

MTAS IPv6 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	Traffic Impact	4
3	IPv6 Configuration	5
3.1	VIP IPv6 Addresses Configuration in the System	8
3.2	Deactivate MTAS	9
3.3	Add Provisioning IPv6 Addresses	9
3.4	Add Diameter IPv6 Address	10
3.5	MTAS Configuration	12





1 Introduction

This document describes how to enable and configure IPv6 for the MTAS towards its peer nodes.

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

No licenses are needed.

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)*
- *Signaling Manager User Guide*

1.1.3 Conditions

The following conditions must apply:

- An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.
- The Signaling Manager is connected.





2 Overview

The MTAS can be configured to use either IPv4 or IPv6 for the interfaces supporting IPv6. The external Media Resource Function Controller (MRFC) must use the same IP version as supported by the interfaces to the Serving CSCF (S-CSCF) and Interrogating CSCF (I-CSCF) (IPv6). External MRFC uses SIP and therefore supports IPv6.

The MTAS can use either IPv4 or IPv6 for the H.248 messages on the Mp interface, depending on the capabilities of the MRFC. This also applies towards the Media Resource Function Processor (MRFP), depending on its capabilities.

More interfaces supporting the IPv6 are shown in Figure 1.

IPv4 and IPv6 cannot be used in parallel on the same “logical” interface by the MTAS. It is possible to configure both IPv6 and IPv4 on the same physical interfaces, for more information, refer to *MTAS SW Installation*.

It is recommended to configure the MTAS with IPv6 after the CSCF and HSS have been configured with IPv6. It is also recommended to remove the A Resource Record in Domain Name System (DNS) server for the MTAS that is connected to the DNS SRV Resource Record used for the MTAS on the ISC interface.

The external interfaces used by the MTAS and whether they support either IPv4 or IPv6, or both, are shown in Figure 1.

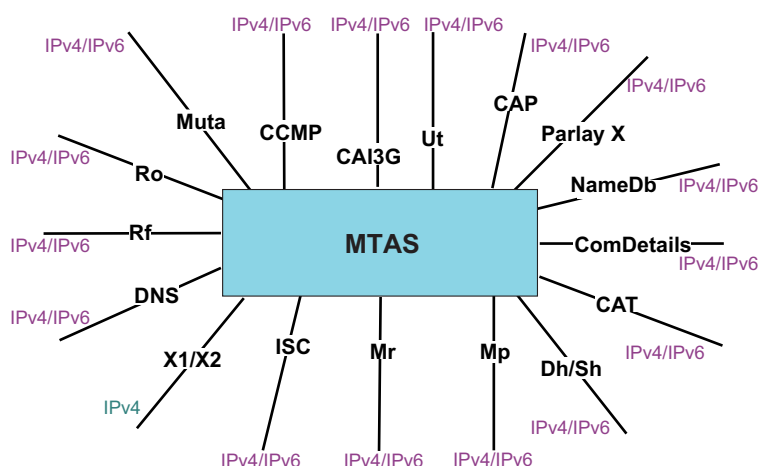


Figure 1 MTAS Interfaces with Supported IP-Protocol Versions



2.1 Traffic Impact

Implementing IPv6 on the MTAS has some impact on the traffic, since the MTAS must be deactivated before it can be configured. Therefore, the traffic must be moved to the secondary MTAS before starting to implement IPv6 on the primary MTAS.

When the implementation is finished, the primary MTAS must be activated before moving back the traffic from the secondary MTAS. After that the user can implement IPv6 on the secondary MTAS.



3 IPv6 Configuration

IPv6 configuration includes the following main activities:

- Adding Diameter IPv6 addresses
- MTAS Configuration

The IP configuration attributes are shown in Table 1.

Table 1 IP Configuration Attributes

Name	Value	Description
platform-vip (IPv4)	____.____.____.____ (for example 10.64.93.116)	<p>The external VIP address of the O&M network using transport protocol IPv4.</p> <p>Observe that a node can use either IPv4, IPv6, or both, as follows:</p> <ul style="list-style-type: none"> • If IPv4 is being used, specify the valid address. • If IPv4 is not being used, specify the value "0.0.0.0". <p>For an explanation of the VIP address concept, refer to <i>Virtual IP Address Management</i>.</p>
platform-vip6 (IPv6)	____:____:____:____:____:____:____:____ (for example 2001:1B70:8294:3d00::3130)	<p>The external VIP address of the O&M network using transport protocol IPv6.</p> <p>Observe that a node can use either IPv4, IPv6, or both, as follows:</p> <ul style="list-style-type: none"> • If IPv6 is being used, specify the valid address. • If IPv6 is not being used, specify the value: "::". <p>For an explanation of the VIP address concept, refer to <i>Virtual IP Address Management</i>.</p>



Table 1 IP Configuration Attributes

Name	Value	Description
cai3g-vip4 (IPv4)	____.____.____.____ (for example 10.64.93.119)	<p>The external VIP address of the CAI3G interface using transport protocol IPv4.</p> <p>Observe that a node can use either IPv4, IPv6, or both, as follows:</p> <ul style="list-style-type: none">• If IPv4 is being used, specify the valid address.• If IPv4 is not being used, specify the value "0.0.0.0". <p>For an explanation of the VIP address concept, refer to <i>Virtual IP Address Management</i>.</p>
cai3g-vip6 (IPv6)	__:__:__:__:__:__:__ (for example 2001:1B70:8294:3d00::3133)	<p>The external VIP address of the CAI3G interface using transport protocol IPv6.</p> <p>Observe that a node can use either IPv4, IPv6, or both, as follows:</p> <ul style="list-style-type: none">• If IPv6 is being used, specify the valid address.• If IPv6 is not being used, specify the value: "::". <p>For an explanation of the VIP address concept, refer to <i>Virtual IP Address Management</i>.</p>
tasvip4 (IPv4)	____.____.____.____ (for example 10.64.93.117)	<p>The VIP address of the traffic network using transport protocol IPv4.</p> <p>Observe that a node can use either IPv4, IPv6, or both, as follows:</p> <ul style="list-style-type: none">• If IPv4 is being used, specify the valid address.• If IPv4 is not being used, specify the value "0.0.0.0". <p>For an explanation of the VIP address concept, refer to <i>Virtual IP Address Management</i>.</p>



Table 1 IP Configuration Attributes

Name	Value	Description
tasvip6 (IPv6)	__:__:__:__:__:__:__ (for example 2001:1B70:8294:3d00::3 131)	<p>The VIP address of the traffic network using transport protocol IPv6.</p> <p>Observe that a node can use either IPv4, IPv6, or both, as follows:</p> <ul style="list-style-type: none"> • If IPv6 is being used, specify the valid address. • If IPv6 is not being used, specify the value: “:”. <p>For an explanation of the VIP address concept, refer to <i>Virtual IP Address Management</i>.</p>
ut-vip4 (IPv4)	____.____.____.____ (for example 10.64.93.118)	<p>The external VIP address of the Ut interface using transport protocol IPv4.</p> <p>Observe that a node can use either IPv4, IPv6, or both, as follows:</p> <ul style="list-style-type: none"> • If IPv4 is being used, specify the valid address. • If IPv4 is not being used, specify the value “0.0.0.0”. <p>For an explanation of the VIP address concept, refer to <i>Virtual IP Address Management</i>.</p>
ut-vip6 (IPv6)	__:__:__:__:__:__:__ (for example 2001:1B70:8294:3d00::3 132)	<p>The external VIP address of the Ut interface using transport protocol IPv6.</p> <p>Observe that a node can use either IPv4, IPv6, or both, as follows:</p> <ul style="list-style-type: none"> • If IPv6 is being used, specify the valid address. • If IPv6 is not being used, specify the value: “:”. <p>For an explanation of the VIP address concept, refer to <i>Virtual IP Address Management</i>.</p>



Table 1 IP Configuration Attributes

Name	Value	Description
sigtran1-vip4 sigtran2-vip4 (IPv4)	____.____.____.____ (for example 10.64.93.120) ____.____.____.____ (for example 10.64.93.121)	<p>The external VIP addresses of the CAP interface using transport protocol IPv4. Both of them must be used.</p> <p>Observe that a node can use either IPv4, IPv6, or both, as follows:</p> <ul style="list-style-type: none"> • If IPv4 is being used, specify the valid address. • If IPv4 is not being used, specify the value “0.0.0.0”. <p>For an explanation of the VIP address concept, refer to <i>Virtual IP Address Management</i>.</p>
sigtran1-vip6 sigtran2-vip6 (IPv6)	_:_:_:_:_:_:_:_ (for example 2001:1B70:8294:3d00::3 134) _:_:_:_:_:_:_:_ (for example 2001:1B70:8294:3d00::3 135)	<p>The external VIP addresses of the CAP interface using transport protocol IPv6. Both of them must be used.</p> <p>Observe that a node can use either IPv4, IPv6, or both, as follows:</p> <ul style="list-style-type: none"> • If IPv6 is being used, specify the valid address. • If IPv6 is not being used, specify the value: “:”. <p>For an explanation of the VIP address concept, refer to <i>Virtual IP Address Management</i>.</p>

3.1 VIP IPv6 Addresses Configuration in the System

This section describes how to configure VIP IPv6 addresses in the system.

3.1.1 Add VIP IPv6 Address to the System

To add a VIP IPv6 address to the system, refer to *Virtual IP Address Management*.

3.1.2 Backup after Adding VIP Address

To create a backup, refer to *Create Backup* and *System Backup and Restore*.



3.1.3 Health Check

After adding a VIP address, ensure that the MTAS is operational by performing a health check, refer to *MTAS Health Check*.

3.2 Deactivate MTAS

Before IPv6 configuration is performed, the MTAS must be deactivated.

To deactivate MTAS before IPv6 implementation:

1. Move the traffic to the secondary MTAS.
2. Deactivate the MTAS, refer to Section *Deactivating MTAS* in *MTAS VNF Management Guide*.

Note: It is recommended to deactivate the MTAS gracefully.

3.3 Add Provisioning IPv6 Addresses

This section describes how to add and connect Provisioning IPv6 addresses.

3.3.1 Add CAI3G IPv6 Addresses

This section describes how to add CAI3G IPv6 addresses.

3.3.1.1 Update cluster.conf and Reboot the Cluster

1. Log on to SC-1:

```
ssh <maintenance_user>@<OAM VIP>
```

2. Edit the `/cluster/etc/cluster.conf` file and add the following lines to the SITE SPECIFIC AND SOLUTION INTEGRATION PARAMETERS section (above the tag Other settings for instance). Replace the tags in “<>” with the correct IP addresses:

```
host all <cai3g-vip6> cai3g-vip6
```

3. Save the file and exit the editor.
4. Reload cluster.conf by executing the following command:

```
SC-1:~ # cluster config -r
```

5. Reload the cluster by executing the following command:

```
SC-1:~ # cluster reboot -a
```



3.3.2 Add Ut IPv6 Addresses

This section describes how to add Ut IPv6 addresses.

3.3.2.1 Update cluster.conf and Reboot the Cluster

1. Log on to SC-1:

```
ssh <maintenance_user>@<OAM VIP>
```

2. Edit the `/cluster/etc/cluster.conf` file and add the following lines to the SITE SPECIFIC AND SOLUTION INTEGRATION PARAMETERS section (above the tag Other settings for instance). Replace the tags in “<>” with the correct IP addresses:

```
host all <ut-vip6> ut-vip6
```

3. Save the file and exit the editor.
4. Reload cluster.conf by executing the following command:

```
SC-1:~ # cluster config -r
```

5. Reload the cluster by executing the following command:

```
SC-1:~ # cluster reboot -a
```

3.4 Add Diameter IPv6 Address

This section describes how to add and connect Diameter IPv6 addresses.

3.4.1 Add CAI3G IPv6 Addresses

This section describes how to add CAI3G IPv6 addresses.

3.4.1.1 Update cluster.conf and Reboot the Cluster

1. Log on to SC-1:

```
ssh <maintenance_user>@<OAM VIP>
```

2. Edit the `/cluster/etc/cluster.conf` file and add the following lines to the SITE SPECIFIC AND SOLUTION INTEGRATION PARAMETERS section (above the tag Other settings for instance). Replace the tags in “<>” with the correct IP addresses:

```
host all <cai3g-vip6> cai3g-vip6
```

3. Save the file and exit the editor.
4. Reload cluster.conf by executing the following command:



```
SC-1:~ # cluster config -r
```

5. Reload the cluster by executing the following command:

```
SC-1:~ # cluster reboot -a
```

3.4.2 Add Ut IPv6 Addresses

This section describes how to add Ut IPv6 addresses.

3.4.2.1 Update cluster.conf and Reboot the Cluster

1. Log on to SC-1:

```
ssh <maintenance_user>@<OAM VIP>
```

2. Edit the `/cluster/etc/cluster.conf` file and add the following lines to the SITE SPECIFIC AND SOLUTION INTEGRATION PARAMETERS section (above the tag Other settings for instance). Replace the tags in “<>” with the correct IP addresses:

```
host all <ut-vip6> ut-vip6
```

3. Save the file and exit the editor.
4. Reload cluster.conf by executing the following command:

```
SC-1:~ # cluster config -r
```

5. Reload the cluster by executing the following command:

```
SC-1:~ # cluster reboot -a
```

3.4.3 Disable Own Node

Disable the own node, refer to *Configure Own Node*.

3.4.4 Add IPv6 to Own Node

Add IPv6 to the own node for Diameter, refer to *Configure Own Node*.

An example of the input when adding IPv6 to the own node for Diameter is shown in Example 1.

```
objectClass: DIA-CFG-NeighbourNode
ipAddressesList: 0:2001:1B70:4292:0251::71
```

Example 1 IPv6 to Own Node Added for TCP



3.4.5 Add IPv6 to Peer Node

Add IPv6 to the peer node for Diameter, refer to *Configure Peer Node and Connections*.

An example of how to add IPv6 to the peer node is shown in Example 2.

```
objectClass: DIA-CFG-NeighbourNode  
ipAddressesList: 0:2001:1B70:4292:0251::73
```

Example 2 IPv6 to Peer Node Adding for TCP

3.4.6 Enable Own Node

Enable the own node, refer to *Configure Own Node*.

3.4.7 Create New Peer Node Connection with IPv6

Create a peer node connection with IPv6, refer to *Configure Peer Node and Connections*.

An example on how to create a peer node connection with IPv6 is shown in Example 3.

```
objectClass: DIA-CFG-Conn  
ipAddressesList: 0:2001:1B70:4292:0251::73
```

Example 3 Create New Peer Node Connection with IPv6

When the IPv6 connections are made, the existing IPv4 connections can be deleted if necessary.

3.4.8 Create Backup after MTAS Configuration

Create a backup, refer to *Create Backup and System Backup and Restore*.

3.5 MTAS Configuration

This section describes the configuration of the MTAS interfaces towards peer nodes and how to change these nodes to IPv6.

Note: To be able to configure the peer nodes, the MTAS must be deactivated. Before the MTAS is activated, the peer nodes must be configured with IPv6 on the affected interfaces.

For more information about the MTAS IP-specific attributes, refer to *Managed Object Model (MOM)*.



3.5.1 SIP Configuration

The `mtasSipIpVersion` configures the MTAS to use IPv6 for SIP for the interfaces ISC, Ma, Mr, and Pw. This attribute must be set to 1 since only one IP version (IPv6 only) can be used.

Check that the `mtasSipIcscfName` attribute is an FQDN.

Change to IPv6 for SIP, refer to Section *Changing IP-version* in *MTAS SIP Management Guide*.

3.5.2 H.248 Configuration

The `mtasMpControllerIpVersion` attribute defines what type of IP protocol the MTAS uses for H.248 messages on the Mp interface towards the MRFP. Whether MTAS supports IPv6 or IPv4 towards the MRFP, depend on the capabilities of the MRFC.

The External MRFC uses SIP and can therefore handle IPv6.

To change the IP protocol version for the MRFC, refer to *MTAS Media Control Management Guide*.

3.5.3 Parlay X Configuration

The `mtasParlayXIpVersion` attribute defines what type of IP protocol the MTAS uses on both the Parlay X interface and the Cr interface. If peers of these interfaces use IPv6, this attribute must be changed for IPv6. The Cr interface is used together with Mr interface for External MRFC deployment.

To change the value of the attribute, refer to *MTAS Parlay X Management Guide*.

3.5.4 NameDB Configuration

The `MtasIdPres.mtasIdPresDbIpVersion` attribute defines the type of IP protocol the MTAS uses for sending and receiving SOAP messages on the NameDb interface to a Calling Name Server. If the Calling Name Server uses IPv6, this attribute must be changed for IPv6.

To change the IP protocol version of the Calling Name Server, refer to *MTAS Calling Name Identity Presentation Management Guide*.

3.5.5 DNS Configuration

The MTAS can use either IPv4 or IPv6 to communicate with the DNS. The IPv6 addresses for the DNS servers must be added if IPv6 is the preferred network protocol.



For more information about the DNS attributes for common components, refer to *Managed Object Model (MOM)*.

To identify the Diameter object for the DNS LDAP object:

1. Supply the distinguished LDAP name for the DNS object. Enter the MTAS address as local address and one or several (one primary and one or several secondary) DNS servers:

```
dn: applicationName=DNS, nodeName=<applNodeName>
```

An example of how to configure DNS for IPv6 is shown in Example 4.

```
dn: applicationName=DNS, nodeName=jambala
DnsLocalAddress: [2001:1B70:4292:0251::76]
objectClass: DNS-Application
DnsServerEntry: 0:[2001:1B70:4292:0250::4]:53
DnsServerEntry: 1:[2001:1B70:4292:0251::6]:53
```

Example 4 Configure DNS

3.5.6 Perform Health Check

Before activating the MTAS, ensure that the MTAS is operational by performing a health check, refer to *MTAS Health Check*.

3.5.7 Activate MTAS

After IPv6 configuration for the MTAS is performed, the MTAS must be activated.

To activate the MTAS:

1. Activate the MTAS, refer to Section *Activating MTAS* in *MTAS VNF Management Guide*.
2. Move the traffic from the secondary MTAS to this MTAS.

3.5.8 Perform a Backup of MTAS

Perform a backup, refer to *Create Backup* and *System Backup and Restore*.