



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 Access Registrar (Prime Access Registrar) supports SS7 messaging over IP (SS7oIP) via SIGTRAN-M3UA, a new transport layer which leverages Stream Control Transmission Protocol (SCTP). Prime Access Registrar supports SIGTRAN-M3UA to fetch the authentication vectors from HLR, which is required for EAP-AKA/EAP-SIM authentication.

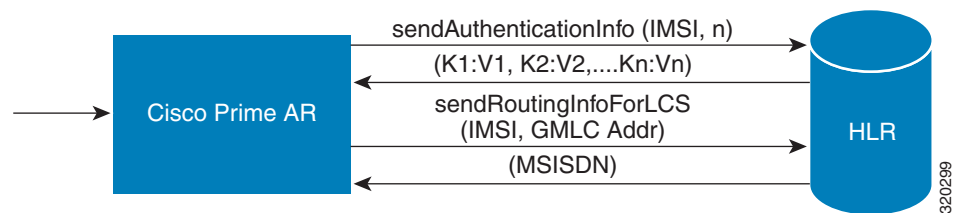


Note

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.

Figure 14-1 **MAP Service**



The Prime Access Registrar server initiates the MAP service. After enabling the MAP service, the Prime Access Registrar 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 Prime Access Registrar. Next, the Prime Access Registrar 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.

Prime Access Registrar provides `map-restore-data` authentication support for `m3ua` services.

Prime Access Registrar supports multiple remote servers with the protocol type, SIGTRAN-M3UA. However, Prime Access Registrar validates and ensures the following when multiple remote servers are available:

- The source port is different for all the remote servers.
- If Origin Point Code (OPC) is different, the routing context is also different for all the remote servers.
- The Destination Point Code (DPC) is different for all the remote servers.
- The NetworkVariant, SubServiceField (SSF), TCAPVariant, NetworkAppearance, and NetworkIndicator values are the same for all the remote servers.

This section describes the following:

- [Prerequisites to SIGTRAN-M3UA](#)
- [Configuring EAP-AKA/EAP-SIM with SIGTRAN-M3UA](#)
- [Configuring M3UA Service](#)
- [Block listing Support for SIGTRAN-M3UA Remote Server, page 14-22](#)
- [Support for SCTP Multihoming in SIGTRAN-M3UA, page 14-22](#)
- [Tuning Global SIGTRAN Parameters, page 14-23](#)
- [SIGTRAN-M3UA Logs, page 14-25](#)

Prerequisites to SIGTRAN-M3UA

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

- ensure that LKSCTP is not available in the Prime Access Registrar server.
- ensure to restart the Prime Access Registrar server whenever you make any configuration changes.
- ensure that you have the 64-bit rpm files for the relevant RHEL and Cent OS versions while installing Prime Access Registrar. For the list of required rpms for the relevant OS versions, see [Required 64-bit rpms for Relevant RHEL OS Versions](#).



Note You must install the rpm versions relevant to the RHEL OS versions while installing the Prime Access Registrar.

- ensure that the ‘bc’ command (which is an arbitrary precision calculator language) is present while installing Prime Access Registrar in a Linux machine. If the ‘bc’ command is not present, install the relevant rpm such as bc-1.06.95-1.el6.x86_64 on that machine.
- ensure that you have the following packages while installing the Prime Access Registrar:
 - gcc version 4.7.0 for RHEL 7.x and gcc version 8.3.1 for RHEL 8.x
 - gdome-config-0.8.1



Note You need to build the gdome-config-0.8.1 package to make it available. For more information, see [Building gdome Package, page 14-4](#)

- xml2-config-2.6.23

- pkg-config-0.15.0
- glib-2.30
- gtk-2.41
- libxml-2.2.6.20

Required 64-bit rpms for Relevant RHEL OS Versions

rpm	RHEL OS Version 7.x	RHEL OS Version 8.x
brotli	No	Yes
c-ares	Yes	Yes
cyrus-sasl-lib	Yes	Yes
gamin	Yes	Yes
glibc	Yes	Yes
gdome2	Yes	Yes
glib	Yes	Yes
glib2	Yes	Yes
json-c	Yes	Yes
keyutils-libs	Yes	Yes
krb5-libs	Yes	Yes
libbson	No	Yes
libcom_err	Yes	Yes
libcurl	Yes	Yes
libicu	Yes	Yes
libidn2	No	Yes
libgcc	Yes	Yes
libmongocrypt	No	Yes
libnghttp2	No	Yes
libnsl	No	Yes
libpsl	No	Yes
libselinux	Yes	Yes
libssh	No	Yes
libstdc++	Yes	Yes
libtool-ltdl	Yes	Yes
libunistring	No	Yes
libxcrypt	No	Yes
libxml2	Yes	Yes
libzstd	No	Yes
lksctp-tools	Yes	Yes

rpm	RHEL OS Version 7.x	RHEL OS Version 8.x
mongo-c-driver-libs	No	Yes
ncurses-libs	Yes	Yes
nss-softokn-freebl	Yes	Yes
nss-util	Yes	Yes
nspr	Yes	Yes
nss	Yes	Yes
openldap	No	Yes
openssl-libs	Yes	Yes
pcre	Yes	Yes
pcre2	No	Yes
pcre-cpp	No	Yes
snappy	No	Yes
sqlite-libs	No	Yes
tcl	No	Yes
unixODBC	No	Yes
xz-libs	No	Yes
zlib	Yes	Yes

Building gdome Package

To build gdome-config-0.8.1 package:

Step 1 Download gdome2-0.8.1.tar.gz package from the location <http://gdome2.cs.unibo.it/#downloads>.

Step 2 Execute the following command:

```
gunzip gdome2-0.8.1.tar.gz
```

Step 3 Untar the package using the following command:

```
tar -xvf gdome2-0.8.1.tar
```

Step 4 Use the **cd** command to move into the package obtained from [Step 3](#).

Step 5 Execute the following commands:

```
./configure --prefix=<GdomeInstallPath> --with-glib-prefix=<GlibInstalledDirectory>
make
make install
```

Where,

- GdomeInstallPath specifies where the Gdome libraries must be placed.
- GlibInstalledDirectory specifies which directory the Glib libraries reside in the filesystem.

Step 6 Now gdome libraries will be available in the location *GdomeInstallPath*.

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 5-1](#) 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 5-3](#) 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 After enabling the SIGTRAN-M3UA remote server, you must ensure to restart the Prime Access Registrar 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 Prime Access Registrar, 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
}
```

Configuring SIGTRAN-M3UA Remote Server

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 port of the HLR.

```
set DestinationPort 2905
```

Step 5 Set the port for the source.

```
set SourcePort 2905
```

Step 6 Set the reactivate timer interval for the remote server.

```
Set the reactivatetimerinterval.
```

Step 7 Set the subsystem number for the local.

```
set LocalSubSystemNumber 149
```



Note Prime Access Registrar supports the following local Sub System Numbers (SSNs) by default:

- SGSN (149)
- VLR (7)
- GMLC (145)

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.

ANSI Support for SIGTRAN

Prime Access Registrar provides ANSI variant support apart from ITU variants in SIGTRAN stack for EAP-SIM and EAP-AKA services to M3UA.

While using this service for authentication, the subscriber identity (IMSI) is obtained from the request. Using this IMSI, the authentication service initiates a request to the SIGTRAN server. This request is to retrieve the configured number of authentication vectors (triplets/quintets) for the IMSI.

The remote SIGTRAN server initiates the IS41 service primitive Authentication Data request with IMSI and number of requested authentication vectors. This will retrieve the authentication vectors from HLR which will be used by the authentication service for authenticating the mobile subscriber.



Note

Prime Access Registrar supports either ITU or ANSI variant in one running instance. Both the variants are not supported simultaneously.

The following shows an example configuration of SIGTRAN-M3UA remote server with ITU variant:

```
[ //localhost/Radius/RemoteServers/m3ua ]
  Name = m3ua
  Description =
  Protocol = sigtran-m3ua)
  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 = GTFRMT_4
  SourceNatureofAddress = INTNUM
  SourceTranslationType = 0
  SourceNumberingPlan = ISDN
  SourceEncodingScheme = BCDEVEN
DestinationGTAddress/
  DestGTDigits = 919845071842
  DestGTFormat = GTFRMT_4
  DestNatureofAddress = INTNUM
  DestTranslationType = 0
  DestNumberingPlan = ISDN
  DestEncodingScheme = BCDEVEN

```

Table 14-1 describes SIGTRAN-M3UA remote server properties.

Table 14-1 *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 SIG-TRAN-M3UA.
SourcePort	The port number in which Prime Access Registrar is installed for M3UA transactions.
LocalSubSystemNumber	The local sub system number is set as 149 by default.
DestinationPort	The destination port number to which Prime Access Registrar connects.
IMSITranslationScript	The scripting point is used to modify the IMSI based on the requirement before sending the request to STP/HLR.

Table 14-1 SIGTRAN-M3UA Stack Properties (continued)

Property	Description
GlobalTitleTranslationScript	This is used to specify the name of the script which is responsible for translating IMSI to Global Title Address (GTA). You can choose to configure block listing as part of the global title translation script for SIGTRAN-M3UA remote server. For more information about block listing, see the “Using Extension Points” chapter of the <i>Cisco Prime Access Registrar 9.2 Administrator Guide</i> .
Timeout	Specifies the time (in seconds) to wait before an authentication request times out; defaults to 15.
MaxTimeOuts	Maximum number of timeouts allowed for the remote server.
MaxSessionLimit	Maximum number of sessions allowed for the remote server.
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. Prime Access Registrar 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, Prime Access Registrar queues the remaining requests, and sends them as soon as the number of outstanding requests drops to this number.
MaxOutstandingRequests	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. Choose ITU or ANSI to represent the network variant switch.
SubServiceField	Specifies the type of network to which this SAP belongs. The possible options are: <ul style="list-style-type: none"> • INT—represents international network • NAT—represents national network • RESERVE—represents reserved network • SPARE—represents spare network

Table 14-1 SIGTRAN-M3UA Stack Properties (continued)


Property	Description
SCCPVariant	The Signaling Connection Control Part (SCCP) variant of the Global Title: <ul style="list-style-type: none"> Select ITU88, ITU92, or ITU96, if NetworkVariant is set to ITU. Select ANS88, ANS92, or ANS96, if NetworkVariant is set to ANS.
TCAPVariant	Required; represents the name of the tcap network variant switch. The possible options are ITU88, ITU92, or ITU96.
NetworkAppearance	Required. A parameter that represents network appearance in the M3UA packet. Value ranges from 0-2147483647 and the default value is 1. This is optional as per the RFC 4666 (http://tools.ietf.org/html/rfc4666 .) You can set this value to 0 to remove network appearance from the data packet.
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. This is the map layer network node number by which the HLR identifies the Prime Access Registrar in the network. 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 Global 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 signaling network. The value ranges from 0-16777215. This value must be less than OPCMask.
DestinationPointCode	Required; represents the destination address of a signaling point in a SS7 network. This value must be less than DPCMask.
RemoteSubSystemNumber	Required; represents the sub system number of the remote server. The RemoteSubSystemNumber is set as 6 by default.
OPCMask	Represents the wild card mask for the origin point code. The value ranges from 0-16777215. Default value is 16383 for ITU and 16777215 for ANSI.
DPCMask	Represents the wild card mask for the destination point code. The value ranges from 0-16777215. Default value is 16383 for ITU and 16777215 for ANSI.
ServiceIndicatorOctet	Represents the service identifier octet. The value ranges from 0-255.

Table 14-1 SIGTRAN-M3UA Stack Properties (continued)

Property	Description
RoutingContext	Required; represents the routing context which ranges from 0-16777215.
SourceIPAddresses	
add 1, add 2,...	Represent the multiple source IP addresses configured on the remote server.
DestinationIPAddresses	
add 1, add 2,...	Represent the multiple destination IP addresses configured on the remote server.
SourceGTAddress	
The following fields are displayed only when you set RTE_GT as RoutingIndicator.	
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. The GT format is GTFRMT_0, GTFRMT_1, or GTFRMT_2 for ANSI variant. GTFRMT_0 is the default format for both ANSI and ITU variants.
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). This must be set based on the length of the GT.
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. The GT format is GTFRMT_0, GTFRMT_1, or GTFRMT_2 for ANSI variant. GTFRMT_0 is the default format for both ANSI and ITU variants.
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.

Table 14-1 SIGTRAN-M3UA Stack Properties (continued)

Property	Description
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. Possible values are DATA, GENERIC, ISDN, ISDNMOB, LANMOB, MARMOB, NWSPEC, TEL, TELEX, and UNKN.
DestEncodingScheme	Required; represents the BCD encoding scheme. The possible values are UNKN (Unknown), BCDODD (BCD Odd), BCDEVEN (BCD Even), or NWSPEC (National specific). This must be set based on the length of the GT.

The following shows an example configuration of SIGTRAN-M3UA remote server with ANSI variant:

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

  STP/
    Name =STP
    Description =
    Protocol = Sigtran-m3ua
    SourcePort = 2905
    LocalSubSystemNumber = 149
    DestinationPort = 2905
    IMSITranslationScript~ =
    Timeout = 15
    MaxTimeOuts = 200
    MaxSessionLimit = 0
    ReactivateTimerInterval = 2000
    LimitOutstandingRequests = FALSE
    MaxOutstandingRequests = 0
    MAPVersion = 2
    NetworkVariant = ANS
    SubServiceField = NAT
    SCCPVariant = ANS92
    TCAPVariant = ITU96
    NetworkAppearance = 1
    NetworkIndicator = NAT
    MLCNumber = 123456789012345
    TrafficMode = LOADSHARE
    LoadShareMode = SLS
    RoutingIndicator = RTE_GT
    GlobalTitleTranslationScript~ =
    MaskPointCode = FALSE
    RoutingParameters/
      OriginPointCode = 13967019
      DestinationPointCode = 13966849
      RemoteSubSystemNumber = 6
      OPCMask = 16777215
      DPCMask = 16777215
      ServiceIndicatorOctet = 3
      RoutingContext = 11
    SourceIPAddresses/
      1. 10.81.78.142
    DestinationIPAddresses/
      1. 10.81.78.145
    SourceGTAddress/
      SourceGTDigits = 919845071842
```

```

SourceGTFormat = GTFRMT_2
SourceTranslationType = 10
DestinationGTAddress/
DestGTDigits = 919845071842
AdditionalDestGTDigits = 9198,2011
DestGTFormat = GTFRMT_2
DestTranslationType = 9

```

Configuring M3UA Service

Prime Access Registrar supports the M3UA service, which is used to fetch MSISDN from IMSI or vice versa through RADIUS packets.

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

Step 1 Launch **aregcmd**.

Step 2 Create an M3UA service.

```
cd /Radius/Services
```

```
add FetchAuthInfo
```

Step 3 Set the type as M3UA.

```
set type M3UA
```

Step 4 Set **AuthorizationInfoLookUp** to one of the following:

- MSISDN-IMSI—To fetch MSISDN in the request and send IMSI in the response to the HLR.
- IMSI-MSISDN—To fetch IMSI in the request and send MSISDN in the response to the HLR.



Note See [Example Configuration, page 14-14](#) for a sample configuration with

- Map-Restore—To fetch the profile information of a subscriber from the HLR. For more information on configuring the M3UA service with Map Restore Data authorization, see [Configuring M3UA Service with Map Restore Data Authorization, page 14-15](#).

```
set AuthorizationInfoLookUp IMSI-MSISDN
```

Step 5 Add M3UA remote server in the remoteServers.

```
cd remoteServers
```

```
Set 1 m3ua
```

Example Configuration

The following shows an example configuration of the M3UA service:

```

[ //localhost/Radius/Services/test ]
Name = test
Description =
Type = m3ua
IncomingScript~ =

```

```
OutgoingScript~ =  
OutageScript~ =  
OutagePolicy~ = RejectAll  
AuthorizationInfoLookUp = IMSI-MSISDN  
RemoteServers/
```

Configuring M3UA Service with Map Restore Data Authorization

Prime Access Registrar provides the Map Restore Data functionality to fetch the profile information of a subscriber from the HLR.

This topic contains the following sections:

- [Map Restore Data Authorization Flow, page 14-15](#)
- [CS Insert Subscriber Data Structure, page 14-16](#)
- [CLI Configuration for Map-Restore-Data, page 14-17](#)

Map Restore Data Authorization Flow

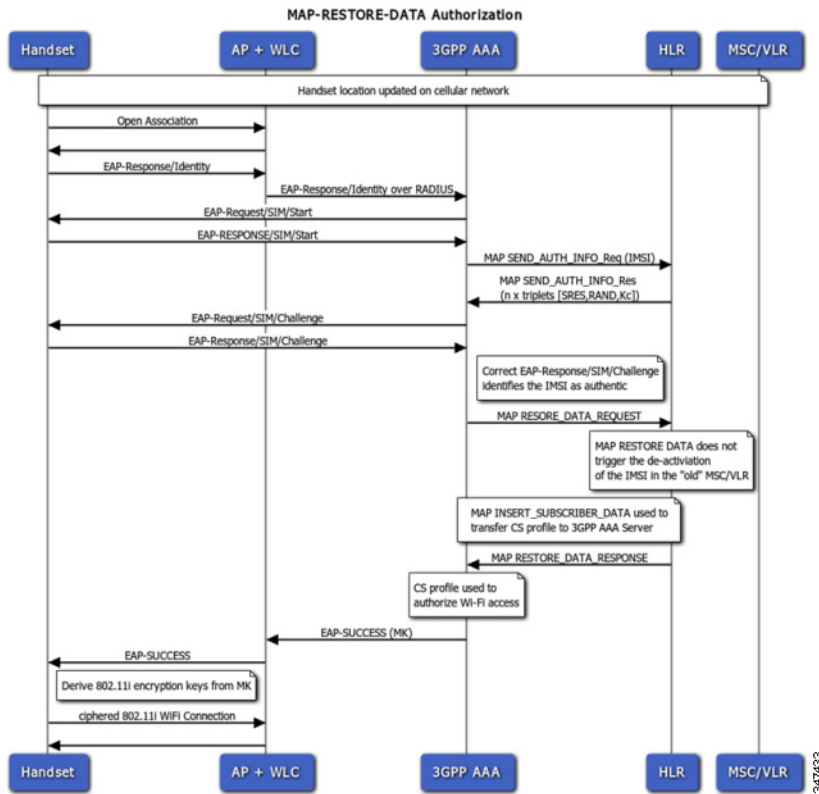
Prime Access Registrar sends a MAP_SEND_AUTH_INFO request to HLR on receiving EAP-SIM / EAP-AKA authentication request and fetches the authentication vectors in MAP_SEND_AUTH_INFO_RES message. Prime Access Registrar checks the IMSI and if it is authentic, sends a MAP_RESTORE_DATA_REQUEST to fetch the profile information from the HLR. HLR then responds with MAP_INSERT_SUBSCRIBER_DATA request to Prime Access Registrar. The request contains the circuit switched (CS) profile information for a subscriber.

Prime Access Registrar server stores the profile information based on the ProfileInfo configuration and sends a MAP_INSERT_SUBSCRIBER_DATA_RESPONSE to HLR. HLR responds with MAP_RESTORE_DATA_RESPONSE to Prime Access Registrar. After successful acknowledgment of MAP_RESTORE_DATA, Prime Access Registrar server maps the fetched profile through RestoreDataMappings to any of the environment variables configured by the user. The CS profile used to authorize WI-FI access which is fetched from HLR can be transported to access point in any of the radius attribute.

The mapping of the values in the response to a profile is possible based on the configuration in the profilemappings configuration.

[Figure 14-2](#) represents the Map-Restore-Data message flow between Prime Access Registrar and HLR.

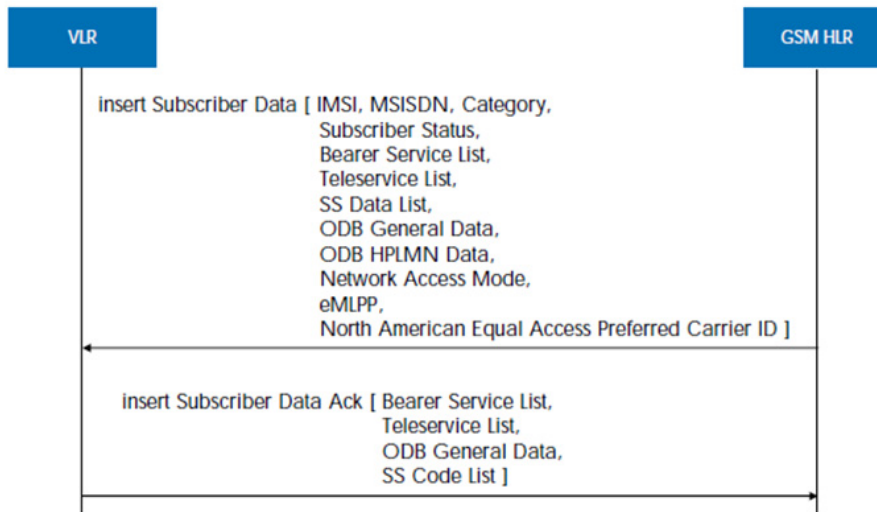
Figure 14-2 Map-Restore-Data Authorization Flow



CS Insert Subscriber Data Structure

Figure 14-3 shows the parameters fetched by Prime Access Registrar on receipt of the subscriber data request.

Figure 14-3 CS Insert Subscriber Data Structure



CLI Configuration for Map-Restore-Data

If you set `AuthorizationInfoLookUp` to **Map-Restore**, two additional properties `ProfileMappings` and `RestoreDataMappings` are displayed.

The restore data mapping parameters include LSA information, LCS information, and subscriber data. You can configure an index with a value or a range to fetch one or more properties from the subscriber data.

The following is an example configuration of an M3UA service with Map-Restore-Data authorization:

```
[ //localhost/Radius/Services/serv1 ]
  Name = serv1
  Description =
  Type = m3ua
  IncomingScript~ =
  OutgoingScript~ =
  OutageScript~ =
  OutagePolicy~ = RejectAll
  AuthorizationInfoLookUp = MAP-RESTORE
  RemoteServers/
    1. server1
  RestoreDataMappings/
    IMSI = imsi
    Naea-PreferredCI = naea
    RoamingRestrictedInSgsnDueToUnsupportedFeature =
    NetworkAccessMode =
    LMUIndicator =
    ISTAlertTimer =
    SuperChargerSupportedInHLR =
    CSAllocationRetentionPriority =
    ChargingCharacteristics =
    AccessRestrictionData =
    UE-ReachabilityRequestIndicator =
    Category =
  LSAInformation/
    CompleteDataListIncluded = completedatalist
    LSAOnlyAccessIndicator =
  LSADataList/
    Index = 6
    LSAIdentity = lsaid
    LSAAttributes = lsaattrib
    LSAActiveModeIndicator = activemode
  SubscriberData/
    MSISDN = msisdn
    SubscriberStatus = substatus
    RoamingRestrictionDueToUnsupportedFeature =
  BearerServiceList/
    Index = 6-10
    BearerService = bearsrvc
  TeleServiceList/
    Index =
    TeleService =
  ProvisionedSS/
    Index = 4-6
  ForwardingInfo/
    FI-SS-Code = fisscode
  ForFeatureList/
    Index = 7-10
    FF-SS-Status = ffsstatus
    ForwardedToNumber =
    ForwardedToSubaddress =
    ForwardingOptions =
```

```

        NoReplyConditionTime =
        LongForwardedToNumber =
        BasicService/
            BS-Ext-BearerService = bsextbsservice
            BS-Ext-Teleservice = bsextteleservice
    CallBarringInfo/
        CB-SS-Code =
        CallBarFeatureList/
            Index =
            CB-SS-Status =
            BasicService/
                CB-Ext-BearerService =
                CB-Ext-Teleservice =
    CugInfo/
        CugSubList/
            Index =
            CugSubscription/
                Cug-Index =
                cug-Interlock =
                IntraCUG-Options =
                BasicServiceGroupList/
                    Index =
                    CUG-Ext-BearerService =
                    CUG-Ext-Teleservice =
    CugInformation/
        Cug-FeatureList/
            Index =
            CUG-Feature/
                BasicService.Ext-BearerService =
                PreferentialCUG-Indicator =
                InterCUG-Restrictions =
    SS-Data/
        SSD-SS-Code =
        SSD-SS-Status =
        SS-SubscriptionOption/
            CliRestrictionOption =
            OverrideCategory =
        BasicServiceGroupList/
            Index =
            BSG-Ext-BearerService =
            BSG-Ext-Teleservice =
    EMLPP-Info/
        MaximumEntitledPriority =
        DefaultPriority =
    ODB-Data/
        ODB-GeneralData =
        ODB-HPLMN-Data =
    RegionalSubscriptionData/
        Index =
        RegionalSubscriptionData =
    VBSSubscriptionData/
        Index =
        VBS-GroupId =
        BroadcastInitEntitlement =
    VGCSSubscriptionData/
        Index =
        VGCS-GroupId =
        AdditionalSubscriptions =
        AdditionalInfo =
        LongGroupId =
    LCSInformation/
        GMLC-List/
            Index =
            GMLC =

```

```

LCS-PrivacyExceptionList/
  Index =
  PE-SS-Code =
  SS-Status =
  LCSNotificationToMSUser =
  ExternalClientList/
    Index =
    ClientIdentity.ExternalAddress =
    ExtCliGMLC-Restriction =
    ExtCliNotificationToMSUser =
  PLMNClientList/
    Index =
    PLMNClient =
  ServiceTypeList/
    Index =
    ServiceTypeIdentity =
    SerTypeGMLC-Restriction =
    SerTypeNotificationToMSUser =
MOLR-List/
  Index =
  MOLR-SS-Code =
  MOLR-SS-Status =
MC-SS-Info/
  MC-SS-Code =
  MC-SS-Status =
  NbrSB =
  NbrUser =
SGSN-CAMEL-SubscriptionInfo/
  GPRS-CSI/
    GPRS-CamelCapabilityHandling =
    GPRS-NotificationToCSE =
    GPRS-CSI-Active =
    GPRS-CamelTDPDataList/
      Index =
      GPRS-TriggerDetectionPoint =
      GPRS-ServiceKey =
      GPRS-GSMSCF-Address =
      DefaultSessionHandling =
  MO-SMS-CSI/
    MOSMS-CamelCapabilityHandling =
    MOSMS-NotificationToCSE =
    MOSMS-CSI-Active =
    SMS-CAMEL-TDP-DataList/
      Index =
      MO-SMS-TriggerDetectionPoint =
      MO-ServiceKey =
      MO-GSMSCF-Address =
      MO-DefaultSMSHandling =
  MT-SMS-CSI/
    MTSMS-CamelCapabilityHandling =
    MTSMS-NotificationToCSE =
    MTSMS-CSI-Active =
    SMS-CAMEL-TDP-DataList/
      Index =
      MT-SMS-TriggerDetectionPoint =
      MT-ServiceKey =
      MT-GSMSCF-Address =
      MT-DefaultSMSHandling =
  MT-SMSCAMELTDP-CriteriaList/
    Index =
    SMS-TriggerDetectionPoint =
    TPDU-TypeCriterion =
MG-CSI/
  MobilityTriggers =

```

```

MG-ServiceKey =
MG-GSMSCF-Address =
MG-NotificationToCSE =
MG-CSI-Active =
ProfileMappings/
  imsi = 100,Profile1
  naea = 20,Profile2
  naea = 30,Profile3

[ //localhost/Radius/Profiles ]
  Entries 1 to 6 from 6 total entries
  Current filter: <all>

  default-PPP-users/
  default-SLIP-users/
  default-Telnet-users/
  Profile1/
  Profile2/
  Profile3/

```

Table 14-2 shows the restore data mapping parameters.

Table 14-2 Restore Data Mappings and Profile Mappings Parameters

Parameter	Description
IMSI	IMSI received in the response from HLR.
Naea-Preferred CI	North American Equal Access preferred Carrier ID List. A list of the preferred carrier identity codes that are subscribed to.
Roaming Restricted In Sgsn Due To Unsupported Feature	Indicates that a subscriber is not allowed to roam in the current Service GPRS Support Node (SGSN) or Cisco Mobility Management Entity (MME) area.
Network Access Mode	The Network Access Mode (NAM) defines if the subscriber is registered to get access to the CS (non-GPRS/EPS network), to the PS (GPRS/EPS) network or to both networks. NAM describes the first level of the subscriber data pseudo-tree below the IMSIroot. It is permanent subscriber data stored in the HSS / HLR and the SGSN with the Gs interface option, and the MME with the SGs interface option.
LMU Indicator	Indicates the presence of an LMU.
IST Alert Timer	Indicates the IST alert timer value that must be used in the Mobile Switching Center (MSC) to inform the HLR about the call activities that the subscriber performs.
Super Charger Supported In HLR	Indicates whether super charger concept is supported in HLR.
CS Allocation Retention Priority	Allocation-retention priority for Circuit Switched (CS). This parameter specifies relative importance to compare with other bearers about allocation and retention of bearer.
ChargingCharacteristics	Subscribed charging characteristics.

Table 14-2 Restore Data Mappings and Profile Mappings Parameters (continued)

Parameter	Description
Access Restriction Data	Allowed Recipient Access Table (RAT) according to subscription data.
UE Reachability Request Indicator	Indicates that the Home Subscriber Server (HSS) is awaiting a notification of user equipment (UE) reachability.
Category	Calling party category
LSA Information	These parameters refer to one or more localized service areas (LSAs) a subscriber may be a member of, together with the priority, the preferential access indicator, the active mode support indicator and active mode indication of each localized service area. The access right outside these localized service areas is also indicated.
Subscriber Data	
MSISDN	MSISDN value in the subscriber data.
Subscriber Status	Barring status of the subscriber, which could be Service Granted or Operator Determined Barring.
Roaming Restriction Due To Unsupported Feature	Indicates that the subscriber is not allowed to roam in the current MSC area.
Bearer Service List	List of extensible bearer services subscribed. Configure the index value to fetch only the required bearer services.
TeleService List	List of extensible teleservices subscribed. Configure the index value to fetch only the required teleservices.
Provisioned SS	List of supplementary services provisioned. Configure the index value to fetch only the required supplementary services.
ODB-Data	Operator Determined Barring (ODB) general data and ODB Home Public Land Mobile Network (HPLMN) specific data.
Regional Subscription Data	List of regional subscription areas (zones) in which the subscriber is allowed to roam. Configure the index value to fetch only the required zones.
VBS Subscription Data	List of Voice Broadcast Services (VBS) subscribed. Configure the index value to fetch only the required VBS.
VGCS Subscription Data	List of Voice Group Call Services (VGCS) subscribed. Configure the index value to fetch only the required VGCS.
LCS Information	
Live Communication Server (LCS) related information for the subscriber.	
GMLC-List	List of Gateway Mobile Location Centers (GMLCs) that are permitted to issue a call/session unrelated or call/session related MT-LR request. Configure the index value to fetch only the required GMLCs.
LCS-Privacy Exception List	Classes of LCS client that are allowed to locate any target Mobile Station (MS). Configure the index value to fetch only the required classes.

Table 14-2 Restore Data Mappings and Profile Mappings Parameters (continued)

Parameter	Description
MOLR-List	Code and status of Mobile Originating Location Request (MO-LR) subscribed. Configure the index value to fetch only the required requests.
MC-SS-Info	Parameters identifying Multicall (MC) supplementary services (SS).
SGSN-CAMEL-Subscription Info	Parameters identifying the subscribers as having Customized Application for Mobile Enhanced Logic (CAMEL) services that are invoked in the SGSN.
ProfileMappings	
Attribute	The RADIUS attribute to map the fetched profile data.
Value:Profile	Value of the attribute.

Configuring Environment Variables to Fetch Subscriber Data Values

You can configure an environment variable to fetch the required values from the subscriber data packets. You can run a script to fetch the environment variable along with the values. See the example below:

```
proc FetchBearerService {request response environ} {
    set bearerService [ $environ get bs-ext ]
    $request trace 2 "BearerService value fetched is " $bearerService
}
```

In the above script bs-ext is the environment variable that is configured. If the values fetched from BearerServiceList are 17,18,19,20 and 21, the above script returns the value 17:18:19:20:21.

Similarly we can run scripts to retrieve other environment variables as well.

Block listing Support for SIGTRAN-M3UA Remote Server

Prime Access Registrar supports block listing of IMSI or IP address values for SIGTRAN-M3UA remote servers.

You can configure a SIGTRAN-M3UA remote server with EAP-SIM or EAP-AKA service, and then choose to configure block listing as part of the global title translation script of the remote server. For more information about block listing, see the “Using Extension Points” chapter of the [Cisco Prime Access Registrar 9.2 Administrator Guide](#).

Support for SCTP Multihoming in SIGTRAN-M3UA

Stream Control Transmission Protocol (SCTP) is an IP transport protocol that supports data exchange between exactly two endpoints. Multihoming feature of SCTP provides the ability for a single SCTP endpoint to support multiple IP addresses. With this feature, each of the two endpoints during an SCTP association can specify multiple points of attachment. Each endpoint will be able to receive messages from any of the addresses associated with the other endpoint. With the use of multiple interfaces, data can be sent to alternate addresses when failures occur and thus Prime Access Registrar runs successfully even during network failures.

Prime Access Registrar allows you to configure multiple source and destination addresses on the remote server. The following shows an example configuration of SIGTRAN-M3UA remote server with multiple source and destination addresses:

```
[ /Radius/RemoteServers/m3ua ]
  Name = m3ua
  Description =
  Protocol = sigtran-m3ua
  SourcePort = 2805
  LocalSubSystemNumber = 149
  DestinationPort = 2855
  IMSITranslationScript~ =
  GlobalTitleTranslationScript~ =
  Timeout = 15
  ReactivateTimerInterval = 300000
  LimitOutstandingRequests = FALSE
  MaxOutstandingRequests = 0
  MAPVersion = 3
  NetworkVariant = ITU
  SubServiceField = NAT
  TCAPVariant = ITU96
  NetworkAppearance = 1
  NetworkIndicator = NAT
  MLCNumber = 123456789012345
  TrafficMode = LOADSHARE
  LoadShareMode = SLS
  RoutingIndicator = RTE_SSN
  RoutingParameters/
  OriginPointCode = 2
  DestinationPointCode = 4
  RemoteSubSystemNumber = 6
  OPCMask = 16383
  DPCMask = 16383
  ServiceIndicatorOctet = 0
  RoutingContext = 11
  SourceIPAddresses/
  DestinationIPAddresses/
--> cd SourceIPAddresses
--> add 1 192.168.0.2
--> add 2 192.168.0.3
--> cd ../DestinationIPAddresses
--> add 1 192.168.0.5
--> add 2 192.168.0.6
```

In the above example, the link between IP addresses 192.168.0.2 and 192.168.0.5 acts as the primary link and the link between IP addresses 192.168.0.3 and 192.168.0.6 acts as the secondary link. With the Multihoming feature, if one of the interfaces in the primary link is down, the secondary link carries the active traffic. On restoration of the IP address, the traffic switches back to the primary link.

Tuning Global SIGTRAN Parameters

Prime Access Registrar provides a CLI tool SigtranXMLEdit that allows you to edit the values of the global SIGTRAN XML parameters. The tool is available under the <installation directory>/bin directory, e.g. /cisco-ar/bin and the parameters are available in the *default.xml* file under the /cisco-ar/m3ua-cfg directory.

[Table 14-3](#) lists the global SIGTRAN parameters that you can edit using the CLI tool.

Table 14-3 Global SIGTRAN Parameter

Parameter	Description
rtoMin	Minimum value of retransmission timeout
rtoMax	Maximum value of retransmission timeout
rtoInitial	Initial value of retransmission timeout
alpha	Retransmission timeout alpha value
beta	Retransmission timeout beta value
maxAssocReTx	Maximum association retransmission
maxPathReTx	Maximum path retransmission
maxInitReTx	Maximum initial retransmission
cookieLife	Cookie life
intervalTm	Heartbeat interval
maxAckDelayTm	SACK period
maxNmbInStrms	Maximum number of inbound streams
maxNmbOutStrms	Maximum number of outbound streams
mtuInitial	Initial value of maximum transmission unit
mtuMinInitial	Minimum Initial value of maximum transmission unit
mtuMaxInitial	Maximum Initial value of maximum transmission unit

To edit the SIGTRAN parameters:

Step 1 Launch the CLI tool **SIGTRANXMLEdit** from the `/cisco-ar/bin` directory.

The tool displays the list of editable parameters available in the `default.xml` file as shown below.

1. RTO min (RTOMI) from the header `_sbSctSapCfg`
2. RTO max (RTOMA) from the header `_sbSctSapCfg`
3. RTO Initial (RTOI) from the header `_sbSctSapCfg`
4. RTO Alpha (RTOA) from the header `_sbGenReCfg`
5. RTO Beta (RTOB) from the header `_sbGenReCfg`
6. Assoc. Max retrans. (AMR) from the header `_sbGenReCfg`
7. Path Max retrans. (PMR) from the header `_sbGenReCfg`
8. Initial retrans. Attempts (IMR) from the header `_sbGenReCfg`
9. Cookie life (VCL) from the header `_sbSctSapReCfg`
10. HB interval (HBI) from the header `_sbSctSapReCfg`
11. SACK period (TSACK) from the header `_sbSctSapReCfg`
12. Streams per association (MIS/MOS) from the header `_sbGenCfg`
13. Maximum Transmission unit (MTU) from the header `_sbGenCfg`

The tool prompts you to enter the new value against the first parameter as shown below.

```
Enter values for the following parameters (just press 'return' to skip):
Maximum number of inbound streams "maxNmbInStrms" [ 1024 ] :
```

In this example, 1024 is the value that exists for the parameter in the `default.xml` file.

Step 2 Type the new value and press ENTER or just press ENTER to skip and proceed to the next parameter. Perform this step for all parameters as shown below.

```
Enter values for the following parameters (just press 'return' to skip):
```



```

Maximum number of inbound streams "maxNmbInStrms" [ 1024 ] : 87
Maximum number of outbound streams "maxNmbOutStrms" [ 1024 ] : 90
Initial value of Maximum Transmission Unit "mtuInitial" [ 1500 ] :
Minimum Initial value of Maximum Transmission Unit "mtuMinInitial" [ 1500 ] : 65
Maximum Initial value of Maximum Transmission Unit "mtuMaxInitial" [ 1500 ] : 33
Maximum initial Retransmission "maxInitReTx" [ 5 ] : 9
Maximum association Retransmission "maxAssocReTx" [ 10 ] : 4
Maximum path Retransmission "maxPathReTx" [ 5 ] : 2
Alpha value "alpha" [ 12 ] : 15
Beta value "beta" [ 25 ] : 34
MaxAckDelayTm "maxAckDelayTm" [ 2 ] : 89<br
  Initial value of Retransmission timeout "rtoInitial" [ 15 ] :
Minimum value of Retransmission timeout "rtoMin" [ 15 ] :
Maximum value of Retransmission timeout "rtoMax" [ 60 ] :
CookieLife "cookieLife" [ 60 ] : 67
IntervalTm "intervalTm" [ 15 ] : 89
Do you want to save all the changes? [ Yes/No ]yes

```

Step 3 When prompted for a confirmation, type **Yes** and press ENTER to save the changes. The tool displays the modified parameters with the new and old values.

```

Changed Value of maxNmbInStrms is 87 <- 1024
Changed Value of maxNmbOutStrms is 90 <- 1024
Changed Value of mtuMinInitial is 65 <- 1500
Changed Value of mtuMaxInitial is 33 <- 1500
Changed Value of maxInitReTx is 9 <- 5
Changed Value of maxAssocReTx is 4 <- 10
Changed Value of maxPathReTx is 2 <- 5
Changed Value of alpha is 15 <- 12
Changed Value of beta is 34 <- 25
Changed Value of maxAckDelayTm is 89 <- 2
Changed Value of cookieLife is 67 <- 60
Changed Value of intervalTm is 89 <- 15
[root@ar-lnx-vm061 bin]#

```

SIGTRAN-M3UA Logs

The following logs are applicable for SIGTRAN-M3UA:

- `stack.log`—Logs the interaction between Prime Access Registrar and STP/HLR.
- `sm.log`—Logs the internal debug information for SIGTRAN-M3UA stack manager.
- `m3ua.log`—Logs the inter-process communication between Prime Access Registrar and SIGTRAN-M3UA stack.
- `cliActivity.log`—Logs the initialization and command interactions.

