

MTAS SIP Management Guide

MTAS

USER GUIDE

Copyright

© Ericsson AB 2016–2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
2	Overview	3
2.1	SIP Error Response	3
3	Session Case Determination	5
4	Change IP-Version	7
5	Change DSCP Marking Value	9
6	Change SIP Ports	11
7	SIP Parameters Configuration	13
8	SIP Traffic from Operation and Maintenance Traffic Separation	15
9	Configure DNS	17
9.1	Add DNS Entry	17
10	Call Out of the Blue	19
11	MTAS Handles OPTIONS (Ping)	21
12	Failover and Greylisting	23
13	Served User	25
14	Originating AS Chaining	27
15	Keepalive Mechanism	29
16	SIP Traffic TCP Connection Handling	33
17	Early BYE Transparent	35





1 Introduction

This document describes how to configure the Session Initiation Protocol (SIP) in the MTAS.

1.1 Prerequisites

It is assumed that the user of this document is familiar with the O&M area, in general.

1.1.1 Licenses

Not Applicable.

1.1.2 Documents

Before starting any procedure in this document, ensure that the following documents are available:

- Ericsson Command-Line Interface User Guide
- Managed Object Model (MOM)

1.1.3 Conditions

The following conditions must apply:

- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.
- The external Virtual IP (VIP) is in a configured state and its address, or addresses, are configured in the cluster configuration before changing the MtasSip Managed Object (MO).





2 Overview

SIP is the session signaling protocol in the MTAS. The MTAS supports SIP over User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

The IMS Service Control (ISC) interface connects the MTAS and the Serving Call Session Control Function (S-CSCF) node. The SIP function terminates the ISC interface on the MTAS side.

Also, the SIP function receives subdomain-routed SIP messages to services hosted by the MTAS. An MTAS service can be identified with a Public Service Identity (PSI).

The configuration of the SIP function involves defining UDP and TCP ports, where SIP messages arrive on the ISC interface. It also involves setting of a few SIP-related timers. The `MtasSip` MO controls the SIP function for an entire MTAS node.

2.1 SIP Error Response

The SIP behavior is affected when the SIP error response is set or changed for the Multimedia Telephony (MMTel), Network Announcement (NA), or Communication Barring (CB) services. A SIP error response is sent when an announcement has been played from the originating or terminating MTAS.





3 Session Case Determination

The session case for a service session handled by the MTAS is determined by the Call Session Control Function (CSCF) and can never change during the session. The CSCF signals this decision by setting the `sescase` and `regstate` attributes of the P-Served-User header, or by forwarding traffic for the different cases to specific dedicated SIP ports in MTAS. MTAS considers the P-Served-User header only when the CM attribute `mtasSipSupportPServedUserHeader` is set to 1.

For more information about the P-Served-User header, refer to [IETF RFC 5502](#).

If dedicated SIP ports are used and the P-Served-User header is required, the session case determined by the `sescase` and `regstate` attributes of the P-Served-User header overrides the receiving port, provided it is not a PSI port. Even if the session case is determined by the P-Served-User header, the selection between the Multimedia Telephony Application Server (MMTel AS) and Service Centralization and Continuity Application Server (SCC AS) triggering is still port-based.

If the generic SIP port is used on the ISC interface, the name of the AS must be specified in the route parameter `as=` included in the Route header, and the P-Served-User header must be included in the initial SIP request. Selection between MMTel AS, SCC AS, or Network AS are then decided by the AS name specified in the Route header. The `sescase` and `regstate` attributes in the P-Served-User header are used to determine the session case.

If the generic SIP port is used on the Ma interface (I-CSCF), the AS name and PSU header are not required. The AS and session case to be used for the session is identified by a PSI service.





4 Change IP-Version

To change the IP-version:

1. Deactivate the `MtasFunction` MO, as described in [MTAS VNF Management Guide](#).
2. Check that the `mtasFunctionAdministrativeState` attribute is set to 0 (Locked).
3. Navigate to the `MtasSip` MO.
4. Change the `mtasSipIpVersion` parameter to one of the following values:
 - “0” to use to IPv4
 - “1” to use to IPv6

The selected IP version is applied to the ISC, Ma, Pw, and Mr interfaces.

For a complete description of the `mtasSipIpVersion` parameter, refer to [Managed Object Model \(MOM\)](#).

5. Click **Submit**.
6. If no other configurations are to be made within the `MtasFunction` MO, activate the MTAS by setting the `mtasFunctionAdministrativeState` attribute to 1 (Unlocked) in the `MtasFunction` MO.
7. Perform a backup, as described in [Create Backup](#).

Note: The MTAS does not support the dual mode for IPv4 or IPv6. Hence the SIP ports can only bind to either IPv4 or IPv6 at a time, see [Section 6](#) on page 11.





5 Change DSCP Marking Value

The MTAS supports Differentiated Services Code Point (DSCP) marking of the outgoing SIP messages. The CM attribute `mtasSipIpDscpMarking` defines the DSCP value which is used for SIP traffic classification. The DSCP is the six most significant bits of the (former) IPv4 TOS octet or the (former) IPv6 Traffic Class octet. It is used to identify the level of service a packet receives in the network.

For more information about DSCP marking, refer to the [IETF RFC 2474](#) specification.

To change the Differentiated Services Code Point (DSCP) marking value:

1. Deactivate the `MtasFunction` MO, as described in [MTAS VNF Management Guide](#).
2. Make sure the `mtasFunctionAdministrativeState` attribute is set to 0 (Locked).
3. Navigate to the `MtasSip` MO.
4. Change the `mtasSipIpDscpMarking` attribute to the desired value (0-63). This selected DSCP value is applied to the ISC, Ma, Pw, and Mr interfaces.

For a complete description of the `mtasSipIpDscpMarking` attribute, refer to [Managed Object Model \(MOM\)](#).

5. Click **Submit**.
6. If no other configurations are to be made within the `MtasFunction` MO, activate the MTAS by setting the `mtasFunctionAdministrativeState` attribute to 1 (Unlocked) in the `MtasFunction` MO.
7. Perform a backup, as described in [Create Backup](#).





6 Change SIP Ports

To change the SIP ports:

1. Deactivate the MtasFunction MO, as described in [MTAS VNF Management Guide](#).
2. Make sure that the mtasFunctionAdministrativeState attribute is set to 0 (Locked).
3. Navigate to the MtasSip MO.
4. Change one or all the following parameters:

General

- mtasSipAsGenericPort
- mtasSipPsiPort
- mtasSipPresencePort

MMTel Traffic

- mtasSipTrafficOriginatingIpPort
- mtasSipTrafficOrigUnregIpPort
- mtasSipTrafficTerminatingIpPort
- mtasSipTrafficTermUnregIpPort

SCC traffic

- mtasSipSccOrigPort
- mtasSipSccOrigUnregPort
- mtasSipSccTermPort
- mtasSipSccTermUnregPort

For a complete description of the parameters, refer to [Managed Object Model \(MOM\)](#).

5. Click **Submit**.
6. If no other configurations are to be made within the MtasFunction MO, activate the MTAS by setting the mtasFunctionAdministrativeState attribute to 1 (Unlocked) in the MtasFunction MO.



7. To open traffic for a new port number, remove VIP Mappings for old UDP and TCP port number, and then insert VIP Mappings with the same data for the new UDP and TCP port number. This is for the used protocol, either IPv4 or IPv6.
For information on VIP Mappings, refer to [Virtual IP Address Management](#).
8. Perform a backup, as described in [Create Backup](#).



7 SIP Parameters Configuration

The MtasSip MO makes it possible to configure other parameters relating to the SIP management. For a complete description of the parameters, refer to [Managed Object Model \(MOM\)](#).





8 SIP Traffic from Operation and Maintenance Traffic Separation

It is possible to separate SIP traffic from O&M traffic, using different VIP addresses. For details about how to add VIP to a live system, and to add aliases in Domain Name System (DNS), refer to cluster configuration. Limitation: cluster configuration is not available in the CPI yet.





9 Configure DNS

If the MTAS needs to look up a hostname, the DNS Resolver is used.

The `DnsLocalAddress` parameter is to be configured such that the DNS communication with the Name Server is displayed on the SIP traffic interface.

Note: On receipt of a truncated DNS response using UDP, MTAS resends the DNS query using TCP.

9.1 Add DNS Entry

Add the DNS entry “+tasvip4” and the “tasvip6” depending on the used IP version.

Note: Always define the “tasvip6” entry, even if it is not used.





10 Call Out of the Blue

The MTAS supports generation of out of the blue initial requests, CM parameter `mtasSipCallOutOfBlueRouting`. The MTAS can send Call Out Of the Blue (COOB) SIP requests direct to the I-CSCF for onward routing in the IMS network. The identity of the I-CSCF used to route messages is configured in CM parameter `mtasSipIcscfName`.

For more information, refer to [Managed Object Model \(MOM\)](#).





11 MTAS Handles OPTIONS (Ping)

The MTAS can receive an OPTIONS request outside a dialog that addresses the MTAS. If MTAS receives an OPTIONS request from a node (usually a CSCF node) that addresses the MTAS as defined by the CM attribute `mtasSipOptionsUri` (a list of URIs), then the MTAS sends a 200 OK as an answer to this OPTIONS (ping) request without any SDP body.

For more information, refer to [Managed Object Model \(MOM\)](#).





12 Failover and Greylisting

When acting as User Agent Client (UAC), the MTAS supports DNS-based redundancy of the next hop SIP server (proxy or User Agent Server (UAS)). When more than one IP address is received from the DNS, the request is resent to the next address if the connection to the first one cannot be established because of connectivity problems, or the request encounters time out.

For more information about DNS configuration, refer to [Managed Object Model \(MOM\)](#).

The failover time-out is defined by the CM attributes `mtasSipFailoverTimeInvite` and `mtasSipFailoverTimeNonInvite`. The failed server is inserted in a Greylist for a configurable time period defined by the CM attributes `IcmpBarringTime` and `mtasFunctionBlackListTime`; that is, the server is used for new requests only when there is no other non-greylisted server or the request sending to all non-greylisted servers has failed.

Table 1 shows the events indicating unreachability and the corresponding timer.

Table 1 Selection of Greylisting Timer Value

Event	Greylisting
ICMP Destination Unreachable (3), net unreachable (0)	<code>IcmpBarringTime</code>
ICMP Destination Unreachable (3), host unreachable (1)	<code>IcmpBarringTime</code>
ICMP Destination Unreachable (3), protocol unreachable (2)	<code>IcmpBarringTime</code>
ICMP Destination Unreachable (3), port unreachable (3)	<code>IcmpBarringTime</code>
ICMP Parameter Problem (12)	<code>IcmpBarringTime</code>
Socket error 52 – Network is unreachable	<code>mtasFunctionBlackListTime</code>
Socket error 61 – Connection refused	<code>mtasFunctionBlackListTime</code>
Socket error 62 – Host is down	<code>mtasFunctionBlackListTime</code>
Socket error 63 – No route to host	<code>mtasFunctionBlackListTime</code>
SIP Transaction time-out (only for INVITE)	<code>mtasFunctionBlackListTime</code>
SIP 503 Response without Retry-After	<code>mtasFunctionBlackListTime</code>
SIP 503 Response with Retry-After	Value of Retry-After header



Whenever a failover is attempted the `MtasFuncFailover` Performance Management (PM) counter is stepped.

The following preconditions must be fulfilled for supporting the failover procedure:

- The IP address: port of the next hop in the Route header is looked up from DNS if the domain name is equal to the value of the `mtasSipIcscfName` or `mtasIdPresCnipCnameServerName` CM attribute. DNS lookup is also applied for messaging on Mr interface or CAT.
- The request creates a Dialog.
- More than one IP address is returned in the DNS response.

The following preconditions must be fulfilled for being subject of the greylisting procedure:

- The IP address: port of the next hop in the Route header is looked up from DNS if the domain name is equal to the value of the `mtasSipIcscfName` or `mtasIdPresCnipCnameServerName` CM attribute. DNS lookup is also applied for messaging on Mr interface or CAT.
- The request failed because of connectivity problems, or the request was an INVITE and the failover timer expired, or a 503 Response is received from the server.

For more information about failover and greylisting, refer to the following documents:

- Managed Object Model (MOM)
- MTAS External Network Configuration



13 Served User

The MTAS can be configured to support the P-Served-User header received in initial requests, with the CM parameter `mtasSipSupportPServedUserHeader`.

This attribute specifies if the P-Served-User headers must be supported. When supported, the served user must be determined from the P-Served-User header when available. Otherwise the served user is determined from the P-Asserted-Id for the originating session case and from the Request URI for the terminating session case.

The served user is the user that originated the request, the user the request was originated on behalf of, or the user the request was terminated on.

For a complete description of the parameters, refer to [Managed Object Model \(MOM\)](#).





14 Originating AS Chaining

The MTAS can be configured to support external triggering of originating services after retargeting, to enable AS chaining, with the CM parameter `mtasSipOriginatingAsChaining`.

The P-Served-User header must be enabled and used by the S-CSCF for Originating AS chaining to work.

When Originating AS chaining is disabled:

- The MTAS triggers originating services after retargeting internally in the MTAS for the terminating session case. There is no AS chaining before the session is routed towards the new target.
- For call out of blue sessions, the MTAS indicates terminating behavior either by not including the “orig” Route parameter or by setting the `noifc=orig` parameter in the Request URI.

When Originating AS chaining is enabled:

- The INVITE is returned to the S-CSCF after retargeting, the S-CSCF initiates triggering of originating services by sending the INVITE to the terminating AS for an originating session case. AS chaining can then be performed before the session is routed towards the new target.
- For call out of blue sessions, the MTAS indicates originating behavior by including the “orig” Route parameter and the P-Served-User header.

Examples for retargeting of sessions are all types of Communication Diversion. For call out of blue sessions, the Adding participant to Conference and Flexible Call Distribution options are available.

For a complete description of the parameters, refer to [Managed Object Model \(MOM\)](#).





15 Keepalive Mechanism

The MTAS supports a Session Keep Alive mechanism based on the SIP Session Timer extension.

For more information about the SIP Session Timer extension, refer to [IETF RFC 4028](#).

The MTAS handles the session timer for each SIP dialog in isolation. There is no session timer information passed between different dialogs. Therefore, a session timer can be enabled on one SIP dialog while disabled on another SIP dialog. It can also be enabled on different dialogs but with different timer expiry values. When the MTAS sends the initial INVITE, it forms the headers relevant for the session timer extension according to the current configuration information, regardless of how session timers are used on other dialogs. The MTAS is flexible in this respect and adapts to the other entities in the SIP signaling path.

The following CM attributes are used by the MTAS to control the normal keepalive handling:

- Min-SE is the shortest possible session interval acceptable to the MTAS. Any INVITE request proposing a lower value is rejected by a 422 Session Interval Too Small response.
- Session-Expires is the preferred session interval. If an INVITE request is received proposing a higher value, the MTAS reduces the session interval to its configured value or the value of the Min-SE header in the received INVITE, whichever is highest. The value of the attribute Session-Expires is used also in the sent INVITES.

To prevent stale end-to-end session from using system recourses, MTAS terminates end-to-end sessions that are not modified or refreshed if there is no signaling during 24 hours. To avoid terminating end-to-end sessions that are active, they must be periodically refreshed, for example by the use of session timers. To prevent the scenario where there is no session timer started on a dialog, for example, where an extension is not being supported by the SIP clients, a session timer is always started when an INVITE, with exception of the initial INVITE, or an UPDATE request or 200 OK for an INVITE or an UPDATE is received even if not requested in the message. The session-interval is in this case the value configured in the attribute `mtasSipDefaultSessionExpiry`, if it is not set to 0. This behavior can be disabled by setting the attribute `mtasSipSuperviseAllSessions` to 0 (false). Disabling the session timer thus introduces a limitation on the duration of an end-to-end session to 24 hours (unless the session is modified or refreshed before this time limit expires). A summary of how the different configuration settings affect the behavior is shown in Table 2.

Table 2 MTAS Behavior Depending on Attribute-Values of `mtasSipSuperviseAllSessions` and `mtasSipDefaultSessionExpiry`

<code>mtasSipSuperviseAllSessions</code>	<code>mtasSipDefaultSessionExpiry</code>	MTAS Behavior
1	≥ 90	A session timer is always started when an INVITE (except initial INVITE) or an UPDATE request or 200 OK for an INVITE or an UPDATE is received even if not requested in the message. The session-interval is in this case the value configured in the attribute <code>mtasSipDefaultSessionExpiry</code> .
1	0	No session timer is started unless the other nodes request it and contains a valid Session-Expires interval in their requests or responses.
0	Any value	MTAS terminates end-to-end sessions that are not modified or refreshed within 24 hours. MTAS does not start a session timer when an INVITE or an UPDATE request or 200 OK for an INVITE or an UPDATE is received if not requested in the message.

It is also possible to force both-way, end-to-end keepalive sending for User Equipment (UE) sessions, by setting the attribute `mtasSipUeSessionTimerSupport` to 0 (false). When the keepalive mechanism is suppressed, the MTAS acts in the following way:

- The MTAS ignores the Session Timer related headers, Session-Expires and Min-SE, and feature tag (timer) in the received SIP messages (both requests and responses) and does not start session timer procedures.
- The MTAS does not include Session Timer related headers and feature tag in the sent SIP messages (both requests and responses).



- The MTAS passes on the received Session Refresh messages, re-INVITE/200 OK/ACK or UPDATE/200 OK, from the incoming dialog to the outgoing dialog or from the outgoing dialog to the incoming dialog.

Note: Forcing the both-way, end-to-end keepalive sending for UE sessions have no effect on the keepalive mechanism used in the non-UE sessions, for example, sessions to the external Media Resource Function Controller (External MRFC) or to the Customized Alerting Tones Server.





16 SIP Traffic TCP Connection Handling

The SIP traffic-related TCP connections are handled by the SipDistributor. The connection is released by MTAS if a connection is in the idle state for a period of time. The duration is configurable through the CM `mtasSipTcpConnectionTimeout` parameter. For a complete description of the parameter, refer to *Managed Object Model (MOM)*.

The TCP connection is bound to source IP address, source port, destination IP address, destination port, and session case. Session case usually means O-MMTelAS, T-MMTelAS, O-SCCAS, T-SCCAS, and so on, and is determined by the top port of the Via header in the outgoing SIP messages.

Each SipDistributor has its own TCP connection handling, which contains the connections created by both the peer node (CSCF) and MTAS. For sending out the SIP messages, each SipDistributor tries to reuse the existing TCP connection.

Reuse of existing TCP connection works as follows:

- The destination IP address of the outgoing SIP message is compared to the stored remote IP addresses of the TCP connection.
- The destination port of the outgoing SIP message is compared to the stored remote ports of the TCP connection.
- The session case of the outgoing SIP message (determined by the top port of the Via header) is compared to the stored session cases of the TCP connection.

Providing the IP address, if destination port and session case are matched, then the TCP connection is reused. Otherwise, a new TCP connection is created. For the outgoing SIP requests, the top port of the Via header is usually related to the arriving port of its corresponding incoming message. For the outgoing SIP responses, it needs to use the same TCP connection as its request, if not, it is lost.

The total number of MTAS-created TCP connections is calculated as follows:

$(\text{Number of SipDistributors}) * (\text{Number of destination CSCFs}) * (\text{MTAS session case})$

The following are descriptions of the factors:

- Number of SipDistributors equals to $(\text{number of PLs}) * (\text{number of vCPUs})$
- Number of destination CSCFs equals to the same destination CSCF IP address and same CSCF port
- MTAS session cases are determined by the top port of the Via header.





17 Early BYE Transparent

The MTAS supports transparent early BYE forward. The CM attribute `mtasSipTransparentEarlyBye` defines whether it is enabled or disabled.

To change the early BYE transparent behavior:

1. Deactivate the `MtasFunction` MO, as described in the [MTAS Node Management Guide](#).
2. Make sure the `mtasFunctionAdministrativeState` attribute is set to 0 (Locked).
3. Navigate to the `MtasSip` MO.
4. Change the `mtasSipTransparentEarlyBye` attribute to one of the following values:

0 to disable early BYE transparent

1 to enable early BYE transparent

For a complete description of the `mtasSipTransparentEarlyBye` parameter, refer to [Managed Object Model \(MOM\)](#).

5. Click **Submit**.
6. If no other configurations are to be made within the `MtasFunction` MO, activate the MTAS by setting the `mtasFunctionAdministrativeState` attribute to 1 (Unlocked) in the `MtasFunction` MO.
7. Perform a backup, as described in [Create Backup](#).