAL,
```

```
        sourceBearerType            [76] BearerType OPTIONAL,
        destBearerType              [77] BearerType OPTIONAL,
        smDefaultMsgId              [78] SmDefaultMessageId OPTIONAL,
        sourceNetworkType           [79] NetworkType OPTIONAL,
        destNetworkType             [80] NetworkType OPTIONAL
    },
    outboundAt                  [23] IMPLICIT OutboundAt OPTIONAL,
    storage                     [24] IMPLICIT StorageInfo OPTIONAL,
    ecResponseData              [34] IMPLICIT SEQUENCE OF EcResponseData OPTIONAL,
    -- insideRejectInfo and insideResponseInfo are mutually exclusive.
    originalMessageFields       [46] OriginalMessageFields OPTIONAL,
    insideRejectInfo            [47] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        atiRoutingRule              [1] IMPLICIT NameString OPTIONAL,
        atiExtConditionRule         [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    insideResponseInfo          [48] IMPLICIT SEQUENCE {
        deliveryResult              [0] IMPLICIT AtDeliveryResult,
        routingErrorCode            [1] IMPLICIT ErrorCode OPTIONAL,
        atiRoutingRule              [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    ssiInfo                     [50] IMPLICIT SsiServiceInfo OPTIONAL
}


-- Following sub-record is included when an inbound operation results in an
-- outbound MT/SM.

OutboundMt ::= SEQUENCE {
    sriSmRoutingAction          [0] SriSmRoutingAction,
    sriSmRejectInfo             [1] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtExtConditionRule          [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    sriSmResponseInfo           [2] IMPLICIT SEQUENCE {
        queryResult                 [0] SriSmQueryResult,
        mapImsi                     [1] ImsiInfo OPTIONAL,
        mapLmsi                     [2] Lmsi OPTIONAL,
        mapMsc                      [3] GsmAddressInfo OPTIONAL,
        mapSgsn                     [4] GsmAddressInfo OPTIONAL,
        mtRoutingRule               [5] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    mtFwdSmToMscRoutingAction   [3] MtFwdSmRoutingAction OPTIONAL,
    mtFwdSmToMscRejectInfo      [4] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtExtConditionRule          [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    mtFwdSmToMscResponseInfo    [5] IMPLICIT SEQUENCE {
       deliveryResult               [0] IMPLICIT MtFwdSmDeliveryResult OPTIONAL,

       mtRoutingRule                [1] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    mtFwdSmToSgsnRoutingAction   [6] MtFwdSmRoutingAction OPTIONAL,
    mtFwdSmToSgsnRejectInfo      [7] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtExtConditionRule          [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    mtFwdSmToSgsnResponseInfo    [8] IMPLICIT SEQUENCE {
       deliveryResult               [0] IMPLICIT MtFwdSmDeliveryResult OPTIONAL,

       mtRoutingRule                [1] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
```

```
    ecResponseData               [9] IMPLICIT SEQUENCE OF EcResponseData OPTIONAL,
    destinationPointCode         [10] IMPLICIT  PointCode OPTIONAL,
    isMultiPartMtMessage         [11] IMPLICIT BOOLEAN OPTIONAL
}

-- 2184
-- Following sub-record is included when an inbound operation results in an
-- outbound SIP.

OutboundSip ::= SEQUENCE {
    mtFwdSmToImsRoutingAction   [6] MtFwdSmRoutingAction OPTIONAL,
    mtFwdSmToImsRejectInfo      [7] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        mtExtConditionRule          [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    mtFwdSmToImsResponseInfo    [8] IMPLICIT SEQUENCE {
        deliveryResult              [0] IMPLICIT MtFwdSmDeliveryResult OPTIONAL,

        mtRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        sipErrorCode                [2] IMPLICIT SipErrorCode OPTIONAL,
        rpErrorCause                [3] IMPLICIT RpErrorCause OPTIONAL,
        tpFailureCause              [4] IMPLICIT TpFailureCause OPTIONAL
    } OPTIONAL,
    ecResponseData               [9] IMPLICIT SEQUENCE OF EcResponseData OPTIONAL,
    iiw                         [60] IMPLICIT IiwId OPTIONAL,
    sipServerAddress            [61] IMPLICIT SipUrl OPTIONAL,
    sipClientName               [62] IMPLICIT NameString OPTIONAL,
    sipEndPointName             [63] IMPLICIT NameString OPTIONAL,
    sipEndPointTransport        [64] IMPLICIT SipTransport OPTIONAL
}

-- Following sub-record is included when an inbound operation results in an
-- outbound MO/SM.

OutboundMo ::= SEQUENCE {
    submissionResult                        [0] IMPLICIT MoFwdSmSubmissionResult,
    smscName                                [1] IMPLICIT NameString,
    rejectCause                             [2] IMPLICIT MoRejectCause OPTIONAL
}

-- Following sub-record is included when an inbound operation results in an
-- outbound AO/SM.
OutboundAo ::= SEQUENCE {
    submissionResult             [0] IMPLICIT AoSubmissionResult,
    applicationName              [1] IMPLICIT NameString,
    applicationShortNumber       [2] IMPLICIT GsmAddress,
    serviceCentreName            [3] IMPLICIT NameString OPTIONAL,
    scNodeName                   [4] IMPLICIT NameString OPTIONAL,
    scTerminationPointName       [5] IMPLICIT NameString OPTIONAL,
    routingErrorCode             [6] IMPLICIT ErrorCode OPTIONAL,
    serviceCentreTimestamp       [7] IMPLICIT GeneralizedTime OPTIONAL,
    smppMessageId                [8] IMPLICIT SmppMessageId OPTIONAL
}

-- Following sub-record is included when an inbound operation results in an
-- outbound AT/SM.

OutboundAt ::= SEQUENCE {
    routingAction               [0] AtRoutingAction,
    rejectInfo                  [1] IMPLICIT SEQUENCE {
        rejectCause                 [0] IMPLICIT RejectCause,
        atRoutingRule               [1] IMPLICIT NameString OPTIONAL,
        atExtConditionRule          [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
```

```
    responseInfo                [2] IMPLICIT SEQUENCE {
        deliveryResult              [0] IMPLICIT AtDeliveryResult,
        routingErrorCode            [1] IMPLICIT ErrorCode OPTIONAL,
        atRoutingRule               [2] IMPLICIT NameString OPTIONAL
    } OPTIONAL,
    applicationName             [3] IMPLICIT NameString,
    applicationShortNumber      [4] IMPLICIT GsmAddress,
    ecResponseData              [5] IMPLICIT SEQUENCE OF EcResponseData OPTIONAL
}

-- Following sub-record is included when an inbound operation results in a
-- storage of the SM.

StorageInfo ::= SEQUENCE {
    storageResult               [0] IMPLICIT StorageResult,
    routingErrorCode            [1] IMPLICIT ErrorCode OPTIONAL,
    -- applicationName and applicationShortNumber are included when the
    -- concerning SM is to be terminated in an application.
    applicationName             [2] IMPLICIT NameString OPTIONAL,
    applicationShortNumber      [3] IMPLICIT GsmAddress OPTIONAL,
    queue                       [4] IMPLICIT QueueIndex
}

-- Following is the construct for a GSM address with country/network
-- information.

GsmAddressInfo ::= SEQUENCE {
    gsmAddress  [0] IMPLICIT GsmAddress,
    -- country/network is only included when the address can be associated with
    -- one of the provisioned countries/networks.
    country      [1] IMPLICIT Country OPTIONAL,
    network      [2] IMPLICIT Network OPTIONAL
}

-- Following is the construct for an SCCP address with country/network
-- information.

SccpAddressInfo ::= SEQUENCE {
    sccpAddress  [0] IMPLICIT SccpAddress,
    -- country/network is only included when the address can be associated with
    -- one of the provisioned countries/networks.
    country      [1] IMPLICIT Country OPTIONAL,
    network      [2] IMPLICIT Network OPTIONAL
}

-- Following is the construct for an IMSI with country/network
-- information.

ImsiInfo ::= SEQUENCE {
    imsi         [0] IMPLICIT Imsi,
    -- country/network is only included when the address can be associated with
    -- one of the provisioned countries/networks.
    country      [1] IMPLICIT Country OPTIONAL,
    network      [2] IMPLICIT Network OPTIONAL
}

-- The following sub-record is included if SSI is enabled
SsiServiceInfo ::= SEQUENCE {
    originatorServices       [0] IMPLICIT SsiServiceString OPTIONAL,
    recipientServices        [1] IMPLICIT SsiServiceString OPTIONAL
}

-- ID of AMS Queue
QueueIndex ::= INTEGER (1..1000)
```

```
-- SMPP message ID
SmppMessageId ::= OCTET STRING -- -- (SIZE (1..64))

-- String used for names of applications, networks, rules, etc.
NameString ::= OCTET STRING (SIZE (1..31))

-- SCCP address.
-- For ITU-T, refer to Q.713 section 3.4 for encoding.
-- For Japanese SS7, refer to JT Q713
-- For ANSI, refer to ANSI T1.112-1996
SccpAddress ::= OCTET STRING (SIZE (0..255))

-- GSM address. Refer to GSM 03.40 version 5.8.1 release 1996 section 9.1.5
-- for encoding.
GsmAddress ::= OCTET STRING (SIZE (0..20))

-- IMSI. Refer to GSM 09.02 for encoding.
Imsi ::= OCTET STRING (SIZE (1..8))

-- LMSI. Refer to GSM 09.02 for encoding.
Lmsi ::= OCTET STRING (SIZE (4))

-- Data Coding Scheme. Refer to GSM 03.38 for encoding.
DataCodingScheme ::= INTEGER (0..255)

-- Protocol ID. Refer to GSM 03.40 version 5.8.1 release 1996 section 9.2.3.9
-- for encoding.
ProtocolId ::= INTEGER (0..255)

-- Message Reference. Refer to GSM 03.40 version 5.8.1 release 1996 section
-- 9.2.3.6 for encoding.
MessageReference ::= INTEGER (0..65535)

-- Message Number. Refer to GSM 03.40 version 5.8.1 release 1996 section
-- 9.2.3.18 for encoding.
MessageNumber ::= INTEGER (0..255)

-- Command Type. Refer to GSM 03.40 version 5.8.1 release 1996 section
-- 9.2.3.19 for encoding.
CommandType ::= INTEGER (0..255)

-- User Data Header. Refer to GSM 03.40 version 5.8.1 release 1996 section
-- 9.2.3.24 for encoding. Note that UDHL is NOT included.
UserDataHeader ::= OCTET STRING (SIZE (0..255))

-- User Data. Refer to GSM 03.40 version 5.8.1 release 1996 section
-- 9.2.3.24 for encoding. Note that 7-bit characters are unpacked to octets.
UserData ::= OCTET STRING (SIZE (0..255))

-- 7-bit characters are unpacked to octets.
UserDataUtf8 ::= OCTET STRING (SIZE (0..255))

-- Status. Refer to GSM 03.40 version 5.8.1 release 1996 section
-- 9.2.3.15 for encoding.
Status ::= INTEGER (0..255)

-- Command Data. Refer to GSM 03.40 version 5.8.1 release 1996 section
-- 9.2.3.21 for encoding.
CommandData ::= OCTET STRING (SIZE (0..255))

-- Country code according to ISO 3166 (e.g. nl for Netherlands)
Country ::= OCTET STRING (SIZE (2..2))

-- Name of mobile network as assigned during configuration of TextPass
Network ::= OCTET STRING (SIZE (1..31))
```

```
-- Priority.
Priority ::= INTEGER (0..255)

-- CIMD Tariff Class
TariffClass ::= INTEGER (0..99)

-- CIMD Service Description.
ServiceDescription ::= INTEGER (0..99)

-- Alphanumeric address
-- When an alphanumeric address contains @ as last character then RTR will replace
 @ with escape(0x1B) and @ character in log file
-- abcdefg@ will be represented as 61 f1 98 5c 36 9f 37 00 ( last character @ is
replaced by escape and @ )
-- abc@ will be represented as 61 f1 78 03 00 ( last character @ is replaced by
escape and @ )
-- abcdefg will be represented as 61 f1 98 5c 36 9f 01  ( no change in this address
 as it does not contain @ in last )
-- abc@defg will be represented as 61 f1 18 40 2e 9b cf ( no change in this address
 as it does not contain @ in last )
AlphanumericAddress ::= VisibleString (SIZE (1..20))

-- Port Number on HUB.
PortNumber ::= INTEGER (0..65535)

-- Point code (for ITU-T, range is 0-16383, for ANSI, range is 0-16777215, for
Japanese SS7, range is 0-65535)
PointCode ::= INTEGER (0..16777215)

-- MXP Error Code
ErrorCode ::= ENUMERATED
{
    errNoError(0),
    errMtTimeout(1),
    errMtAbsentSubscriber(2),
    errMtSystemFailure(3),
    errMtDataMissing(4),
    errMtUnexpectedDataValue(5),
    errMtFaciltyNotSupported(6),
    errMtUnidentifiedSubscriber(7),
    errMtIllegalSubscriber(8),
    errMtIllegalEquipment(9),
    errMtSubscriberBusyForMtSm(10),
    errMtInvalidSmeAddress(11),
    errMtEquipmentProtocolError(12),
    errMtEquipmentNotSmEquipped(13),
    errMtMemoryCapacityExceeded(14),
    errMtOtherMapError(15),
    errMtTcapAborted(16),
    errMtSccpAborted(17),
    errMtNoPagingError(18),
    errMtImsiDetachError(19),
    errMtRoamingRestrictions(20),
    errMtShortMsgType0NotSupportedError(21),
    errMtCanNotReplaceShortMsgError(22),
    errMtUnspecifiedProtocolIdError(23),
    errMtMsgClassNotSupportedError(24),
    errMtUnspecifiedDataCodingSchemeError(25),
    errMtTpduNotSupported(26),
    errMtSimStorageFullError(27),
    errMtNoSmStorageCapabilityInSimError(28),
    errMtErrorInMs(29),
    errMtSimApplToolKitbusyError(30),
    errMtSimDataDownloadError(31),
```

```
    errMtApplSpecificError(32),
    errMtEquipUnspecifiedErrorCause(33),
    errMtUeDeregistered(34),
    errMtNoResponseViaIpsmGw(35),
    errMtBlockedByMtRule(65535),
    errSrismTimeout(16777217),
    errSrismSystemFailure(16777218),
    errSrismDataMissing(16777219),
    errSrismUnexpectedDataValue(16777220),
    errSrismFacilityNotSupported(16777221),
    errSrismUnknownSubscriber(16777222),
    errSrismAbsentSubscriber(16777223),
    errSrismCallBarred(16777224),
    errSrismTeleserviceNotProvisioned(16777225),
    errSrismOtherMapError(16777226),
    errSrismTcapAborted(16777227),
    errSrismSccpAborted(16777228),
    errSrismMsDeregisteredError(16777229),
    errSrismMsPurgedError(16777230),

    errAtSystemError(33554433),
    errAtShuttingDown(33554434),
    errAtMxpFailure(33554435),
    errAtMxpTimeout(33554436),
    errAtTxFailure(33554437),
    errAtTemporaryError(33554438),
    errAtPermanentDestError(33554439),
    errAtPermanentMsgError(33554440),
    errAtAppNotAvailable(33554441),
    errAtSourceNotAvailable(33554442),
    errAtBlockedByThroughputControl(33554443),
    errAtLoginInvalid(33554444),
    errAtLoginNotAllowed(33554445),
    errAtLoginTooManySessions(33554446),
    errAtLoginNoSmscConnection(33554447),
    errAtAlreadyLoggedIn(33554448),
    errAtOperationNotAllowed(33554449),
    errAtOperationNotSupported(33554450),
    errAtResponseTimeout(33554451),
    errAtInvalidSyntax(33554452),
    errAtInvalidChecksum(33554453),
    errAtBlockedByAtRule(33554454),
    errAtRecipientError(33554455),
    errAtAppNotExisting(33554456),
    errAtInvalidMsgType(33554457),
    errAtInvalidMsg(33554458),
    errAtInvalidTimePeriod(33554459),
    errAtInvalidAddress(33554460),
    errAtMsgNotFound(33554461),
    errAtDeliveryInProgress(33554462),
    errAtTransparent(33554463),
    errAtLoginNoResources(33554464),
    errAtTxWindowFull(33554465),
    errAtMaxMessagesBuffered(33554466),
    errAtInvalidBindStatus(33554467),
    errAtNoRoutingRule(33554468),
    errAtConversionFailed(33554469),

    errAmsDeviceNotActive(50331649),
    errAmsDbError(50331650),
    errAmsStoreFull(50331651),
    errAmsQueueFull(50331652),
    errAmsRecipBufferFull(50331653),
    errAmsInvalidQueue(50331654),
    errAmsInvalidMessage(50331655),
```

```
    errAmsInvalidValidityTime(50331656),
    errAmsInvalidDeferredDelivery(50331657),
    errAmsStorageRateExceeded(50331658),
    errAmsDeliveryAttemptsExceeded(50331659),
    errRtrBlockedByThroughputControl(67108864),
    errRtrStorageFailure(67108865),
    errRtrTimeout(67108866),
    errRtrBlockedByRule(67108867),
    errRtrNoRuleMatching(67108868),
    errRtrLicenseExceeded(67108869),
    errRtrOriginatorInBlackList(67108870),
    errRtrOriginatorNotInWhiteList(67108871),
    errRtrMessageTooLong(67108872),
    errMoTimeout(83886083),
    errMoDropped(83886084),
    errMoDiscarded(83886085),
    errMoTprRejected(83886086),
    errMoSystemFailure(83886089),
    errMoDataMissing(83886090),
    errMoUnexpectedDataValue(83886091),
    errMoFacilityNotSupported(83886092),
    errMoUnknownServiceCentre(83886093),
    errMoServiceCentreCongestion(83886094),
    errMoInvalidSmeAddress(83886095),
    errMoSubscriberNotScSubscriber(83886096),
    errMoOtherMapError(83886097),
    errMoTcapAborted(83886098),
    errMoSccpAborted(83886099),
    errHssOtherError(100663297),
    errCapScfUnavailable(117440512),
    errCapUnassignedNumber(117440513),
    errCapUnidentfiedSubscriber(117440514),
    errCapCongestion(117440515),
    errCapFacilityNotSupported(117440516),
    errCapSmTransferRejected(117440517)
}


-- Billing ID as passed with UCP or SMPP AO/SM.
BillingId ::= OCTET STRING -- -- (SIZE (1..1024))

-- Some bits of an SMS-SUBMIT PDU. Refer to GSM 03.40 version 5.8.1 release 1996
-- section 9.2.3 for details regarding the bits.
SmsSubmitServices ::= BIT STRING {
    rejectDuplicates(5),
    statusReportRequest(2),
    userDataHeaderIndication(1),
    replyPath(0)
}

-- Some bits of an SMS-COMMAND PDU. Refer to GSM 03.40 version 5.8.1 release 1996
-- section 9.2.3 for details regarding the bits.
SmsCommandServices ::= BIT STRING {
    statusReportRequest(2),
    userDataHeaderIndication(1)
}

-- Some bits of an SMS-DELIVER PDU. Refer to GSM 03.40 version 5.8.1 release 1996
-- section 9.2.3 for details regarding the bits. Note that GSM 03.40 uses inversed
-- logic for more-messages-to-send (i.e. 0=MMS, 1=no MMS). The bit in the log uses
-- postive logic ((i.e. 0=no MMS, 1=MMS).
SmsDeliverServices ::= BIT STRING {
    moreMessagesToSend(5),
    statusReportIndication(2),
    userDataHeaderIndication(1),
```

```
    replyPath(0)
}

-- Some bits of an SMS-STATUS-REPORT PDU. Refer to GSM 03.40 version 5.8.1 release
 1996
-- section 9.2.3 for details regarding the bits.  Note that GSM 03.40 uses inversed
-- logic for more-messages-to-send (i.e. 0=MMS, 1=no MMS). The bit in the log uses
-- postive logic ((i.e. 0=no MMS, 1=MMS).
StatusReportServices ::= BIT STRING {
    moreMessagesToSend(5),
    statusReportQualifier(2)
}

-- Notification types.
NotificationType ::= BIT STRING {
    deliveryNotification (0),
    nonDeliveryNotification (1),
    bufferedNotification (2)
} (SIZE (8))

IgnoredRejectCauses ::= BIT STRING {
    unknownSccpSmscAddress(9),
    unknownMapSmscAddress(10),
    conflictingSmscAddress(11),
    spoofingSccpSmscAddress(12),
    spoofingMapSmscAddress(13),
    spoofedOriginatorAddress(19)
} (SIZE (32))

-- Result of an AO/SM
AoSubmissionResult ::= ENUMERATED {
    successful(0),
    sourceError(1),
    routingError(2),
    destinationTempError(3),
    destinationPermError(4),
    messagePermError(5)
}

-- Result of an AT/SM
AtDeliveryResult ::= ENUMERATED {
    successful(0),
    sourceError(1),
    routingError(2),
    destinationTempError(3),
    destinationPermError(4),
    messagePermError(5)
}

-- Result of storing an SM.
StorageResult ::= ENUMERATED {
    successful (0),
    destinationTempError(3),
    destinationPermError(4),
    messagePermError(5),
    queueFull(6),
    databaseError(7),
    invalidQueue(8),
    invalidStoreMessage(9),
    deviceNotOperating(10),
    amsStorageFull(11),
    recipientQueueFull(12),
    invalidValidity(13),
    invalidDeferred(14),
    storageRateExceeded(15)
```

```
}

-- Result of an MO-ForwardSM operation
MoFwdSmSubmissionResult ::= ENUMERATED {
    success(0),
    timeout(1),
    dropped(2),
    discarded(3),
    rejectedByTextPass(4),
    rejectedByApplication(5),
    unknown(6),
    systemFailureError(10),
    dataMissingError(11),
    unexpectedDataValueError(12),
    facilityNotSupportedError(13),
    invalidSmeAddressError(81),
    unknownServiceCentreError(85),
    scCongestionError (86),
    subscriberNotScSubscriberError (87),
    otherErrors(99),
    sccpAborted(100),
    tcapAborted(127)
}

-- Result of an SendRoutingInfoForSM operation
SriSmQueryResult ::= ENUMERATED {
    success(0),
    timeout(1),
    systemFailureError(10),
    dataMissingError(11),
    unexpectedDataValueError(12),
    facilityNotSupportedError(13),
    unknownSubscriberError(14),
    absentSubscriberError(15),
    callBarredError(16),
    teleServiceNotProvisionedError(17),
    otherErrors(99),
    sccpAborted(100),
    msDeregisteredError(108),
    msPurgedError(109),
    fallbackToMapVersion1Requested(125),
    fallbackToMapVersion2Requested(126),
    tcapAborted(127)
}

-- Result of an MT-ForwardSM operation
MtFwdSmDeliveryResult ::= ENUMERATED {
    success(0),
    timeout(1),
    systemFailureError(10),
    dataMissingError(11),
    unexpextedDataValueError(12),
    facilityNotSupportError(13),
    absentSubscriberError(15),
    unidentifiedSubscriberError(18),
    illegalSubscriberError(19),
    illegalEquipmentError(20),
    subscriberBusyForMtSmsError(21),
    invalidSmeAddressError(81),
    equipmentProtocolError(82),
    equipmentNotSmEquippedError(83),
    memoryCapacityExceededError(84),
    otherErrors(99),
    sccpAborted(100),
    noPagingError(105),
```

```
    imsiDetachedError(106),
    roamingRestrictionsError(107),
    shortMsgType0NotSupportedError(110),
    canNotReplaceShortMsgError(111),
    unspecifiedProtocolIdError(112),
    msgClassNotSupportedError(113),
    unspecifiedDataCodingSchemeError(114),
    tpduNotSupported(115),
    simStorageFullError(116),
    noSmStorageCapabilityInSimError(117),
    errorInMs(118),
    simApplToolKitbusyError(119),
    simDataDownloadError(120),
    applSpecificError(121),
    equipUnspecifiedErrorCause(122),
    ueDeregistered(123),
    noResponseViaIpsmGw(124),
    fallbackToMapVersion1Requested(125),
    fallbackToMapVersion2Requested(126),
    tcapAborted(127)

}

-- Result of a delivery attempt as reported in a notification on an AO/SM.
DeliveryStatus ::= ENUMERATED
{
    noStatusAvailable (0),
    inProgress (1),
    validityPeriodExpired (2),
    deliveryFailed (3),
    deliverySuccessful (4),
    noResponse (5),
    lastNoResponse (6),
    cancelled (7),
    deleted (8),
    deletedByCancel (9),
    scheduled (10),
    accepted (11),
    rejected (12),
    skipped (13),
    replaced (14)
}

-- Routing action for an AO/SM
AoRoutingAction ::= ENUMERATED {
    routeToSmsc(0),
    routeToMs(2),
    routeToMsFallbackToSmsc(3),
    discardWithNak(4),
    discardWithAck(5),
    storeForDeliveryToMs(6),
    routeToMsFallbackToStorage(7),
    storeForDeliveryToApplication(8),
    routeToApplicationFallbackToStorage(9),
    storeForForwardingAsAo(10),
    routeToSmscFallbackToStorage(11)
}

-- Routing action for an outgoing AT/SM or notification on an AO/SM
AtRoutingAction ::= ENUMERATED {
    pass(0),
    blockWithTemporaryError(1),
    blockWithPermanentError(2),
    blockWithAck(3)
}
```

```
-- Routing action for an incoming AT/SM or notification on an AO/SM
AtiRoutingAction ::= ENUMERATED {
    -- need to keep supporting the old ATO actions for backwards compatibility
    pass(0),
    blockWithTemporaryError(1),
    blockWithPermanentError(2),
    blockWithAck(3),
    -- the ATI routing actions, starting at 10.
    discardWithAck(10),
    discardWithTempError(11),
    discardWithPermMessageError(12),
    discardWithPermRecipientError(13),
    routeToApplication(14),
    routeToApplicationFallbackToStorage(15),
    storeForDeliveryToApplication(16),
    routeToSmscAsAo(17),
    routeToSmscAsAoFallbackToStorage(18),
    storeForForwardingToSmscAsAo(19)
}

-- Routing action for an MO-ForwardSM operation
MoFwdSmRoutingAction ::= ENUMERATED {
    routeToSmsc(0),
    routeToApplication(1),
    routeToMs(2),
    routeToMsFallbackToSmsc(3),
    discardWithNak(4),
    discardWithAck(5),
    routeToMsFallbackToApplication(6),
    discardWithNoResponse(7),
    storeForDeliveryToMs(8),
    routeToMsFallbackToStorage(9),
    storeForDeliveryToApplication(10),
    routeToApplicationFallbackToStorage(11),
    routeToSmscAsAo(12),
    routeToMsFallbackToSmscAsAo(13),
    routeToAoSmscGroup(14),
    routeToMsFallbackToAoSmscGroup(15)
}

-- Routing action for an SendRoutingInfoForSM operation
SriSmRoutingAction ::= ENUMERATED {
    pass(0),
    blockWithTemporaryError(1),
    blockWithPermanentError(2),
    discardSilently(3),
    pretendSuccess(4),
    release(5)
}

-- Routing action for an MT-ForwardSM operation
MtFwdSmRoutingAction ::= ENUMERATED {
    pass(0),
    blockWithTemporaryError(1),
    blockWithPermanentError(2),
    discardSilently(3),
    pretendSuccess(4),
    release(5)
}

AmsMessageId ::= OCTET STRING -- -- (SIZE (5))
    -- Order should be the same as AMS_message_id_t
    -- First byte is the AMS identifier
    -- last 4 bytes is the message identifier
```

```
GsmStatusReportType ::= ENUMERATED
{
    phase1 (1),
    phase2 (2)
}

-- twisted nibble encoded, first byte contains number of valid bytes.
-- in case of an odd number of digits, a 0-nibble is used as filler.
RoutingNumber ::= OCTET STRING (SIZE (2..5))

-- Human-readable CSV containing service names
SsiServiceString ::= OCTET STRING (SIZE(0..4096))

EndToEndAckRequest ::= BIT STRING -- -- {
-- --     readAck (0),
-- --     userAck (1)
-- -- } (SIZE (8))

EndToEndMessageType ::= ENUMERATED
{
    normalMessage (0),
    userAck (1),
    readAck (2),
    deliveryReceipt (3),
    intermediateNotification (4)
}

Privacy ::= ENUMERATED
{
    notRestricted (0),
    restricted (1),
    confidential (2),
    secret (3)
}

NumberOfMessages ::= INTEGER -- -- (0..65535)
-- number of messages in a mailbox

Language ::= ENUMERATED
{
    unspecified (0),
    english (1),
    french (2),
    spanish (3),
    german (4),
    portuguese (5),
    cantonese (6),
    mandarin (7),
    kangul (8),
    bahasa (9),
    hindi (10),
    urdu (11),
    tagalog (12),
    youroba(13),
    swahili (14),
    gaelic (15),
    hebrew (16),
    nihongo (17),
    russian (18),
    arabic (19),
    dutch(20),
    italian (21),
    polish (22),
    vietnamese (23),
```

```
    greek (24),
    yiddish (25),
    thai (26),
    laotian (27),
    persian (28),
    frenchCreole (29),
    armenian (30),
    navaho (31),
    hungarian (32),
    monKhmer (33),
    gujarathi (34),
    ukrania (35),
    czech (36),
    pennsylvaniaDutch (37),
    miao (38),
    norwegian (39),
    slovak (40),
    swedish (41),
    serbian (42),
    kru (43),
    rumanian (44),
    lithuanian (45),
    finnish (46),
    punjabi (47),
    formosan (48),
    croatian (49),
    bosnian (50),
    turkish (51),
    llocano (52),
    bengali (53),
    danish (54),
    flemish (55),
    syrian (56),
    tamil (57),
    samoan (58),
    malayalam (59),
    cajun (60),
    amharic (61)
}

PayloadType ::= ENUMERATED
{
    wdp(0),
    wcmp(1)
}

SubAddress ::= OCTET STRING --  --(SIZE(2..23))
-- binary data, encoded according to ANSI-41.

UserResponseCode ::= INTEGER (0..255)

DisplayTime ::= ENUMERATED
{
    temporary(0),
    default(1),
    invoke(2)
}

DigitMode ::= ENUMERATED
{
    tbcd(0),
    ascii(1)
}

CallbackNum ::= SEQUENCE
```

```
{
    digitMode       [0] DigitMode,
    address         [1] GsmAddress
}

Presentation ::= OCTET STRING -- -- (SIZE(1))
-- binary data, encoded according to CMT-136

CallbackNumAtag ::= OCTET STRING -- -- (SIZE(0..65))
-- binary data, encoded according to CMT-136

CallbackNumber ::= SEQUENCE
{
    number          [0] CallbackNum,
    presentation    [1] Presentation OPTIONAL,
    alphaTag        [2] CallbackNumAtag OPTIONAL
}

MsValidityIndicator ::= ENUMERATED
{
    indefinitely(0),
    powerDown(1),
    regAreaChanges(2),
    displayOnly(3),
    relative(4)
}

TimeUnit ::= ENUMERATED
{
    second(0),
    minute(1),
    hour(2),
    day(3),
    week(4),
    month(5),
    year(6)
}

MsValidityPeriod ::= SEQUENCE
{
    unit        [0] TimeUnit,
    multiplier  [1] INTEGER
}

AlertOnMessageDelivery ::= ENUMERATED
{
    default(0),
    lowPriority(1),
    mediumPriority(2),
    highPriority(3)
}

SmsSignal ::= OCTET STRING --  -- (SIZE(2))
-- binary data, encoded according to CMT-136

BearerType ::= ENUMERATED
{
    unknown(0),
    sms(1),
    csd(2),
    packetData(3),
    ussd(4),
    cdpd(5),
    dataTAC(6),
    flexReflex(7),
```

```
    cellBroadcast(8)
}

SmDefaultMessageId ::= INTEGER (0..255)

NetworkType ::= ENUMERATED
{
    unknown(0),
    gsm(1),
    tdma(2),
    cdma(3),
    pdc(4),
    phs(5),
    iden(6),
    amps(7),
    pagingNetw(8)
}

XsMessageTypeInfo ::= ENUMERATED
{
    forwardedMessage (1),
    copiedMessage (2),
    forwardedToEmail(3),
    copiedToEmail(4)
}

Protocol ::= ENUMERATED
{
    ucp (0),
    cimd (1),
    smpp (2)
}

-- Internal event for diagnostics:
Event ::= INTEGER

MnpViolation ::= ENUMERATED
{
    mnpViolationNone(0),
    mnpViolationForeignCountry(1),
    mnpViolationNumberOfForeignNetwork(2),
    mnpViolationMscOfForeignNetwork(3),
    mnpViolationInvalidImsi(4),
    mnpViolationForeignImsi(5),
    mnpViolationCallBarred(6),
    mnpViolationTsvcNotProv(7),
    mnpViolationImsiNeeded(8)
}

MsgCommand ::= ENUMERATED
{
    commandInvalid(1),
    commandMqcaModify(2),
    commandMqcaQuery(3),
    commandMqcaCancel(4),
    commandMqcaAlert(5)
}

ModifyResult ::= ENUMERATED
{
    successful(0),
    messageNotFound(1),
    deliveryInProgress(2),
    notAllowed(3),
    noAmsAvailable(4),
```

```
    databaseError(5),
    invalidMessage(6)
}

CancelMode ::= ENUMERATED
{
    allByDestination (0),
    singleById       (2)
}

EcResponseData ::= SEQUENCE
{
    extConditionRule [0] IMPLICIT NameString,
    applicationName  [1] IMPLICIT NameString,
    clientIpAddress  [2] IMPLICIT INTEGER,
    evaluationResult [3] IMPLICIT BOOLEAN,
    -- all fields below should be optional.
    attributesSet    [4] IMPLICIT EcAttributeMask OPTIONAL,
    attributesReset  [5] IMPLICIT EcAttributeMask OPTIONAL,
    diameterStatus   [6] IMPLICIT DiameterStatus OPTIONAL,
    textInEvaluationResponse [7] IMPLICIT TextInEvaluationResponse OPTIONAL,
    -- 2184
    ldapError        [8] IMPLICIT INTEGER OPTIONAL,
    recepientDomain  [9] IMPLICIT RecepientDomain OPTIONAL
}

RecepientDomain ::= ENUMERATED
{
    ss7Domain (0),
    imsDomain (1),
    ss7ThenImsDomain (2),
    imsThenSs7Domain (3)
}

TextInEvaluationResponse ::= OCTET STRING (SIZE(0..255))
-- any text that the EC application needs to add to log, encoded in UTF-8.

RejectCause ::= ENUMERATED {
    invalidSccpSmscAddress(0),
    invalidMapSmscAddress(1),
    invalidRecipientAddress(2),
    invalidOriginatorAddress(3),
    invalidImsi(4),
    invalidMscAddress(5),
    forgingMscAddress(6),
    forgingImsi(7),
    forgingLmsi(8),
    unknownSccpSmscAddress(9),
    unknownMapSmscAddress(10),
    conflictingSmscAddresses(11),
    spoofingSccpSmscAddress(12),
    spoofingMapSmscAddress(13),
    unsolicitedMtForwardSm(14),
    matchingMtRoutingRule(15),
    matchingMtExternalConditionRule(16),
    matchingMoRoutingRule(17),
    matchingMoExternalConditionRule(18),
    spoofedOriginatorAddress(19),
    matchingAoRoutingRule(20),
    matchingAoExternalConditionRule(21),
    matchingAtRoutingRule(22),
    matchingAtExternalConditionRule(23),
--    matchingCdmaMoRoutingRule(24),
--    matchingCdmaMoExternalConditionRule(25),
    mnpViolation(26),
```

```
    matchingAtiRoutingRule(27),
    matchingAtiExternalConditionRule(28),
    noSpaceForSegmentingHeader(29),
    earlyRecipientSriSmFailure(30),
    originatorListViolation(31),
    messageTooLong(32),
    originatorThroughputViolation(33),
    matchingSriqRoutingRule(34),
    unidentfiedSubscriber(35),
    absentSubscriber(36),
    facilityNotSupported(37),
    deliveryFailure(38),
    systemFailure(39),
    subscriberBusyForMtSms(40),
    illegalSubscriber(41),
    illegalEquipment(42),
    matchingMtiRoutingRule(43),
    unknownSubscriber(44)
}

EcAttributeMask ::= BIT STRING (SIZE(32))
-- string of 32 boolean values, 1 means applicable, 0 means do nothing

DiameterStatus ::= INTEGER (-9..6000)
-- result code of the Diameter answer, as received by the PBC

MoRejectCause ::= ENUMERATED {
    increaseInLengthMakesTransparentRoutingImpossible(0)
}

--2184

IiwId ::= SEQUENCE
{
    hostId                      [0] INTEGER,
    portNumber                  [1] PortNumber OPTIONAL
}

SipErrorCode ::= INTEGER
RpErrorCause ::= INTEGER
TpFailureCause ::= INTEGER
DiameterShResultCode ::= INTEGER

ImsUserState ::= ENUMERATED
{
    registered(0),
    notRegistered(1),
    registeredUnregServices(2),
    authenticationPending(3)
}

SipUrl ::= VisibleString (SIZE (1..128))
TelUrl ::= VisibleString (SIZE (1..128))

-- ExpireValue. Refer to TS 29.228 Appendixes B2.2 and B2.3
-- And also refer RFC 3261 Section 20.19
ExpireValue ::=  OCTET STRING (SIZE (4))

RegistrationType ::= ENUMERATED
{
    explicitDeRegistration (0),
    failureDeRegistration   (1),
    registration (2)
}
```

```
AtmRequestResult ::= ENUMERATED
{
    success(0),
    timeout(1),
    dataMissingError(11),
    unexpectedDataValueError(12),
    unknownSubscriberError(14),
    callBarredError(16),
    teleserviceNotProvisionedError(17),
    atmNotAllowedError(41),
    bearerServiceNotProvisionedError(42),
    illegalSSOperationError(43),
    ssSubscriptionViolationError(44),
    ssErrorStatus(45),
    ssIncompatibilityError(46),
    informationNotAvailableError(47),
    otherErrors(99),
    tcapAborted(127)
}

SipTransport ::= ENUMERATED
{
    tcp (0),
    udp (1),
    sctp(2)
}

END
```

Note: The `timestamp` field of the log represents the time when the log is generated for incoming rules and outgoing rules. The log is always created when the processing of the rules (either on the incoming leg, or on the outgoing leg) are finished. For instance, if other components (database server, intermediate storage) are involved in the message processing, the additional time difference will be introduced between the time when the message arrives in the system, and the timestamp of the log. Also any network delay will increase the difference. Therefore, the timestamp of the log record is likely different from the arrival time of the message.

Note: The `ecResponseData` field directly inside the `suspectMtFwdSmWithCountryAndNetworkInfo` and `trustedMtFwdSmWithCountryAndNetworkInfo` records the MTOX rule information.

Appendix B

Event ASN.1 Data Types

Topics:

B.1 Event ASN.1 Data Types

This appendix provides the event ASN.1 data types (as defined in `event.asn1`) used to generate the RTR log records.

```
-- ------------------------------------------------------------------------
--
--   (c) Copyright 2004-2015 NewNet
--
--   This software is proprietary to and embodies the confidential technology
--   of NewNet. Possession, use, duplication or dissemination of the
--   software and media is authorized only pursuant to a valid written license
--   from NewNet.
--
-- ------------------------------------------------------------------------
-- $Id: event.asn1,v 1.51 2015/02/03 06:01:57 a3kuma10 Exp $
-- ------------------------------------------------------------------------

LOGGING DEFINITIONS IMPLICIT TAGS ::=
BEGIN

Event ::= [APPLICATION 30] SEQUENCE {
    timeStamp                  [0] GeneralizedTime,                  --(Timestamp
 for the event)
    objectId                    [1] ObjectIdentifier,
    objectType                  [2] Object
}


Object ::= CHOICE {
    rogueTcap                  [1] SpoofAttempt,                    --(Rogue TCAP
 message that cannot be matched to an existing dialog)
    shortMessage                [2] ShortMessage,
    routingInfoQuery            [3] RoutingInfoQuery

    -- add new object types here.
}

--------------------------
-- Short Message Events --
--------------------------

ShortMessage ::= CHOICE {
    -- GSM / SS7 side events
    gsmOrigInRequest               [0] EvtSmGsmOrigInRequest,
    gsmOrigInResponse              [1] EvtSmGsmOrigInResponse,
    gsmOrigOutRequest              [2] EvtSmGsmOrigOutRequest,
    gsmOrigOutResponse             [3] EvtSmGsmOrigOutResponse,
    gsmOrigRejection               [4] EvtSmGsmOrigRejection,
    gsmTermInRequest               [5] EvtSmGsmTermInRequest,
    gsmTermInResponse              [6] EvtSmGsmTermInResponse,
    gsmTermOutRequest              [7] EvtSmGsmTermOutRequest,
    gsmTermOutResponse             [8] EvtSmGsmTermOutResponse,
    gsmTermRejection               [9] EvtSmGsmTermRejection,
    gsmRoutingInfoQuery           [10] EvtSmGsmRoutingInfoQuery,

    -- application side events
    appOrigInRequest              [20] EvtSmAppOrigInRequest,
    appOrigInResponse             [21] EvtSmAppOrigInResponse,
    appOrigOutRequest             [22] EvtSmAppOrigOutRequest,
    appOrigOutResponse            [23] EvtSmAppOrigOutResponse,
```

```
    appOrigRejection              [24] EvtSmAppOrigRejection,
    appTermInRequest              [25] EvtSmAppTermInRequest,
    appTermInResponse             [26] EvtSmAppTermInResponse,
    appTermOutRequest             [27] EvtSmAppTermOutRequest,
    appTermOutResponse            [28] EvtSmAppTermOutResponse,
    appTermRejection              [29] EvtSmAppTermRejection,

    -- IMS side events
    imsOrigInRequest              [40] EvtSmImsOrigInRequest,
    imsOrigInResponse             [41] EvtSmImsOrigInResponse,
    imsOrigRejection              [44] EvtSmImsOrigRejection,
    imsTermOutRequest             [45] EvtSmImsTermOutRequest,
    imsTermOutResponse            [46] EvtSmImsTermOutResponse,

    -- AMS events
    amsStoreRequest               [60] EvtSmAmsStoreRequest,
    amsStoreResponse              [61] EvtSmAmsStoreResponse,
    amsDeliveryAttempt            [62] EvtSmAmsDeliveryAttempt,
    amsTermination                [63] EvtSmAmsTermination,
    amsDeliveryRejection          [64] EvtSmAmsDeliveryRejection,

    -- central processing events
    routingDecision               [70] EvtSmRoutingDecision,
    externalCondition             [71] EvtSmExternalCondition,
    notification                  [72] EvtSmNotification,
    smCopied                      [73] EvtSmCopied,
    copyCreated                   [74] EvtSmCopyCreated,
    copyRejection                 [75] EvtSmCopyRejection,
    forwardAttempt                [76] EvtSmForwardAttempt,
    forwardRejection              [77] EvtSmForwardRejection,
    prepaidCharging               [78] EvtSmPrepaidCharging,
    smAutoReplied                 [79] EvtSmAutoReplied,
    autoReplyCreated              [80] EvtSmAutoReplyCreated,
    signatureInserted             [81] EvtSmSignatureInserted,

    -- auxiliary events
    endpoints                     [90] EvtSmEndpoints,
    finalStatus                   [91] EvtSmFinalStatus
}

-------------------------------------
-- ShortMessage events (EvtSmXyz) --
-------------------------------------

-- Incoming GSM MO message
EvtSmGsmOrigInRequest ::= SEQUENCE
{
    originator                  [0] GsmAddress,         -- MAP sm-RP-OA
    recipient                   [1] GsmAddress,         -- GSM 03.40 TP-DA
    smsc                        [2] GsmAddress,         -- MAP sm-RP-DA
    originatingAddress          [3] SccpMscSgsnAddress, -- SCCP CgPA
    message                     [4] SmMessage,
    pid                         [5] ProtocolId,
    originatorImsi              [6] ImsiInfo OPTIONAL,
    statusReportRequest         [7] GsmStatusReportPhase OPTIONAL,
    validityExpirationTime      [8] UnixTimestamp OPTIONAL,
    deferredDeliveryTime        [9] UnixTimestamp OPTIONAL,
    originatingPointCode       [10] PointCode OPTIONAL
}

-- Response to incoming GSM MO message
EvtSmGsmOrigInResponse ::= GsmResponse

-- Outgoing GSM MO message
EvtSmGsmOrigOutRequest ::= SEQUENCE
```

```
{
    smscAddress                [0] SccpAddressInfo,  -- SCCP CdPA
    smscName                   [1] NameString OPTIONAL
}

-- Response to outgoing GSM MO message
EvtSmGsmOrigOutResponse ::= GsmResponse

-- Reject causes for incoming GSM MO message
EvtSmGsmOrigRejection ::= CHOICE
{
    spoofingDetected           [0] EmptySequence,
    droppedDueToDecimation     [1] EmptySequence,
    fallbackUnavailable        [2] EmptySequence,
    storageUnavailable         [3] EmptySequence,
    invalidMoTag               [4] EmptySequence,
    invalidOriginatorAddress   [5] EmptySequence,
    invalidMscAddress          [6] EmptySequence,
    invalidMapSmscAddress      [7] EmptySequence,
    invalidRecipientAddress    [8] EmptySequence,
    throughputLimit            [9] ThroughputLimit,
    noCamelChargingServer     [10] EmptySequence,
    noRoutingPathAvailable    [11] EmptySequence,
    mnpViolation              [12] EmptySequence,
    segmentationImpossible    [13] EmptySequence,
    callerAborted             [14] EmptySequence

    -- more reject causes other than "routing decision"...
}

--     rejectedByApp              [2] RejectedByApp,
--     rejectedByRouter           [3] EmptySequence,

-- Incoming GSM MT Request
EvtSmGsmTermInRequest ::= SEQUENCE
{
    originator                 [0] GsmAddress,          -- GSM 03.40 TP-OA
    recipient                  [1] GsmAddress OPTIONAL, -- inherited from previous
 SRI-SM
    smsc                       [2] GsmAddress,          -- MAP sm-RP-OA
    terminatingAddress         [3] SccpMscSgsnAddress,  -- SCCP CdPA
    message                    [4] SmMessage,
    recipientImsi              [5] ImsiInfo,
    smscTimestamp              [6] UnixTimestamp,
    pid                        [7] ProtocolId
}

-- Response to incoming GSM MT Request
EvtSmGsmTermInResponse ::= GsmResponse

-- Outgoing GSM MT Request
EvtSmGsmTermOutRequest ::= SEQUENCE
{
    terminatingAddress         [0] SccpMscSgsnAddress, -- SCCP CdPA
    recipientImsi              [1] ImsiInfo,
    destinationPointCode       [2] PointCode OPTIONAL
}

-- Response to outgoing GSM MT Request
EvtSmGsmTermOutResponse ::= GsmResponse

-- Reject causes for incoming GSM MT message
EvtSmGsmTermRejection ::= CHOICE
{
    unsolicitedMessage         [1] EmptySequence,
```

```
                                                    -- 2 == deprecated disapproved,
                                                  -- see externalCondition instead.

    invalidSccpMscAddress       [3] EmptySequence,
    invalidMapSmscAddress       [4] EmptySequence,
    invalidRecipientAddress     [5] EmptySequence,
    invalidOriginatorAddress    [6] EmptySequence,
    invalidImsi                 [7] EmptySequence,
    invalidMscAddress           [8] EmptySequence,
    forgingMscAddress           [9] EmptySequence,
    forgingImsi                [10] EmptySequence,
    forgingLmsi                [11] EmptySequence,
    unknownSccpSmscAddress     [12] EmptySequence,
    unknownMapSmscAddress      [13] EmptySequence,
    conflictingSmscAddress     [14] EmptySequence,
    spoofingSccpSmscsAddress   [15] EmptySequence,
    spoofingMapSmscAddress     [16] EmptySequence

    -- more reject causes other than "routing decision"...
}

-- GSM HLR Query & Result
EvtSmGsmRoutingInfoQuery ::= SEQUENCE
{
    msisdn                      [0] GsmAddress, -- MAP msisdn
    result                      [1] GsmRoutingInfoQueryResult
}


-- Incoming AO Request
EvtSmAppOrigInRequest ::= SEQUENCE
{
    originator                  [0] GsmAddress,
    recipient                   [1] GsmAddress,
    application                 [2] EsmeApplication OPTIONAL,
    message                     [3] SmMessage,
    notificationRequested       [4] AppNotificationRequest OPTIONAL,
    validityExpirationTime      [5] UnixTimestamp OPTIONAL,
    deferredDeliveryTime        [6] UnixTimestamp OPTIONAL
}

-- Response to incoming AO Request
EvtSmAppOrigInResponse ::= GenericResponse

-- Outgoing AO Request
EvtSmAppOrigOutRequest ::= SEQUENCE
{
    smsc                        [0] SmAppServiceCentre,
    application                 [1] EsmeApplication OPTIONAL
}

-- Response to outgoing AO Request
EvtSmAppOrigOutResponse ::= GenericResponse

-- Reject causes for incoming AO message
EvtSmAppOrigRejection ::= CHOICE
{
    -- RTR range
    throughputLimit             [0] ThroughputLimit,
    noCamelChargingServer       [1] EmptySequence,
    messageTooLong              [2] EmptySequence,
    segmentationImpossible      [3] EmptySequence,
    originatorListViolation     [4] EmptySequence,
```

```
    -- HUB range
    sendMxpReqFailed          [10] EmptySequence,
    timeoutMxpReq             [11] EmptySequence,
    appNotAuthorised          [12] EmptySequence,
    appNotAllowed             [13] EmptySequence,
    systemError               [14] EmptySequence

}

-- Incoming AT Request
EvtSmAppTermInRequest ::= SEQUENCE
{
    originator                 [0] GsmAddress,
    recipient                  [1] GsmAddress,
    serviceCentre              [2] SmAppServiceCentre,
    application                [3] EsmeApplication,
    message                    [4] SmMessage
}

-- Response to incoming AT Request
EvtSmAppTermInResponse ::= GenericResponse

-- Outgoing AT Request
EvtSmAppTermOutRequest ::= SEQUENCE
{
    application                [0] EsmeApplication
}

-- Response to outgoing AT Request
EvtSmAppTermOutResponse ::= GenericResponse

-- Reject causes for incoming AT message
EvtSmAppTermRejection ::= CHOICE
{
-- RTR range
    throughputLimit            [0] ThroughputLimit,

-- HUB range
    sendMxpReqFailed          [10] EmptySequence,
    timeoutMxpReq             [11] EmptySequence,
    smscNotAllowed            [12] EmptySequence,
    systemError               [13] EmptySequence
}

-- Incoming IMS MO Request
EvtSmImsOrigInRequest ::= SEQUENCE
{
    originator                 [0] GsmAddress, -- built from URI (note) --
    recipient                  [1] GsmAddress, -- GSM 03.40 TP-DA --
    fromUri                    [2] URI,
    toUri                      [3] URI,
    message                    [4] SmMessage
}

-- (note): this number is taken from the tel: URI in the P-Asserted-Identity, --
-- and is encoded as if it were a MAP AddressString with TON = internat. (1)  --
-- and NPI = ISDN E164 (1). --

-- Response to incoming IMS MO Request
EvtSmImsOrigInResponse ::= CHOICE
{
    success                    [0] EmptySequence,
    failure                    [1] EvtSmImsOrigInFailure
-- note: a timeout on the RTR side will be encoded as an rp error TemporaryFailure
 --
```

```
}

EvtSmImsOrigInFailure ::= CHOICE
{
    sipError                    [0] INTEGER, -- see IANA assignments for SIP --
    rpCause                     [1] INTEGER  -- see Short Message RP 24.011 --
}

-- Reject Causes for incoming IMS MO message
EvtSmImsOrigRejection ::= CHOICE
{
    noRouterAvailable      [0] EmptySequence,
    mtResponseNotExpected  [1] EmptySequence,
    invalidOriginator      [2] EmptySequence,
    invalidRecipient       [3] EmptySequence,
    badSipRequest          [4] EmptySequence,
    noRoutingPathAvailable [5] EmptySequence  -- generated by RTR.
}

-- Outgoing IMS MT Request
EvtSmImsTermOutRequest ::= SEQUENCE
{
    fromUri                     [0] URI,
    toUri                       [1] URI
}

-- Response to outgoing IMS MT Request
EvtSmImsTermOutResponse ::= CHOICE
{
    success                     [0] EmptySequence,
    failure                     [1] EvtSmImsTermOutFailure,
    timeout                     [2] EmptySequence
}

EvtSmImsTermOutFailure ::= CHOICE
{
    sipError                    [0] INTEGER, -- see IANA assignments for SIP --
    rpCause                     [1] INTEGER  -- see Short Message RP 24.011 --
}

-- Attempt to store an SM in a AMS
EvtSmAmsStoreRequest ::= SEQUENCE
{
    id                          [0] INTEGER,         -- AMS - ID
    queue                       [1] INTEGER,
    bufferedSrRequested         [2] BOOLEAN,
    storeAfterDeliveryAttempt   [3] BOOLEAN
}

-- Response to store attempt
EvtSmAmsStoreResponse ::= CHOICE
{
    success                     [0] AmsStoreParameters,
    failure                     [1] AmsStoreFailure,
    timeout                     [2] EmptySequence
}

-- Attempt of the AMS to deliver a SM (possibly as AO)
EvtSmAmsDeliveryAttempt ::= SEQUENCE
{
    moreMessagesToSend          [0] BOOLEAN
}

-- Indication of AMS that SM terminated inside AMS
EvtSmAmsTermination ::= SEQUENCE
```

```
{
    reason                      [0] AmsTerminationReason
}

-- RTR-internal rejection of a AMS delivery attempt
EvtSmAmsDeliveryRejection ::= CHOICE
{
    throughputLimit             [0] ThroughputLimit,
    destinationUnavailable      [1] EmptySequence
}

-- (Rule-based) routing decision for an SM
EvtSmRoutingDecision ::= SEQUENCE
{
    action                      [0] RoutingAction,
    rule                     [1] RoutingRule OPTIONAL -- not present upon "default
 routing"
}

-- The result of an external condition evaluation.
EvtSmExternalCondition ::= SEQUENCE
{
    application                 [0] EcApplication,
    result                      [1] BOOLEAN,
    rule                        [2] RoutingRule OPTIONAL,
    signatureRequested          [3] BOOLEAN OPTIONAL
}

-- A notification or status report has been created for the SM at hand.
EvtSmNotification ::= EmptySequence

-- A copy has been created of the SM at hand
EvtSmCopied ::= SEQUENCE
{
    childId                     [0] ObjectIdentifier,
    destination                 [1] GeneralizedAddress
}

EvtSmCopyCreated ::= SEQUENCE
{
    parentId                    [0] ObjectIdentifier,
    serviceName                 [1] NameString
}

EvtSmCopyRejection ::= CHOICE
{
    nonHplmnRecipient           [0] EmptySequence,
    loopPrevented               [1] EmptySequence,
    recipientValidationFailed   [2] EmptySequence,
    storageUnavailable          [3] EmptySequence,
    emailCopyFailed             [4] EmptySequence
}

EvtSmForwardAttempt ::= SEQUENCE
{
    destination                 [0] GeneralizedAddress
}

EvtSmForwardRejection ::= CHOICE
{
    loopPrevention              [0] EmptySequence,
    simDataDownload             [1] EmptySequence,
    nonHplmnBNumber             [2] EmptySequence,
    nonHplmnCNumber             [3] EmptySequence,
    unsupportedCNumber          [4] EmptySequence,
```

```
    emailForwardingFailed       [5] EmptySequence
}

-- Prepaid charging parameters
EvtSmPrepaidCharging ::= SEQUENCE
{
    result                      [0] PrepaidChargingResult,
    chargedParty                [1] GeneralizedAddress,
    protocol                    [2] ChargingProtocol
}

-- An Auto-Reply message has been issued for this SM.
EvtSmAutoReplied ::= SEQUENCE
{
   childId                  [0] ObjectIdentifier  -- ID of the Auto-Reply message.
}

-- An Auto-Reply message has been created.
EvtSmAutoReplyCreated ::= SEQUENCE
{
    parentId                    [0] ObjectIdentifier, -- ID of original SM.
    serviceName                [1] NameString,       -- name of requesting service.

    message                     [2] SmMessage
}

-- A signature has been inserted to a (inbound) SM.
EvtSmSignatureInserted ::= SEQUENCE
{
    serviceName                 [0] NameString
}

-- Auxiliary event for the CCI to search for messages.
EvtSmEndpoints ::= SEQUENCE
{
    originator          [0] GeneralizedAddress,
    recipient          [1] GeneralizedAddress OPTIONAL -- may be missing for MT-MT
 routing
}

EvtSmFinalStatus ::= SEQUENCE
{
    finalStatusCode             [0] FinalStatusCode
}

--------------------------------------------------
-- Shared ShortMessage - specific types (SmXyz) --
--------------------------------------------------

SmMessage ::= SEQUENCE
{
    data                        [0] SmData OPTIONAL,  -- user data without header
    concatenationInfo           [1] ConcatInfo OPTIONAL,
    userDataHeaderInfo          [2] UserDataHeaderInfo OPTIONAL
}

SmData ::= SEQUENCE
{
    length                      [0] INTEGER,
   content                   [1] SmContent OPTIONAL -- presence depends on license
}

SmContent ::= CHOICE
{
    text                        [0] SmText,           -- if readable text.
```

```
    data                        [1] OCTET STRING      -- if binary data.
}

SmText ::= VisibleString (SIZE (0..1024))             -- UTF-8 encoded.

SmGsmMapError ::= ENUMERATED
{
    other(0),
    systemFailure(1),
    dataMissing(2),
    unexpectedDataValue(3),
    facilityNotSupported(4),
    unknownSubscriber(5),
    absentSubscriber(6),
    callBarred(7),
    teleServiceNotProvisioned(8),
    unidentifiedSubscriber(9),
    illegalSubscriber(10),
    illegalEquipment(11),
    subscriberBusyForMtSms(12),
    invalidSmeAddress(13),
    equipmentProtocol(14),
    equipmentNotSmEquipment(15),
    memoryCapacityExceeded(16),
    unknownServiceCentre(17),
    scCongestion(18),
    subscriberNotScSubscriber(19),
    msgWaitList(20),
    noPagingError(21),                    -- BG2318: Separate Absent Subscriber
errors/ Add new MAP errors
    imsiDetachedError(22),
    roamingRestrictionsError(23),
    msDeregisteredError(24),
    msPurgedError(25),
    shortMsgType0NotSupportedError(26),
    canNotReplaceShortMsgError(27),
    unspecifiedProtocolIdError(28),
    msgClassNotSupportedError(29),
    unspecifiedDataCodingSchemeError(30),
    tpduNotSupported(31),
    simStorageFullError(32),
    noSmStorageCapabilityInSimError(33),
    errorInMs(34),
    simApplToolKitbusyError(35),
    simDataDownloadError(36),
    applSpecificError(37),
    equipUnspecifiedErrorCause(38),
    ueDeregistered(39),
    noResponseViaIpsmGw(40)
}

SmAppServiceCentre ::= SEQUENCE
{
    smscName                    [0] NameString,
    nodeName                    [1] NameString,
    terminationPointName        [2] NameString
}

--------------------------------
-- Routing Info Query Events  --
--------------------------------

RoutingInfoQuery ::= CHOICE
{
    -- GSM / SS7 side events (HLR)
```

```
    gsmInRequest                [0] EvtRiqGsmInRequest,
    gsmInResponse               [1] EvtRiqGsmInResponse,
    gsmOutRequest               [2] EvtRiqGsmOutRequest,
    gsmOutResponse              [3] EvtRiqGsmOutResponse,

    -- IMS side (HSS)

    imsOutRequest               [4] EvtHssUserDataRequest, -- UDR --
    imsOutResponse              [5] EvtHssUserDataAnswer  -- UDA --
}


-------------------------------
-- HSS Query Events          --
-------------------------------

EvtHssUserDataRequest ::= SEQUENCE
{
    publicId                    [0] URI,
    imsUserState               [1] BOOLEAN, -- whether query involves imsUserState
 --
    scscfName                  [2] BOOLEAN  -- whether query involves scscfName --
}

EvtHssUserDataAnswer ::= CHOICE
{
    success                     [0] HssUserDataQuerySuccess,
    failure                     [1] HssUserDataQueryFailure,
    timeout                     [2] NULL
}

HssUserDataQuerySuccess ::= SEQUENCE
{
    -- maybe it will be useful to log the publicId again here as [0]? --
    imsUserState                [1] ImsUserState OPTIONAL,
    scscfName                   [2] URI OPTIONAL
}

HssUserDataQueryFailure ::= EmptySequence -- to be understood and defined --

ImsUserState ::= ENUMERATED
{
    notRegistered(0),
    registered(1),
    registeredUnregServices(2),
    authenticationPending(3)

}

-----------------------------------------
-- Routing Info Query events (EvtRiqXyz)  --
-----------------------------------------

-- Incoming GSM query (SRI-SM)
EvtRiqGsmInRequest ::= SEQUENCE
{
    msisdn                      [0] GsmAddress
}

-- Response to incoming GSM query
EvtRiqGsmInResponse ::= GsmRoutingInfoQueryResult

-- Outgoing GSM query (SRI-SM)
EvtRiqGsmOutRequest ::= EmptySequence
```

```
-- Response to outgoing GSM query
EvtRiqGsmOutResponse ::= GsmRoutingInfoQueryResult

-----------------------------------------
-- (Shared) GSM - specific types (GsmXyz) --
-----------------------------------------

GsmRoutingInfoQueryResult ::= CHOICE
{
    success                     [0] GsmRoutingInfoQuerySuccess,
    failure                     [1] GsmFailure,
    timeout                     [2] EmptySequence
}

GsmRoutingInfoQuerySuccess ::= SEQUENCE
{
    msc                         [0] GsmAddress OPTIONAL,
    sgsn                        [1] GsmAddress OPTIONAL,
    imsi                        [2] ImsiInfo
}

GsmResponse ::= CHOICE
{
    success                     [0] EmptySequence,
    failure                     [1] GsmFailure,
    timeout                     [2] EmptySequence
}

GsmFailure ::= SEQUENCE
{
    reason                      [0] GsmFailureReason
}

GsmFailureReason ::= CHOICE
{
    sccpAborted                 [0] NULL,
    tcapAborted                 [1] NULL,
    mapError                    [2] SmGsmMapError
}

-- this is a MAP AddressString (29.002) OR --
-- a BCD Called Party Address (24.008), from RP (24.011), OR --
-- a TP-Address (23.040) --
--
-- The more common TypeOfNumber values and Numbering Plan values   --
-- map correctly between these standards. Some other values don't. --

GsmAddress ::= SEQUENCE {
    ton                         [0] TypeOfNumber,
    npi                         [1] NumberingPlan,
    address                     [2] Address,
    country                     [3] Country OPTIONAL,
    network                     [4] Network OPTIONAL
}

-----------------------------------------
-- (Shared) IMS - specific types (ImsXyz) --
-----------------------------------------

URI ::= UTF8String

-----------------------------------------
-- (Shared) AMS - specific types (AmsXyz) --
-----------------------------------------
```

```
AmsStoreParameters ::= SEQUENCE
{
    messageIdentifier           [0] AmsMessageId,
    amsNodeAddress              [1] AmsNodeAddress,
    validityExpirationTime      [2] UnixTimestamp OPTIONAL,
    serviceCentreTimestamp      [3] UnixTimestamp OPTIONAL
}

AmsStoreFailure ::= CHOICE
{
    temporaryError                  [0] MxipErrorCode,
    permanentErrorOnThisMessage     [1] MxipErrorCode,
    permanentErrorOnThisRecipient   [2] MxipErrorCode
}

AmsTerminationReason ::= ENUMERATED
{
    expired(0),
    deleted(1),
    replaced(2)
}

AmsNodeAddress ::= CHOICE
{
    ipv4                        [0] Ipv4Address
}

-----------------------------------------
-- Shared SCCP - specific types (SccpXyz) --
-----------------------------------------

SccpMscSgsnAddress ::= CHOICE
{
    msc                         [0] SccpAddressInfo,
    sgsn                        [1] SccpAddressInfo
}

--------------------------
-- miscellaneous  types --
--------------------------

GenericResponse ::= CHOICE
{
    success                     [0] EmptySequence,
    failure                     [1] EmptySequence,
    timeout                     [2] EmptySequence
}

NameString ::= OCTET STRING (SIZE (1..31))

UnixTimestamp ::= INTEGER(0..1000000000000)            -- A large value forces the
 type of long long

RoutingRule ::= SEQUENCE
{
    name                        [0] NameString,
    type                        [1] RuleType
}

RuleType ::= ENUMERATED
{
    mo(0),
    mt(1),
    ao(2),
    ato(3),
```

```
    ati(4),
    unsupported(5),
    mti(6),
    igm(7)
}

ThroughputLimit ::= SEQUENCE
{
    cause                       [0] ThroughputLimitCause
}

ThroughputLimitCause ::= ENUMERATED
{
    license(0),
    rule(1),
    application(2),
    applicationGroup(3),
    serviceClass(4),
    serviceCenter(5)
}

MxipErrorCode ::= INTEGER

GeneralizedAddress ::= SEQUENCE {
    address                     [0] Address,
    country                     [1] Country OPTIONAL,
    network                     [2] Network OPTIONAL
}

Address ::= VisibleString (SIZE (0..38))             -- can be numeric or
alphanumeric (UTF-8)

EsmeApplication ::= SEQUENCE {
    shortNumber                 [0] ShortNumber,
    name                        [1] NameString
}

ShortNumber ::= VisibleString (SIZE (1..38))

ConcatInfo ::= SEQUENCE {
    totalSeg                    [0] INTEGER(0..255),
    currentSeg                  [1] INTEGER(0..255),
    ref                         [2] INTEGER(0..65535)
}

-- comma-separated UTF-8 string of user data header information
-- element names. Upon overflow, the last character is '%'.
UserDataHeaderInfo ::= VisibleString (SIZE (0..64))

GsmStatusReportPhase ::= INTEGER(1..2)

AppNotificationRequest ::= BIT STRING {
    delivery(0),
    nonDelivery(1),
    buffered(2)
}

ObjectIdentifier ::= OCTET STRING (SIZE (1..32))

AmsMessageId ::= OCTET STRING(SIZE(5))

RoutingAction ::= ENUMERATED {
    blockPermanent(0),
    blockTemporary(1),
    blockWithAck(2),
```

```
    blockWithNoResponse(3),
    discardWithAck(4),
    discardWithNak(5),
    discardWithNoResponse(6),
    discardWithPermError(7),
    discardWithPermRecipientError(8),
    discardWithTempError(9),
    pass(10),
    release(11),
    storeForApp(12),
    storeForForwardingAsAo(13),
    storeForMobileStation(14),
    toApp(15),
    toAppFallbackStore(16),
    toMobileStation(17),
    toMobileStationFallbackApp(18),
    toMobileStationFallbackSmsc(19),
    toMobileStationFallbackSmscAsAo(20),
    toMobileStationFallbackStore(21),
    toSmsc(22),
    toSmscAsAo(23),
    toSmscFallbackStore(24),
    toSmscAsAoFallbackStore(25)
}

ImsiInfo ::= SEQUENCE {
    imsi                        [0] Imsi,
    country                     [1] Country OPTIONAL,
    network                     [2] Network OPTIONAL
}

Imsi        ::= OCTET STRING (SIZE (1..20))

SpoofAttempt ::= CHOICE {
    anchor                      [0] SpoofAttemptAnchorParams
}

TcapHeader ::= SEQUENCE {
    tcapMessageType             [1] TcapTag,                            --(Type of
 Message)
   tcapOrigTransId            [2] TcapTransId OPTIONAL,             --(Originator
 Transaction ID)
   tcapDestTransId            [3] TcapTransId,                      --(Destination
 Transaction ID)
    protoVersionTag             [4] ProtocolVersion OPTIONAL,           --(Dialog
version number)
    dialogTag                   [5] TcapTag OPTIONAL,                   --(Type of
 Dialog)
   appContext                [6] ApplicationContext OPTIONAL        --(Application
 Context Name in text)
}

SpoofAttemptAnchorParams ::= SEQUENCE {
    mtp                         [0] MtpHead,
    sccp                        [1] SccpHead,
    tcap                        [2] TcapHeader
}

MtpHead ::= SEQUENCE {
    mtp3OrigPointCode           [0] PointCode                           --(MTP3
originating point code)
}

PointCode ::= INTEGER (0..16777215)
```

```
SccpHead ::= SEQUENCE {
    cgPa                        [0] SccpAddressInfo,                    --(SCCP
calling party address)
    cdPa                        [1] SccpAddressInfo                     --(SCCP
called party address)
}

TcapTag ::= ENUMERATED { unknown(0), dialoguerequest(96), dialogueresponse(97),
begin(98), end(100), continue(101), abort(103)}

TcapTransId ::= OCTET STRING (SIZE (0..4))

ApplicationContext ::= VisibleString (SIZE (0..1024))

SccpAddressDigits ::= VisibleString (SIZE (0..20))

GlobalTitle ::= SEQUENCE {
    np                          [0] NumberingPlan OPTIONAL,
    number                      [1] SccpAddressDigits OPTIONAL,
    nai                         [2] NatureOfAddress OPTIONAL
}

SccpAddress ::= SEQUENCE {
    pointCode                   [0] PointCode OPTIONAL,
    subSystemNumber             [1] SubSystemNumber OPTIONAL,
    globalTitle                 [2] GlobalTitle
}

SccpAddressInfo ::= SEQUENCE {
    sccpAddress                 [0] SccpAddress,
    country                     [1] Country OPTIONAL,
    network                     [2] Network OPTIONAL
}

-- Numbering Plan and Type of Number (Nature of Address) are in a format --
-- suitable for the GsmAddress type. See GsmAddress. --
-- Note that the missing values in this enumeration correspond to --
-- conflicting values between the address formats, or spare/reserved. --

NumberingPlan ::= ENUMERATED {
    unknown(0),
    isdnTelephony(1), -- E.164 numbering plan --

    data(3), -- X.121 --
    telex(4), -- F.69 --

    national(8),
    private(9)
}

TypeOfNumber ::= ENUMERATED {
    unknown(0),
    international(1),
    national(2),
    networkSpecific(3),
    -- 4 is subscriber nr OR dedicated access, short code --
    alphaNumeric(5) -- (note) --
}

-- (note): alphaNumeric is 23.040 only, but is important --
-- enough to earn its enum value. It is 'reserved' in --
-- both 29.002 and 24.008. --

ProtocolVersion ::= INTEGER (0..255)
```

```
SubSystemNumber ::= INTEGER (0..255)

-- This is NatureOfAddress as used in SCCP Global Titles. --
-- Beware, it is NOT the 29.002 AddressString Nature of Address! --

NatureOfAddress ::= ENUMERATED
{
    unknown(0),
    subscriberNumber(1),
    reservedForNationalUse(2),
    nationalSignificantNumber(3),
    internationalNumber(4)
}

Country ::= VisibleString (SIZE (2..2))

Network ::= VisibleString (SIZE (1..31))

ProtocolId ::= INTEGER (0..255)

EmptySequence ::= SEQUENCE { }

Ipv4Address ::= VisibleString -- -- (SIZE (1..16))

EcApplication ::= SEQUENCE
{
    name                        [0] NameString
}

FinalStatusCode ::= ENUMERATED
{
    delivered(0),
    forwarded(1),
    rejected(2),        -- (nak)
    deleted(3),         -- accepted but not delivered/forwarded
    dropped(4)          -- no response
}

PrepaidChargingResult ::= ENUMERATED
{
    success(0),
    subscriberUnknown(1),
    notEnoughCredit(2),
    chargingServerUnavailable(3),
    chargingServerNotResponding(4),
    otherError(5)
}

ChargingProtocol ::= CHOICE
{
    camel       [0] EmptySequence,
    diameter    [1] EmptySequence,
    smppPlus    [2] EmptySequence
}

END
```

Appendix C

Log Record Reject Causes

Topics:

C.1 Log Record Reject Causes

The log records contain reject causes that indicate the type of error that occurred. This table describes the reject causes.

Reject Cause	Explanation
invalidSccpSmscAddress (0)	• The SCCP address of the SMSC contained an invalid digit (not 0-9) or was longer than 15 digits. • A message from a trusted SMSC was send via the suspect path. • An MT or SRI-SM message from a suspect SMSC was not in international format. • An MT or SRI-SM message from a suspect SMSC was not routed on global title (GT).
invalidMapSmscAddress (1)	The service center address in the MAP layer contained an invalid digit (not 0-9) or was longer than 20 digits.
invalidRecipientAddress (2)	The recipient address contained an invalid digit (not 0-9) or was longer than 20 digits.
invalidOriginatorAddress (3)	The originator address contained an invalid digit (not 0-9) or was longer than 20 digits.
invalidImsi (4)	The IMSI was too long or contained an invalid digit (not 0-9).
invalidMscAddress (5)	• The MSC or SGSN address was longer than 15 digits or contained an invalid digit (not 0-9). • The MSC address could not be found (in the case of a suspect MtForwardSm). • The SGSN address could not be found (in the case of a suspect MtForwardSm).
forgingMscAddress (6)	The SMSC was addressing a suspect MtForwardSm to the virtual point code of the FWL (this should not occur, as the SRI-SM should direct the message to the GT of the FWL).
forgingImsi (7)	A suspect MtForwardSm was received with an IMSI that was not given out before or was past the timeout value.
forgingLmsi (8)	A suspect MtForwardSm was received with a LMSI that was not given out before or was past the timeout value.
unknownSccpSmscAddress (9)	A suspect MtForwardSm was received with a SCCP address that did not match any network number ranges or network prefixes, or did not match any configured country.
unknownMapSmscAddress (10)	A suspect MtForwardSm was received with a MAP layer service center address that did not match any network number ranges or network prefixes, or did not match any configured country.

Reject Cause	Explanation
conflictingSmscAddresses (11)	A suspect MtForwardSm was received in which the MAP service center address did not correspond to the SCCP calling party (CGPA) address.
spoofingSccpSmscAddress (12)	A spoofed suspect MtForwardSm was detected (spoofing was done on the SCCP address).
spoofingMapSmscAddress (13)	A spoofed suspect MtForwardSm was detected (spoofing was done on the MAP service center address).
unsolicitedMtForwardSm (14)	A suspect MtForwardSm was received without a corresponding SRI-SM. The IMSI is from the operator itself, but is outside the range allocated for IMSIs by the FWL.
matchingMtRoutingRule (15)	An MtForwardSm was rejected because of an MTOR rule.
matchingMtExternalConditionRule (16)	An MtForwardSm was rejected because of an MTOX rule.
matchingMoRoutingRule (17)	An MoForwardSm was rejected because of an MOR rule.
matchingMoExternalConditionRule (18)	An MoForwardSm was rejected because of an MOX rule.
spoofedOriginatorAddress (19)	A spoofed MoForwardSm was detected (spoofing was done on the originator address).
matchingAoRoutingRule (20)	An AO message was rejected because of an AOR rule. If the log record does not indicate a rule name, this means that the message was rejected because it did not match any AOR rule.
matchingAoExternalConditionRule (21)	An AO message was rejected because of an AOX rule.
matchingAtRoutingRule (22)	An AT message was rejected because of an ATOR rule.
matchingAtExternalConditionRule (23)	An AT message was rejected because of an ATOX rule.
mnpViolation (26)	An MO message was rejected because of an MNP violation.
matchingAtiRoutingRule (27)	An AT message was rejected because of an ATIR rule.
matchingAtiExternalConditionRule (28)	An AT message was rejected because of an ATIX rule.
noSpaceForSegmentingHeader (29)	According to specifications , a message was rejected because there was no space for a segmenting header. If an AO message, submitted via SMPP, contains `sar` fields and the "total messages" value is greater than 1, then the message is a segment of a sequence of concatenated messages. To forward such an AO message through an MT path, requires the sar fields be converted to a user data header. This requires the RTR to prefix six or seven bytes to each segment. There may exist scenarios where such prefixing will result in an individual segment greater than

Reject Cause	Explanation
	140 bytes. In this case the message is undeliverable by the MT path and the following line will be logged to syslog: `Application <xxx> of ID <xx> sent unexpected data` Applications are required to explicitly divide long messages into segments of 133 bytes or less, allowing just enough space for the user data header.
earlyRecipientSriSmFailure(30)	A message was rejected because Early recipient SendRoutingInfoForSm failed with a Permanent Error.
originatorListViolation(31)	A message was rejected because the originator of the message AO/SM fails to comply with the configured originator list. If the originator white list is configured, the originator should be part of this list. If the originator black list is configured, the originator should NOT be part of this list.
messageTooLong(32)	The message was rejected because the payload of the message was long and it was configured to reject the message if the payload of the AO/SM is long for a single MT/SM.
originatorThroughputViolation(33)	A message was rejected because throughput of the originator was exceeding against any one of the following controlling instance • the originating application • the originating application group • the service class
matchingSriqRoutingRule(34)	A SendRoutingInfoForSm was rejected because of an SRIQ rule.
unidentfiedSubscriber(35)	A message was rejected because the subscriber is not registered in the PLMN (i.e. mobile subscriber is no longer being served by the MSC or SGSN address that was returned in the MAP-SRI response).
absentSubscriber(36)	A message was rejected because the subscriber was not available. The reason of the subscriber unavailable can be IMSI was detached, no paging error or roaming restricted etc.
facilityNotSupported(37)	A message was rejected because the terminating network has no SMS support in the network.
deliveryFailure(38)	A message was rejected because a) the destination MS had no memory capacity available to store the message b) protocol error occurred on the destination MS equipment c) the destination MS equipment was not equipped to handle the message.

Reject Cause	Explanation
systemFailure(39)	A message was rejected because of a problem in another entity. The type of entity or network resource may be indicated by a network resource parameter.
subscriberBusyForMtSms(40)	A message was rejected because congestion was encountered at the visited MSC.
illegalSubscriber(41)	A message was rejected because the destination MS failed authentication.
illegalEquipment(42)	A message was rejected because the IMEI of the destination MS was blacklisted in the EIR.
matchingMtiRoutingRule(43)	A MT message was rejected because of a MTIR rule.
unknownSubscriber(44)	A message was rejected because there is no directory number for the mobile subscriber (GSM 09.02).

C.2 Log Record Ignored Reject Causes

A reject cause is something that may happen during the processing of a message which may or may not cause the processed message to be rejected.

If that *reject cause* does not actually lead to the rejection of the message, but is ignored (due to the configuration), it is called an *ignored reject cause*. You may want to ignore a reject cause because you want to be graceful and keep processing the message anyway.

The corresponding configuration parameters are:

- `firewallmtactionforunknownsccpaddress`
- `firewallmtactionforunknownmapaddress`
- `firewallmtactionforconflictingaddress`
- `firewallmtactionforsccpsmscaddressspoofing`
- `firewallmtactionformapsmscaddressspoofing`

The reject cause is *ignored* whenever the parameter is set to `"pass"` rather than any of the block-actions, but the ignored reject cause will be flagged `(1)` in the `IgnoredRejectCauses` bitmask in the log record. If the reject cause has not occurred, the flag is not raised and the bit is not set (0).

The log records contain the following ignored reject causes:

- `unknownSccpSmscAddress (9)`
- `unknownMapSmscAddress (10)`
- `conflictingSmscAddress (11)`
- `spoofingSccpSmscAddress (12)`
- `spoofingMapSmscAddress (13)`
- `spoofedOriginatorAddress (19)`

Appendix D

Industry Standard Compliance

Topics:

D.1 SS7 Stack Software

The RTR SS7 stack software complies with the following industry standard specifications:

- ITU-Q.2110 (SSCOP)
- ITU-Q.2140 (SSCF-NNI)
- ITU-Q.2210 (MTP3b)
- ITU-T Q.701-Q.704, Q.706, Q.707 (MTP)
- ITU-T Q.711-Q.714, Q.716, (SCCP)
- ITU-T Q.771-Q.775 (TCAP)
- Japanese SS7 JT Q.711-JT Q.714 (SCCP)
- ETSIGSM 09.02 / 3GPP 29.002
- ETSIGSM 03.40 /3GPP 23.040

Appendix E

Country Codes

Topics:

E.1 ISO 3166 Country Codes

For an up-to-date list of all country codes, refer to the ISO organisation's Web site at *http://www.iso.org*.

Country [Code]	Code - Country
Afghanistan [**AF**]	**AD** - Andorra
Albania [**AL**]	**AE** - United Arab Emirates
Algeria [**DZ**]	**AF** - Afghanistan
American Samoa [**AS**]	**AG** - Antigua and Barbuda
Andorra [**AD**]	**AI** - Anguilla
Angola [**AO**]	**AL** - Albania
Anguilla [**AI**]	**AM** - Armenia
Antarctica [**AQ**]	**AN** - Netherlands Antilles
Antigua and Barbuda [**AG**]	**AO** - Angola
Argentina [**AR**]	**AQ** - Antarctica
Armenia [**AM**]	**AR** - Argentina
Aruba [**AW**]	**AS** - American Samoa
Australia [**AU**]	**AT** - Austria
Austria [**AT**]	**AU** - Australia
Azerbaijan [**AZ**]	**AW** - Aruba
Bahamas [**BS**]	**AZ** - Azerbaijan
Bahrain [**BH**]	**BA** - Bosnia and Herzegovina
Bangladesh [**BD**]	**BB** - Barbados
Barbados [**BB**]	**BD** - Bangladesh
Belarus [**BY**]	**BE** - Belgium
Belgium [**BE**]	**BF** - Burkina Faso
Belize [**BZ**]	**BG** - Bulgaria
Benin [**BJ**]	**BH** - Bahrain
Bermuda [**BM**]	**BI** - Burundi
Bhutan [**BT**]	**BJ** - Benin
Bolivia [**BO**]	**BM** - Bermuda
Bosnia and Herzegovina [**BA**]	**BN** - Brunei Darussalam
Botswana [**BW**]	**BO** - Bolivia

Country [Code]	Code - Country
Bouvet Island [**BV**]	**BR** - Brazil
Brazil [**BR**]	**BS** - Bahamas
British Indian Ocean Territory [**IO**]	**BT** - Bhutan
Brunei Darussalam [**BN**]	**BV** - Bouvet Island
Bulgaria [**BG**]	**BW** - Botswana
Burkina Faso [**BF**]	**BY** - Belarus
Burundi [**BI**]	**BZ** - Belize
Cambodia [**KH**]	**CA** - Canada
Cameroon [**CM**]	**CC** - Cocos (Keeling) Islands
Canada [**CA**]	**CD** - Congo, The Democratic Republic Of The
Cape Verde [**CV**]	**CF** - Central African Republic
Cayman Islands [**KY**]	**CG** - Congo
Central African Republic [**CF**]	**CH** - Switzerland
Chad [**TD**]	**CI** - Cote D'ivoire
Chile [**CL**]	**CK** - Cook Islands
China [**CN**]	**CL** - Chile
Christmas Island [**CX**]	**CM** - Cameroon
Cocos (Keeling) Islands [**CC**]	**CN** - China
Colombia [**CO**]	**CO** - Colombia
Comoros [**KM**]	**CR** - Costa Rica
Congo [**CG**]	**CU** - Cuba
Congo, The Democratic Republic Of The [**CD**]	**CV** - Cape Verde
Cook Islands [**CK**]	**CX** - Christmas Island
Costa Rica [**CR**]	**CY** - Cyprus
Cote D'ivoire [**CI**]	**CZ** - Czech Republic
Croatia [**HR**]	**DE** - Germany
Cuba [**CU**]	**DJ** - Djibouti
Cyprus [**CY**]	**DK** - Denmark
Czech Republic [**CZ**]	**DM** - Dominica
Denmark [**DK**]	**DO** - Dominican Republic
Djibouti [**DJ**]	**DZ** - Algeria
Dominica [**DM**]	**EC** - Ecuador
Dominican Republic [**DO**]	**EE** - Estonia

Country [Code]	Code - Country
Ecuador [**EC**]	**EG** - Egypt
Egypt [**EG**]	**EH** - Western Sahara
El Salvador [**SV**]	**ER** - Eritrea
Equatorial Guinea [**GQ**]	**ES** - Spain
Eritrea [**ER**]	**ET** - Ethiopia
Estonia [**EE**]	**FI** - Finland
Ethiopia [**ET**]	**FJ** - Fiji
Falkland Islands (Malvinas) [**FK**]	**FK** - Falkland Islands (Malvinas)
Faroe Islands [**FO**]	**FM** - Micronesia, Federated States Of
Fiji [**FJ**]	**FO** - Faroe Islands
Finland [**FI**]	**FR** - France
France [**FR**]	**GA** - Gabon
French Guiana [**GF**]	**GB** - United Kingdom
French Polynesia [**PF**]	**GD** - Grenada
French Southern Territories [**TF**]	**GE** - Georgia
Gabon [**GA**]	**GF** - French Guiana
Gambia [**GM**]	**GH** - Ghana
Georgia [**GE**]	**GI** - Gibraltar
Germany [**DE**]	**GL** - Greenland
Ghana [**GH**]	**GM** - Gambia
Gibraltar [**GI**]	**GN** - Guinea
Greece [**GR**]	**GP** - Guadeloupe
Greenland [**GL**]	**GQ** - Equatorial Guinea
Grenada [**GD**]	**GR** - Greece
Guadeloupe [**GP**]	**GS** - South Georgia and South Sandwich Islands
Guam [**GU**]	**GT** - Guatemala
Guatemala [**GT**]	**GU** - Guam
Guinea [**GN**]	**GW** - Guinea-Bissau
Guinea-Bissau [**GW**]	**GY** - Guyana
Guyana [**GY**]	**HK** - Hong Kong
Haiti [**HT**]	**HM** - Heard Island and Mcdonald Islands
Heard Island and Mcdonald Islands [**HM**]	**HN** - Honduras
Holy See (Vatican City State) [**VA**]	**HR** - Croatia

Country [Code]	Code - Country
Honduras [**HN**]	**HT** - Haiti
Hong Kong [**HK**]	**HU** - Hungary
Hungary [**HU**]	**ID** - Indonesia
Iceland [**IS**]	**IE** - Ireland
India [**IN**]	**IL** - Israel
Indonesia [**ID**]	**IN** - India
Iran, Islamic Republic Of [**IR**]	**IO** - British Indian Ocean Territory
Iraq [**IQ**]	**IQ** - Iraq
Ireland [**IE**]	**IR** - Iran, Islamic Republic Of
Israel [**IL**]	**IS** - Iceland
Italy [**IT**]	**IT** - Italy
Jamaica [**JM**]	**JM** - Jamaica
Japan [**JP**]	**JO** - Jordan
Jordan [**JO**]	**JP** - Japan
Kazakhstan [**KZ**]	**KE** - Kenya
Kenya [**KE**]	**KG** - Kyrgyzstan
Kiribati [**KI**]	**KH** - Cambodia
Korea, Democratic People's Republic Of [**KP**]	**KI** - Kiribati
Korea, Republic Of [**KR**]	**KM** - Comoros
Kuwait [**KW**]	**KN** - Saint Kitts and Nevis
Kyrgyzstan [**KG**]	**KP** - Korea, Democratic People's Republic Of
Lao People's Democratic Republic [**LA**]	**KR** - Korea, Republic Of
Latvia [**LV**]	**KW** - Kuwait
Lebanon [**LB**]	**KY** - Cayman Islands
Lesotho [**LS**]	**KZ** - Kazakhstan
Liberia [**LR**]	**LA** - Lao People's Democratic Republic
Libyan Arab Jamahiriya [**LY**]	**LB** - Lebanon
Liechtenstein [**LI**]	**LC** - Saint Lucia
Lithuania [**LT**]	**LI** - Liechtenstein
Luxembourg [**LU**]	**LK** - Sri Lanka
Macao [**MO**]	**LR** - Liberia
Macedonia, The Former Yugoslav Republic Of [**MK**]	**LS** - Lesotho
	LT - Lithuania

Country [Code]	Code - Country
Madagascar [**MG**]	**LU** - Luxembourg
Malawi [**MW**]	**LV** - Latvia
Malaysia [**MY**]	**LY** - Libyan Arab Jamahiriya
Maldives [**MV**]	**MA** - Morocco
Mali [**ML**]	**MC** - Monaco
Malta [**MT**]	**MD** - Moldova, Republic Of
Marshall Islands [**MH**]	**MG** - Madagascar
Martinique [**MQ**]	**MH** - Marshall Islands
Mauritania [**MR**]	**MK** - Macedonia, former Yugoslav Republic of
Mauritius [**MU**]	**ML** - Mali
Mayotte [**YT**]	**MM** - Myanmar
Mexico [**MX**]	**MN** - Mongolia
Micronesia, Federated States Of [**FM**]	**MO** - Macao
Moldova, Republic Of [**MD**]	**MP** - Northern Mariana Islands
Monaco [**MC**]	**MQ** - Martinique
Mongolia [**MN**]	**MR** - Mauritania
Montserrat [**MS**]	**MS** - Montserrat
Morocco [**MA**]	**MT** - Malta
Mozambique [**MZ**]	**MU** - Mauritius
Myanmar [**MM**]	**MV** - Maldives
Namibia [**NA**]	**MW**- Malawi
Nauru [**NR**]	**MX** - Mexico
Nepal [**NP**]	**MY** - Malaysia
Netherlands [**NL**]	**MZ** - Mozambique
Netherlands Antilles [**AN**]	**NA** - Namibia
New Caledonia [**NC**]	**NC** - New Caledonia
New Zealand [**NZ**]	**NE** - Niger
Nicaragua [**NI**]	**NF** - Norfolk Island
Niger [**NE**]	**NG** - Nigeria
Nigeria [**NG**]	**NI** - Nicaragua
Niue [**NU**]	**NL** - Netherlands
Norfolk Island [**NF**]	**NO** - Norway
Northern Mariana Islands [**MP**]	**NP** - Nepal

Country [Code]	Code - Country
Norway [**NO**]	**NR** - Nauru
Oman [**OM**]	**NU** - Niue
Pakistan [**PK**]	**NZ** - New Zealand
Palau [**PW**]	**OM** - Oman
Palestinian Territory, Occupied [**PS**]	**PA** - Panama
Panama [**PA**]	**PE** - Peru
Papua New Guinea [**PG**]	**PF** - French Polynesia
Paraguay [**PY**]	**PG** - Papua New Guinea
Peru [**PE**]	**PH** - Philippines
Philippines [**PH**]	**PK** - Pakistan
Pitcairn [**PN**]	**PL** - Poland
Poland [**PL**]	**PM** - Saint Pierre and Miquelon
Portugal [**PT**]	**PN** - Pitcairn
Puerto Rico [**PR**]	**PR** - Puerto Rico
Qatar [**QA**]	**PS** - Palestinian Territory, Occupied
Reunion [**RE**]	**PT** - Portugal
Romania [**RO**]	**PW** - Palau
Russian Federation [**RU**]	**PY** - Paraguay
Rwanda [**RW**]	**QA** - Qatar
Saint Helena [**SH**]	**RE** - Reunion
Saint Kitts and Nevis [**KN**]	**RO** - Romania
Saint Lucia [**LC**]	**RU** - Russian Federation
Saint Pierre and Miquelon [**PM**]	**RW** - Rwanda
Saint Vincent and The Grenadines [**VC**]	**SA** - Saudi Arabia
Samoa [**WS**]	**SB** - Solomon Islands
San Marino [**SM**]	**SC** - Seychelles
Sao Tome and Principe [**ST**]	**SD** - Sudan
Saudi Arabia [**SA**]	**SE** - Sweden
Senegal [**SN**]	**SG** - Singapore
Seychelles [**SC**]	**SH** - Saint Helena
Sierra Leone [**SL**]	**SI** - Slovenia
Singapore [**SG**]	**SJ** - Svalbard and Jan Mayen
Slovakia [**SK**]	**SK** - Slovakia

Country [Code]	Code - Country
Slovenia [**SI**]	**SL** - Sierra Leone
Solomon Islands [**SB**]	**SM** - San Marino
Somalia [**SO**]	**SN** - Senegal
South Africa [**ZA**]	**SO** - Somalia
South Georgia and South Sandwich Islands [**GS**]	**SR** - Suriname
Spain [**ES**]	**ST** - Sao Tome and Principe
Sri Lanka [**LK**]	**SV** - El Salvador
Sudan [**SD**]	**SY** - Syrian Arab Republic
Suriname [**SR**]	**SZ** - Swaziland
Svalbard and Jan Mayen [**SJ**]	**TC** - Turks and Caicos Islands
Swaziland [**SZ**]	**TD** - Chad
Sweden [**SE**]	**TF** - French Southern Territories
Switzerland [**CH**]	**TG** - Togo
Syrian Arab Republic [**SY**]	**TH** - Thailand
Taiwan, Province Of China [**TW**]	**TJ** - Tajikistan
Tajikistan [**TJ**]	**TK** - Tokelau
Tanzania, United Republic Of [**TZ**]	**TL** - Timor-Leste
Thailand [**TH**]	**TM** - Turkmenistan
Timor-Leste [**TL**]	**TN** - Tunisia
Togo [**TG**]	**TO** - Tonga
Tokelau [**TK**]	**TR** - Turkey
Tonga [**TO**]	**TT** - Trinidad and Tobago
Trinidad and Tobago [**TT**]	**TV** - Tuvalu
Tunisia [**TN**]	**TW** - Taiwan, Province Of China
Turkey [**TR**]	**TZ** - Tanzania, United Republic Of
Turkmenistan [**TM**]	**UA** - Ukraine
Turks and Caicos Islands [**TC**]	**UG** - Uganda
Tuvalu [**TV**]	**UM** - United States Minor Outlying Islands
Uganda [**UG**]	**US** - United States
Ukraine [**UA**]	**UY** - Uruguay
United Arab Emirates [**AE**]	**UZ** - Uzbekistan
United Kingdom [**GB**]	**VA** - Holy See (Vatican City State)
United States [**US**]	**VC** - Saint Vincent and The Grenadines

Country [Code]	Code - Country
United States Minor Outlying Islands [**UM**]	**VE** - Venezuela
Uruguay [**UY**]	**VG** - Virgin Islands, British
Uzbekistan [**UZ**]	**VI** - Virgin Islands, U.S.
Vanuatu [**VU**]	**VN** - Viet Nam
Venezuela [**VE**]	**VU** - Vanuatu
Viet Nam [**VN**]	**WF** - Wallis and Futuna
Virgin Islands, British [**VG**]	**WS** - Samoa
Virgin Islands, U.S. [**VI**]	**YE** - Yemen
Wallis and Futuna [**WF**]	**YT** - Mayotte
Western Sahara [**EH**]	**YU** - Yugoslavia
Yemen [**YE**]	**ZA** - South Africa
Yugoslavia [**YU**]	**ZM** - Zambia
Zambia [**ZM**]	**ZW** - Zimbabwe
Zimbabwe [**ZW**]	

Appendix F

Command-Line Tools

Topics:

F.1 Introduction

This annex describes the following Command-Line Interface (CLI) tools:

- `m3ua_link`
- `ss7_link`
- `tp_ccdr`
- `tp_ecdr`
- `tp_fcdr`
- `tp_lcdr`
- `tp_ncdr`
- `tp_scdr`
- `tp_gttupdate`
- `tp_event`
- `tp_log`

F.2 Scriptable Tools

Many of the command-line interface (CLI) tools are scriptable. You can provide options on the command line or via a standard input (without requiring a terminal), and each tool reports exit codes that can allow a script to react when errors occur.

All tools described in this section return exit code:

- 0 upon success
- 1 if an error occurs

For example, `tp_status` returns 0 when all configured processes are running. It returns 1 when one process is not available.

F.3 m3ua_link

The `m3ua_link` tool allows you to:

- Show the status of the M3UA link.
- Enable or disable the M3UA SGP admin state.
- Display the information fields for all the peer SGPs, along with the M3UA SGP information.
- Enable or disable the M3UA ASP admin state.
- Display the information of all configured ASPs in multi-instance mode.

Link changes that are made using the `m3ua_link` tool are stored in volatile memory. Therefore, these settings are lost when the RTR/SCR restarts.

The `m3ua_link` utility is supported for multi-instance. The tool executes for all instances running on a system.

For executing the m3ua_link utility on a multi-instance system, ensure that the following lines are present in the semi-static configuration file and ensure that {HOME} is set to the HOME directory of the NMM user.

```
<fxferfile
  localpath="{HOME}/etc/MGRdevices.xml.gz"
  serverpath="/usr/TextPass/etc/MGRdevices.xml.gz"
/>
```

If the file MGRdevices.xml.gz is not present in the {HOME}/etc folder of that user, then the m3ua_link utility will use the default SNMP port of that user. In this case, the information for all the instances will not be fetched using the m3ua_link utility.

The instances information is read from MGRdevices.xml.gz and used by the m3ua_link tool.

Note:

- The SCR information is not present in the MGR GUI, so the port information of the SCR cannot be extracted from MGRdevices.xml.gz.
- The port information of the SCR is calculated from the port information received for the RTR from MGRdevices.xml.gz.
- For fetching the information of the SCR, the SCR should be running along with the RTR for that instance.

F.3.1 Synopsis

- To retrieve the M3UA link status information:

  ```
  m3ua_link [<product>] [<system> [associationname]]
  ```

- To enable the Admin State of an SGP:

  ```
  m3ua_link [<product>] --enable <system> <associationname>
  ```

- To disable the Admin State of an SGP:

  ```
  m3ua_link [<product>] --disable <system> <associationname>
  ```

- To retrieve the information fields for all the peer SGPs:

  ```
  m3ua_link [<product>] --peers [<system> [associationname]]
  ```

- To enable the Admin State of an ASP:

  ```
  m3ua_link [<product>] --enableasp <system> <associationname>
  ```

- To disable the Admin State of an ASP:

  ```
  m3ua_link [<product>] --disableasp <system> <associationname>
  ```

- To see usage:

  ```
  m3ua_link --help
  m3ua_link -h
  m3ua_link -?
  ```

Note:

1. Where <product> is:

   ```
   --textpass|-p| --tp_scr|-s
   ```

2. If `<product>` is not mentioned or any product is specified except MAP Screener, then by default, the `m3ua_link` tool operates on the RTR. To direct the `m3ua_link` tool to operate on the MAP screener, specify `--tp_scr/-s`.
3. If `<system>` is not mentioned in the command line, `localhost` is taken as the system.
4. An error will be thrown in case of invalid syntax.

F.3.2 Options

Option	Description
no option	Retrieves the M3UA SGP status information: • Signalling the gateway name • Operational state (disabled, blocked, down, up, or congested) • SCTP Operational State (adminDisabled, closed, cookieWait, cookieEchoed, established, shutdownPending, shutdownSent, shutdownReceived, shutdownAckSent or expectingConnectFromPeer) • Virtual SPC status (inactive, activating, active, or deactivating) • Actual SPC status (inactive, activating, active, or deactivating) **Note:** If M3UA AS and ASP are defined, the AS and ASP information is displayed as well. If M3UA ASP is defined, then the following information is displayed: • ASP name • Operational State (adminDisabled, blocked, down, up, or congested) • SCTP Operational State(adminDisabled, closed, cookieWait, cookieEchoed, established, shutdownPending, shutdownSent, shutdownReceived, shutdownAckSent or expectingConnectFromPeer) • Routing Context • RC Operational State (adminDisabled, blocked, activating and active). Here, RC Operational State is linked to AS Operational State. If M3UA AS is defined, then the following information is displayed: • AS name • Operational State (adminDisabled, blocked, activating and active) • Routing Context • Ratio of Active ASPs and Total ASPs
--enable	Allows enabling the M3UA SGP admin state. **Note:** • In case the SGP is associated to any route with adminState set to inactive(0), the command will also enable those routes. • Enabling of routes depends on MTP destination and SGP both. • Associated SGP and destination must be active to activate a route. If not, enabling of route will fail, but the enabling of SGP will pass.

Option	Description
	• In case the enabling of an SGP or MTP Route fails, the error received would be printed on the screen. If it succeeds, the message for successful SNMP set will be printed.
--enableasp	Allows enabling the M3UA ASP admin state. **Note:** In case the enabling of an ASP fails, the error received would be printed on the screen. If it succeeds, the message for successful SNMP set will be printed.
--disableasp	Allows disabling the M3UA ASP admin state. **Note:** In case the disabling of an ASP fails, the error received would be printed on the screen. If it succeeds, the message for successful SNMP set will be printed.
--disable	Allows disabling the M3UA SGP admin state. **Note:** • In case the SGP is associated to any route with adminState set to active(1), the command will also disable those routes. • In case the disabling of an SGP or MTP route fails, the error received would be printed on the screen. If it succeeds, the message for successful SNMP set will be printed.
--peers	Retrieves the M3UA SGP status and peer SGPs information: • Signaling gateway name • Operational state (disabled, blocked, down, up, or congested) • SCTP Operational State (adminDisabled, closed, cookieWait, cookieEchoed, established, shutdownPending, shutdownSent, shutdownReceived, shutdownAckSent or expectingConnectFromPeer) • Virtual SPC status (inactive, activating, active, or deactivating) • Actual SPC status (inactive, activating, active, or deactivating) • IP address of the SGP peers • Operational Status of the remote address associated with a peer SGP (adminDisabled, blocked, notRegistered, actingAsPrimary, or actingAsSecondary) • Congestion Window for the remote address associated with a peer SGP • Retransmission Timeout for the remote address associated with a peer SGP • Receive Window for a peer SGP
--help/-h/-?	Displays usage
<product>	Specifies the Mobile Messaging component to act on. **Note:** • `<product>` is `--textpass|-p| --tp_scr|-s` • If `<product>` is not mentioned or any product is specified except MAP Screener, then by default, the tool operates on the RTR. To direct the tool to operate on the MAP Screener, specify `--tp_scr/-s`.

F.3.3 Operands

Operand	Description
system	Host name or IPV4 address of the Router. **Note:** • IP address 0.0.0.0 is not supported. • IP address 127.0.0.1 is not supported • IPV6 address is not supported.
associationname	Name of the M3UA SGP or ASP.

F.3.4 Output for Different Options of `m3ua_link`

Suppose 2 NMM users are configured on a system: `textpass` and `tp_user01`.

- M3UA SGPs, SGP-1 and SGP-2, are configured on `textpass` user:
  - SGP-1 is configured with peer IP address "10.0.0.1"
  - SGP-2 is configured with peer IP address "10.0.0.2"
- M3UA SGPs, SGP-2 and SGP-3, are configured on `tp_user01` user:
  - SGP-2 is configured with multiple IP addresses for SCTP multi-homing - "10.0.0.3" and "10.0.0.5"
  - SGP-3 is configured with peer IP addresses "10.0.0.4"
- M3UA ASPs, ASP-1 and ASP-2, are configured on textpass user:
  - ASP-1 is configured with IP addresses "10.0.0.1"
  - ASP-2 is configured with IP addresses "10.0.0.2"
- M3UA ASPs, ASP-2 and ASP-3, are configured on tp_user01 user:
  - ASP-2 is configured with IP address "10.0.0.3"
  - ASP-3 is configured with IP address "10.0.0.4"

Below are output samples of `m3ua_link` with different options:

- (no option): Shows the status of M3UA link for all the instances running on the system.

```
m3ua_link
Reading information from localhost:11861
 SGP-NAME OPSTATE SCTP-OPSTATE APC-OPSTATE VPC-OPSTATE
 SGP-1 down cookieWait Inactive Inactive
 SGP-2 down cookieWait Inactive Inactive

 ASP-NAME OPSTATE SCTP-OPSTATE RC RC-OPSTATE
 ASP-1           down cookieWait 700 activating
 ASP-2           down cookieWait 710 activating

Reading information from localhost:16002
 SGP-NAME OPSTATE SCTP-OPSTATE APC-OPSTATE VPC-OPSTATE
 SGP-2 down cookieWait Inactive Inactive
 SGP-3 down cookieWait Inactive Inactive
```

```
ASP-NAME OPSTATE SCTP-OPSTATE RC RC-OPSTATE
ASP-2  up established 720 Active
ASP-3  Down cookieWait 730 activating
```

- `--enable/--disable`: Allows enabling or disabling the M3UA SGP on all instances running on the system.

  1. In case the SGP is associated to any route with adminState set to inactive(0), the enable command will also enable those routes.
  2. Associated SGP and destination must be active to activate a route. If not, enabling of route will fail, but the enabling of SGP will pass.
  3. In case the SGP is associated to any route with adminState set to active(1), the disable command will also disable those routes.
  4. In case the enabling/disabling of an SGP fails, the error received would be printed on the screen and in case the enabling/disabling is successful, message for successful SNMP set would be printed.

```
m3ua_link --disable localhost SGP-2
Reading information from localhost:11161
           SNMP set of associated route:mtpRouteAdminState.1.1 to inactive is
successful
           SNMP set of associated route:mtpRouteAdminState.2.1 to inactive is
successful
           SNMP set of associated route:mtpRouteAdminState.3.1 to inactive is
successful
           SNMP set of associated route:mtpRouteAdminState.4.1 to inactive is
successful
           SNMP set of associated route:mtpRouteAdminState.5.1 to inactive is
successful
           SNMP set of m3uaSgpAdminState.2 to inactive is successful

Reading information from localhost:16002
           SNMP set of associated route:mtpRouteAdminState.1.1 to inactive is
successful
           SNMP set of m3uaSgpAdminState.1 to inactive is successful
```

```
m3ua_link --enable localhost SGP-2

Reading information from localhost:11161
           SNMP set of m3uaSgpAdminState.2 to active is successful
           SNMP set of associated route:mtpRouteAdminState.1.1 to active is
successful
           SNMP set of associated route:mtpRouteAdminState.2.1 to active is
successful
           SNMP set of associated route:mtpRouteAdminState.3.1 to active is
successful
           SNMP set of associated route:mtpRouteAdminState.4.1 to active is
successful
           ERROR: SNMP: setting associated route:mtpRouteAdminState.5.1 to 1
failed with reason:Received badValue(3) error-status at error-index 1

Reading information from localhost:16002
           SNMP set of m3uaSgpAdminState.1 to active is successful
           SNMP set of associated route:mtpRouteAdminState.1.1 to active is
successful
```

- `--enableasp/--disableasp`: Allows enabling or disabling the M3UA ASP SGP on all instances running on the system.

1. In case the enabling/disabling of an ASP fails, the error received would be printed on the screen and in case the enabling/disabling is successful, message for successful SNMP set would be printed on the screen.

   - When the `disableasp` command returns success:

     ```
     m3ua_link --disableasp localhost local
     Reading information from localhost:11161
               SNMP set of m3uaAspAdminState.1 to inactive is successful
     ```

   - When the `disableasp` command returns failure:

     ```
     m3ua_link --disableasp localhost ASP-1
     Reading information from localhost:11161
     ERROR: SNMP: setting m3uaAspAdminState.1 to 0 failed with reason:Received
     badValue(3) error-status at error-index 1
     ```

   - When the `enableasp` command returns success:

     ```
     m3ua_link --enableasp localhost ASP-1
     Reading information from localhost:11161
               SNMP set of m3uaAspAdminState.1 to active is successful
     ```

   - When the `enableasp` command returns failure:

     ```
     m3ua_link --enableasp localhost ASP-1
     Reading information from localhost:11161ERROR: SNMP: setting
     m3uaAspAdminState.1 to 1 failed with reason:Received badValue(3) error-status
      at error-index 1
     ```

- `--peers`: Displays information for all the peer SGPs across all the instances running on the system:

  1. If the peer information for a particular SGP is required, then both `<system>` and `<associationname>` must be specified.
  2. If two or more remote addresses are configured for a peer SGP, then the information would be retrieved and displayed for each such address.

  ```
  m3ua_link  --peers
  Reading information from localhost:11861

   SGP-NAME OPSTATE SCTP-OPSTATE APC-OPSTATE VPC-OPSTATE PEER STATE CWND RTO RWND
   SGP-1 down cookieWait Inactive Inactive 10.0.0.1 notRegistered 0 0 0
   SGP-2 down cookieWait Inactive Inactive 10.0.0.2 notRegistered 0 0 0

  Reading information from localhost:16002

   SGP-NAME OPSTATE SCTP-OPSTATE APC-OPSTATE VPC-OPSTATE PEER STATE CWND RTO RWND
   SGP-2 down cookieWait Inactive Inactive 10.0.0.3 notRegistered 0 0 0
        10.0.0.5 notRegistered 0 0 0
   SGP-3 down cookieWait Inactive Inactive 10.0.0.4 notRegistered 0 0 0
  ```

F.4 ss7_link

The `ss7_link` tool allows diagnosis of an SS7 link, including:

- Showing the status of the link (including error conditions)
- Receiving and displaying all traps related to the link
- Enabling or disabling the link

The `ss7_link` tool operates on the Router by default. To direct the `ss7_link` tool to operate on the MAP screener, specify `--tp_scr`.

F.4.1 Synopsis

```
ss7_link [--tp_scr] system <linkset <slc>>
ss7_link [--tp_scr] --activate system <linkset <slc>>
ss7_link [--tp_scr] --deactivate system <linkset <slc>>
ss7_link [--tp_scr] --traps system <linkset <slc>>
```

F.4.2 Options

Option	Description
no option	Provides information about the SS7 link: • Linkset to which it belongs • Signalling link code • Trunk and timeslot that it uses • Operational state • Indication of whether it is being traced • Error conditions
--activate	Enables one or more SS7 links.
--deactivate	Disables one or more SS7 links.
--traps	Writes all generic and license-related traps (in a readable format) to the standard output path.

F.4.3 Operands

Operand	Description
system	Host name or IP address of the Router.
linkset	Name of an SS7 linkset.
slc	Signalling link code(s) of an SS7 linkset.

Note: Link changes that are made using the `ss7_link` tool are stored in volatile memory. Therefore, these settings are lost when the Router restarts.

F.5 tp_ccdr

The `tp_ccdr` tool enables decoding a Comverse CDR file. `tp_ccdr` converts one or more CDR files to readable text.

F.5.1 Synopsis

```
tp_ccdr -help
tp_ccdr --option=<option_value> --output=<directory|file> <files>
```

F.5.2 Options

Option	Description
--output	Specifies the location in which to place the output. `directory` specifies the directory in which to place the output. `file` indicates the file name to use.
--option	Specifies the option value which will be used to identify the set of optional parameters present in the CDR file. This is a mandatory field. Method for assingning the option_value is explained below.
--help	Prints the usage of tp_ccdr

The value of the "option_value" depends on the number of optional fields that are configured to be included in the Comverse CDR record. For mapping the optional CCDR fields to this "option_value", it is treated as a bitstring of 4 bits such that each optional field corresponds to a particular bit position as shown below. Note that bit1 is the least significant bit and bit4 is the most significant bit.

Optional CCDR Field Name	Bit Position in "option_value"
saOptionsIntN	1
Prepaid Indicator (saOptionsCharN)	2
Diameter Details	3
includeconcatenatedmsginfoinccdr	4

For example:

- If only the "saOptionsIntN" optional field is selected to be included in the CCDR then while decoding only bit1 will be true (1), rest all will be false(0). Thus the value of the "option_value" parameter will be '1'.
- If both "saOptionsIntN" and "Diameter Details" are configured to be included in the CCDR, then only bit1 and bit3 will be TRUE(1) and rest all will be FALSE(0), making the value of "option_value" as '5'.
- If "Prepaid Indicator", "Diameter Details" and "includeconcatenatedmsginfoinccdr " are configured to be included in the CCDR, then only bit1, bit3 and bit4 will be TRUE(1) and rest all will be FALSE(0), making the value of "option_value" as '13'.
- If only "includeconcatenatedmsginfoinccdr" is configured to be included in the CCDR then only bit4 will be TRUE(1) and rest all will be FALSE(0), thus the value of "option_value" will be '8'.
- In case none of the optional parameters is configured to be included in CCDR then all the bits will be FALSE(0), hence the value of "option_value" will be '0'.

F.5.3 Operands

Operand	Description
files	One or more CDR file(s) to convert.

F.5.4 Handling of Alphanumeric Addresses

The following fields support an alphanumeric address when the TON is 5 and 'Alphanumeric Orig Allowed' field is set to TRUE in the corresponding CCDR billing profile on MGR GUI:

- Source_id
- Target_id
- Original_target
- Notif_ext:source

F.6 tp_ecdr

The `tp_ecdr` tool enables decoding an Ericsson CDR file. `tp_ecdr` converts one or more CDR files to readable text.

F.6.1 Synopsis

```
tp_ecdr --output=<directory|file> <files>
```

F.6.2 Options

Option	Description
--output	Specifies the location in which to place the output. `directory` specifies the directory in which to place the output. `file` indicates the file name to use.

F.6.3 Operands

Operand	Description
files	One or more CDR file(s) to convert.

F.7 tp_fcdr

The `tp_fcdr` tool enables decoding an LCMG (ex-CMG) CDR file. `tp_fcdr` converts one or more ASN.1 CDR files to readable text.

F.7.1 Synopsis

```
tp_fcdr --ud_decrypt_key_file=<key_file> --output=<directory|file> <files>
```

F.7.2 Options

Option	Description
--output	Specifies the location in which to place the output. `directory` specifies the directory in which to place the output. `file` indicates the file name to use.
--ud_decrypt_key_file	Specifies the location of the key file to use for decrypting the SMS content. `key_file` indicates the file name to use. **Note:** If the key file is not given as an option, the default path (`/usr/TextPass/.crypt/ud_crypto_key`) will be used.

F.7.3 Operands

Operand	Description
files	One or more CDR file(s) to convert.

F.7.4 Handling of Alphanumeric Addresses

The following fields contain an alphanumeric address when the TON is 5:

- untranslOrigAddressGSM
- untranslRecipAddressGSM
- smscPresentationAddressGSM
- orglOrigAddressGSM
- orglRecipAdressGSM
- orglNotifAddressGSM

These alphanumeric addresses are encoded in 7-bit packed encoding according to 3GPP TS 23.038 and 3GPP TS 23.040. However, in contrast with the address fields in MAP messages, the length of the CDR fields is encoded in octets, not in nibbles (4-bit semi-octets). Therefore, a decoding issue can occur when the alphanumeric address contains seven or eight characters, as the difference cannot be determined from the CDR address length field.

The recommended algorithm is, if a CDR address is eight octets long and ends with seven zero (0) bits, the seven zeroes are not decoded as a meaningful character (because 000 0000 is @). This functionality allows distinguishing between, for example, `12345678` and `1234567`, because the last octet of `1234567` is `0000 0000`, while the last octet of `12345678` is `0111 0000`. Therefore, `1234567@` is decoded/encoded as `1234567`.

F.8 tp_lcdr

The `tp_lcdr` tool enables decoding an LCMG (Telepath) CDR file. `tp_lcdr` converts one or more CDR files to readable text.

F.8.1 Synopsis

```
tp_lcdr --output=<directory|file> <file>
```

```
tp_lcdr --format=<customformat> <file>
```

F.8.2 Options

Option	Description
--output	Specifies the location in which to place the output. `directory` specifies the directory in which to place the output. `file` indicates the file name to use.
--format	Formats the CDR file according to a custom LCDR field format.

F.8.3 Operands

Operand	Description
files	One or more CDR file(s) to convert or format.
customformat	Sequence of numbers (separated by the @ symbol) representing the custom LCDR field format to apply to the indicated CDR file.

F.8.4 Sample Usage

The following command applies a custom LCDR format to a CDR file:

```
--format=@19@1@2@3@6@4@5@7@10@11@12@13@91@92@202@203@205@206
cdr-test_20081120_142848_609.dat
```

F.9 tp_ncdr

The `tp_ncdr` tool enables decoding a Nokia CDR file. `tp_ncdr` converts one or more CDR files to readable text.

F.9.1 Synopsis

```
tp_ncdr --output=<directory|file> <files>
```

F.9.2 Options

Option	Description
--output	Specifies the location in which to place the output. `directory` specifies the directory in which to place the output. `file` indicates the file name to use.

F.9.3 Operands

Operand	Description
files	One or more CDR file(s) to convert.

F.10 tp_3g_cdr

The `tp_3g_cdr` tool enables decoding a 3G CDR file. `tp_3g_cdr` converts one or more CDR files to readable text.

F.10.1 Synopsis

```
tp_3g_cdr <files>
```

F.10.2 Operands

Operand	Description
files	One or more CDR file(s) to convert.

Note: Decoding of the Comverse 3G CDR file is possible only when the generated CDR file is present in the available directory, i.e. all the three sections are present in the CDR file. For more information on Comverse 3G CDR refer section 5.8 in RTR Billing Manual.

F.11 tp_scdr

The `tp_scdr` tool enables decoding a SS.8 CDR file. `tp_scdr` converts one or more CDR files to readable text.

F.11.1 Synopsis

```
tp_scdr [--ascii] [--optional] <files>
```

F.11.2 Options

Option	Description
--ascii	Specifies if the decoded SS8 CDR has to be displayed in ASCII format. Refer Appendix C in the RTR Billing Manual for more details.
--optional	Specifies that the CDR file which tp_scdr needs to decode contains SCDR records having one or more optional parameters. **Important:** In case you are decoding a CDR file containing SCDR records without any optional parameter (i.e. having only the mandatory parameters), then DO NOT use this option. Incorrect use of this option would lead to errors while decoding the CDR file and generating the output. Refer Section 4.6 in the RTR Billing Manual, for more information related to SCDR and optional parameter.

F.11.3 Operands

Operand	Description
files	One or more CDR file(s) to convert.

F.12 tp_gttupdate

The `tp_gttupdate` tool enables the dynamic addition or deletion of GTT rules, MTP destinations, and SCCP load share set.

The `tp_gttupdate` tool validates the configuration files, and then retrieves data from all devices that are configured to run on the host (`tpconfig` attributes `runtextpassprocess` and `runtextscrprocess` in the host-specific configuration file). You can use the `--textpass` and `--tp_scr` options to specify a single device instead of both devices.

The tool compares the retrieved device data and the configuration files and checks for added or removed GTT rule, MTP destination, and SCCP load share set items. The tool uses the following key attributes for comparison:

- Combination of input attributes for a GTT rule
- Name of an MTP destination
- Name of an SCCP load share set

If the tool detects these items, it modifies the running devices to match the configuration:

- If the item with the key is present in the configuration but is not present in the device data, the tool considers the item to be new and adds it to the device after validation.
- If the item with the key is not present in the configuration but is present in the device, the tool considers the item to be deleted and removes it from the device after validation
- If the item with the key is present in the configuration and in the device, and all attributes and subordinates match, then the tool considers them to be identical.

Validation of detected actions consists of the following:

- Adding a GTT rule—Validate if the referred-to `outputmtpdestination` or referred-to `outputloadshareset` exists
- Deleting a GTT rule—None
- Adding a destination—Validate if the point code of the destination is unique
- Deleting a destination—Validate if the destination is not referred to in a GTT rule
- Adding a SCCP load share set —Validate if the referred-to `mtpdestination` for each member of a load share set exists.
- Deleting a SCCP load share set —Validate if the SCCP load share set is not referred to in a GTT rule (as `outputloadshareset`).

Validation and actions are performed in the following order:

1. Add destination
2. Add SCCP load share set
3. Add GTT rule
4. Delete GTT rule
5. Delete SCCP load share set
6. Delete destination

Note: As part of adding a SCCP load share set, all its subordinate members are automatically added as well. Similarly, while deleting a SCCP load share set, all its subordinate members are also deleted.

Actions are executed on the devices after all changes are collected and validated, unless the `--validateonly` option is specified.

CAUTION:

The `tp_gttupdate` tool updates running device configuration. It is always recommended to run it with the `--validateonly` option first and verify the actions before executing them.

Using the `specific-config-file` and `common-config-file` operands without `--validateonly` can result in inconsistency between the device and the default configuration used during starting the device.

Do not run multiple instances of `tp_gttupdate` in parallel; this can result in inconsistent device configuration.

F.12.1 Messages

All info, warning and error messages are sent to the syslog with `user.info`, `user.warning` and `user.error` log levels.

Info messages are also sent to the standard output (`stdout`); warning and error messages are sent to standard error (`stderr`).

F.12.2 Unsupported Operations

The tool does not support the changing of attributes. If a change in any attribute other than the key or subordinate (i.e. route or SCCP load share set member) is detected, the tool reports it in a warning message and ignores the item for further action. If you need to make an attribute change, you should restart the RTR and/or MAP Screener (SCR) process(es).

The tool does not support the addition or deletion of destinations with type STP or linkset subordinates (these destinations are reported in an INFO message and are excluded from comparison). However, they are used for validation, if needed. If you need to change these items, you should restart the RTR and/or MAP Screener (SCR) process(es).

F.12.3 Synopsis

```
tp_gttupdate [--validateonly] [--textpass] [--tp_scr]
 [specific-config-file [common-config-file]]
```

F.12.4 Options

Option	Description
--validateonly	Validates configuration changes and then stops processing.
--textpass --tp_scr	Only updates the specified device (Router or MAP Screener). By default, both devices are updated if they are configured in the specific configuration file (`tpconfig` attributes `runtextpassprocess` and `runtextscrprocess`).

F.12.5 Operands

Operand	Description
specific-config-file	This file will be used for configuration instead of the default host-specific configuration file.
common-config-file	This file will be used for configuration instead of the default common configuration file. If specified, this file must follow the specific configuration file operand.

F.13 tp_event

The `tp_event` tool enables decoding an event log file created by an event log profile. `tp_event` converts one or more event log files to readable text. Executing `tp_event` without any options reads the event log file from `stdin`, and writes to `stdout`.

F.13.1 Synopsis

```
tp_event [<inputfile>] [<outputfile>]
```

F.13.2 Options

Option	Description
`-h`	Prints a help message.

F.13.3 Operands

Operand	Description
`inputfile`	Read event log file from `<inputfile>`.
`outputfile`	Write event log to `<outputfile>`.

F.14 tp_log

The `tp_log` tool enables decoding a log file created by a log profile. `tp_log` converts one or more log files to readable text.

Note: If an alphanumeric GSM Address has the special character "@" at the end and its total length is a multiple of 7 (in characters), `tp_log` will strip off the ending "@". For example, the alphanumeric GSM Address "`testing@`" will be decoded as "`testing`".

F.14.1 Synopsis

```
tp_log --ud_decrypt_key_file=<key_file> --output=<directory|file> <files>
```

F.14.2 Options

Option	Description
`--output`	Specifies the location in which to place the output.

Option	Description
	`directory` specifies the directory in which to place the output. `file` indicates the file name to use.
--ud_decrypt_key_file	Specifies the location of the key file to use for decrypting the SMS content. `key_file` indicates the file name to use. **Note:** If the key file is not given as an option, the default path (`/usr/TextPass/.crypt/ud_crypto_key`) will be used.

F.14.3 Operands

Operand	Description
`files`	One or more log file(s) to convert.

Appendix G

Sample Configuration Files

Topics:

G.1 Sample Common Configuration File

```
<!--
    In order to avoid having to keep the configuration files on
    potentially many RTR nodes in sync, all semi-static configuration
    parameters that apply to all RTR nodes equally should be specified
    in the common_config.txt file, distributed from the OAM node.
    (See fxferfile-tag in {hostname}_config.txt.) The RTR operator
    manual provides a per-config-parameter suggestion on which file
    to put it into.
-->

<tpconfig

    virtualpointcode="5354"
    commonaddress="491111122222"

    countrycode="49"
    mobilecountrycode="262"
    mobilenetworkcode="02"

  >

</tpconfig>
```

G.2 Sample Host-Specific Configuration File

```
<tpconfig
runtextpassprocess="true"
runtpfclientprocess="true"
ipaddress="127.0.0.1"
pointcode="5352"
gtaddressinfo="491720499014"
>
<!--
SIGTRAN configuration, M3UA ASP role.
Use multiple IP addresses for SCTP multi-homing
-->
<m3ualocaladdress spec="10.0.0.9"/>
<m3ualocaladdress spec="10.0.0.10"/>
<!--
If the SS.7 related connectivity configuration is symmetric,
it is recommended to place it into the common_config.txt,
in order to avoid having to keep the configuration in sync
between a potentially large number of nodes.
The RTR can run without SS.7 connectivity (e.g. as part of a
pure application gateway. In that case, no SS.7 related
configuration is necessary.
If SS.7 connectivity is achieved using SIGTRAN (M3UA), the RTR
plays the role of an ASP, and the configuration defines peer
SGP nodes and the RTR's connectivity to them as follows:
-->
<m3uasgp name="SGP-1"
sctplocalport="2906"
sctpremoteport="2906"
useforvirtualpointcode="false"
>
```

```
<!-- Use multiple IP addresses for SCTP multi-homing -->
<remoteaddress spec="10.1.3.3"/>
<remoteaddress spec="10.1.3.103"/>
</m3uasgp>
<m3uasgp name="SGP-2"
sctplocalport="2907"
sctpremoteport="2907"
>
<remoteaddress spec="10.1.3.4"/>
<remoteaddress spec="10.1.3.104"/>
</m3uasgp>
<!-- an STP, reachable through both SGPs is declared as follows: -->
<destination name="STP-1" type="stp" pointcode="5215">
<route m3uasgp="SGP-1"/>
<route m3uasgp="SGP-2"/>
</destination>
<!-- and an SMSC, reachable only through SGP-1 like this: -->
<destination name="SMSC-A" type="smsc" pointcode="5216">
<route m3uasgp="SGP-1"/>
</destination>
<!--
SCCP load share set configuration for distributing the outgoing SCCP traffic load
among a set of pre-defined MTP destinations that are referenced by a single GTT
rule:
-->
<sccploadshareset name="STP_set2" >
<member mtpdestination="SMSC-A" subsystemnumber="7" priority="4" weight="6"/>
<member mtpdestination="STP-1" subsystemnumber="7" priority="4" weight="4"/>
</sccploadshareset>
<!--
SCCP-layer routing decisions are controlled by global title
translation (GTT) rules. They adhere to the following pattern:
-->
<!-- to route on PC/SSN to a previously declared MSC, do: -->
<gttrule
inputgtaddressinfo="491722279*"
outputroutingindicator="ssn"
outputgtindicator="0"
outputmtpdestination="MSC-Y"
/>
<!-- to distribute the outgoing SCCP traffic load among a set of pre-defined MTP
destinations do: -->
<gttrule
inputgtaddressinfo="491722278*"
outputroutingindicator="ssn"
outputgtindicator="0"
outputloadshareset="STP_set2"
/>
<fxferfile
localpath="/usr/TextPass/etc/common_config.txt"
serverpath="/usr/TextPass/etc/common_config.txt"
validate="/usr/TextPass/bin/tp_config --validatecommonconfig SERVERFILE"
/>
<fxferfile
localpath="/usr/TextPass/etc/MGRdata.xml.gz"
serverpath="/usr/TextPass/etc/MGRdata.xml.127.0.0.1.gz"
/>
<trapreceiver ipaddress="127.0.0.1" udpport="11173" />
</tpconfig>
```

G.3 Sample Trap Filter Configuration

The trap filter configuration example below ensures that all traps except `linkRxUtilisationGrowing` and `linkTxUtilisationGrowing` will be sent to the alarm station.

```
<trapreceiver ipaddress="192.168.1.100" udpport="162">

   <blacklist>
      <sms trap="linkRxUtilisationGrowing"/>
      <sms trap="linkTxUtilisationGrowing"/>
   </blacklist>

   <whitelist>
      <sms trap="*"/>
   </whitelist>

</trapreceiver>
```

G.4 Sample SIGTRAN Common Configuration File

Example of a common configuration file for a RTR with a SIGTRAN only interface:

Note: This example includes RTR, HUB, AMS, and FAF configuration items.

```
<tpconfig
    ipaddress="10.0.0.13"
    pointcode="5352"
    gtaddressinfo="491720499014"
    runtpfclientprocess="true"
    runtextpassprocess="true"
    runtextamsprocess="true"
    runqclidprocess="true"
    runtexthubprocess="true"
    runtextfafprocess="true"

    maxallowedconfigerrors="0"
    firewallmospoofingcheckcondition="never"
    requiress7connectivity="false"

    hubipaddressowninternal="10.0.0.13"
    hubipfailovercontrol="false"
    hubipfailovertimeout="0"
    hublifecheckinterval="10"
    hubreconnectdelay="5"
    hubscterminationpointretrydelay="30"
    hubenabletcpkeepalive="false"
    hubmaxmxpresponsetime="30"
    hubmaxmipresponsetime="5"
    hubmaxmxptprretries="1"
    hublogparsingerrors="true"
    hubpropverifychecksum="false"
    hubmaxtotalapplicationsessions="1000"
    hubsessionusagethreshold1="50"
    hubsessionusagethreshold2="70"
    hubsessionusagethreshold3="85"
    hubsessionusagethreshold4="95"
    hubsessionusagethreshold5="100"
    hubenableappoutsidesessiontraps="false"
```

```
    hubenableappinsidesessiontraps="false"
    hubenablescterminationpointsessiontraps="false"
    hubenablescnodesessiontraps="false"
    hubenableservicecentresessiontraps="false"
    hubenableapplicationtraps="false"
    hubenablemessageidprefixing="false"
    hubenablevendorspecificbillingid="false"
    hubvendorspecificbillingidtag="5121"
    hubvendorspecificbillingformattag="255"
    hubenablevendorspecificcontentrating="false"
    hubvendorspecificcontentratingtag="5124"
    hubsmppv34notificationtextformat="truncate"
    hublegacyucpapplicationsupport="disabled"
    hubucpmt4defaultgsmencoding="packed7bit"
    hubucpinquirytext1="Destination"
    hubucpinquirytext2="identification:"
    hubucpdeletetext3="Destination"
    hubucpdeletetext4="identification:"
    hubucpdeletetext5="has been deleted."
    hubucplonginquirydeleteresponse="false"
    hubucphandlingucp02="forwardunknown"

    hubenableoutsidesmppunbind="false"
    huboutsidesmppunbindmaxresponsetime="5"
    hubenableinsidesmppunbind="false"
    hubinsidesmppunbindmaxresponsetime="5"
    hubmaxdelayedmessages="1001"


    >
<!--
      scdrrouterid="1"
-->


  <!-- SIGTRAN configuration, M3UA ASP role -->
  <m3ualocaladdress spec="10.0.0.13"/>
  <m3uasgp name="sgp1"
        useforvirtualpointcode="true"
        sctplocalport="2906"
        sctpremoteport="2907"
      >
    <remoteaddress spec="10.0.0.97"/>
  </m3uasgp>


     <fafprop
       normalisationmap="0oO&#246;&#214;&#10;1iIlL!\/&#10;2zZ&#10;3eE&#10;4aA&#228;

       &#196;&#10;5sS&#223;&#10;6&#10;7tT&#10;8bB&#10;9gG&#10;cC&#10;dD&#10;fF&#10;

       hH&#10;jJ&#10;kK&#10;mM&#10;nN&#10;pP&#10;qQ&#10;rR&#10;uU&#252;&#220;&#10;

        vV&#10;wW&#10;xX&#10;yY"
     />

    <fafeci host="10.0.0.13" port="9500" user="RIO" pass="pass1"/>


  <fxferfile
      localpath="/usr/TextPass/etc/common_config.txt"
      serverpath="/usr/TextPass/etc/common_config.txt"
      validate="/usr/TextPass/bin/tp_config --validatecommonconfig SERVERFILE"
   />
  <fxferfile
```

```
      localpath="/usr/TextPass/etc/MGRdata.xml.gz"
      serverpath="/usr/TextPass/etc/MGRdata.xml.10.0.0.13.gz"
   />

  <trapreceiver ipaddress="127.0.0.1" udpport="11173"/>
        <whitelist>
            <apc trap="applicationIncorrectOutsideUcpPassword"/>
            <apc trap="applicationIncorrectOutsideSmppPassword"/>
            <hub trap="rtrUnAvailable"/>
            <hub trap="outsideListenerOperationalStateChanged"/>
        </whitelist>
  </trapreceiver>

</tpconfig>
```

Appendix H

Common SMS Counters for IMS and SS7

Topics:

H.1 Introduction

Below are SMS Counters that occur when the router process the traffic between SS7 and IMS network. or Application and IMS network .The SMS Counters are divided in three categories, listed below:

- SMS Counters common for SS7 and IMS
- SMS Counters common for Application and IMS
- SMS Counters for SS7 only, Not for IMS

H.2 SMS Counters Common for IMS and SS7

Below are the SMS counters that occur when the router processes the traffic between mobile and IMS network:

- smsCntMoDataMisErrorCounter
- smsCntMoDiscard
- smsCntMoDiscardWithNakCounter
- smsCntMoFacNotSuppErrorCounter
- smsCntMoInvSmeAddrErrorCounter
- smsCntMoMoFailure
- smsCntMoMoFailure
- smsCntMoMoSuccess
- smsCntMoMoSuccess
- smsCntMoMtAmsFallbackNotAppliedDueToPermErrorOnPrimary
- smsCntMoMtAmsFallbackNotAppliedDueToUnavailability
- smsCntMoMtAmsFallbackSuccess
- smsCntMoMtAmsPrimaryFailure
- smsCntMoMtAoFallbackNotAppliedDueToPermErrorOnPrimary
- smsCntMoMtAoFallbackNotAppliedDueToUnavailability
- smsCntMoMtAtFallbackNotAppliedDueToPermErrorOnPrimary
- smsCntMoMtAtFallbackNotAppliedDueToUnavailability
- smsCntMoMtFailure
- smsCntMoMtFromAmsPermanentMessageError
- smsCntMoMtFromAmsPermanentRecipientError
- smsCntMoMtFromAmsSuccess
- smsCntMoMtFromAmsTemporaryError
- smsCntMoMtMoFallbackFailure
- smsCntMoMtMoFallbackNotAppliedDueToPermErrorOnPrimary
- smsCntMoMtMoFallbackNotAppliedDueToUnavailability
- smsCntMoMtMoFallbackNotAppliedDueToUnavailability
- smsCntMoMtMoFallbackSuccess
- smsCntMoMtMoPrimaryFailure
- smsCntMoMtMoPrimaryFailure

- smsCntMoMtMoPrimarySuccess
- smsCntMoMtMoPrimarySuccess
- smsCntMoMtSuccess
- smsCntMoMtToAmsFailure
- smsCntMoMtToAmsSuccess
- smsCntMoMtToAmsSuccess
- smsCntMoOtherErrorsCounter
- smsCntMoRejectedByTprCounter
- smsCntMoScCongErrorCounter
- smsCntMoSubNotScSubErrorCounter
- smsCntMoSuccessfulCounter
- smsCntMoSysFailErrorCounter
- smsCntMoTotalCounter
- smsCntMoUnexpDataValErrorCounter
- smsCntMoUnkScErrorCounter
- smsCntRecvMoFwdSmCounter
- smsCntRecvMoFwdSmWithPhaseStatusReportRequestCounter
- smsCntRecvMoFwdSmWithoutStatusReportRequestCounter
- smsCntSentMoFwdSmCounter
- smsCntMtAbsSubErrorCounter
- smsCntMtAoFailure
- smsCntMtAoSuccess
- smsCntMtAtFailure
- smsCntMtAtSuccess
- smsCntMtDataMisErrorCounter
- smsCntMtEquipNotSmEquipErrorCounter
- smsCntMtEquipProtErrorCounter
- smsCntMtFacNotSuppErrorCounter
- smsCntMtFallbackToVersionCounter
- smsCntMtIllEquipErrorCounter
- smsCntMtIllSubErrorCounter
- smsCntMtInvSmeAddrErrorCounter
- smsCntMtMemCapExcErrorCounter
- smsCntMtMtFailure
- smsCntMtMtFailure
- smsCntMtMtSuccess
- smsCntMtMtSuccess
- smsCntMtMtToAmsFailure
- smsCntMtMtToAmsSuccess
- smsCntMtOtherErrorsCounter
- smsCntMtSccpAbortedCounter
- smsCntMtSubBusyForMtSmErrorCounter
- smsCntMtSuccessfulCounter
- smsCntMtSysFailErrorCounter
- smsCntMtTcapAbortedCounter
- smsCntMtTimeoutCounter

- smsCntMtTotalCounter
- smsCntMtUnexpDataValErrorCounter
- smsCntMtUnidenSubErrorCounter
- smsCntRecvInfScCounter
- smsCntRecvMtFwdSmCounter
- smsCntRecvMtHomeRoutedTrustedScrambledCounter
- smsCntRecvMtMatchingMtRoutingRuleCounter
- smsCntRecvMtPassedCounter
- smsCntRecvRogueTcapEndCounter
- smsCntRepStsFallbackToVersionCounter
- smsCntRepStsSuccessCounter
- smsCntRepStsSysFailErrorCounter
- smsCntRepStsTimeoutCounter
- smsCntRepStsTotalCounter
- smsCntSentAnyTimeModActCounter
- smsCntSentAnyTimeModDeActCounter
- smsCntSentFakeRepStsCounter
- smsCntSentInfScCounter
- smsCntSentMtFwdSmCounter
- smsCntSentMtFwdSmWithOrdinaryMessageCounter
- smsCntSentMtFwdSmWithPhaseStatusReportCounter
- smsCntSentRepStsCounter
- smsCntSentSriSmCounter
- smsCntSipoMessagesBarred
- smsCntSiptMessagesBarred

H.3 SMS Counters common for Application and IMS

Below are the SMS counters that occur when the router processes the traffic between Application and IMS network:

- smsCntMoAoFailure
- smsCntMoAoSuccess
- smsCntMoAtAmsFallbackNotAppliedDueToPermErrorOnPrimary
- smsCntMoAtAmsFallbackNotAppliedDueToUnavailability
- smsCntMoAtAmsFallbackSuccess
- smsCntMoAtAmsPrimaryFailure
- smsCntMoAtFromAmsPermanentMessageError
- smsCntMoAtFromAmsPermanentRecipientError
- smsCntMoAtFromAmsTemporaryError
- smsCntMoAtToAmsFailure
- smsCntMoAtToAmsSuccess
- smsCntAoAoFromAmsDeleted
- smsCntAoAoFromAmsExpired
- smsCntAoAoFromAmsPermanentMessageError

- smsCntAoAoFromAmsPermanentRecipientError
- smsCntAoAoFromAmsReplaced
- smsCntAoAoFromAmsSuccess
- smsCntAoAoFromAmsTemporaryError
- smsCntAoMtAmsSuccess
- smsCntAoMtAoFallbackNotAppliedDueToPermErrorOnPrimary
- smsCntAoMtAoFallbackNotAppliedDueToUnavailability
- smsCntAoMtFailure
- smsCntAoMtFromAmsDeleted
- smsCntAoMtFromAmsExpired
- smsCntAoMtFromAmsPermanentMessageError
- smsCntAoMtFromAmsPermanentRecipientError
- smsCntAoMtFromAmsReplaced
- smsCntAoMtFromAmsSuccess
- smsCntAoMtSuccess
- smsCntAoMtToAmsSuccess
- smsCntOutsideAoDestinationPermanentMessageError
- smsCntOutsideAoDestinationPermanentRecipientError
- smsCntOutsideAoDestinationTemporaryError
- smsCntOutsideAoSuccess
- smsCntOutsideAoTotal
- smsCntOutsideAtDestinationPermanentRecipientError
- smsCntOutsideAtDestinationTemporaryError
- smsCntOutsideAtSuccess
- smsCntOutsideAtTotal

H.4 SMS Counters for SS7 Only, Not for IMS

Below are the SMS counters that occur when the router processes the traffic between SS7 and IMS network, But not relevant to IMS traffic:

- smsCntRecvSriSmCounter
- smsCntRecvSriSmMatchingMtRoutingRuleCounter
- smsCntRecvSriSmPassedCounter
- smsCntSriSmAbsSubErrorCounter
- smsCntSriSmCallBarredErrorCounter
- smsCntSriSmDataMisErrorCounter
- smsCntSriSmFacNotSuppErrorCounter
- smsCntSriSmFallbackToVersionCounter
- smsCntSriSmSccpAbortedCounter
- smsCntSriSmSuccessCounter
- smsCntSriSmSysFailErrorCounter
- smsCntSriSmTcapAbortedCounter
- smsCntSriSmTeleServNotProvErrorCounter
- smsCntSriSmTimeoutCounter

- smsCntSriSmTotalCounter
- smsCntSriSmUnexpDataValErrorCounter
- smsCntSriSmUnkSubErrorCounter

Appendix I

References

Topics:

I.1 References

1. 3GPP TS 29.002 version 3.20 Release 1999; Digital cellular telecommunications systems (Phase2+); Mobile Application Part (MAP) specification
2. 3GPP TS 23.066 version 4.0.0 Release 4; Digital cellular telecommunications systems (Phase2+) (GSM); Universal Mobile Telecommunications System (UMTS); Support of Mobile Number Portability (MNP); Technical Realisation; Stage 2
3. Simple Network Management Protocol (IETF - RFC 1157)
4. Red Hat Linux documentation (*http://www.redhat.com/docs*)
5. NewNet Mobile Messaging RTR Billing Manual
6. NewNet Mobile Messaging Tools Operator Manual
7. NewNet Mobile Messaging MGR Operator Manual
8. NewNet Mobile Messaging HUB Operator Manual
9. NewNet Mobile Messaging PBC Operator Manual
10. NewNet Mobile Messaging FAF Operator Manual
11. NewNet Mobile Messaging LGP Operator Manual
12. NewNet Mobile Messaging EMG Operator Manual
13. NewNet Mobile Messaging Firewall Guide
14. NewNet Mobile Messaging IIW Operator Manual
15. GSM Association AA.50, SMS Fraud Criteria, Version 3.1, April 2005
16. GSM Association IR.71, SMS SS7 Fraud Prevention, Version 3.1, 30 March 2005
17. C-Ares documentation (*http://c-ares.haxx.se/*)
18. NewNet MAP Screener Product Description

Glossary

#

3G	3rd Generation An International Telecommunication Union (ITU) specification for the third generation of mobile communications technology. 3G promises increased bandwidth and works over wireless air interfaces such as GSM, TDMA, and CDMA. The new EDGE air interface has been developed specifically to meet the bandwidth needs of 3G.
3GPP	3rd Generation Partnership Project

A

ABL	Automatic Blacklisting An enhanced anti-spam and anti-fraud functionality, wherein the FAF filters screen incoming MO/MT messages received from the RTR and, if a message is detected as `spam` or `fraudulent` based on the appropriately configured filter conditions, sends an automatic provisioning request to the SPF to blacklist the corresponding originator or recipient subscriber for either a specified duration of time or permanently.
ACK	Data Acknowledgement
AMS	Active Message Store Provides store-and-forward functionality for SMS messages.

A

ANSI	American National Standards Institute An organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. ANSI develops and publishes standards. ANSI is a non-commercial, non-government organization which is funded by more than 1000 corporations, professional bodies, and enterprises.
AO	Application Originated Short message traffic that is originated by an application.
AOR	Application-Originated Routing Routing rule that operates on application-originated (AO) messages. Address of Record
AOX	Application-Originated eXternal condition External condition rule that operates on application-originated (AO) messages.
APD	Application Processor DCM bootstrap code
application	The telecommunications software that is hosted on the platform. A service provided to subscribers to a network; for example, voice over IP (VoIP), video on demand (VoD), video conferencing, or gaming.
ARP	Address Resolution Protocol

A

	ARP monitoring uses the Address Resolution Protocol to determine whether a remote interface is reachable.
	Auto Reply service
	Personalized SMS auto reply service. This service is provided by the Mobile Messaging XS-ARP component.
AS	Application Server
	A logical entity serving a specific Routing Key. An example of an Application Server is a virtual switch element handling all call processing for a unique range of PSTN trunks, identified by an SS7 DPC/OPC/CIC_range. Another example is a virtual database element, handling all HLR transactions for a particular SS7 DPC/OPC/SCCP_SSN combination. The AS contains a set of one or more unique Application Server Processes, of which one or more normally is actively processing traffic.
	Application Simulator
	Test tool that can simulate applications and/or SMSCs.
ASN.1	Abstract Syntax Notation One
ASP	Application Server Process
	A process instance of an Application Server. An Application Server Process serves as an active or standby process of an Application Server (e.g., part of a distributed virtual switch or database). Examples of ASPs are processes (or process instances of) MGCs, IP SCPs or IP HLRs. An ASP contains an SCTP end-point, and may be

A

	configured to process signaling traffic within more than one Application Server.
AT	Application Terminated Short message traffic that terminates at an application.
ATI	Any Time Interrogation An ATI message allows an external server to interrogate an HLR and obtain information about the location and/or state of a GSM subscriber. Incoming application-terminated
ATIC	Incoming application-terminated counting Counting rule that operates on incoming application-terminated (AT) messages.
ATIR	Incoming application-terminated routing Routing rule that operates on incoming application-terminated (AT) messages.
ATIX	Incoming application-terminated eXternal condition External condition rule that operates on incoming application-originated (AO) messages.
ATO	Outgoing application-terminated
ATOC	Outgoing application-terminated counting

A

	Counting rule that operates on outgoing application-terminated (AT) messages.
ATOR	Outgoing application-terminated routing Routing rule that operates on outgoing application-terminated (AT) messages.
ATOX	Outgoing application-terminated eXternal condition External condition rule that operates on outgoing application-originated (AO) messages.

B

BWL	Black and Whitelist service Personalized short message black and whitelist service. This service is provided by the Mobile Messaging XS-BWL component.

C

CAMEL	Customized Applications for Mobile networks Enhanced Logic
CCI	Customer Care Interface A Web-based interface that allows customer care agents to assist SMS subscribers.
CDMA	Code Division Multiple Access A channel access method used by radio communication technologies. CDMA employs spread-spectrum technology and a special coding scheme (where each transmitter is assigned a code) to allow multiple users to be multiplexed over the

C

same physical channel. CDMA, the most common cellular wireless technology deployed in North America, is being replaced by GSM. See also GSM.

CdPA

Called Party Address

The field in the SCCP portion of the MSU that contains the additional addressing information of the destination of the MSU. Gateway screening uses this additional information to determine if MSUs that contain the DPC in the routing label and the subsystem number in the called party address portion of the MSU are allowed in the network where the EAGLE 5 ISS is located.

CDR

Call Detail Record

This refers to the recording of all connections in a database to permit activities such as billing connection charges or network analysis. CDR files are used in public switched networks, IP networks, for IP telephony, and mobile communications networks.

Charging Data Record

Used for user billing: a telecom provider transfers them from time to time in order to send bills to their users.

CgPA

Calling Party Address

The point code and subsystem number that originated the MSU. This point code and subsystem number are contained in the calling party address in the SCCP portion of the signaling information field of the MSU. Gateway screening uses this information to determine if

C

	MSUs that contain this point code and subsystem number area allowed in the network where the EAGLE 5 ISS is located.
CIMD	Computer Interface for Message Distribution Proprietary SMSC protocol developed by Nokia.
CPY	Copy to Phone service Personalized short message copy service that provides MO and MT copy to phone functionality. This service is provided by the Mobile Messaging XS-CPY component.
CSCF	Call Session Control Function
CSV	Comma-separated values The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline is a special character or sequence of characters signifying the end of a line of text).
CTA	Copy to Application service Personalized short message copy to application service that provides originator copy to application ("Sent Items") and/or recipient copy to application ("Inbox") functionality. This service is provided by the Mobile Messaging XS-CPY component.
CTE	Copy to Email service

C

	Personalized short message copy to email service, which allows MT short messages to be copied to one or more e-mail addresses provisioned by a subscriber. This service is provided by the Mobile Messaging XS-CPY component.

D

daemon	A process that runs in the background (rather than under the direct control of a user) and performs a specified operation at predefined times or in response to certain events. Generally speaking, daemons are assigned names that end with the letter "d." For example, sentryd is the daemon that runs the Sentry utility.
DCS	Data Coding Scheme
DDN	Dialout Delivery Notification
Diameter	Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in both local and roaming AAA situations. Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty.
DIL	Distribution List service

D

	Personalized short message distribution list service. This service is provided by the Mobile Messaging XS-DIL component.
DMF	Direct Message Filter Application component that consumes Intercept files generated by RTR, so it must run with RTR on the same Traffic Element. This component will regularly monitor for new Intercept Files generated by the RTR.
DPC	Destination Point Code DPC refers to the scheme in SS7 signaling to identify the receiving signaling point. In the SS7 network, the point codes are numeric addresses which uniquely identify each signaling point. This point code can be adjacent to the EAGLE 5 ISS, but does not have to be.

E

E.164	The international public telecommunication numbering plan developed by the International Telecommunication Union.
EC	External Condition Condition that is passed on the external condition interface.
ECI	External condition interface Interface for communicating with external condition applications.
ECM	External condition message

E

Message that is passed on the external condition interface.

F

FAF

Firewall Advanced Filter

Works in combination with the Firewall to filter messages, modify message content, and alert network operators of increases in SMS-related traffic.

FCDR

SMSC-compatible ASN.1 CDR format

FDA

First Delivery Attempt

Approximately 85 to 90 percent of SMS traffic gets through on first delivery attempt (FDA). That means that all of the initial processing that the SMSC does to store, query and forward messages is to a certain extent a waste of processing power — it would be much more cost-effective for an operator if a less expensive piece of equipment could first attempt to deliver the message.

FTE

Personalized short message forward to email service, which allows MT short messages to be forwarded (unconditionally) to one or more e-mail addresses provisioned by a subscriber.

This service is provided by the Mobile Messaging XS-FWD component.

FWD

Forward service

Personalized short message forward service. This service is provided by

F

	the Mobile Messaging XS-FWD component.
FWL	Firewall Helps protect subscribers from receiving unwanted messages and provides statistical information and message details about inbound suspect messages.

G

GPRS	General Packet Radio Service A mobile data service for users of GSM mobile phones.
GSM	Global System for Mobile Communications
GT	Global Title Routing Indicator
GTAI	Global Title Address Information
GTT	Global Title Translation A feature of the signaling connection control part (SCCP) of the SS7 protocol that the EAGLE 5 ISS uses to determine which service database to send the query message when an MSU enters the EAGLE 5 ISS and more information is needed to route the MSU. These service databases also verify calling card numbers and credit card numbers. The service databases are identified in the SS7 network by a point code and a subsystem number.
GUI	Graphical User Interface

G

The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

H

HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server A central database for subscriber information.
HUB	Works in combination with the Router to manage traffic to and from SMS applications.

I

Icache	Intermediate Cache Enables the Mobile Messaging system to store the state and certain parameters of a short message while it is being processed by an external SMSC.
IGM	See IS41 GSM Migration
IGMC	Internally generated message counting Counting rule that operates on internally generated messages (IGM).
IGMR	Internally generated message routing

I

	Routing rule that operates on internally generated messages (IGM).
IGMX	Internally generated message external condition External condition (EC) rule that operates on internally generated messages (IGM).
IIW	IMS InterWorking Works in combination with the router to provide gateway functionality between IMS domain and SS7 domain.
IMS	IP Multimedia Subsystem These are central integration platforms for controlling mobile communications services, customer management and accounting for mobile communications services based on IP. The IMS concept is supported by 3GPP and the UMTS Forum and is designed to provide a wide range of application scenarios for individual and group communication.
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network A network design that provides an open platform for developing, providing and managing services.
IP	Internet Protocol IP specifies the format of packets, also called datagrams, and the

I

	addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.
ISDN	Integrated Services Digital Network Integrates a number of services to form a transmission network. For example, the ISDN network integrates, telephony, facsimile, teletext, Datex-J, video telephony and data transfer services, providing users with various digital service over a single interface: voice, text, images, and other data.
ITU	International Telecommunications Union

L

LDAP	Lightweight Directory Access Protocol A protocol for providing and receiving directory information in a TCP/IP network.

M

M3UA	SS7 MTP3-User Adaptation Layer M3UA enables an MTP3 User Part to be connected to a remote MTP3 via a reliable IP transport.
MAP	Mobile Application Part

M

MGR	A Web-based interface for managing NewNet Mobile Messaging components. Prior to Suite 6, the Configuration Manager (CM) provided this functionality.
MIB	Management Information Database
MIP	Management Information Protocol NewNet proprietary protocol used for communication between the Mobile Messaging HUB, RTR, and AMS components.
MMTS	More-Messages-To-Send When multiple messages to a single destination are pending, MMTS delivers the messages to the destination using a single TCAP dialogue toward the MSC.
MNC	Mobile Network Code A number that identifies a mobile phone carrier. Used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator/carrier. See also MCC.
MNP	Mobile Number Portability
MO	Mobile Originated Refers to a connection established by a mobile communication subscriber. Everything initiated by the mobile station is known as mobile originated.
MOR	Mobile-Originated Routing

M

	Routing rule that operates on mobile-originated (MO) messages.
MOX	Mobile-Originated eXternal condition External condition rule that operates on mobile-originated (MO) messages.
MS	Mobile Station The equipment required for communication with a wireless telephone network.
MSC	Mobile Switching Center
MSISDN	Mobile Station International Subscriber Directory Number The MSISDN is the network specific subscriber number of a mobile communications subscriber. This is normally the phone number that is used to reach the subscriber.
MSU	Message Signal Unit The SS7 message that is sent between signaling points in the SS7 network with the necessary information to get the message to its destination and allow the signaling points in the network to set up either a voice or data connection between themselves. The message contains the following information: • The forward and backward sequence numbers assigned to the message which indicate the position of the message in the traffic stream in relation to the other messages.

M

- The length indicator which indicates the number of bytes the message contains.
- The type of message and the priority of the message in the signaling information octet of the message.
- The routing information for the message, shown in the routing label of the message, with the identification of the node that sent message (originating point code), the identification of the node receiving the message (destination point code), and the signaling link selector which the EAGLE 5 ISS uses to pick which link set and signaling link to use to route the message.

MT	Mobile Terminated All transmissions that reach the mobile station and are accepted by it, such as calls or short messages.
MTFSM	Mobile Terminated Forward Short Message
MTI	Incoming mobile-terminated
MTIC	Incoming mobile-terminated counting Counting rule that operates on incoming mobile-terminated (MT) messages.
MTIR	Incoming mobile-terminated routing Routing rule that operates on incoming mobile-terminated (MT) messages.

M

MTIX	Incoming mobile-terminated external condition External condition (EC) rule that operates on incoming mobile-terminated (MT) messages.
MTO	Outgoing mobile-terminated
MTOC	Outgoing mobile-terminated counting Counting rule that operates on outgoing mobile-terminated (MT) messages.
MTOR	Outgoing mobile-terminated routing Routing rule that operates on outgoing mobile-terminated (MT) messages.
MTOX	Outgoing mobile-terminated external condition External condition (EC) rule that operates on outgoing mobile-terminated (MT) messages.
MTP	Message Transfer Part The levels 1, 2, and 3 of the SS7 protocol that control all the functions necessary to route an SS7 Message Signal Unit through the network.
MTP2	Message Transfer Part, Level 2
MTP3	Message Transfer Part, Level 3
MXP	Message eXchange Protocol NewNet proprietary protocol used for communication between the

M

Mobile Messaging HUB, RTR, and AMS components.

N

NAK
Negative Acknowledgment

NCDR
Nokia SMSC-compatible CDR format

NPI
Number Plan Indicator

O

OPC
Originating Point Code

OS
Operating System

P

PBC
Prepaid Billing Controller

Performs prepaid charging using the Diameter, CAMEL, or SMPP+ interface.

PC
Point Code

The identifier of a signaling point or service control point in a network. The format of the point code can be one of the following types:

- ANSI point codes in the format network indicator-network cluster-network cluster member (**ni-nc-ncm**).
- Non-ANSI domestic point codes in the format network indicator-network cluster-network cluster member (**ni-nc-ncm**).
- Cluster point codes in the format network indicator-network cluster-* or network indicator-*-*.

P

	• ITU international point codes in the format **zone-area-id**. • ITU national point codes in the format of a 5-digit number (**nnnnn**), or 2, 3, or 4 numbers (members) separated by dashes (**m1-m2-m3-m4**) as defined by the Flexible Point Code system option. A group code is required (**m1-m2-m3-m4-gc**) when the ITUDUPPC feature is turned on. • 24-bit ITU national point codes in the format main signaling area-subsignaling area-service point (**msa-ssa-sp**). • 16-bit Japanese SS7 international point codes in the format of a 5-digit decimal number (nnnnn), or 3 numbers separated by dashes, i.e. Main number area - Sub number area - Unit number (M-S-U).
PDU	Protocol Data Unit
PID	Password ID Process ID Protocol ID
ping	A network tool used to determine if a target host can be reached across an IP network. Ping estimates the round-trip time and packet loss (if any) rate between hosts.
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network.

Q

Q

QoS	Quality of Service Control mechanisms that guarantee a certain level of performance to a data flow.

R

RN	Routing Number
RTR	Router Routes all types of SMS traffic.

S

SAR	Segmentation and Reassembly
SC	Site Collector System Controller
SCCP	Signaling Connection Control Part
SCF	Service Control Function
SCR	service-configuration request
SCTP	Stream Control Transmission Protocol
SCTP	Stream Control Transmission Protocol An IETF transport layer protocol, similar to TCP that sends a message in one operation. The transport layer for all standard IETF-SIGTRAN protocols. SCTP is a reliable transport protocol that operates on top of a connectionless packet network such

S

	as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.
SGP	Signaling Gateway Process A process instance of a Signaling Gateway. It serves as an active, backup, load-sharing, or broadcast process of a Signaling Gateway [RFC 4666].
SGSN	Serving GPRS Support Node
SIG	Signature service Personalized SMS signature service. This service is provided by the Mobile Messaging XS-SIG component.
SIGTRAN	The name given to an IETF working group that produced specifications for a family of protocols that provide reliable datagram service and user layer adaptations for SS7 and ISDN communications protocols. The most significant protocol defined by the SIGTRAN group was the Stream Control Transmission Protocol (SCTP), which is used to carry PSTN signalling over IP. The SIGTRAN group was significantly influenced by telecommunications engineers intent on using the new protocols for adapting VoIP networks to the PSTN with special regard to signaling applications. Recently, SCTP is finding applications beyond its original purpose wherever reliable datagram service is desired.

S

SIM	Subscriber Identity Module An ID card the size of a credit card for GSM network subscribers, and is typically referred to as a chip card or smartcard.
SIP	Session Initiation Protocol
SIPO	SIP Message Originated from a user equipment in an IMS Network
SIPT	SIP Message Terminated to a user equipment in an IMS Network.
SLC	Signaling Link Code
SM	Short Message
SmartLimit	AT&T service that provides parental control of wireless services.
SMPP	Short Message Peer-to-Peer Protocol An open, industry standard protocol that provides a flexible data communications interface for transfer of short message data.
SMS	Short Message Service
SMSC	Short Message Service Center
SNMP	Simple Network Management Protocol.

S

	An industry-wide standard protocol used for network management. The SNMP agent maintains data variables that represent aspects of the network. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups.
SPC	Secondary Point Code The SPC enables the EAGLE 5 ISS to assume more than one point code for SS7 routing. The EAGLE 5 ISS uses the SPC for routing and provisioning as if the SPC were an actual point code of the EAGLE 5 ISS. The EAGLE 5 ISS supports one ANSI true point code and up to seven secondary point codes. Spare Point Code
SPF	Subscriber Provisioning Framework The Mobile Messaging solution to enable the configuration, control and application of subscriber-specific services. The SPF provides a framework to store and retrieve service-specific data through a variety of provisioning interfaces.
SS7	Signaling System #7
SSCF	Service Specific Coordination Function The primary task of the SSCF (Service Specific Coordination Function) is to map the services provided by the lower layers of the SAAL to the needs of a specific higher layer user. For the ATM

S

	high-speed signaling link, the higher layer user is the MTP-3 protocol.
SSI	Service Subscription Information The Mobile Messaging SSI can be queried to determine the applicable personalized subscriber services of the originator and recipient of the message.
SSN	SS7 Subsystem Number The subsystem number of a given point code. The subsystem number identifies the SCP application that should receive the message, or the subsystem number of the destination point code to be assigned to the LNP subsystem of the EAGLE 5 ISS. Subsystem Number A value of the routing indicator portion of the global title translation data commands indicating that no further global title translation is required for the specified entry. Subsystem Number Used to update the CdPA.
STP	Signal Transfer Point The STP is a special high-speed switch for signaling messages in SS7 networks. The STP routes core INAP communication between the Service Switching Point (SSP) and the Service Control Point (SCP) over the network.
STV	Statistics Viewer Collects statistical data about NewNet Mobile Messaging components and displays it in the Manager.

S

SUA	SCCP User Adaptation Layer A protocol for the transport of any SCCP-User signaling over IP using the SCTP. The protocol is designed to be modular and symmetric, to allow it to work in diverse architectures.

T

TCAP	Transaction Capabilities Application Part
TCP	Transfer Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access A time division multiplex approach which assigns a fixed number of slots per round. The slots can reflect the requirements of the individual stations. If these requirements are known, TDMA can support high efficiency.
TFP	TransFer Prohibited (Msg) A procedure included in the signaling route management (functionality) used to inform a signaling point of the unavailability of a signaling route.
TFR	Transfer Restricted
TNL	NewNet Mobile Messaging Network Layer NewNet proprietary interface over which Mobile Messaging components communicate.

T

TON	Type of Number
Tools	A collection of command-line tools for managing and troubleshooting NewNet Mobile Messaging components.
TRA	Traffic Restarting Allowed
trap	A mechanism used in the context of SNMP (Simple Network Management Protocol) for one-way event notification.
TT	Translation Type Resides in the Called Party Address (CdPA) field of the MSU and determines which service database is to receive query messages. The translation type indicates which Global Title Translation table determines the routing to a particular service database.

U

UCP	Universal Computer Protocol Protocol used to connect to SMSCs.
UDH	User Data Header
UDP	User Datagram Protocol
UDT	Unitdata Transfer
UE	User Equipment

V

V

VPC	Virtual Path Connection Virtual Point Code
VSMSC	Virtual SMSC Virtual SMSC is a feature of an Acision SMSC to have separate SMS Application routing and different billing file content for MO messages with a different SMSC Address.

X

XML	eXtensible Markup Language A version of the Standard Generalized Markup Language (SGML) that allows Web developers to create customized tags for additional functionality.
XS	eXternal Service Value-adding component that communicates with the Router to provide a service.
XS-ARP	eXternal Service Auto Reply component eXternal Service component that provides SMS auto reply functionality.
XS-CPY	Short Message Copy component eXternal Service component that can send a copy of MO, MT, and AT short messages to MSISDNs.
XS-FWD	Short Message Forward component eXternal Service component that can forward short messages to MSISDNs.

X

XS-TIE	Text Insertion Engine component eXternal Service component that can insert additional text in a short message that is bound for home network subscriber.
XUDT	Extended Unit Data