Wireless Support

This chapter provides the following information about using Cisco Prime Access Registrar (Prime Access Registrar) for wireless support:

Mobile Node-Home Agent Shared Key

In a mobile wireless environment, a Home Agent (HA) can request a Mobile Node-Home Agent (MN-HA) shared key from the home Prime Access Registrar RADIUS server during a mobile IP registration request (RRQ) from a Packet Data Serving Node (PDSN). Prime Access Registrar supports distribution of the shared key in this environment. Prime Access Registrar encrypts the shared key using MD5 encryption before sending the key back to the HA in an Access-Accept packet.

When an HA receives an RRQ from a PDSN, the HA authenticates the RRQ using a MN-HA shared key. If the HA does not have the MN-HA shared key, it retrieves the MN-HA shared key from the Prime Access Registrar server by sending an Access-Request packet containing the 3GPP2 VSA CDMA-MN-HA-SPI (SPI attribute). Prime Access Registrar then sends the CDMA-MN-HA-Shared-Key corresponding to the user if the user has been successfully authenticated.

This section contains the following topics:

Use Case Example

When HA receives an RRQ from a PDSN, it authenticates the RRQ by using a MN-HA shared key. If the HA does not have the MN-HA shared key, it retrieves the MN-HA shared key from the Prime Access Registrar server by sending an Access-Request packet containing the 3GPP2 vendor-specific attribute (VSA) CDMA-MN-HA-SPI, the Security Parameter Index (SPI attribute).

The Prime Access Registrar server then sends the CDMA-MN-HA-Shared-Key corresponding to the user if the user has successfully authenticated subject to the following rules:

1. If there is an incoming SPI and no configured SPI, the Prime Access Registrar server authenticates the user as usual and does not include a configured shared-key (if there is one) in the reply.
2. If the incoming SPI does not match the configured SPI, the Prime Access Registrar server authenticates the user as usual, but does not include the configured shared-key (if there is one) in the reply.
3. If the incoming SPI matches the configured SPI, but there is no shared-key configured, the Prime Access Registrar server proceeds with normal authentication. Since there is no shared-key, it will not be included in the reply.
4. If the incoming SPI matches the configured SPI and a configured shared-key exists, the Prime Access Registrar server proceeds to encrypt the MCD5 shared-key and include it in the Access-Accept.

The key to including the shared key in an Access-Accept is in matching the values of the SPI attribute.

Configuring User Attributes

Prime Access Registrar server supports user-specific attributes which enables the Prime Access Registrar server to return attributes on a per-user or per-group basis without having to use profiles.

Configuring the User Attributes

To configure a user with the CDMA-MN-HA-SPI VSA to request a MN-HA shared key:

Step 1 Log into the Prime Access Registrar server and launch **aregcmd**.

Log in as a user with administrative rights such as user **admin**.

Step 2 Change directory to the attribute directory of the user.

cd /Radius/UserLists/Default/bob/Attributes

Step 3 Set the CDMA-MN-HA-SPI VSA to the appropriate shared-key value.

set CDMA-MN-HA-SPI 1124

```
set CDMA-MN-HA-SPI 1124
```

Step 4 Set the CDMA-MN-HA-SPI VSA to the appropriate shared-key value.

set CDMA-MN-HA-Shared-Key secret112

```
set CDMA-MN-HA-Shared-Key secret112
```

Step 5 Validate and save your changes.

validate

save

3GPP2 Home Agent Support

The Prime Access Registrar server supports 3GPP2 home agents. This support enables mobile IP clients that authenticate through a Prime Access Registrar RADIUS server to be told which home agent they should use.

Every Mobile IP client has a home domain that is served by a group of Home Agents (HA). The Mobile IP client sets up a tunnel to one (and only one) HA during a session while it roams. Typically, the domain can be determined by the Mobile IP client's network access identifier (NAI).

Note The NAI is the userID submitted by the client during PPP authentication. In roaming, the purpose of the NAI is to identify the user as well as to assist in the routing of the authentication request.

During the authentication and authorization phase for each Mobile IP client, the RADIUS server must decide which HA from a group of HAs should be chosen to serve the client. This is called dynamic HA assignment.

This section contains the following topics:

Home-Agent Resource Manager

Prime Access Registrar supports dynamic HA assignment with a new resource manager type called home-agent. You configure the home-agent resource manager with a list of IP addresses. The Prime Access Registrar server assigns those addresses to clients whose request dictionary has the right attributes to indicate that an assignment should be done. This is similar to the *ip-dynamic* resource manager.

Unlike the ip-dynamic resource manager, HAs are not exclusively allocated to an individual session but are shared among a set of sessions.

Load Balancing

The goal of dynamic HA assignment is to have load balancing among HAs. The Prime Access Registrar server achieves this by evenly distributing mobile clients among HAs. At the same time, the Prime Access Registrar server ensures that the same HA is always assigned to the same Mobile IP client for the same session.

Configuring the Home Agent Resource Manager

To create a new resource manager using the **aregcmd** command:

Step 1 Use the **cd** command to change to the **Radius /ResourceManagers** level.

--> **cd /Radius/ResourceManagers**

```
[ //localhost/Radius/ResourceManagers ]

    Entries 0 to 0 from 0 total entries
    Current filter: <all>
```

Step 2 Use the **add** command to specify the name of a resource manager to create.

--> **add home-agent-pool**

```
--> Added home-agent-pool
```

Step 3 Use the **cd** command to change to the **Radius /ResourceManagers/home-agent-pool** level.

--> **cd home-agent-pool**

```
[ //localhost/Radius/ResourceManagers/home-agent-pool ]

    Name = home-agent-pool
    Description =
    Type =
```

Step 4 Use the **set** command to set the resource manager type to **home-agent**.

--> **set type home-agent**

Step 5 Use the **ls** command to view the subdirectories under home-agent-pool.

--> ls

```
[ //localhost/Radius/ResourceManagers/home-agent-pool ]

    Name = home-agent-pool
    Description =
    Type = home-agent
    Home-Agent-IPAddresses/
```

Step 6 Use the **cd** command to change to the **Radius/ResourceManagers/home-agent-pool/Home-Agent-IPAddresses** level.

--> **cd Home-Agent-IPAddresses**

```
[ //localhost/Radius/ResourceManagers/home-agent-pool/Home-Agent-IPAddresses ]
```

Step 7 Use the **add** command to add a single IP address or a range of IP addresses.

--> **add 209.165.200.200-209.165.200.254**

```
--> Added 209.165.200.200-209.165.200.254
```

Querying and Releasing Sessions

The **aregcmd** program has been modified to support a new filter for **query-session** and **release-session**. You can use this filter to restrict a request (either query or release) to just the sessions with a given home-agent IP address. For example, consider the following command line.

--> **query-session /radius with-home-agent 10.10.10.1**

This command line will return all sessions that have a home-agent resource equal to the IP address 10.10.10.1.

Querying sessions using **aregcmd** displays the home-agent resource in each session as:

HA ddd.ddd.ddd.ddd

where each *ddd* is a decimal number from 0-255.

Access Request Requirements

When the home-agent resource manager receives an Access-Request that contains a CDMA-HA-IP-Addr attribute, the home-agent resource manager checks the response dictionary to see if it already has a CDMA-HA-IP-Addr attribute. If it does, then the Mobile IP client has been assigned a HA address already and the resource manager does not need to do anything.

If the value of the CDMA-HA-IP-Addr attribute in the request dictionary is 0.0.0.0, the home-agent resource manager assigns a HA and puts a new CDMA-HA-IP-Addr attribute whose value is the IP address of the HA in the response dictionary.

If the value of the CDMA-HA-IP-Addr attribute is not 0.0.0.0, the Mobile IP client has been assigned a HA address already. The home-agent resource manager copies the attribute (with its value) from the request dictionary into the response dictionary.

The Prime Access Registrar server might select the session manager based on the domain (using the rule engine, dynamic properties, or scripting), and it allows each session manager to have its own home-agent resource manager.

New 3GPP2 VSAs in the Cisco Prime Access Registrar Dictionary

Prime Access Registrar supports 3GPP2 vendor-specfic attributes (VSAs) in the vendor-specific dictionary in **/Radius/Advanced/Attribute Dictionary**.

Note There is no planned support for the Accounting-Container (3GPP2/6) attribute because it has different syntax than other vendor-specfic attributes (VSAs) and requires special processing.

Session Correlation Based on User-Defined Attributes

All the session objects are maintained in one dictionary keyed by a string.

You can define the keying material to the session dictionary through a newly introduced environment variable, Session-Key. If the Session-Key is presented at the time of session manager process, it will be used as the key to the session object for this session. The Session-Key is of type string. By default, the Session-Key is not set. It's value should come from attributes in the incoming packet and is typically set by scripts. For example, CLID can be used to set the value of Session-Key.

Use the script UseCLIDAsSessionKey as defined in the script **rexscript.c** to specify that the Calling-Station-Id attribute that should be used as the session key to correlate requests for the same session. This is a typical case for 3G mobile user session correlation. You can provide your own script to define other attributes as the session key.

In the absence of the Session-Key variable, the key to the session will be created based on the string concatenated by the value of the NAS and the NAS-Port.

There is a new option *with-key* available in **aregcmd** for query-sessions and release-sessions to access sessions by Session-Key.

Managing Multiple Accounting Start/Stop Messages

Since the PDSN is aware when it sends a RADIUS stop followed by a start record, it inserts the new Session Continue attribute (3GPP2/48) into the stop record. The existence of the Session Continue attribute denotes that a start record will immediately be sent and the packet data session continues on the PDSN.

When Prime Access Registrar receives an accounting stop packet, the following two conditions trigger a release of a session and its resources:

- There is no 3GPP2/48 Session Continue attribute in the stop packet and the number of accounting stops received is greater or equal to the starts received for this session
- The 3GPP2/48 Session Continue attribute is present in the stop packet, but its value is zero (0)

Note One of the conditions above must be true to release the session and its resources.

NULL Password Support

Prime Access Registrar introduced a new Prime Access Registrar environment variable, *Allow-NULL-Password*. At authentication time, if the following three conditions are met, user authentication is bypassed:

1. Allow-NULL-Password environment variable is set to TRUE.
2. The User-Password or CHAP-Password must be NULL in the incoming request. (If it is not NULL, normal password checking will occur.)
3. A user record exists for this user.

By default, the *Allow-NULL-Password* environment variable is not set.

Note You should be aware of the security impact when using the NULL Password feature.

You can set this environment variable in three different ways:

1. For the user in local database, one new field ***AllowNullPassword*** is added in the user record. When Prime Access Registrar fetches a user record for authentication, if this field is set to TRUE and Allow-NULL-Password environment variable does not exist, it sets *Allow-NULL-Password* environment variable to TRUE.
2. If the user record is in LDAP database, then the *LDAPToEnvironmentMappings* must be defined to map an attribute in LDAP user record to *Allow-NULL-Password* environment variable.
3. Through scripting which allows the decision to be made based on runtime conditions, such as attributes in the access-request or policies.

3GPP Compliance

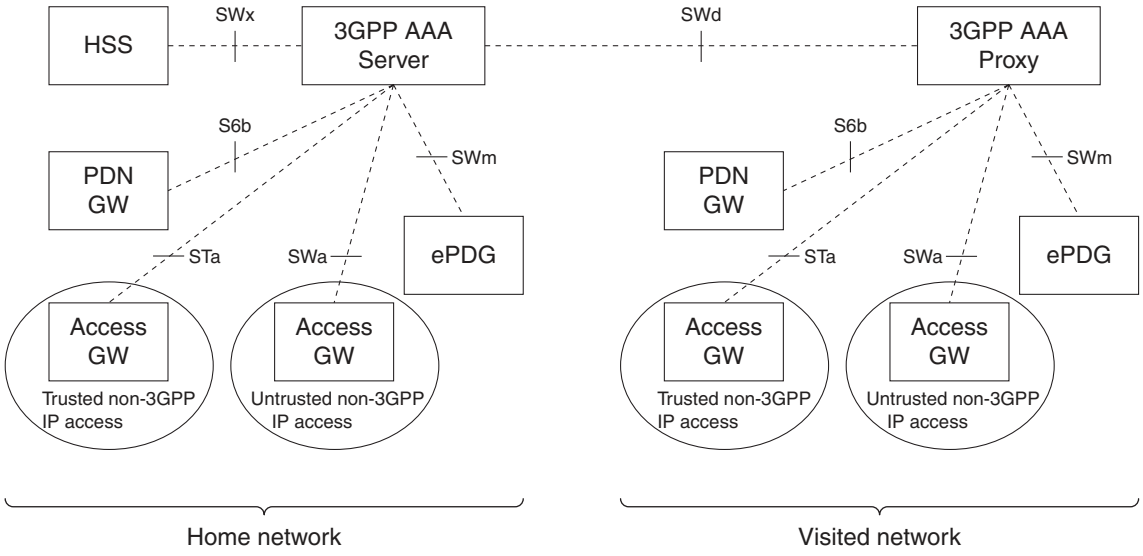
Prime Access Registrar supports 3GPP compliance by implementing the following (refer to RFC 29.273):

- SWa reference point between an untrusted non-3GPP IP access and a 3GPP AAA server/proxy. See SWa Access Authentication and Authorization, page 20-8.
- STa reference point between a trusted non-3GPP access and a 3GPP AAA server/proxy. See STa Access Authentication and Authorization, page 20-8.
- SWm reference point between an Evolved Packet Data Gateway (ePDG) and a 3GPP AAA server/proxy. See SWm Access Authentication and Authorization, page 20-9.
- SWd reference point between a 3GPP AAA server and a 3GPP AAA proxy. See SWd Access Authentication and Authorization, page 20-9.
- SWx reference point between a Home Subscriber Server (HSS) and a 3GPP AAA server. See SWx Authentication Procedure, page 20-10.
- S6b reference point between a PDN GW and a 3GPP AAA server/proxy. See S6b Authentication and Authorization Procedure, page 20-10.

This topic also contains the following sections:

Figure 20-1 depicts the various interfaces used for 3GPP compliance in a mobile network.

Figure 20-1 3GPP Interfaces



SWa Access Authentication and Authorization

The SWa reference point is defined between a non-3GPP IP access and a 3GPP AAA server or between a non-3GPP IP access and a 3GPP AAA proxy.

The SWa access authentication and authorization procedure includes the following steps:

1. The 3GPP AAA server issues an unsolicited re-auth request towards the untrusted non-3GPP access, indicating that both re-authentication and re-authorization of the user is needed.
2. Upon receipt of such a request, the untrusted non-3GPP access responds to the request and indicates the disposition of the request. This procedure is mapped to the Diameter command codes Re-Auth-Request and Re-Auth-Answer.
3. Upon receiving the re-auth request, the untrusted non-3GPP access immediately invokes the SWa authentication and authorization procedure requesting the identity of the user through EAP and using DER/DEA commands, with the same session-ID.
4. If the re-authentication of the user is not successful, the untrusted non-3GPP access detaches the user.

STa Access Authentication and Authorization

The STa reference point is defined between a non-3GPP access network and a 3GPP AAA Server or between a non-3GPP access network and a 3GPP AAA Proxy.

Prime Access Registrar decides whether a non-3GPP access network is trusted or untrusted by using the access authentication and authorization procedure executed between the non-3GPP access network and the 3GPP AAA server. This is implemented by the STa and SWa reference points sharing the same Diameter application and partly sharing the same authentication and authorization procedure. The STa

and SWa reference points are clearly distinguished after the exchange of the first authentication and authorization messages, during which trusted/untrusted decision is made by the 3GPP AAA server and this decision is communicated to the non-3GPP access network.

The trusted non-3GPP access authentication and authorization requires DiaEAP with EAP-AKA or EAP-AKA`. Prime Access Registrar implements the STa access authentication and authorization procedure based on the mobility parameters transported by the non-3GPP access network to the 3GPP AAA server.

This procedure follows the SWa authentication and authorization procedure, with the following differences:

- Information elements that reflect information about the user's service request and about the access network are mandatorily included in the authentication and authorization request.
- The information elements that describe the user's subscription profile are downloaded to the non-3GPP access network.

SWm Access Authentication and Authorization

The SWm reference point is defined between the ePDG and the 3GPP AAA server or between the ePDG and the 3GPP AAA proxy. It is used to authenticate and authorize a UE by transporting mobility parameters that are needed for the S2b interface. In particular this information may include the Packet Data Network (PDN) GW identity(s) and Access Point Name (APN(s)) currently allocated to a UE during a previous attach in a 3GPP access.

The SWm reference point performs authentication and authorization based on the reuse of the DER/DEA command set defined in the Diameter EAP application. The SWm access authentication and authorization procedure includes the following steps:

- The UE transmits a ‘tunnel establishment request’ message to the ePDG in order to establish a connection to the PDN.
- The ePDG initiates access authentication and authorization request to the 3GPP AAA server.
- During the access authentication and authorization procedure, the ePDG provides mobility parameters of the UE to the 3GPP AAA Server.
- The 3GPP AAA server performs IP mobility mode selection appropriately and upon successful authorization, it returns mobilty mode information back to the ePDG.

SWd Access Authentication and Authorization

The SWd reference point is defined between a 3GPP AAA proxy and a 3GPP AAA server. The SWd interface is used in roaming scenarios where the 3GPP AAA proxy is located in the visited network and the 3GPP AAA server is located in the home network. The 3GPP AAA proxy acts as a Diameter proxy agent and forwards Diameter commands between the Diameter client and the Diameter server.

When used in connection with an STa reference point, the SWd interface supports the trusted non-3GPP access authentication and authorization procedure. For this procedure, the 3GPP AAA proxy forwards the Diameter commands received from the 3GPP AAA server and the trusted non-3GPP access network as a stateful Diameter proxy.

When used in connection with the SWm reference point, the SWd interface supports the untrusted non-3GPP access authentication and authorization procedure. For this procedure, the 3GPP AAA proxy forwards the Diameter commands received from the 3GPP AAA server and the ePDG as a stateful Diameter proxy.

SWx Authentication Procedure

The SWx is a reference point defined between a HSS and a 3GPP AAA server. It is used in AAA server registration of a new user.

The authentication procedure includes the following steps:

1. The 3GPP AAA server registers the current 3GPP AAA server address in the HSS for a given user when a new subscriber has been authenticated by the 3GPP AAA server.
2. The 3GPP AAA server informs the HSS about the current PDN GW identity and APN being used for a given UE, or that a certain PDN GW and APN pair is no longer used.
3. Accordingly, the 3GPP AAA server may de-register the currently registered 3GPP AAA server in the HSS for a given user and purge any related non-3GPP user status data in the HSS. This occurs if the UE for some reason has been disconnected from the non-3GPP access.

HSS Initiated Update of User Profile

The subscriber profile management procedures over SWx include the subscriber profile push and the subscriber profile request. The SWx reference point enables the following:

- Indication to the 3GPP AAA server of change of non-3GPP subscriber profile within HSS.
- Activation and deactivation of the subscriber and equipment trace in the PDN GW.

This procedure is used between the 3GPP AAA Server and the HSS and is invoked by the HSS during the following circumstances:

- When the subscriber profile has been modified and needs to be sent to the 3GPP AAA Server. This may happen due to a modification in the HSS.
- To update the 3GPP AAA Server with the identity of a dynamically allocated PDN GW, which is included in the APN-Configuration AVP in the user profile as a result of the first PDN connection establishment associated with an APN over 3GPP access.

This procedure is mapped to the Diameter command codes Push-Profile-Request (PPR) and Push-Profile-Answer (PPA). An IMSI Range based mechanism is provided to select the HSS server. In the CLI, if the MultiplePeersPolicy is IMSIRangeBased, then the ranges are configured as a list and from them the HSS server is selected.

S6b Authentication and Authorization Procedure

The S6b reference point is defined between a PDN GW and a 3GPP AAA server (for non-roaming case, or roaming with home routed traffic to PDN GW in home network) and between a PDN GW and a 3GPP AAA proxy.The S6b interface protocol is based on Diameter. It uses the Diameter base protocol and also supports Diameter EAP application. The EAP methods EAP-AKA and EAP-AKA` are used.

The authentication and authorization procedure includes the following steps:

1. The S6b interface enables authentication and authorization between the UE and the 3GPP AAA server/proxy.
2. When the UE performs the DSMIPv6 initial attach, it runs an IKEv2 exchange with the PDN GW. In this exchange, EAP AKA is used for UE authentication over IKEv2. The PDN GW acts as an IKEv2 responder and an EAP pass-through authenticator for this authentication.

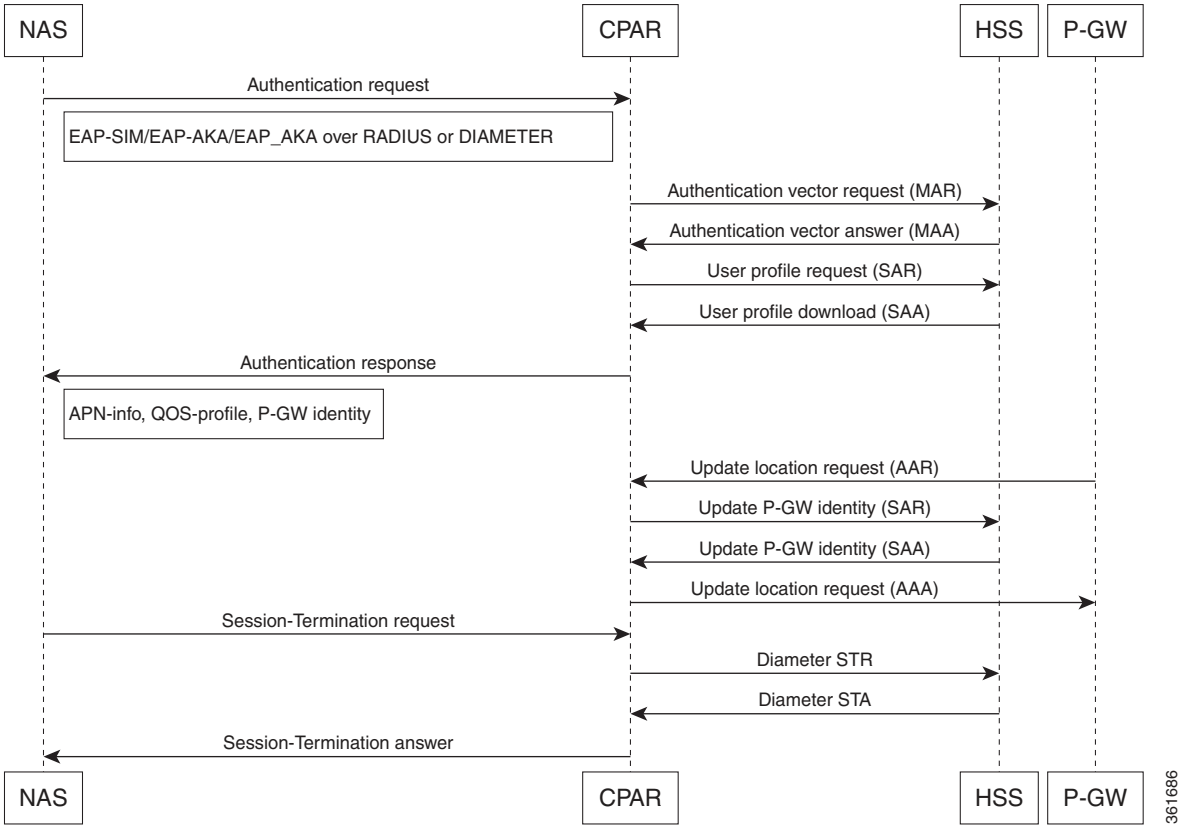
3. The S6b authentication and authorization procedure is invoked by the PDN GW after receiving an IKE_SA_AUTH message from the UE. The S6b reference point performs authentication based on reuse of the DER/DEA command set defined in Diameter EAP.

3GPP Call Flows

When Prime Access Registrar receives an authentication or authorization request from any of the access points, it sends the packet to the rules and policy engine for processing. The rules and policies are added in the configuration of Prime Access Registrar. Client, vendor, and server scripting points are provided in order to modify any AVPs in the packet or to decide upon the type of service that the packet requires. For example, if the service is Radius-to-Diameter translation, Prime Access Registrar performs the translation of Radius packet to Diameter packet and sends it to the remote server. The service also has scripting points that can be used to modify the incoming packets. Once authentication or authorization is done for the packet session management can be performed for the packet by storing the user sessions in a session cache, if the authentication or authorization is successful. The server, client, vendor, and service outgoing scripting points can be used to modify the response packet.

Figure 20-2 depicts the call flows implemented for 3GPP.

Figure 20-2 3GPP Call Flows



This topic contains the following sections:

- CLI for 3GPP Authorization, page 20-12
- CLI for 3GPP Reverse Authorization, page 20-12

CLI for 3GPP Authorization

Following is the CLI for 3GPP authorization service:

```
[ //localhost/Radius/Services/3gpp-authz-diameter]
    Name = 3gpp-authz-diameter
    Description = STa to SWx authz (update-gw, get-profile , push-profile from HSS, de-reg
from HSS )
    Type = 3gpp-authorization
    Protocol = Diameter
    IncomingScript~ =
   OutgoingScript~=
   SessionManager =
   DiameterProxyService =

[ //localhost/Radius/Services/3gpp-authz-radius]
    Name = 3gpp-authz-radius
    Description = STa to SWx authz (update-gw, get-profile , push-profile from HSS, de-reg
from HSS )
    Type = 3gpp-authorization
    Protocol = Radius
    SessionManager =
    TranslationService =

[ //localhost/Radius/Services/3gpp-authz-radius]
    Name = 3gpp-authz-radius
    Description = STa to SWx authz (update-gw, get-profile , push-profile from HSS, de-reg
from HSS )
    Type = 3gpp-reverse-authorization
     Protocol = Radius
    PreRequestTranslationScript~ =
    PostRequestTranslationScript~ =
    PreResponseTranslationScript~ =
    PostResponseTranslationScript~ =
    EnvMapping/
    ForwardMapping/
    ReverseMapping/
    ResponseMapping/

[ //localhost/Radius/Services/3gpp-authz]
    Name = 3gpp-authz-radius
    Description = STa to SWx authz (update-gw, get-profile , push-profile from HSS, de-reg
from HSS )
    Type = 3gpp-reverse-authorization
    Protocol = Diameter
    Incoming~ =
   Outgoing~=
    SessionManager =
    RequestMapping/
    EnvMapping/
    ResponseMapping/
```

CLI for 3GPP Reverse Authorization

3GPP reverse authorization is used during RADIUS to Diameter translation. You can set the corresponding parameter to TRUE during the RADIUS to Diameter conversion. In this case, the request command mapping must not be defined because a new diameter request is created from the radius request by the 3GPP reverse authorization service. For more information about RADIUS<->Diameter translations, see Translation Framework for Diameter, page 8-23.

Following is the CLI for 3GPP reverse authorization service:

```
[ //localhost/Radius/Services/reverse ]
Name = reverse
Description =
Type = 3gpp-reverse-authorization
IncomingScript~ =
OutgoingScript~ =
SessionManager = cache
TranslationService = diatorad
ProxyService =

[ //localhost/Radius/Services/diatorad ]
Name = diatorad
Description =
Type = diameter-radius
ProxyServiceName = rad-proxy
PreRequestTranslationScript~ =
PostRequestTranslationScript~ =
PreResponseTranslationScript~ =
PostResponseTranslationScript~ =
RequestMapping/
CommandMappings/
PPR = Radius-Access-Request
RAR = Radius-CoA-Request
AVPMappings/
Auth-Session-State = Cisco-AVPair
user-name = user-name
AVPsToBeAdded/
EnvironmentMappings/
ResponseMapping/
ResultCodeMappings/
Radius-CoA-ACK = Diameter-Success
Radius-CoA-NAK = Diameter-Unable-To-Deliver
AVPMappings/
AVPsToBeAdded/
EnvironmentMappings/
```