SIGTRAN-M3UA

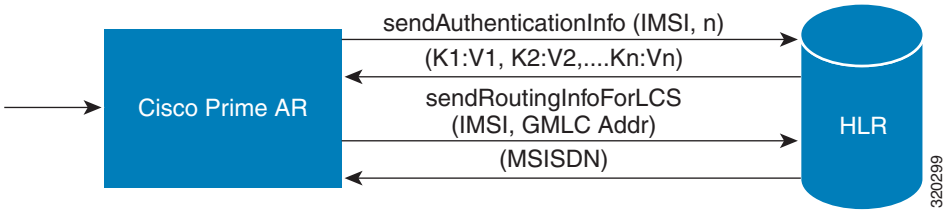
SIGTRAN, a working group of the Internet Engineering Task Force (IETF), has defined a protocol for the transport of real-time signaling data over IP networks. Cisco Prime Access Registrar (Prime Access Registrar) supports SS7 messaging over IP (SS7oIP) via SIGTRAN-M3UA, a new transport layer which leverages 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.

Prime Access Registrar supports SIGTRAN-M3UA in both Linux and Solaris platforms.

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 22-1 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. For more information, see Configuring M3UA Service with Map Restore Data Authorization, page 22-13.

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

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 following 32-bit rpm files while installing the Cisco Prime Access Registrar *without* SIGTRAN_M3UA process in RHEL 6.2 on Linux:
  - 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
  - nspr-4.8.8-3.el6.i686.rpm
  - nss-util-3.12.10-2.el6.i686.rpm
- ensure that you have the following 32-bit rpm files while installing the Prime Access Registrar *with* SIGTRAN_M3UA process in RHEL 6.2 on Linux:
  - 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
  - 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 verions relevant to the RHEL OS versions while installing the Prime Access Registrar.

- ensure that you have the following packages while installing the Prime Access Registrar on Solaris:
  - gcc version-3.4.6
  - 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 22-3

  - xml2-config-2.6.23
  - pkg-config-0.15.0
  - glib-2.30
  - gtk-2.41
  - libxml-2.2.6.20

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 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 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.

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

```
[ //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 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.
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.
GlobalTitleTranslationScript	This is used to specify the name of the script which is responsible for translating IMSI to Global Title Address (GTA).
Timeout	Specifies the time (in seconds) to wait before an authentication request times out; defaults to 15.
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.

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

Property	Description
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** Prime Access Registrar supports only ITU value.
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. This is the map layer network node number by which the HLR identifies the Prime Acces 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 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.
RemoteSubSystemNumber	Required; represents the sub system number of the remote server. The RemoteSubSyatemNumber is set as 6 by default.
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.

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

Property	Description
ServiceIndicatorOctet	Represents the service identifier octet. The value ranges from 0-255.
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	
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). 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.
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 22-1 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.
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.

Blacklisting IMSI Values

Prime Access Registrar allows you to blacklist one or more IMSI values available in the EAP-SIM or EAP-AKA requests forwarded to an HLR. A scripting point option is provided such that you can set an environment dictionary variable Blacklisted-IMSI to ***TRUE*** or ***FALSE*** to blacklist or whitelist IMSI values respectively. An IMSI value marked as blacklisted is rejected and will not be forwarded to the HLR.

To blacklist an IMSI value:

Step 1 Configure a SIGTRAN-M3UA remote server as described in Configuring SIGTRAN-M3UA Remote Server, page 22-6.

Step 2 Configure an EAP-AKA or EAP-SIM service with the SIGTRAN-M3UA remote server. See Configuring EAP-AKA/EAP-SIM with SIGTRAN-M3UA, page 22-4 for an example.

Step 3 Run the following script:

```
proc CheckBlackList {request response environ}
{
    set imsi [ $environ get IMSI ]
    if { [ string compare $imsi 984579621012345 ] == 0 }
    {
        $environ put Blacklisted-IMSI TRUE
        $environ put Notification-Code 19384
    }
}
```

Where, ***CheckBlackList*** is the entrypoint variable of the global title translation script *checklist*, as shown in the example below:

```
[ //localhost/Radius/Scripts/checklist ]
    Name = checklist
    Description =
    Language = tcl
    Filename = tclscript.tcl
    EntryPoint = CheckBlackList
    InitEntryPoint =
    InitEntryPointArgs =
```

If the environment variable *Blacklisted-IMSI* is set as ***TRUE*** and if the IMSI value available in the incoming script matches the given string, then that IMSI is blacklisted and will not be forwarded to the HLR. You can configure a notification code to represent failure. If no notification code is set, 16384 representing *General Failure* is sent upon rejection of an IMSI value.

Note Notification code is applicable only for EAP-SIM service.

Additionally, you can configure the script to compare the incoming IMSI against the configured IMSIs and take appropriate action as to whether blacklist or whitelist the incoming IMSI.

Configuring M3UA Service

Prime Access Registrar supports the M3UA service, which is used to fetch MSISDN from IMSI or vice versa 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 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 22-13 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 22-13.

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

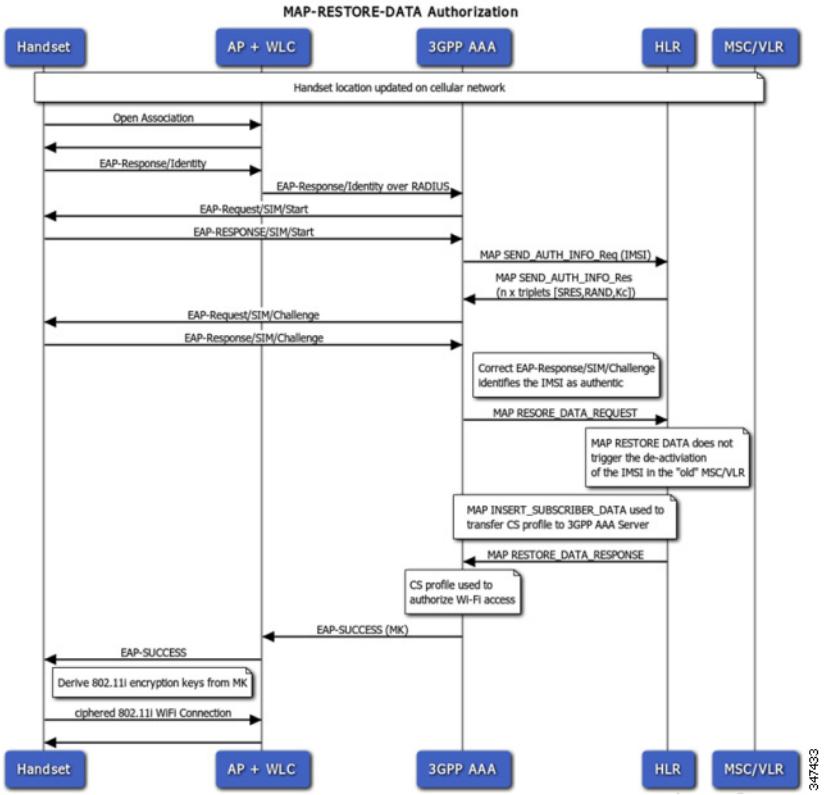
Prime Access Registrar sends a MAP_SEND_AUTH_INFO request to HLR on receiving EAP-SIM / EAP-AKA authentication request and fetches the authentication vectors in MAP_SEND_AUTH_INFO_RES message. Prime Access Registrar checks the IMSI and if it is authentic, sends a MAP_RESTORE_DATA_REQUEST to fetch the 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 22-2 represents the Map-Restore-Data message flow between Prime Access Registrar and HLR.

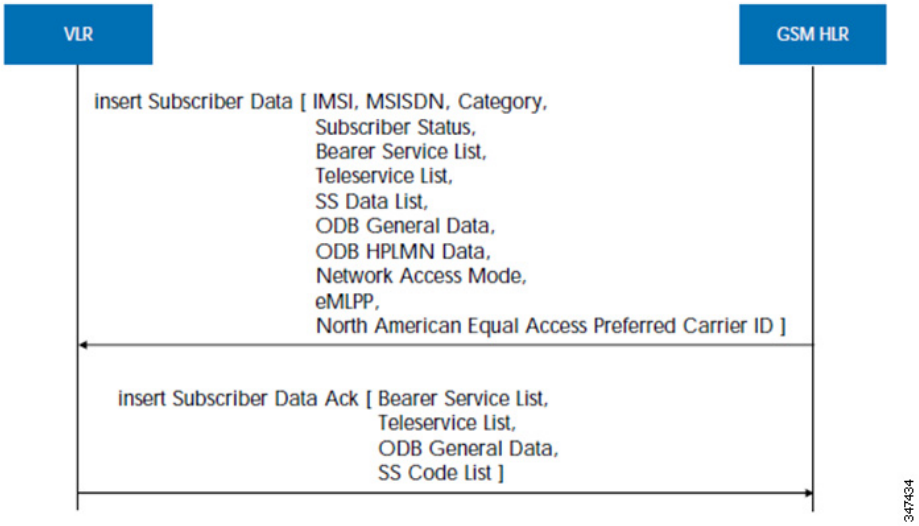
Figure 22-2 Map-Restore-Data Authorization Flow



CS Insert Subscriber Data Structure

Figure 22-3 shows the parameters fetched by Prime Access Registrar on reciept of the subscriber data request.

Figure 22-3 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 = activmode
        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 = ffssstatus
                        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 22-2 shows the restore data mapping parameters.

Table 22-2 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 ifthe 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 22-2 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 22-2 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.

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.