



CHAPTER 22

SIGTRAN-M3UA

SIGTRAN, a working group of the Internet Engineering Task Force (IETF), has defined a protocol for the transport of real-time signaling data over IP networks. Cisco Prime AR supports SS7 messaging over IP (SS7oIP) via SIGTRAN-M3UA, a new transport layer which leverages Stream Control Transmission Protocol (SCTP). Cisco Prime AR supports SIGTRAN-M3UA to fetch the authentication vectors from HLR, which is required for EAP-AKA/EAP-SIM authentication.



Note

You have SIGTRAN-M3UA interface support in addition to the existing SUA interface support.

The EAP-AKA and EAP-SIM authentication service is extended to use M3UA. When using M3UA service for authentication, the subscriber identity (IMSI) is used to send a request to HLR and receives information from HLR containing the authentication information for authenticating an user. The authentication service initiates a request to the SIGTRAN server using IMSI, which retrieves the configured number of authentication vectors from HLR, i.e Triplets or Quintets.

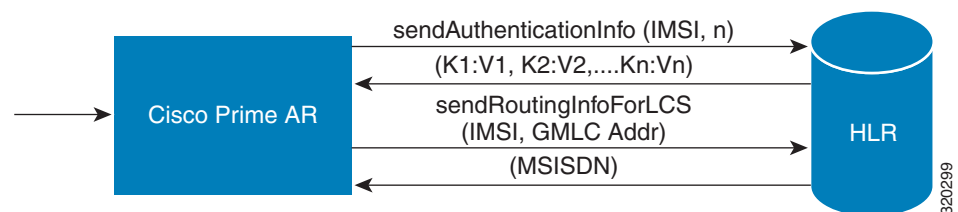


Note

When you install SIGTRAN-M3UA remote server for the first time or update the existing installation, you need to update the ip address of Cisco Prime AR where it is been installed in *network.data* and *cli_client.conf* files. Also, you must restart Cisco Prime AR to have the changes reflected.

If the LocalSubSystemNumber is not set as SGSN(149), you need to make the same change in the *default.xml* file, located at */cisco-ar/m3ua-cfg/*.

Figure 22-1 **MAP Service**



The Cisco Prime AR server initiates the MAP service. After enabling the MAP service, the Cisco Prime AR server sends a *sendAuthenticationInfo* request that contains IMSI and the number of requested authentication vectors to HLR. The HLR sends a response containing the requested vectors information

to Cisco Prime AR. Next, the Cisco Prime AR server sends a `sendRoutinginfoForLCS` request that contains IMSI and the GMLC address to HLR. The HLR sends a response containing the MSISDN information for authenticating the mobile subscribers.

**Note**

Cisco Prime AR 6.0 supports only one remote server with the protocol type, SIGTRAN-M3UA.

This section describes the following:

- [Prerequisites to SIGTRAN-M3UA](#)
- [Configuring EAP-AKA/EAP-SIM with SIGTRAN-M3UA](#)
- [Configuring M3UA Service](#)

Prerequisites to SIGTRAN-M3UA

Before enabling the SIGTRAN-M3UA remote server, you must do the following:

- ensure that LKSTCP is not available in the Cisco Prime AR server.
- ensure to restart the Cisco Prime AR server whenever you make any configuration changes.
- ensure that the following rpm files are not installed while installing the Cisco Prime AR in RHEL 6.2:
 - `nss-softokn-freebl-3.12.9-11.el6.i686.rpm`
 - `glibc-2.12-1.47.el6.i686.rpm`
 - `ncurses-libs-5.7-3.20090208.el6.i686.rpm`
 - `ncurses-devel-5.7-3.20090208.el6.i686.rpm`
 - `ncurses-5.7-3.20090208.el6.i686.rpm`
 - `nspr-4.8.8-3.el6.i686.rpm`
 - `nss-util-3.12.10-2.el6.i686.rpm`
- ensure that the following rpm files are installed while installing the Cisco Prime AR in RHEL 6.2:
 - `nss-softokn-freebl-3.12.9-11.el6.i686.rpm`
 - `glibc-2.12-1.47.el6.i686.rpm`
 - `ncurses-libs-5.7-3.20090208.el6.i686.rpm`
 - `ncurses-devel-5.7-3.20090208.el6.i686.rpm`
 - `ncurses-5.7-3.20090208.el6.i686.rpm`
 - `nspr-4.8.8-3.el6.i686.rpm`
 - `nss-util-3.12.10-2.el6.i686.rpm`
 - `gamin-0.1.10-9.el6.i686.rpm`
 - `libselinux-2.0.94-5.2.el6.i686.rpm`
 - `glib2-2.22.5-6.el6.i686.rpm`
 - `zlib-1.2.3-27.el6.i686.rpm`
 - `libxml2-2.7.6-4.el6.i686.rpm`
 - `gdome2-0.8.1-1.i386.rpm`
 - `glib-1.2.10-33.el6.i686.rpm`

- libgcc-4.4.6-3.el6.i686.rpm
- libstdc++-4.4.6-3.el6.i686.rpm

**Note**

You must install the rpm versions relevant to the RHEL OS versions while installing the Cisco Prime AR.

Configuring EAP-AKA/EAP-SIM with SIGTRAN-M3UA

You can use `aregcmd` to create and configure the service of type `eap-aka` or `eap-sim`, see [EAP-AKA](#) or [EAP-SIM](#) for more information.

To configure EAP-AKA service with SIGTRAN-M3UA remote server:

-
- Step 1** Launch `aregcmd`.
- Step 2** Create an EAP-AKA service.
- ```
cd /Radius/Services

add eap-aka-service
```
- Step 3** Set type as `eap-aka`.
- ```
set eap-aka
```
- Step 4** Add `m3ua` remote server in the `remoteServers`
- ```
cd remoteServers/

Set 1 m3ua
```
- 

The following shows an example configuration for EAP-AKA service with SIGTRAN-M3UA remote server support, see [Table 9-1](#) to know more about EAP-AKA service properties.

```
[//localhost/Radius/Services]
 Entries 1 to 2 from 2 total entries
 Current filter: <all>

 eap-aka/
 Name = eap-aka
 Description =
 Type = eap-aka
 AlwaysRequestIdentity = False
 EnableIdentityPrivacy = False
 PseudonymSecret = <encrypted>
 PseudonymRenewtime = "24 Hours"
 PseudonymLifetime = Forever
 Generate3GPPCompliantPseudonym = False
 EnableReauthentication = False
 MaximumReauthentications = 16
 ReauthenticationTimeout = 3600
 ReauthenticationRealm =
```

```

AuthenticationTimeout = 120
QuintetGenerationScript~ =
UseProtectedResults = False
SendReAuthIDInAccept = False
Subscriber_DBLookup = sigTRAN-m3UA
FetchAuthorizationInfo = FALSE
MultipleServersPolicy = Failover
IncomingScript~ =
OutgoingScript~ =
OutageScript~ =
RemoteServers/

```

To configure EAP-SIM service with SIGTRAN-M3UA remote server:

- 
- Step 1** Launch **aregcmd**.
- Step 2** Create an EAP-SIM service.
- ```
cd /Radius/Services
add eap-sim-service
```
- Step 3** Set type as eap-sim.
- ```
set eap-sim
```
- Step 4** Add m3ua remote server in the remoteServers
- ```
cd remoteServers
Set 1 m3ua
```
-

The following shows an example configuration for EAP-SIM service with SIGTRAN-M3UA remote server support, see [Table 9-6](#) to know more about EAP-SIM service properties.

```

eap-sim/
Name = eap-sim
Description =
Type = eap-sim
NumberOfTriplets = 2
UseSimDemoTriplets = False
AlwaysRequestIdentity = False
EnableIdentityPrivacy = False
PseudonymSecret = <encrypted>
PseudonymRenewtime = "24 Hours"
PseudonymLifetime = Forever
Generate3GPPCompliantPseudonym = False
EnableReauthentication = False
MaximumReauthentications = 16
ReauthenticationTimeout = 3600
ReauthenticationRealm =
TripletCacheTimeout = 0
AuthenticationTimeout = 120
UseProtectedResults = False
SendReAuthIDInAccept = False
SubscriberDBLookup = SigTRAN-M3UA
FetchAuthorizationInfo = FALSE
MultipleServersPolicy = Failover
IncomingScript~ =

```

```
OutgoingScript~ =
OutageScript~ =
RemoteServers/
```

**Note**

Before enabling the SIGTRAN-M3UA remote server, you must ensure to restart the Cisco Prime AR server whenever you make any configuration changes.

**Note**

If you set `FetchAuthorizationInfo` as `TRUE` for EAP-AKA or EAP-SIM service for SIGTRAN-M3UA in Cisco Prime AR, it fetches the MSISDN information from HLR in response. The following is an example script for reading the MSISDN information from the response,

```
proc MapMSISDN {request response environ} {
$environ get AuthorizationInfo
}
```

You can configure the SIGTRAN-M3UA remoteserver under **/Radius/RemoteServers**.

To configure the SIGTRAN-M3UA remote server:

Step 1 Launch **aregcmd**.

Step 2 Create sigtran-m3ua remote server.

```
cd /r/remoteservers/

add M3UA

cd M3UA

set protocol sigtran-m3ua
```

Step 3 Set the `Subscriber_DBLookup`.

```
set Subscriber_DBLookup SIGTRAN-M3UA
```

Step 4 Set the hostname and port of the HLR.

```
set hostName 10.81.78.140

set DestinationPort 2905
```

Step 5 Set the IP address and port for the source.

```
set SourceIPAddress 10.81.78.142

set SourcePort 2905
```

Step 6 Set the `reactivatetimerinterval`.

Step 7 Set the subsystem number for the local.

```
set LocalSubSystemNumber 149
```

Step 8 Set `routingindicator`.

Set routingindicator rte_gt**Step 9** Set mlcnumber.**Set mlcnumber****Step 10** Set routingparameters.**cd routingparameters/****set OriginPointCode 2****set DestinationPointCode 4****set RemoteSubSystemNumber 6****set OPCMask 16383****set DPCMask 16383****set RoutingContext 11****Step 11** Set the source and destination gt parameters.**Step 12** Set the numbering plan, encoding scheme, format, and digits for source.**Step 13** Set the numbering plan, encoding scheme, format, and digits for destination.

The following shows an example configuration of SIGTRAN-M3UA remote server support:

```
[ //localhost/Radius/RemoteServers/m3ua ]
  Name = m3ua
  Description =
  Protocol = sigtran-m3ua)

  HostName = 10.81.78.138
  SourceIPAddress = 10.81.78.139
  SourcePort = 2905
  LocalSubSystemNumber = 149
  DestinationPort = 2905
  IMSITranslationScript~ =
  GlobalTitleTranslationScript~ = setGT
  Timeout = 15
  ReactivateTimerInterval = 2000
  LimitOutstandingRequests = FALSE
  MaxOutstandingRequests = 0
  MaxRetries = 3
  MAPVersion = 2
  NetworkVariant = ITU
  SubServiceField = NAT
  TCAPVariant = ITU96
  NetworkAppearance = 1
  NetworkIndicator = NAT
  MLCNumber = 123456789012345
  TrafficMode = LOADSHARE
  LoadShareMode = SLS
  RoutingIndicator = RTE_GT
  RoutingParameters/
    OriginPointCode = 2
    DestinationPointCode = 4
```

```

RemoteSubSystemNumber = 6
OPCMask = 16383
DPCMask = 16383
ServiceIndicatorOctet = 0
RoutingContext = 11
SourceGTAddress/
SourceGTDigits = 919845071842
SourceGTFormat = GTRMT_4
SourceNatureofAddress = INTNUM
SourceTranslationType = 0
SourceNumberingPlan = ISDN
SourceEncodingScheme = BCDEVEN
DestinationGTAddress/
DestGTDigits = 919845071842
DestGTFormat = GTRMT_4
DestNatureofAddress = INTNUM
DestTranslationType = 0
DestNumberingPlan = ISDN
DestEncodingScheme = BCDEVEN

```

Table 22-1 describes SIGTRAN-M3UA remote server properties.

Table 22-1 SIGTRAN-M3UA Stack Properties

Property	Description
Name	Required; inherited from the upper directory.
Description	An optional description of the service.
Protocol	Represents the type of remote server. The value should be SIGTRAN-M3UA.
HostName	IP address of the remote server.
SourceIPAddress	The local IP address in which Cisco Prime AR is installed.
SourcePort	The port number in which Cisco Prime AR is installed for M3UA transactions.
LocalSubSystemNumber	The local sub system number is set as 149 by default.
DestinationPort	The destination port number to which Cisco Prime AR connects.
IMSITranslationScript	The scripting point is used to modify the IMSI based on the requirement before sending the request to STP/HLR.
Timeout	Specifies the time (in seconds) to wait before an authentication request times out; defaults to 120.
ReactivateTimerInterval	Specifies the time interval (in milliseconds) to activate an inactive server; defaults to 300000 ms (which is 5 minutes).
LimitOutstandingRequests	Required; the default is FALSE. Cisco Prime AR uses this property in conjunction with the MaxOutstandingRequests property to tune the RADIUS server's use of the HLR. When you set this property to TRUE, the number of outstanding requests for this RemoteServer is limited to the value you specified in MaxOutstandingRequests. When the number of requests exceeds this number, Cisco Prime AR queues the remaining requests, and sends them as soon as the number of outstanding requests drops to this number.

Table 22-1 **SIGTRAN-M3UA Stack Properties (continued) (continued)**

Property	Description
MaxOutstandingRe- quests	Required when you have set the LimitOutstandingRequests to TRUE. The number you specify, which must be greater than zero, determines the maximum number of outstanding requests allowed for this remote server.
TrafficMode	The mode of the traffic for the HLR. The possible values are LOADSHARE or ACTSTANDBY.
LoadShareMode	Required. The TrafficMode is set as LOADSHARE, which is a type of load sharing scheme. When there is more than one associations with HLR, then the load sharing is set as Signaling Link Selection (SLS). SLS is done based on a simple round-robin basis.
MAPVersion	The version of the MAP. The possible values are 2 or 3. Specify the MAP version that the HLR supports, i.e, 2 or 3 during the configuration.
NetworkVariant	Required. Represents the network variant switch.  Note Cisco Prime AR supports only ITU value in 6.0 version.
SubServiceField	Specifies the type of network to which this SAP belongs. The possible options are INT and NAT which represents international network and national network respectively.
TCAPVariant	Required; represents the name of the tcap network variant switch. The possible options are ITU88, ITU92, or ITU96.
NetworkAppearance	Required. Represents the network appearance code which ranges from 0-2147483647.
NetworkIndicator	The network indicator used in SCCP address. The possible options are NAT and INT which represents international network and national network respectively.
MLCNumber	Required, if you select FetchAuthorizationInfo as True in EAP-AKA or EAP-SIM services. Also, required for M3UA service for fetching the MSISDN from the HLR. The MLC number is configured in E.164 format.  Note MLC is a max-15 digit number.
RoutingIndicator	Required; represents the routing indicator. The possible values are Route on Gloabl Title(RTE_GT) or Route on Sub System Number(RTE_SSN). You can use either RTE_GT or RTE_SSN value to route the packets for HLR.
RoutingParameters	
OriginPointCode	Required; represents the originating point of a message in a signalling network. The value ranges from 0-16777215.
DestinationPointCode	Required; represents the destination address of a signalling point in a SS7 network.
RemoteSubSystemNum- ber	Required; represents the sub system number of the remote server. The RemoteSubSyatemNumber is set as 6 by default.

Table 22-1 SIGTRAN-M3UA Stack Properties (continued) (continued)

Property	Description
OPCMask	Represents the wild card mask for the origin point code. The value ranges from 0-16777215.
DPCMask	Represents the wild card mask for the destination point code. The value ranges from 0-16777215.
ServiceIndicatorOctet	Represents the service identifier octet. The value ranges from 0-255.
RoutingContext	Required; represents the routing context which ranges from 0-16777215.
SourceGTAddress	
SourceGTDigits	Required; an unique number to identify the source.
SourceGTFormat	Required; represents the format of the global translation (GT) rule. The possible values are GTFRMT_0, GTFRMT_1, GTFRMT_2, GTFRMT_3, GTFRMT_4, or GTFRMT_5.
SourceNatureofAddress	Required; represents the type of the source address. The possible values are ADDR_NOTPRSNT (Address not present), SUBNUM (Subscriber number), NATSIGNUM (National significant number), or INTNUM (International number.)
SourceTranslationType	Required; represents the type of translation. The possible values ranges from 0-255.
SourceNumberingPlan	Required; represents the numbering plan of the network that the subscriber uses. For example, land mobile numbering plan, ISDN mobile numbering plan, private or network specific numbering plan.
SourceEncodingScheme	Required; represents the BCD encoding scheme. The possible values are UNKN (Unknown), BCDODD (BCD Odd), BCDEVEN (BCD Even), or NWSPEC (National specific.)
DestinationGTAddress	
The following fields are displayed only when you set RTE_GT as RoutingIndicator.	
DestGTDigits	Required; an unique number to identify the destination.
DestGTFormat	Required; represents the format of the global translation (GT) rule. The possible values are GTFRMT_0, GTFRMT_1, GTFRMT_2, GTFRMT_3, GTFRMT_4, or GTFRMT_5.
DestNatureofAddress	Required; represents the type of the destination address. The possible values are ADDR_NOTPRSNT (Address not present), SUBNUM (Subscriber number), NATSIGNUM (National significant number), or INTNUM (International number.)
DestTranslationType	Required; represents the type of translation. The possible values ranges from 0-255.
DestNumberingPlan	Required; represents the numbering plan of the network that the subscriber uses. For example, Land mobile numbering plan, ISDN mobile numbering plan, private or network specific numbering plan.
DestEncodingScheme	Required; represents the BCD encoding scheme. The possible values are UNKN (Unknown), BCDODD (BCD Odd), BCDEVEN (BCD Even), or NWSPEC (National specific.)

Configuring M3UA Service

Cisco Prime AR supports the M3UA service, which is used to fetch MSISDN from IMSI through RADIUS Packets, see [Chapter 4, “M3UA,”](#) for more information.

To configure the M3UA service with SIGTRAN-M3UA remote server:

Step 1 Launch **aregcmd**.

Step 2 Create an M3UA service.

cd /Radius/Services

add FetchMSISDN

Step 3 Set the type as M3UA.

set type M3UA

Step 4 Add M3UA remote server in the remoteServers.

cd remoteServers

Set 1 m3ua
