



Using Cisco Prime Access Registrar Server Features

This chapter provides information about how to use the Cisco Prime Access Registrar (Prime Access Registrar) server features.

This chapter contains the following sections:

- [Incoming Traffic Throttling](#)
- [Backing Store Parsing Tool](#)
- [Configurable Worker Threads Enhancement](#)
- [Session-Key Lookup](#)
- [Query-Notify](#)
- [Support for Windows Provisioning Service](#)
- [Command Completion](#)
- [Service Grouping Feature](#)
- [SHA-1 Support for LDAP-Based Authentication](#)
- [Dynamic Attributes](#)
- [Tunneling Support Feature](#)
- [xDSL VPI/VCI Support for Cisco 6400](#)
- [Apply Profile in Cisco Prime Access Registrar Database to Directory Users](#)
- [Directory Multi-Value Attributes Support](#)
- [MultiLink-PPP \(ML-PPP\)](#)
- [Dynamic Updates Feature](#)
- [NAS Monitor](#)
- [Automatic Information Collection \(arbug\)](#)
- [Simultaneous Terminals for Remote Demonstration](#)
- [Support for RADIUS Check Item Attributes](#)
- [User-Specific Attributes](#)
- [Packet of Disconnect](#)
- [Dynamic DNS](#)

- [Dynamic Service Authorization Feature](#)
- [Remote Session Management](#)
- [Wx Interface Support for SubscriberDB Lookup](#)
- [Smart Grid Solution Management](#)
- [Lawful Interception \(LI\) Support in Prime Access Registrar](#)
- [TACACS+ Support for AAA](#)

Incoming Traffic Throttling

Prime Access Registrar offers two options to tackle traffic bursts by limiting incoming traffic. You will find two properties, `MaximumIncomingRequestRate` and `MaximumOutstandingRequests`, under `/Radius/Advanced` to limit the incoming traffic.

This contains the following sections:

- [MaximumIncomingRequestRate](#)
- [MaximumOutstandingRequests](#)

MaximumIncomingRequestRate

You can use the `MaximumIncomingRequestRate` property to limit incoming traffic in terms of “allowed requests per second”.

For example, if you set the `MaximumIncomingRequestRate` to n , then at any given second, only n requests are accepted for processing. In the next second, another n requests are accepted regardless of whether the requests accepted earlier are processed or not. This condition serves as a soft limit.

The `MaximumIncomingRequestRate` property by default is zero (disabled).

MaximumOutstandingRequests

You can use the `MaximumOutstandingRequests` property to limit incoming traffic in terms of “requests processed”.

For example, if you set the `MaximumOutstandingRequests` to n , n requests are accepted for processing. Further requests are accepted only after processing some of these requests and sending the replies back. This condition serves as a hard limit.

The `MaximumOutstandingRequests` property by default is zero (disabled).



Note

You can enable either of these properties independent of the other.

Configuring the MaximumOutstandingRequests

To configure the `MaximumIncomingRequestRate` or `MaximumOutstandingRequests` property:

- Step 1** Log into `aregcmd`.
- Step 2** Change directory to `/Radius/Advanced`.

Step 3 Set the `MaximumIncomingRequestRate` or `MaximumOutstandingRequests` property to non-zero values.

```
set MaximumIncomingRequestRate n
```

or

```
set MaximumOutstandingRequests n
```

where *n* is any nonzero value.

Step 4 Save the configuration; enter:

```
save
```

Step 5 Reload the server; enter:

```
reload
```

Backing Store Parsing Tool

Prime Access Registrar tool, **carbs.pl**, helps to analyze the session backing store files. You will find this tool under `/cisco-ar/bin` directory.

Using `carbs.pl`, you can:

- Get information about the active, stopped, and stale RADIUS sessions.
- Clear phantom sessions manually.
- Process the binary log files and get information in a user-readable format.

The syntax is:

```
carbs.pl [-a] [-d <dir>] [-f <logfile>] [-v] [p] [-o <output>] [-h]
```

-a—All session statistics (active, stale, stopped)

-d—<Directory> Default: .

-f—<Filename> Default: 00*.log

-v—verbose Default: off

-p—Clear phantom sessions

-o—<Filename> Output log to TEXT

-h—Help, usage

[Table 9-1](#) lists the options available with `carbs.pl` and their description.

Table 9-1 *Carbs.pl Options and Description*

Option	Description
-d<directory>	Optional. Accepts a directory as parameter with no trailing slash. You can use this option to change the default directory to scan for BackingStore log files. Default is current directory.
-f<logfile>	Optional. Accepts a logfile as parameter with no leading or trailing slashes. You can use this option to change the default log files. Allows you to enter individual logfile name as well as wildcard characters surrounded by single quotes.
-v	Optional. No parameters. You can use this option to get total session count and phantom session count.
-p	Optional. No parameters. Generates a list of phantom sessions. You can use this option to clear the stale sessions.
-o	Optional. Accepts <output file> as parameter. You can use this option to convert BackingStore log files to readable files and write the results to the output file specified.
-a	Optional. No parameters. You can use this option to print all session statistics, such as per-NAS stale session count, total active sessions, and total stale sessions.
-h	You can use this option to get help with usage of carbs.pl.

Configurable Worker Threads Enhancement

Prime Access Registrar provides a configurable variable you can use to increase the number of worker threads to handle a greater number of RADIUS packets during peak operating periods. This variable controls the processing of greater number of RADIUS packets than expected during peak operating periods.

The variable, `RADIUS_WORKER_THREAD_COUNT`, is found in the **arserver** file under `/cisco-ar/bin/arserver` and controls the number of worker threads the Prime Access Registrar server creates. You can increase the number of worker threads to help make more efficient use of the server's CPU.



Note

Before you increase the setting for `RADIUS_WORKER_THREAD_COUNT`, you should be certain that you are running into a worker thread starvation issue. If you use scripts that consume a lot of processing and memory, you might run out of memory if you create too many worker threads.

Increasing the number of worker threads also increases memory utilization.

The purpose of this enhancement is to take advantage of spare CPU bandwidth which was not being used in earlier releases of Prime Access Registrar due to a lower number of worker threads. At times, the worker threads would be stuck doing work that took a long time to complete, like running a script. Having more threads will help mitigate these situations and will help improve on the latency created due to lack of free worker threads.

**Note**

Before modifying the RADIUS_WORKER_THREAD_COUNT variable, consult with a TAC representative to ensure that modifying the RADIUS_WORKER_THREAD_COUNT is warranted.

Modifying the RADIUS WORKER THREAD COUNT

To modify the RADIUS_WORKER_THREAD_COUNT variable:

Step 1 Log into the Prime Access Registrar server as a root user and change directory to **/cisco-ar/bin**.

Step 2 Use a text editor and open the **arserver** file.

Step 3 Locate the line with the RADIUS_WORKER_THREAD_COUNT variable.

```
#change this to configure number of worker threads  
RADIUS_WORKER_THREAD_COUNT=256
```

Step 4 Modify the number of RADIUS worker threads to the number you choose.

**Note**

There is no upper limit to the number of RADIUS worker threads you can enable in your Prime Access Registrar server, but you should take care not to exceed your server's memory capacity.

Step 5 Save the file and restart the Prime Access Registrar server.

Session-Key Lookup

The Session-Key Lookup feature enables you to identify the Session Manager and Session Key of an existing session based on certain attributes associated with that session, such as the Mobile Station Integrated Services Digital Network (MSISDN) number.

The Session-Key Lookup feature requires the following enhancements to Prime Access Registrar software:

- Enabling a query service to be invoked for Ascend-IP-Allocate packets
- Enabling the setting of the Session-Key and Session-Manager environment variables by a query operation
- Performing session management after the query operation
- A new environment variable, Set-Session-Mgr-And-Key-Upon-Lookup, which when set to TRUE causes a session-cache Resource Manager to set the Session-Manager and Session-Key environment variables during the query lookup.

The Session-Key Lookup feature is useful in a scenario where an existing session requires an update from an incoming Ascend-IPA-Allocate packet (from a different NAS or device) with modified authorization attributes. Note that this Ascend-IPA-Packet might not have the exact set of attributes as

the original packet that created the session. However, the Ascend-IPA-Allocate packet must contain at least one attribute that can uniquely identify the session (such as the MSISDN number) and should contain the same UserName of the original session.

The Session-Key Lookup feature works in tandem with the RADIUS Query feature, where a RADIUS Query service is defined with the unique attribute (such as the MSISDN number) as the query-key and is configured to query all session managers. The Query-Service environment variable is set to the defined RADIUS Query service and the new environment variable (Set-Session-Mgr-And-Key-Upon-Lookup) is set to TRUE for this Ascend-IPA-Allocate packet. This triggers a query operation on all the live sessions. If there is a match, the Session-Manager and Session-Key of that session is used for subsequent session management. During session management, the session cache is updated with the modified authorization attributes.

The Session-Manager (or any outgoing script that executes after the Session-Manager Outgoing Script) should not reject the packet when doing a Session-Key lookup. Doing so causes the session to be deleted.

Query-Notify

The Query-Notify feature enables you to store information about Wireless Application Protocol (WAP) gateways that have queried for User Identity-IP Address mapping and send appropriate messages to the WAP gateway when the subscriber logs out of the network.

Prime Access Registrar has been enhanced to update the session cache with the attribute-value pairs of an interim accounting update packet. This ensures the Prime Access Registrar server provides updated or current information to the WAP gateway during the proxy of interim records or query of the session cache.

Prime Access Registrar has been enhanced to also notify the WAP gateways that have queried a session with interim accounting update packets. If a WAP gateway does not respond to the Interim accounting update packets, the Prime Access Registrar server times out and retries by notifying the WAP gateways again. If there is no response after all the retries, the proxy packet is deleted and no change is made to the session or the WAP gateway's state in the Prime Access Registrar server. You can configure the number of retries under **/Radius/Clients/notificationproperties**.

The accounting response packet from the Prime Access Registrar server to the GPRS Gateway Support Node (GGSN) is independent of the proxy operation to the WAP gateways. The accounting response packet is sent back immediately without waiting for responses from the WAP gateways.

The Query-Notify feature also enables you to quarantine IP addresses for a configurable amount of time if a WAP gateway does not respond to Accounting-Stop packets sent by the Prime Access Registrar server.

The Prime Access Registrar server stores information about clients (usually the IP address) that queried for particular user information and sends RADIUS Accounting-Stop packets to those clients when the Prime Access Registrar server receives the Accounting-Stop packet. There is no intermediate proxy server between the Prime Access Registrar server and the WAP gateway.

To support the Query-Notify feature, the Prime Access Registrar server's *radius-query* service has been modified to also store information like the IP address about the clients queried for cached information. The information is stored in the user session record along with the cached information so it is available after a server reload.

Configuring the Query-Notify feature

To configure the Query-Notify feature:

-
- Step 1** Configure the Clients object under **/Radius/Clients**.
- Step 2** Set the EnableNotifications property to TRUE.
- The EnableNotifications property indicates that a client can receive Accounting-Stop notifications from the Prime Access Registrar server. When EnableNotifications is set to TRUE, a sub-directory named NotificationProperties appears in client object configuration.
- Step 3** Configure the properties under the client's NotificationProperties subdirectory.
- See , for information about how to configure these properties.
- Step 4** Configure a list of attributes to store under **/Radius/Advanced/Attribute Groups/<Notification Group>** where *<notification group>* is the name of an Attribute Group containing a list of attributes to be stored.
-

This section contains the following topics:

- [Call Flow](#)
- [Configuration Examples](#)
- [Memory and Performance Impact](#)

Call Flow

This section describes the call flow of the Query-Notify feature.

1. The Prime Access Registrar server caches information from an from Accounting-Start.
This information is usually from a GGSN when a subscriber enters into the network.
2. When a WAP gateway receives a request to authenticate a subscriber, it queries the Prime Access Registrar server using an Access-Request packet to retrieve the cached information for that subscriber.
3. The Prime Access Registrar server responds with Access-Accept if an entry is found for the subscriber in its cache; otherwise the server returns an Access-Reject.

The Prime Access Registrar server sends an Access-Accept packet to the WAP gateway. The list of attributes sent in this Access-Accept will depends on radius-query service configuration.



Note You use **aregcmd** to configure the attributes for the Access-Accept packet in the AttributesToBeReturned subdirectory under a radius-query service type.

4. If the Prime Access Registrar server finds a cache entry for the subscriber and if the EnableNotifications property is set to TRUE, the Prime Access Registrar server stores the client IP address in the subscriber's cache.
5. If the Prime Access Registrar server receives an Accounting-Interim-Update packet from the GGSN, it responds by sending an Accounting-Response packet then sends the Accounting-Interim-Update packets to all the queried clients of the WAP Gateways.

If the WAP gateway queried clients do not respond to the Accounting-Interim-Update packets, the Prime Access Registrar server times out and retries by notifying the WAP gateways again. If there is no response after all the retries, the proxy packet is deleted and no change is made to the session or the WAP gateway's state in the Prime Access Registrar server. The `StaleSessionTimeout` property under **/Radius/Advanced** is not applicable for Accounting-Interim-Update packets.

6. When the subscriber logs out of the network, the Prime Access Registrar server receives an Accounting-Stop packet and responds by sending an Accounting-Response back to the client.

Before releasing the subscriber's session, the Prime Access Registrar server looks for any client IP addresses in the subscriber's cache. If it finds any, the Prime Access Registrar server sends Accounting-Stop packets to those clients with the attributes configured in the `NotificationAttributeGroup` subdirectory for each client.

The Prime Access Registrar server forms the attributes with those attributes in the session cache and from the Accounting-Stop packet. The Prime Access Registrar server uses the value configured for the `Port` property in the `NotificationProperties` subdirectory as the destination port for the Accounting-Stop packet and uses the client's shared secret.

The Prime Access Registrar server then waits for Accounting-Response packets from each client to which it has sent Accounting-Stop packets. The Prime Access Registrar server waits for the time interval configured in the `InitialTimeout` property configured in the `NotificationProperties` subdirectory before sending another Accounting-Stop packet. If it does not receive an Accounting-Response packet, the Prime Access Registrar server sends additional Accounting-Stop packets until the number of attempts reaches the value configured in the `MaxTries` property in the `NotificationProperties` subdirectory.

7. When the Prime Access Registrar server receives an Accounting-Response packet from each client, the server releases the subscriber session.

If the Prime Access Registrar server does not receive Accounting-Response packets from all clients after the configured time and attempts, the server maintains the subscriber session for the time interval configured in the `StaleSessionTimeout` property in **/Radius/Advanced** then releases the subscriber session.

The Prime Access Registrar server maintains the subscriber session to address the quarantine IP address requirement. The Prime Access Registrar server must quarantine IP addresses if a WAP gateway does not respond to Accounting-Stop sent by the Prime Access Registrar server. The length of time an IP address is quarantined depends on the value of the `InitialTimeOut` property under the `NotificationProperties` subdirectory of **/Radius/Clients/wap_gateway**.

8. If the `StaleSessionTimeout` property is TRUE for a subscriber session, the Prime Access Registrar server rejects any query requests from clients for this session cache. After the `StaleSessionTimeout` expires, the Prime Access Registrar server will again send Accounting-Stop to all the clients listed in the session and proceeds to delete this subscriber session regardless of the status of the Accounting-Stop.

Configuration Examples



Note

In addition to the following configuration, the `StaleSessionTimeout` property must be set in **/Radius/Advanced**. This property has a default value of 1 hour.

The following shows an example configuration for a Query-Notify client:

```
[ //localhost/Radius/Clients/wap-gateway1 ]
  Name = wap-gateway1
  Description =
  IPAddress = 10.100.10.1
  SharedSecret = secret
  Type = NAS
  Vendor =
  IncomingScript~ =
  OutgoingScript~ =
  EnableDynamicAuthorization = FALSE
  NetMask =
  EnableNotifications = TRUE
  NotificationProperties/
    Port = 1813
    InitialTimeout = 5000
    MaxTries = 3
    NotificationAttributeGroup = notifyGroup
```

The following shows an example configuration for a Query-Notify AttributeGroup:

```
[ //localhost/Radius/Advanced/AttributeGroups/notifyGroup ]
  Name = notifyGroup
  Description =
  Attributes/
    1. User-Name
    2. Acct-Session-Id
    3. NAS-Identifier
    4. NAS-Port
```

Memory and Performance Impact

Using the Query-Notify feature will have the following effects:

- There will be a memory impact because the Prime Access Registrar server caches IP addresses of clients queried in the session record.
- There will be an impact on performance because the Prime Access Registrar server has to persist the cached IP address information before responding to **radius-query** requests.

Support for Windows Provisioning Service

Prime Access Registrar supports Microsoft's Windows Provisioning Service (WPS). WPS provides hotspot users with seamless service to public WLAN hotspots by using Microsoft Windows-based clients. The Microsoft WPS solution requires Microsoft-based software in the data center for the RADIUS server and the provisioning server.

This section contains the following topics:

- [Call Flow](#)
- [Example Configuration](#)
- [Unsupported Features](#)

Call Flow

The following is the WPS process and Wireless Internet Service Provider (WISP) packet sequence for a new wireless client login at a Wi-Fi hotspot location:

1. The client discovers the WISP network at a Wi-Fi hotspot.
2. The client authenticates as guest (with null username and credentials) to the Prime Access Registrar server .
3. The client is provisioned and a new account is created.
4. The client is authenticated using the new account credentials and accesses the Internet.

The Prime Access Registrar server performs the following functions during WPS:

1. Detects the guest subscriber login from the null username and null credentials during PEAPv0 (MS-PEAP) authentication.
2. Grants a successful login and returns a *sign-up* URL of the provisioning server as a PEAP-Type-Length-Value (TLV) in the next Access-Challenge Packet.

The following is an example value for the URL PEAP-TLV:

```
http://www.example.com/provisioning/master.xml#sign up
```

Where *#sign up* is the parameter for this action and is a required element of the value.

The sign-up URL value is passed when the user authenticates as guest. The sign-up URL is a fragment within the Master URL. You can also configure other fragments to be returned in the Master URL. See [Master URL Fragments, page 9-11](#) for more information about the different fragments.

3. Sends a VLAN-ID or IP filter (or both) in the final Access-Accept packet to restrict the guest user's accessibility to only the Provisioning server.
4. Authenticates using the user configuration in the user database after the client is provisioned and a new account is created.

Example Configuration

The following shows an example configuration for the WPS feature:

```
[ //localhost/Radius/Services/peapv0 ]
  Name = peapv0
  Description =
  Type = peap-v0
  IncomingScript~ =
  OutgoingScript~ =
  MaximumMessageSize = 1024
  PrivateKeyPassword = <password>
  ServerCertificateFile = <path_to_ServerCertificateFile>
  ServerRSAKeyFile = <path_to_ServerRSAKeyFile>
  CACertificateFile = <path_to_CACertificateFile>
  CACertificatePath = <path_to_CACertificatePath>
  ClientVerificationMode = Optional
  VerificationDepth = 4
  EnableSessionCache = True
  SessionTimeout = "5 Minutes"
  AuthenticationTimeout = 120
  TunnelService = eap-mschapv2
  EnableWPS = True
  MasterURL = http://www.example.com/provisioning/master.xml
```

```
WPSGuestUserProfile = WPS-Guest-User-Profile
```

When you set the EnableWPS property to TRUE, you must provide values for the properties MasterURL and WPSGuestUserProfile. See [Environment Variables, page 9-11](#) for more information.

Environment Variables

The following two environment variables are used to support WPS:

- [Send-PEAP-URI-TLV](#)
- [Master-URL-Fragment](#)

Send-PEAP-URI-TLV

Send-PEAP-URI-TLV property is a Boolean value used by the authenticating user service to make the PEAP-V0 service include the URI PEAP-TLV in the protected success message. Under different circumstances Prime Access Registrar might send back different fragments within the MasterURL to the client, as described above.

The conditions under which this has to be sent is best known to the user authentication service (the service that is specified within the eap-mschapv2 service, which in turn is the tunnel service for PEAP-V0 service). So when it decides that it needs to send back the URL it can set this variable to TRUE. The default value for this is FALSE.

Master-URL-Fragment

The Prime Access Registrar authenticating user service uses Master-URL-Fragment to set the fragment within the Master URL that needs to be sent back. The Prime Access Registrar user authentication service sets the fragment to different values under different circumstances. While the Send-PEAP-URL-TLV indicates whether to send the URL or not, Master-URL-Fragment is used to intimate which fragment within the URL needs to be sent. If this variable is not set and if it is required to send the URL, '#signup' will be sent by default.

Master URL Fragments

The following sections describe the different fragments the RADIUS server might send to the AP in the Master URL:

- [Sign up](#)
- [Renewal](#)
- [Password change](#)
- [Force update](#)

Sign up

This value is passed when the user authenticates as guest. The following is an example value for the URL PEAP-TLV:

```
http://www.example.com/provisioning/master.xml#sign up
```

where #sign up is the parameter for this action and a required element of the value.

Renewal

This value is passed when the user's account is expired and needs renewal before network access can be granted. The following is an example value for the URL PEAP-TLV:

```
http://www.example.com/provisioning/master.xml#renewal
```

where #renewal is the parameter for this action and a required element of the value.

Password change

This value is passed when the user is required to change the account password. An example value for the URL PEAP-TLV is:

```
http://www.example.com/provisioning/master.xml#passwordchange
```

where #passwordchange is the parameter for this action and a required element of the value.

Force update

This value is passed when the WISP requires the Wireless Provisioning Services on the client to download an updated XML master file. This method of updating the XML master file on the client should be used only to correct errors; otherwise, the TTL expiry time in the XML master file is used to provide background updates. The following is an example value for the URL PEAP-TLV:

```
http://www.example.com/provisioning/master.xml#forceupdate
```

where #forceupdate is the parameter for this action and a required element of the value.

Unsupported Features

The following features are part of the Microsoft WPS functionality, but are not supported in the Prime Access Registrar:

- [Account Expiration and Renewal](#)
- [Password Changing and Force Update](#)

Account Expiration and Renewal

When the user creates an account and logs in with that account, the RADIUS server authenticates and authorizes the request and sends back an Access-Accept with a Session-Timeout attribute. The Access Point (AP) then forces the wireless client to reauthenticate for every timeout value. When there is one timeout duration left in the user account, the RADIUS server needs to send back a *renewal* URL (a URL fragment within the master URL) to the client for the user to renew the account.

Prime Access Registrar does not support this feature because the interface the Prime Access Registrar server has with the CiscoSecure Remote Agent does not have provisions to get the expiration information of user account. However, this release does provide an environment variable to copy the URL fragment and to control whether or not to send the URL using another environment variable. This can be used to send the renewal URL. There are some limitations, however.

Password Changing and Force Update

The Password Changing option is passed when the user is required to change the account password. Force Update option is passed when the WISP requires the Wireless Provisioning Services on the client to download an updated XML master file.

These functions are not possible in this release for the same reason mentioned above, the loose coupling between Prime Access Registrar and the CiscoSecure Remote Agent. Additionally, there is no known use case for this. As mentioned above, you can use the newly added environment variables to trigger these options.

Command Completion

Prime Access Registrar's command completion feature provides online help by listing possible entries to the current command line when you press the Tab key after entering a partial command. The Prime Access Registrar server responds based on:

- The location of the cursor including the current directory
- Any data you have entered on the command line prior to pressing the Tab key

The command completion feature emulates the behavior of Cisco IOS and Kermit. When you press the Tab key after entering part of a command, the Prime Access Registrar server provides any identifiable object and property names. For example, after you first issue **aregcmd** and log into Prime Access Registrar, enter the following:

```
cd <Tab>
```

```
Administrators/ Radius/
```

Pressing the Tab key consecutively displays possible context-sensitive choices.

In the following example, after changing directory to **/Radius/services/local-file** an administrator wants to see the possible types of authentication services that can set.

```
cd /Radius/services/local-file
```

```
//localhost/Radius/Services/local-file ]
Name = local-file
Description =
Type = file
IncomingScript~ =
OutgoingScript~ =
OutagePolicy~ = RejectAll
OutageScript~ =
FilenamePrefix = accounting
MaxFileSize = "10 Megabytes"
MaxFileAge = "1 Day"
RolloverSchedule =
```

```
set type <Tab>
```

```
eap-leap      file      local      radius-session
eap-md5       group    odbc       rex
eap-sim       ldap     radius     tacacs-udp
```

Values can also be tab-completed. For example, if you decide to set the local-file service's type to file, you can do the following:

```
set type f<Tab>
```

and the command line completes to:

```
set type file
```

Service Grouping Feature

The Service Grouping feature enables you to specify multiple services (called *subservices*) to be used with authentication, authorization, or accounting requests. The general purpose is to enable multiple Remote Servers to process requests.

Perhaps the most common use of this feature will be to send accounting requests to multiple Remote Servers thus creating multiple accounting logs. Another common use might be to authenticate from more than one Remote Server where, perhaps the first attempt is rejected, other Remote Servers can be attempted and an Access-Accept obtained.

Clearly, in the accounting request example, each request must be successfully processed by each subservice in order for the originator of the accounting request to receive a response. This is known as a *logical AND* of each of the subservice results. In the authenticate example, the first subservice which responds with an accept is returned to the client or if all subservices respond with *reject*, then a reject is returned to the client. This is known as a *logical OR* of each of the subservice results.

A Service is specified as a Group Service by setting its type to *group*, specifying the ResultRule (AND or OR) and specifying one or more subservices in the GroupServices subdirectory. The subservices are called in numbered order and as such are in an indexed list similar to Remote Server specification in a radius Service. Incoming and outgoing scripts for the Group Service can be optionally specified.

A subservice is any configured non-Group Service. When a Group Service is used, each subservice is called in exactly the same manner as when used alone (such as if specified as the DefaultAuthenticationService). Incoming and Outgoing scripts are executed if configured and Outage Policies are honored.

This section contains the following topics:

- [Configuration Example - AccountingGroupService](#)
- [Configuration Example 2 - AuthenticationGroupService](#)

Configuration Example - AccountingGroupService

To configure an accounting Group Service to deliver accounting requests to multiple Remote Servers:

Step 1 The first task is to set up the subservices which are to be part of the AccountingGroupService. Since subservices are merely configured Services which have been included in a service group, you need only define two new Services.

For this example, we will define two new radius Services called *OurAccountingService* and *TheirAccountingService*. A provider might want to maintain duplicate accounting logs in parallel with their bulk customer's accounting logs.

Step 2 Change directory to **/radius/services**. At the command line, enter the following:

cd /radius/services

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

Step 3 At the command line, enter the following:

```
add OurAccountingService
```

```
add TheirAccountingService
```

The configuration of these Services is very similar to standalone Radius accounting service. Step-by-step configuration instructions are not provided, but the complete configuration is shown below:

```
[ //localhost/Radius/Services/OurAccountingService ]
Name = OurAccountingService
Description =
Type = radius
IncomingScript = OurAccountingInScript
OutgoingScript = OurAccountingOutScript
OutagePolicy = RejectAll
OutageScript =
MultipleServersPolicy = Failover
RemoteServers/
  1. OurPrimaryServer
  2. OurSecondaryServer

[ //localhost/Radius/Services/TheirAccountingService ]
Name = TheirAccountingService
Description =
Type = radius
IncomingScript = TheirAccountingInScript
OutgoingScript = TheirAccountingOutScript
OutagePolicy = RejectAll
OutageScript =
MultipleServersPolicy = Failover
RemoteServers/
  1. TheirPrimaryServer
  2. TheirSecondaryServer
```

The next step is to create the new **AccountingGroupService**. The purpose of this Service is to process Accounting requests through both **OurAccountingService** and **TheirAccountingService**.

Step 4 At the command line, enter the following:

```
add AccountingGroupService
```

```
Added AccountingGroupService
```

```
cd AccountingGroupService
```

```
[ //localhost/Radius/Services/AccountingGroupService ]
Name = AccountingGroupService
Description =
Type =
IncomingScript =
OutgoingScript =
```

set type group

```
Set Type group
```

Step 5 Set the ResultRule to *AND* to ensure that both services process the accounting request successfully.

set ResultRule AND

```
Set ResultRule AND
```

Is

```
[ //localhost/Radius/Services/AccountingGroupService ]
Name = AccountingGroupService
Description =
Type = group
IncomingScript =
OutgoingScript =
ResultRule = AND
GroupServices/
```

set IncomingScript AcctGroupSvcInScript**set OutgoingScript AcctGroupSvcOutScript**

Add OurAccountingService and TheirAccountingService as subservices of the Group Service.

Step 6 At the command line, enter the following:

cd GroupServices

```
[ //localhost/Radius/Services/AccountingGroupService/GroupServices ]
```

set 1 OurAccountingService

```
Set 1 OurAccountingService
```

Set 2 TheirAccountingService

```
Set 2 TheirAccountingService
```

Is

```
[ //localhost/Radius/Services/AccountingGroupService ]
Name = AccountingGroupService
Description =
Type = group
IncomingScript = AcctGroupSvcInScript
OutgoingScript = AcctGroupSvcOutScript
ResultRule = AND
GroupServices/
  1. OurAccountingService
  2. TheirAccountingService
```


This completes the setup of the AccountingGroupService. To use this Service simply set it as the DefaultAccountingService and/or configure a policy/rule set which will select this Service. Essentially, this can be used in the same manner as any other standalone service.

Summary of Events

The following describes the flow of what happens when a client sends an accounting request which is processed by the AccountingGroupService:

1. ActGroupSvcInScript is executed.
2. OurAccountingService is called.
3. OurAccountingService's Incoming Script, OurAccountingInScript is called.
4. The request is sent to the Remote Server OurPrimaryServer and/or OurSecondaryServer, if necessary.
5. If a response is not received, because we used the **AND** ResultRule, the request failed and no response is sent to the client and the request is dropped. If a response is received, then the process continues.
6. OurAccountingService's Outgoing Script, OurAccountingOutScript is called.
7. TheirAccountingService is called.
8. TheirAccountingService's Incoming Script, TheirAccountingInScript is called.
9. The request is sent to the Remote Server TheirPrimaryServer and/or TheirSecondaryServer, if necessary.
10. If a response is not received, because we used the **AND** ResultRule, the request failed and no response is sent to the client and the request is dropped. If a response is received, then the process continues.
11. TheirAccountingService's Outgoing Script, TheirAccountingOutScript is called.
12. AcctGroupSvcOutScript is executed.
13. Standard processing continues.

Configuration Example 2 - AuthenticationGroupService

To configure a Group Service for the purposes of providing alternate Remote Servers for a single authentication:



Note

If Service A rejects the request, try Service B.

Step 1

The first task is to set up the subservices which are to be part of the AuthenticationGroupService. Since subservices are merely configured Services which have been included in a service group, we will simply define two new Services. For simplicity, we will define two new radius Services called AuthenticationServiceA and AuthenticationServiceB.

Step 2

At the command line, enter the following:

```
cd /radius/services

[ //localhost/Radius/Services ]
```

```

Entries 1 to 2 from 2 total entries
Current filter: <all>
local-file/
local-users/

```

add AuthenticationServiceA

add AuthenticationServiceB

Step 3 The configuration of these Services is very similar to standalone Radius authentication service. Step-by-step configuration instructions are not provided, but the complete configuration is shown below:

```

[ //localhost/Radius/Services/AuthenticationServiceA ]
  Name = AuthentictionServiceA
  Description =
  Type = radius
  IncomingScript = AuthAInScript
  OutgoingScript = AuthAOutScript
  OutagePolicy = RejectAll
  OutageScript = AuthAOutageScript
  MultipleServersPolicy = Failover
  RemoteServers/
    1. PrimaryServerA
    2. SecondaryServerA

[ //localhost/Radius/Services/AuthenticationServiceB ]
  Name = AuthentictionServiceB
  Description =
  Type = radius
  IncomingScript = AuthBInScript
  OutgoingScript = AuthBOutScript
  OutagePolicy = RejectAll
  OutageScript = AuthBOutageScript
  MultipleServersPolicy = Failover
  RemoteServers/
    1. PrimaryServerB
    2. SecondaryServerB

```

The next step is to create the new "AuthenticationGroupService". The purpose of this Service is to process authentication requests through both AuthenticationServiceA and AuthenticationServiceB if AuthenticationServiceA rejects the request.

Step 4 At the command line, enter the following:

add AuthenticationGroupService

```
Added AuthenticationGroupService
```

cd AuthenticationGroupService

```
[ //localhost/Radius/Services/AuthenticationGroupService ]
  Name = AuthenticationGroupService
  Description =
  Type =
  IncomingScript =
  OutgoingScript =
```

set type group

```
Set Type group
```

Next set the ResultRule to **OR** because we want to ensure that if the first subservice rejects the request, we then try the second subservice. If the second subservice rejects the request, then the response to the client is a reject.

Step 5 At the command line, enter the following:

set ResultRule OR

```
Set ResultRule OR
```

Set IncomingScript AuthGroupSvcInScript

```
Set OutgoingScript AuthGroupSvcOutScript
```

Set IncomingScript AuthGroupSvcInScript

```
Set OutgoingScript AuthGroupSvcOutScript
```

ls

```
[ //localhost/Radius/Services/AuthenticationGroupService ]
  Name = AuthenticationGroupService
  Description =
  Type = group
  IncomingScript = AuthGroupSvcInScript
  OutgoingScript = AuthGroupSvcOutScript
  ResultRule = OR
  GroupServices/
```

Now we must add the services we created "AuthenticationServiceA" and "AuthenticationServiceB" as subservices of the Group Service.

Step 6 At the command line, enter the following:

cd GroupServices

```
[ //localhost/Radius/Services/AuthenticationGroupService/GroupServices ]
```

set 1 AuthenticationServiceA

```
Set 1 AuthenticationServiceA
```

Set 2 AuthenticationServiceB

```
Set 2 AuthenticationServiceB
```

Is

```
[ //localhost/Radius/Services/AuthenticationGroupService ]
  Name = AuthenticationGroupService
  Description =
  Type = group
  IncomingScript = AuthGroupSvcInScript
  OutgoingScript = AuthGroupSvcOutScript
  ResultRule = OR
  GroupServices/
    1. AuthenticationServiceA
    2. AuthenticationServiceB
```

This completes the setup of the AuthenticationGroupService. To use this Service simply set it as the DefaultAuthenticationService and/or configure a policy/rule set which will select this Service. Essentially, this can be used in the same manner as any other standalone Service.

Summary of Events

The following describes the flow of what happens when a client sends an Authentication request which is processed by the AuthenticationGroupService:

1. AuthGroupSvcInScript is executed.
2. AuthenticationServiceA is called.
3. AuthenticationServiceA's Incoming Script, AuthAInScript is called.
4. If the response is a reject or the request is dropped (due to an Outage Policy):
 - a. AuthenticationServiceA's Outgoing Script, AuthAOutScript is called.
 - b. Processing continues with the next service.
5. If the response is an Accept:
 - a. AuthenticationServiceA's Outgoing Script, AuthAOutScript is called.
 - b. Skip to step 9.
6. AuthenticationServiceB is called.
7. AuthenticationServiceB's Incoming Script, AuthBInScript is called.
8. Since this is the last subservice in our Group Service:
 - a. AuthenticationServiceB's Outgoing Script, AuthBOutScript is called.

- b. Regardless of whether the request is Accepted or Rejected, processing will continue at step 9.
9. AuthGroupSvcOutScript is executed.
10. Standard processing continues.

SHA-1 Support for LDAP-Based Authentication

The Prime Access Registrar server supports secure hash algorithm (SHA-1) for LDAP-based authentication. This feature enables the Prime Access Registrar server to authenticate users whose passwords are stored in LDAP servers and hashed using the SHA-1 encoding scheme.

SHA-1 support actually adds functionality for the following three features to Prime Access Registrar:

- Authentication of PAP access requests against an LDAP user entry that uses the SHA-algorithm to the hash password attribute
- Authentication of PAP access requests against an LDAP user entry that uses the SSHA algorithm to hash the password attribute
- Configuration of the Prime Access Registrar server to dynamically determine how password attributes retrieved from LDAP are encrypted and process them accordingly

This enhancement is 100% backwards compatible. All previously supported values for the PasswordEncryptionStyle property are still supported and still provide the same behavior. The only noticeable change is that **dynamic** is now the default value for the PasswordEncryptionStyle property.

This section contains the following topics:

- [Remote LDAP Server Password Encryption](#)
- [Dynamic Password Encryption](#)
- [Logs](#)

Remote LDAP Server Password Encryption

Apart from the two values, none and crypt, of the **PasswordEncryptionStyle** property on a Remote LDAP Server, SHA-1 supports adds three additional values for the PasswordEncryptionStyle property. [Table 9-2](#) lists the valid values for this property and describes the corresponding behavior.

Table 9-2 Remote LDAP Server Password Encryption Style Values

PasswordEncryptionStyle	Cisco Prime Access Registrar Behavior
none	All passwords retrieved from this LDAP server are assumed to be returned to Prime Access Registrar as clear text. (There is no change in this functionality.)
crypt	All passwords retrieved from this LDAP server are assumed to be returned to Prime Access Registrar as passwords encrypted using the UNIX <i>crypt</i> algorithm. (There is no change in this functionality.) Passwords can be preceded by the {crypt} prefix, which is stripped before comparing passwords.

Table 9-2 Remote LDAP Server Password Encryption Style Values (continued)

PasswordEncryptionStyle	Cisco Prime Access Registrar Behavior
SHA-1	<p>All passwords retrieved from this LDAP server are assumed to be returned to Prime Access Registrar as a Base64-encoded version of the user's password after it has been hashed using the SHA-1 mechanism (as defined by Netscape).</p> <p>Passwords can be preceded by the {sha} prefix, which is stripped before comparing passwords.</p>
SSHA-1	<p>All passwords retrieved from this LDAP server are assumed to be encrypted/hashed using the SSHA mechanism (as defined by Netscape). Passwords can be preceded by the {ssha} prefix, which is stripped before comparing passwords.</p> <p>Note This is a Netscape/iPlanet-specific mechanism.</p>
EAP-Mschapv2	<p>All passwords received from the LDAP server are expected to be returned to Prime Access Registrar as NT LAN Manager (NTLM) V1 hashes using the MD4 algorithm (RFC1320). NTLM v1 hashes are generated from the clear text password provided by the user. The NTLM passwords are stored with an NTLMv1= prefix in the database as shown in the example below.</p> <p>Example: NTLMv1=5B3844FB41E27C48A93B6C8C6864FB83</p> <p>This password encryption style is also applicable for Oracle-based authentication.</p>
dynamic	<p>The value instructs Prime Access Registrar to choose the encryption mechanism on a case-by-case basis after it determines the presence of a known prefix, which the LDAP server prepends to the value of the password attribute.</p> <p>For example, if the following was returned from an LDAP server as a password attribute: {SHA}qZk+NkcGgWq6PiVxeFDCbJzQ2J0=, the password would be processed using the SHA-1 mechanism. This value will be the new default for the PasswordEncryptionStyle property.</p>

Dynamic Password Encryption

When using the dynamic setting for the PasswordEncryptionStyle property on a Remote LDAP Server, the Prime Access Registrar server looks for the prefixes listed in [Table 9-3](#) to determine if encryption or a hash algorithm should be used during password comparison.



Note

Password prefixes are not case-sensitive.

Table 9-3 Remote LDAP Server Password Prefix Values

Password Prefix	Encryption/Hash Algorithm Used
none	None; when no known prefix is found, the password attribute is assumed to be in clear text.
{crypt}	UNIX crypt algorithm
{sha}	Secure Hash Algorithm, version 1 (SHA-1)
{ssha}	SSHA-1, as defined by Netscape.
{NTLMv1}	MD4 algorithm (RFC1320).

The default value for the PasswordEncryptionStyle property on a Remote LDAP Server is **dynamic**.

**Note**

Using the *dynamic* setting for the PasswordEncryptionStyle property will require a bit more processing for each password comparison. When using dynamic, the Prime Access Registrar server must examine each password for a known prefix. This should have no visible impact on performance.

Logs

Turn on trace to level 4 to indicate (via the trace log) which password comparison method is being used.

Dynamic Attributes

Prime Access Registrar supports dynamic values for the configuration object properties listed below. Dynamic attributes are similar to UNIX shell variables. With dynamic attributes, the value is evaluated at run time. All of the objects that support dynamic attributes will have validation turned off in **aregcmd**.

This section contains the following topics:

- [Object Properties with Dynamic Support](#)
- [Dynamic Attribute Format](#)
- [Configuration](#)
- [Example](#)
- [Notes](#)
- [Validation](#)

Object Properties with Dynamic Support

The following object properties support dynamic values:

Radius

DefaultAuthenticationService

DefaultAuthorizationService

DefaultAccountingService

DefaultSessionManager

IncomingScript

OutgoingScript



Note Do not use the following environment variables:
 Accounting-Service for the **/Radius/DefaultAccountingService**, Authentication-Service for the **/Radius/DefaultAuthenticationService**, or Authorization-Service for the **/Radius/DefaultAuthorizationService**
 User-Profile for the **BaseProfile**, User-Group for the **Group**, User-Authorization for the **AuthorizationScript**, Session-Manager for the **DefaultSessionManager**, or Session-Service for the **DefaultSessionService**.

/Radius/Clients

client1/

IncomingScript

OutgoingScript

/Radius/Userlist/Default

user1/

Group

BaseProfile

AuthenticationScript

AuthorizationScript

/Radius/UserGroup

Group1/

BaseProfile

AuthenticationScript

AuthorizationScript

/Radius/Vendor

Vendor1/

IncomingScript

OutgoingScript

/Radius/Service

Service1/

IncomingScript

OutgoingScript

OutageScript

OutagePolicy

/Radius/RemoteServers

remoteserver1/

IncomingScript


```

OutgoingScript
Remoteldapservers1/
Searchpath
Filter

```



Note To differentiate the properties that support dynamic attributes, we place a tilde (~) after each property, as in IncomingScript~. However, when the Prime Access Registrar administrator is required to set values for those properties, continue to use the original property name, such as set IncomingScript \${elrealm} {Test}. The tilde is only for visual effect, and including the tilde will generate an error (“310 command Failed.”)

Dynamic Attribute Format

The format of the dynamic attribute is:

```

${eq|attribute-name}{default-name}

```

where **e** stands for environment dictionary, **q** stands for request dictionary, and **p** stands for response dictionary. You can use e, q, and p in any order. The attribute name is the name for the attribute from environment dictionary, request dictionary, or response dictionary.

For example,

```

/Radius
DefaultAuthenticationService = ${eq|realm}{local-users}

```

The default Authentication Service is determined at run time. Prime Access Registrar first checks to see if there is one value of **realm** in the environment dictionary. If there is, it becomes the value of DefaultAuthenticationService. If there is not, check the value of realm in the request dictionary. If there is one value, it becomes the value of DefaultAuthenticationService. Otherwise, local-users is the DefaultAuthenticationService. If we do not set local-users as the default value, the DefaultAuthenticationService is *null*. The same concept applies to all other attribute properties.

The validation for the dynamic values of the object property will only validate the default value. In the above example, Prime Access Registrar will do validation to check whether local-users is one of services defined in the service subdirectory.



Note

When setting specific property values, do not use the tilde (~) in the property name. Doing so generates a *310 Command Failed* error.

Tunneling Support Feature

Tunneling support is strictly based upon the IETF RFC: “RADIUS Attributes for Tunnel Protocol Support” (<http://www.ietf.org/rfc/rfc2868.txt>).

Table 9-4 lists the tunneling attributes supported in this Prime Access Registrar release.

Table 9-4 Tunneling Attributes Supported by Prime Access Registrar

Attribute Number	Attribute
64	Tunnel-Type
65	Tunnel-Medium-Type
66	Tunnel-Client-Endpoint
67	Tunnel-Server-Endpoint
69	Tunnel-Password
81	Tunnel-Private-Group-ID
82	Tunnel-Assignment-ID
83	Tunnel-Preference
90	Tunnel-Client-Auth-ID
91	Tunnel-Server-Auth-ID

The tunneling attribute has the following format:

(1 byte)	(1 byte)	(1 byte)	(variable number of bytes)
Type	Length	Tag	Value

This section contains the following topics:

- [Configuration](#)
- [Example](#)
- [Notes](#)
- [Validation](#)

Configuration

1. Configure the tag attributes as untagged attributes under the **/Radius/Advanced/Attribute Dictionary** directory (for example, **Tunnel-Type**).
2. Attach the “_tag” tag to these attributes when configuring the attributes under all of the other directories as tagged attributes (for example, **Tunnel-Type_tag10** under the **/Radius/Profiles/test** directory). Without the tag number, the default value is (**_tag = _tag0**).

Example

```

/Radius/Advanced/Attribute Dictionary
  /Tunnel-Client-ID
    Name = Tunnel-Client-Endpoint
    Description =
    Attribute = 66
    Type = STRING
    Min = 0
    Max = 253

/Radius/Profiles/test

```

```
Name = test
Description =
/Attributes
  Tunnel-Client-Endpoint_tag3 = "129.56.112.1"
```

Notes

1. “_tag” is reserved for the tunneling attributes. No other attributes should include this suffix.
2. The tag number value can range from 0 through 31.

Validation

The Prime Access Registrar server checks whether the tag attributes are defined under the **/Radius/Advanced/Attribute Dictionary** directory. The server also checks whether the tag number falls within the range (0-31).

xDSL VPI/VCI Support for Cisco 6400

To provide this support, a distinction must be made between device authentication packets and regular user authentication packets. This section contains the following topics:

- [Using User-Name/User-Password for Each Cisco 6400 Device](#)
- [Format of the New User-Name Attribute](#)

Using User-Name/User-Password for Each Cisco 6400 Device

This approach assumes that for every 6400 NAS, a device-name/device-password is created for each. Following are the required changes:

For each NAS in Prime Access Registrar:

```
Name = test6400-1
Description =
IPAddress = 209.165.200.224
SharedSecret = secret
Type = NAS
Vendor =
IncomingScript =
OutgoingScript =
Device-Name = theDevice
Device-Password = thePassword
```

When the 6400 sends out the device authentication packet, it might have different **User-Name/User-Password** attributes for each 6400 NAS. When Prime Access Registrar receives the packet, it tries to obtain the **Device-Name/Device-Password** attributes from the NAS entry in the Prime Access Registrar configuration database. When the **User-Name/User-Password** in the packet match the configured **Device-Name/Device-Password** attribute values, Prime Access Registrar assumes that it must get the device. The next step is to replace the **User-Name** attribute with the concatenated `<module>/<slot>/<port>` string. From this point, the packet is treated as a regular packet.

**Note**

A user record with the name of the concatenated string must be created.

Format of the New User-Name Attribute

After the device is identified, the **User-Name** attribute is replaced with the new value. This new value is the concatenation of 6400 *<module>/<slot>/<port>* information from the **NAS-Port** attribute and the packet is treated as a regular user authentication from this point on.

**Note**

This format only supports NAS Port Format D. See Cisco IOS documentation for more information about NAS port formats.

The format of the new **User-Name** attribute is the **printf** of “%s-%d-%d-%d-%d-%d” for the following values:

NAS-IP—in dot format of the **NAS-IP-Address** attribute. For example, 10.10.10.10.

slot—apply mask 0xF0000000 on **NAS-Port** attribute and shift right 28 bits. For example, **NAS-Port** is 0x10000000, the slot value is 1.

module—apply mask 0x08000000 on **NAS-Port** attribute and shift right 27 bits. For example, **NAS-Port** is 0x08000000, the module value is 1.

port—apply mask 0x07000000 on **NAS-Port** attribute and shift right 24 bits. For example, **NAS-Port** is 0x06000000, the port value is 6.

VPI—apply mask 0x00FF0000 on **NAS-Port** attribute and shift right 16 bits. For example, **NAS-Port** is 0x00110000, the VPI value is 3.

VCI—apply mask 0x0000FFFF on **NAS-Port** attribute. For example, **NAS-Port** is 0x00001001, the VCI value is 9.

Apply Profile in Cisco Prime Access Registrar Database to Directory Users

You can define the **User-Profile** and **User-Group** environment variables in the directory mapping and Prime Access Registrar will apply the profiles defined in the Prime Access Registrar database to each directory user having any of these two variables set.

This section contains the following topics:

- [User-Profile](#)
- [User-Group](#)
- [Example User-Profile and User-Group Attributes in Directory User Record](#)

User-Profile

This attribute is of type string with the format:

<Value1>::<Value2> ...

The **User-Profile** attribute is intended to hold a list of profile names. *<Value1>* and *<Value2>* represent the names of the profiles. They are separated by the “:” character, therefore, the “:” can not be part of the profile name. The order of values in the string has significance, as the profiles are evaluated from left to right. In this example, profile *<Value2>* is applied after profile *<Value1>*.

Assume the user record has a field called `UserProfile` that holds the name of the profile that applies to this user. This field is mapped to the environment attribute **User-Profile**. Following is how the mapping is done with **aregcmd**:

```
QuickExample/
  Name = QuickExample
  Description =
  Protocol = ldap
  IPAddress = 209.165.200.224
  Port = 389
  ReactivateTimerInterval = 300000
  Timeout = 15
  HostName = QuickExample.company.com
  BindName =
  BindPassword =
  UseSSL = FALSE
  SearchPath = "o=Ace Industry, c=US"
  Filter = (uid=%s)
  UserPasswordAttribute = password
  LimitOutstandingRequests = FALSE
  MaxOutstandingRequests = 0
  MaxReferrals = 0
  ReferralAttribute =
  ReferralFilter =
  PasswordEncryptionStyle = None
  LDAPToEnvironmentMappings/
    UserProfile = User-Profile
  LDAPToRadiusMappings/
```

After Prime Access Registrar authenticates the user, it checks whether **User-Profile** exists in the environment dictionary. If it finds **User-Profile**, for each value in **User-Profile**, Prime Access Registrar looks up the profile object defined in the configuration database and adds all of the attributes in the profile object to the response dictionary. If any attribute is included in more than one profile, the newly applied profile overrides the attribute in the previous profile.

User-Group

You can use the **User-Group** environment variable to apply the user profile as well. In Prime Access Registrar, a user can belong to a user group, and that user group can have a pointer to a user profile. When Prime Access Registrar finds that a packet has **User-Group** set, it obtains the value of the **User-Profile** within the user group, and if the **User-Profile** exists, it applies the attributes defined in the user profile to that user.

Note that in Prime Access Registrar, every user can also directly have a pointer to a user profile. Prime Access Registrar applies profiles in the following order:

1. If the user profile defined in the user group exists, apply it.
2. If the user profile defined in the user record exists, apply it.

The profile in **User-Group** is more generic than in **User-Profile**. Therefore, Prime Access Registrar applies the profile from generic to more specific.

Example User-Profile and User-Group Attributes in Directory User Record

You can use an existing user attribute in the user record to store profile info. When this is a new attribute, we suggest you create a new auxiliary class **AR_UserRecord** for whichever user class is used.

AR_User_Profile and **AR_User_Group** are two optional members in this class. They are of type string. The mapping is as follows:

```
LDAPToEnvironmentMappings/
  AR_User_Profile = User-Profile
  AR_User_Group = User-Group
```

Directory Multi-Value Attributes Support

If any attributes mapped from the LDAP directory to the Prime Access Registrar response dictionary are multivalued, the attributes are mapped to multiple RADIUS attributes in the packet.

MultiLink-PPP (ML-PPP)

Prime Access Registrar supports MultiLink-PPP (ML-PPP). ML-PPP is an IETF standard, specified by RFC 1717. It describes a Layer 2 software implementation that opens multiple, simultaneous channels between systems, providing additional bandwidth-on-demand, for additional cost. The ML-PPP standard describes how to split, recombine, and sequence datagrams across multiple B channels to create a single logical connection. The multiple channels are the ports being used by the Network Access Server (NAS).

During the AA process, Prime Access Registrar authenticates the user connection for each of its channels, even though they belong to the same logical connection. The Authentication process treats the multilink connection as if it is multiple, single link connections. For each connection, Prime Access Registrar creates a session dedicated for management purposes. The session stays active until you logout, which subsequently frees up all of the ports in the NAS assigned to each individual session, or until the traffic is lower than a certain threshold so that the secondary B channels are destroyed thereafter. Prime Access Registrar has the responsibility of maintaining the active session list and discards any session that is no longer valid in the system, by using the accounting stop packet issued from NAS. The multiple sessions that were established for a single logical connection must be destroyed upon the user logging out.

In addition, the accounting information that was gathered for the sessions must be aggregated for the corresponding logical connection by the accounting software. Prime Access Registrar is only responsible for logging the accounting start and accounting stop times for each session. As those sessions belong to the same bundle, IETF provides two standard RADIUS attributes to identify the related multilink sessions. The attributes are **Acct-Multi-Session-Id** (attribute **50**) and **Acct-Link-Count** (attribute **51**), where **Acct-Multi-Session-Id** is a unique Accounting identifier used to link multiple related sessions in a log file, and **Acct-Link-Count** provides the number of links known to have existed in a given multilink session at the time the Accounting record was generated. The Accounting software is responsible for calculating the amount of the secondary B channel's connection time.

The secondary B channel can go up and down frequently, based upon traffic. The Ascend NAS supports the **Target-Util** attribute, which sets up the threshold for the secondary channel. When the traffic is above that threshold the secondary channel is up, and when the traffic is below that threshold, the secondary B channel is brought down by issuing an Accounting stop packet to Prime Access Registrar. On the other hand, if you bring down the primary channel (that is, log out), the secondary B channel is also destroyed by issuing another Accounting stop packet to Prime Access Registrar.

Table 9-5 lists ML-PPP related attributes.

Table 9-5 ML-PPP Attributes

Number	Attribute	Cisco NAS (IOS 11.3 Release)	Ascend NAS
44	Acct-Session-Id	Supported	Supported
50	Acct-Multi-Session-Id	Supported	Supported
51	Acct-Link-Count	Supported	Supported
62	Port-Limit	Supported	Supported
124	Target-Util	Not Supported	Supported
125	Maximum-Channels	Supported	Supported

Following are sample configurations for ML-PPP:

```

/RADIUS
  /Profile
    /Default-ISDN-Users
      Name = Default-ISDN-Users
      Description =
      Attributes/
        Port-Limit = 2
        Target-Util = 70
        Session-Timeout = 70

/RADIUS
  /UserGroups
    /ISDN-Users
      Name = ISDN-Users
      Description = " Users who always use ISDN"
      BaseProfile = Default-ISDN-Users
      Authentication-Script =
      Authorization-Script =

```

The **Port-Limit** attribute controls the number of concurrent sessions a user can have. The **Target-Util** attribute controls the threshold level at which the second B channel should be brought up.

Dynamic Updates Feature

The Dynamic Updates feature enables changes to server configurations made using **aregcmd** to take effect in the Prime Access Registrar server after issuing the **save** command, eliminating the need for a server **reload** after making changes.

Table 9-6 lists the RADIUS object and its child objects. For each object listed, the **Add** and **Modify or Delete** columns indicate whether a dynamic update occurs after adding, modifying, or deleting an object or attribute. Entries in the **Add** and **Modify or Delete** columns also apply to child objects and child attributes of the objects listed, unless the child object is explicitly listed below the object, such as **/RADIUS/Advanced/Ports** or **/RADIUS/Advanced/Interfaces**.

Table 9-6 Dynamic Updates Effect on Radius Server Objects

Object	Add	Modify or Delete
Radius	Yes	Yes
UserLists	Yes	Yes
UserGroups	Yes	Yes
Policies	Yes	Yes
Clients	Yes	Yes
Vendors	Yes	Yes
Scripts	Yes	Yes
Services	Yes	Yes
SessionManagers	Yes	No
ResourceManagers	Yes	No
Profiles	Yes	Yes
Rules	Yes	Yes
Translations	Yes	Yes
TranslationGroups	Yes	Yes
RemoteServers	Yes	No
Replication	No	No
Advanced	Yes	Yes
SNMP	No	No
Ports	No	No
Interfaces	No	No

The Dynamic Updates feature is subject to the following limitations:

- Changes to the Ports or Interfaces objects are not dynamically updated. An **aregcmd reload** command must be issued for these changes to be propagated to the Prime Access Registrar server.
- Changes (modifications and deletions) to existing Session Manager and Resource Manager objects are not dynamically updated. An **aregcmd reload** command must be issued for these changes to be propagated to the Prime Access Registrar server. However, additions of new Session Manager and Resource Manager objects are dynamically updated. Active sessions and allocated resources are preserved in this case.
- Changes to the Prime Access Registrar configuration might not be immediately propagated to the server. Dynamic updates are only carried out in a *safe* environment (that is, when packets are not being processed and when packet processing can be delayed until the changes can be made on the server safely). Dynamic updates will yield to packet processing when appropriate, thus not significantly impacting server performance.
- Changes to SNMP require the Prime Access Registrar server to be restarted (**/etc/init.d/arservagt restart**)

NAS Monitor

The ability to monitor when a NAS is *down* (really only unreachable from Prime Access Registrar) is provided by **nasmonitor**. This program will repeatedly query a TCP port at the specified IP address until the device (NAS) is reachable. If the NAS is not reachable after a period of time, a warning e-mail is sent; if the NAS is still not reachable after another period of time, a message is sent to Prime Access Registrar to release all sessions associated with that NAS. The port to query, the query frequency, the first time interval, the back-off time interval, and the E-mail address to send to are all configurable (with defaults); the only required parameter is the NAS IP address. This program will work for any device that has a TCP port open; it can either be run by hand, when desired, or put in a **cron** job. See **nasmonitor -h** for details.

**Note**

You must have **telsh** installed in **/usr/local/bin** to use **nasmonitor**. **telsh** is part of the standard Tcl installation that can be downloaded from <http://www.scriptics.com>.

Automatic Information Collection (arbug)

You can use the script **arbug** to collect information about your Prime Access Registrar server. The results are collected into a tarball that can be e-mailed or **ftped** to Cisco as requested.

arbug collects all the relevant information needed to report a problem to Prime Access Registrar support. The goal of the **arbug** script is to make sure all the necessary information is collected.

**Note**

The **arbug** script neither updates nor replaces any system or Prime Access Registrar-related configuration.

This section contains the following topics:

- [Running arbug](#)
- [Files Generated](#)

Running arbug

To run the **arbug** script, change directory to **/cisco-ar/bin** and enter the following:

```
./arbug
```

The following is a typical sequence.

```
Looking around...
Cluster:
User: admin
Password:
The report /tmp/arbug.10085/arbug.tar is ready to send; you
may want to compress it first using gzip or compress.
hostname user_name bin>
```

Files Generated

The **arbug** script generates five files that are compressed into a tarball. Table 9-7 provides a summary of the information found in each of the files.

Table 9-7 Files Generated by *arbug*

File	Description
car.debug.tar.*	Machine-specific information including OS type, RAM details, disk space information, swap space information, patch information and open file details.
car.config.tar.*	Prime Access Registrar server configuration, server statistics, database dump by taking the administrator username and password as the input.
car.confini.tar.*	Information about ODBC .ini files and SNMP configuration
car.core.tar.*	Core files if any are present
car.logcscrsr.tar.*	Information from scripts directory, certificate directory, license directory

Simultaneous Terminals for Remote Demonstration

Multiple people can view and interact in a single demonstration by using the *share-access* program, a standard GNU release with a special configuration for use with Prime Access Registrar. To run **screen**, a technical support specialist (CSE or DE) will **telnet** to your server and log in as *cisco*. While you run **/opt/CSCOar/bin/share-access** (assuming **/opt/CSCOar** is the Prime Access Registrar path) as *root*, the CSE or DE runs **/opt/CSCOar/bin/share-access -r root**. Now both people (or more) can see what the other types, as well as the results of the commands entered. The special Prime Access Registrar configuration only allows *root* and *cisco* to run **screen**. To end a **share-access** session, type Control-D.

Support for RADIUS Check Item Attributes

Prime Access Registrar supports RADIUS check item attributes configuration at the user and group levels. You can configure the Prime Access Registrar server to check for attributes that must be present or attributes that must not be present in the Access-Request packet for successful authentication.

When using check item attributes, the Prime Access Registrar server will reject Access-Requests if:

- Any of the configured check item attributes are not present in the Access-Request packet
- Any of the Access-Request packet's check item attribute values do not match with those configured check item attribute values

For remote servers using either LDAP or ODBC, Prime Access Registrar allows for mapping of certain LDAP or ODBC fields to check item attributes. The mapped attributes can be used as check item attributes while processing the Access-Request packets.

When you configure check item attributes at both the user and group levels, the Prime Access Registrar server first checks the attributes of the user level before those of the group level. The Prime Access Registrar server must first authenticate the user's password in the Access-Request before validating the check item attributes.

The Prime Access Registrar server logs details about any rejected Access-Requests as a result of check items processing.

Configuring Check Items

You use **aregcmd** to configure check item attributes.

Configuring User Check Items

To configure UserList check item attributes:

-
- Step 1** Log into the Prime Access Registrar server, and use **aregcmd** to navigate to **//localhost/Radius/UserLists/default/bob**.

```
[ //localhost/Radius/UserLists/Default/bob ]
Name = bob
Description =
Password = <encrypted>
AllowAnonymousPassword = FALSE
Enabled = TRUE
Group~ = PPP-users
BaseProfile~ =
AuthenticationScript~ =
AuthorizationScript~ =
UserDefined1 =
Attributes/
CheckItems/
```

- Step 2** Change directory to CheckItems.

cd CheckItems

```
[ //localhost/Radius/UserLists/Default/bob/CheckItems ]
```

- Step 3** Use set to add any attributes to be used as check items.

set calling-Station-Id 4085551212

save

Configuring Usergroup Check Items

To configure UserGroups check item attributes:

-
- Step 1** Log into the Prime Access Registrar server, and use **aregcmd** to navigate to **//localhost/Radius/UserGroups/Default**.

cd /Radius/UserGroups/Default

```
[ //localhost/Radius/UserGroups/Default ]
Name = Default
Description = "Users who sometimes connect using PPP and sometimes connect "
BaseProfile~ =
AuthenticationScript~ =
AuthorizationScript~ = AuthorizeService
Attributes/
CheckItems/
```

- Step 2** Change directory to CheckItems.

cd CheckItems

```
[ //localhost/Radius/UserGroups/Default/CheckItems ]
```

Step 3 Use set to add any attributes to be used as check items.

```
set NAS-IP-Address 10.10.10.10
```

```
save
```

User-Specific Attributes

The 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.

The Prime Access Registrar server includes a property called HiddenAttributes to the User and UserGroup object. The HiddenAttributes property contains a concatenation of all user-level reply attributes. The HiddenAttributes property is not displayed, nor can the value be set or unset using the command-line interface.

The order of application of attributes is as follows:

1. UserGroup Base Profile
2. UserGroup Attributes
3. User Base Profile
4. User Attributes

The value of the HiddenAttributes property is used dynamically to construct and populate a virtual *attributes* directory in the User object. All values from the Attributes directory will go into the HiddenAttributes property. This occurs transparently when the administrator issues a save command.

Packet of Disconnect

Prime Access Registrar supports the Packet of Disconnect (POD) feature that enables the Prime Access Registrar server to send disconnect requests (PODs) to a NAS so that all the session information and the resources associated with the user sessions can be released. Prime Access Registrar can also determine when to trigger and send the POD.

For example, when a PDSN handoff occurs during a mobile session, the new PDSN sends out a new access-request packet to Prime Access Registrar for the same user. Prime Access Registrar should detect this handoff by the change in NAS-Identifier in the new request and trigger sending a POD to the old PDSN if it supports POD. Prime Access Registrar also provides an option for administrator to initiate sending POD requests through the command-line interface (CLI) for any user session. Prime Access Registrar forwards POD requests from external servers to the destination NAS.

This section contains the following topics:

- [Configuring Packet of Disconnect](#)
- [Proxying POD Requests from External Servers](#)

- [CLI Options for POD](#)

Configuring Packet of Disconnect

This section describes how to configure the POD feature in the following:

- [Configuring the Client Object](#)
- [Configuring a Resource Manager for POD](#)

Configuring the Client Object

You should enable POD for each client object that might want to send disconnect requests to those clients. You enable POD in a client object using the `EnableDynamicAuthorization` property. This property is set to `FALSE` by default when you create a client object. The following example shows the default configuration for a new client object, `NAS1`.

```
[ //localhost/Radius/Clients/NAS1 ]
  Name = nas1
  Description =
  IPAddress =
  SharedSecret =
  Type = NAS
  Vendor =
  IncomingScript~ =
  OutgoingScript~ =
  EnableDynamicAuthorization = FALSE
```

If the Prime Access Registrar server might send a POD to this client, set the `EnableDynamicAuthorization` property to `TRUE`. When you set this property to `TRUE`, the Prime Access Registrar server creates a `DynamicAuthorizationServer` subdirectory under the client object. The following example shows a newly created `DynamicAuthorizationServer` subdirectory:

```
[ //localhost/Radius/Clients/NAS1/DyanamicAuthorizationServer ]
  Port = 3799
  DynamicAuthSharedSecret =
  InitialTimeout = 5000
  MaxTries = 3
  PODAttributeGroup =
  COAAttributeGroup =
```

The default port is 3799. You can change the port, if desired.

The property `DynamicAuthSharedSecret` is initially set to the same as value as the client's `SharedSecret` property when you set `EnableDynamicAuthorization` to `TRUE`. You can chose to configure a different secret for POD in this subdirectory.

The `InitialTimeout` property represents the number of milliseconds used as a timeout for the first attempt to send a POD packet to a remote server. For each successive retry on the same packet, the previous timeout value used is doubled. You must specify a number greater than zero, and the default value is 5000 (or 5 seconds).

The `MaxTries` property represents the number of times to send a proxy request to a remote server before deciding the server is offline. You must specify a number greater than zero, and the default is 3.

The `PODAttributeGroup` property points to a group of attributes to be included in a disconnect-request packet sent to this client.

You can create and configure the PODAttributeGroup in the **/Radius/Advanced/AttributeGroups/** directory. The default group contains commonly used POD attributes NAS-Port and Acct-Session-Id.

The COAAttributeGroup property is used with the Change of Authorization (CoA) feature, also known as hot-lining.

Configuring a Resource Manager for POD

Prime Access Registrar provides a resource manager type called *session-cache*. When you set a resource manager to session-cache, the resource manager's configuration contains a subdirectory called **AttributesToBeCached**. The following is an example Resource Manager set to type session-cache:

```
[ //localhost/Radius/ResourceManagers/PODresourceMgr ]
  Name = PODresourceMgr
  Description =
  Type = session-cache
  OverwriteAttributes = FALSE
  AttributesToBeCached/
  QueryMappings/
```

The attributes you configure under the **AttributesToBeCached** directory are cached in the session record during session management. The cached attributes are then sent in the disconnect-request for this session.

The OverwriteAttributes property indicates whether to overwrite the existing attributes if there are any in the session record. Since this resource manager can be invoked during Access-Request as well as Accounting-Start processing, the OverwriteAttributes can be used to control if the attributes cached during Access-Request processing can be overwritten with the attributes available during Accounting-Start processing.

The following is an example of a typical session-cache resource manager:

```
[ //localhost/Radius/ResourceManagers/RM-New ]
  Name = RM-New
  Description =
  Type = session-cache
  OverwriteAttributes = TRUE
  AttributesToBeCached/
    1. Framed-IP-Address
    2. CDMA-Correlation-ID
  QueryMappings/
```

The attributes used in the example can be added as an indexed list using **add** or **set** commands (in any order).

Proxying POD Requests from External Servers

Prime Access Registrar can also proxy the disconnect requests received from external servers. To make Prime Access Registrar listen for external POD requests, the ListenForDynamicAuthorizationRequests property under **/Radius/Advanced** should be set to TRUE. The default value for this is FALSE. The default POD listening port is 3799. However this can be changed by configuring a new port of type *pod* under **/Radius/Advanced/Ports** and setting the new port number accordingly.

For security reasons, the source of a POD request should be configured as a remote server in Prime Access Registrar and the remote server should be configured to accept PODs. Set the property AcceptDynamicAuthorizationRequests to TRUE to do this. The default for this is FALSE. POD requests from unauthorized sources are silently discarded.

CLI Options for POD

Prime Access Registrar has options for the **query-sessions** and **release-sessions** CLI commands that enable querying or releasing sessions based on the session's age. Another option enables querying or releasing sessions based on any valid RADIUS attribute available in the user's session record. This section contains the following topics:

- [query-sessions](#)
- [release-sessions](#)

query-sessions

The syntax for using **query-sessions** *with-Age* option is the following:

```
query-sessions <path> with-Age <value>
```

Where <path> is the path to the server, session-manager or resource manager and <value> is the minimum age of the session specified in minutes or hours with options M, Minutes, H or Hours. This command returns all sessions that are older than the given age value.

The syntax for using **query-sessions** *with-Attribute* option is the following:

```
query-sessions <path> with-Attribute <name> <value>
```

Where <name> is the RADIUS attribute name and <value> is the value of the attribute to be matched. This command returns the sessions where a session record contains and matches the attribute value specified in <value> field.

release-sessions

The syntax for using **release-sessions** *with-Age* option is:

```
release-sessions <path> with-Age <value>
```

Where, <path> is the path to the server, session-manager or resource manager and <value> is the minimum age of the session specified in minutes or hours with options M for Minutes, H for Hours. This command returns all sessions that are older than the given age value.

The syntax for using **release-sessions** *with-Attribute* option is:

```
release-sessions <path> with-Attribute <name> <value>
```

Where, <name> is the RADIUS attribute name and <value> is the value of the attribute to be matched. This command returns the sessions where a session record contains and matches the attribute value specified in <value> field.

A new option is also available for **release-sessions** command to enable an administrator to trigger sending a POD for a user after the session is released.

```
release-sessions <path> with-<type> <value> [send-pod]
```

Where, <path> is the path to the server, Session Manager, or Resource Manager and <type> is one of the following: NAS, User, IP-Address ID, or Age. The **release-sessions** command with an optional [send-pod] at the end results in Prime Access Registrar sending a POD request. The PoD requests are directed to port number configured in /radius/clients/<client name>/DynamicAuthorizationServer/port. By default it is set to 3799. To configure udp xxx, set the port value as:

```
/radius/clients/<client name>/DynamicAuthorizationServer/port = xxx
```

Configuring Change of Authorization Requests

Prime Access Registrar supports Change of Authorization (CoA) requests as defined in Internet RFC 3576 that provides a way to change authorization status of users already logged on to the network. The CoA feature, also known as hot-lining, provides a wireless operator the ability to efficiently address issues with users that might otherwise be unauthorized to access packet data services. When a problem occurs that causes a user to be unauthorized to use the packet data service, a wireless operator can use the CoA feature to resolve the problem and return the user's packet data services.

When a user is hot-lined, their packet data service is redirected to a hot-line application that notifies the user of issues that might be blocking their access to normal packet data services. Hot-lining provides users with a way to address the issues blocking their access, such as billing issues, a prepaid account that has been depleted, or an expired credit card.

The CoA feature provides an option to the wireless operator administrator to send CoA packets to the client device when a user needs to be hot-lined. When to send a CoA request to a user depends on the wireless operator's site-specific policies.

Configuring the Client Object

You should enable CoA for each client object that might want to send CoA requests to those clients. You enable CoA in a client object using the EnableDynamicAuthorization property. This property is set to FALSE by default when you create a client object. The following example shows the default configuration for a new client object, NAS1.

```
[ //localhost/Radius/Clients/NAS1 ]
  Name = nas1
  Description =
  IPAddress =
  SharedSecret =
  Type = NAS
  Vendor =
  IncomingScript~ =
  OutgoingScript~ =
  EnableDynamicAuthorization = FALSE
```

If the Prime Access Registrar server might send a CoA request to this client, set the EnableDynamicAuthorization property to TRUE. When you set this property to TRUE, the Prime Access Registrar server creates a DynamicAuthorizationServer subdirectory under the client object. The following example shows a newly created DynamicAuthorizationServer subdirectory:

```
[ //localhost/Radius/Clients/NAS1/COA ]
  Port = 3799
  DynamicAuthSharedSecret =
  InitialTimeout = 5000
  MaxTries = 3
  PODAttributeGroup =
  COAAttributeGroup =
```


The default port is 3799. You can change the port, if desired.

The property `DynamicAuthSharedSecret` is initially set to the same as value as the client's `SharedSecret` property when you set `EnableDynamicAuthorization` to `TRUE`. You can chose to configure a different secret for CoA in this subdirectory.

The `InitialTimeout` property represents the number of milliseconds used as a timeout for the first attempt to send a CoA packet to a remote server. For each successive retry on the same packet, the previous timeout value used is doubled. You must specify a number greater than zero, and the default value is 5000 (or 5 seconds).

The `MaxTries` property represents the number of times to send a proxy request to a remote server before deciding the server is offline. You must specify a number greater than zero, and the default is 3.

The `COAAttributeGroup` property points to a group of attributes to be included in a CoA request packet sent to this client.

You can create and configure the `COAAttributeGroup` in the `/Radius/Advanced/AttributeGroups/` directory. The default group is not set to any value by default. When an attribute group is configured, the Prime Access Registrar server includes the attributes in this group in a CoA request. The values for these attributes are fetched from the user's session record.

The CoA attribute group configuration can be used with a session-cache Resource Manager. For example, any new attributes that are to be sent in a CoA request can be configured for caching by the session-cache Resource Manager so they will be available in the session record when it is to be sent in the CoA request.

The CoA request might also contain AV pairs from the optional profile name in the `query-session` CLI command used to send the CoA request. In a 3GPP2 scenario, a profile containing the `Filter-Id` attribute set to a value "Hot-Line Active" can be included when a user is to be hot-lined. This can be used as a hot-line profile possibly containing other attributes as desired by the wireless operator. Another profile might be defined containing the `Filter-Id` attribute with the value "Hot-Line Normal." This profile can be used with the `query-session` CLI command to bring the user back to normal.

The CoA request packet sent by the Prime Access Registrar server conforms to internet RFC 3756. In response to a CoA request initiated by the Prime Access Registrar server, the client should respond with a `COA-ACK` if it is able to hot-line the user based on credentials available in the CoA request. If the client is unable to hot-line the user for any reason, the client can include an error-cause attribute with the appropriate reason in a `COA-NAK` packet.

The Prime Access Registrar server logs all CoA responses. If the Prime Access Registrar server does not receive a response to a CoA request within the timeout period, it will retransmit for the configured number of retries, then logs an error if no response is received.

The Prime Access Registrar server forwards proxied CoA requests sent by external servers to the destination NAS. The CoA requests are proxied based on the `NAS-IP-Address` in the incoming request. The proxied CoA requests from external servers are forwarded to the destination NAS only if the source IP address is configured to accept dynamic authorization requests. The responses received from the NAS (either `COA-ACK` or `COA-NAK`) are forwarded back to the source where the Prime Access Registrar server received the original proxy request.

Dynamic DNS

Prime Access Registrar supports the Dynamic DNS protocol providing the ability to update DNS servers. The dynamic DNS updates contain the hostname/IP Address mapping for sessions managed by Prime Access Registrar.

You enable dynamic DNS updates by creating and configuring new Resource Managers and new Remote Servers, both of type *dynamic-dns*. The dynamic-dns Resource Managers specify which zones to use for the forward and reverse zones and which Remote Servers to use for those zones. The dynamic-dns Remote Servers specify how to access the DNS Servers.

This section contains the following topics:

- [Configuring Dynamic DNS](#)
- [Testing Dynamic DNS with radclient](#)

Configuring Dynamic DNS

Before you configure Prime Access Registrar you need to gather information about your DNS environment. For a given Resource Manager you must decide which forward zone you will be updating for sessions the resource manager will manage. Given that forward zone, you must determine the IP address of the primary DNS server for that zone. If the dynamic DNS updates will be protected with TSIG keys, you must find out the name and the base64 encoded value of the secret for the TSIG key. If the resource manager should also update the reverse zone (ip address to host mapping) for sessions, you will also need to determine the same information about the primary DNS server for the reverse zone (IP address and TSIG key).

If using TSIG keys, use **aregcmd** to create and configure the keys. You should set the key in the Remote Server or the Resource Manager, but not both. Set the key on the Remote Server if you want to use the same key for all of the zones accessed through that Remote Server. Otherwise, set the key on the Resource Manager. That key will be used only for the zone specified in the Resource Manager.

Configuring the Dynamic DNS

To configure the dynamic-dns remote server:

Step 1 Launch **aregcmd**.

Step 2 Create the dynamic-dns TSIG Keys:

```
cd /Radius/Advanced/DDNS/TSIGKeys
add foo.com
```

This example named the TSIG Key, **foo.com**, which is related to name of the example DNS server we use. You should choose a name for TSIG keys that reflects the DDNS client-server pair (for example, **foo.bar** if the client is **foo** and the server is **bar**), but you should use the name of the TSIG Key as defined in the DNS server.

Step 3 Configure the TSIG Key:

```
cd foo.com
set Secret <base64-encoded string>
```

The Secret should be set to the same base64-encoded string as defined in the DNS server. If there is a second TSIG Key for the primary server of the reverse zone, follow these steps to add it, too.

Step 4 Use **aregcmd** to create and configure one or more dynamic-dns Remote Servers.

Step 5 Create the dynamic-dns remote server for the forward zone:

```
cd /Radius/RemoteServers
```

add ddns

This example named the remote server *ddns* which is related to the remote server type. You can use any valid name for your remote server.

Step 6 Configure the dynamic-dns remote server:

```
cd ddns
```

```
set Protocol dynamic-dns
```

```
set IPAddress 10.10.10.1 (ip address of primary dns server for zone)
```

```
set ForwardZoneTSIGKey foo.com
```

```
set ReverseZoneTSIGKey foo.com
```

If the reverse zone will be updated and if the primary server for the reverse zone is different than the primary server for the forward zone, you will need to add another Remote Server. Follow the previous two steps to do so. Note that the IP Address and the TSIG Key will be different.

You can now use **aregcmd** to create and configure a resource manager of type dynamic-dns.

Step 7 Create the dynamic-dns resource manager:

```
cd /Radius/ResourceManagers
```

```
add ddns
```

This example named the service *ddns* which is related to the resource manager type but you can use any valid name for your resource manager.

Step 8 Configure the dynamic-dns resource manager.

```
cd ddns
```

```
set Type dynamic-dns
```

```
set ForwardZone foo.com
```

```
set ForwardZoneServer DDNS
```

Finally, reference the new resource manager from a session manager. Assuming that the example configuration was installed, the following step will accomplish this. If you have a different session manager defined you can add it there if that is appropriate.

Step 9 Reference the resource manager from a session manager:

```
cd /Radius/SessionManagers/session-mgr-1/ResourceManagers
```

```
set 5 DDNS
```



Note The Property AllowAccountingStartToCreateSession must be set to TRUE for dynamic DNS to work.

Step 10 Save the changes you have made.

Testing Dynamic DNS with radclient

After the Resource Manager has been defined it must be referenced from the appropriate Session Manager. You can use **radclient** to confirm that dynamic DNS has been properly configured and is operational.

Testing the Dynamic DNS using Radclient

To test Dynamic DNS using radclient:

Step 1 Launch **aregcmd** and set the trace to level 4.

```
aregcmd
```

Login to the Prime Access Registrar server as an administrative user.

```
trace 4
```

Step 2 Launch **radclient**.

```
cd /opt/CSCOAr/bin
```

```
radclient
```

Step 3 Create an Accounting-Start packet

```
acct_request Start username
```

Example:

```
set p [ acct_request Start bob ]
```

Step 4 Add a Framed-IP-Address attribute to the Accounting-Start packet

Step 5 Send the Accounting-Start packet

```
$p send
```

Step 6 Check the **aregcmd** trace log and the dns server to verify that the host entry was updated in both the forward and reverse zones.

Dynamic Service Authorization Feature

Typically, Prime Access Registrar does not allow sending another Access-Request to the remote server after the user is connected to the LDAP servers for user authentication. The Dynamic Service Authorization feature allows you to access external databases such as LDAP and Oracle first to know which remote servers authenticated services need to be relayed. This feature enables Prime Access Registrar to determine whether to send access-accept back to the client or to send another access-request to the remote server such as LDAP and Oracle. Prime Access Registrar is able to perform this activity multiple times in a single access-request.

Configuring Dynamic Service Authorization Feature

Configuring the dynamic service authorization involves:

- [Setting Up the Environment Variable](#)
- [Configuring the Script for the Dynamic Service Authorization](#)

Setting Up the Environment Variable

Before configuring the dynamic service authorization feature, you must set the following three environment variables in Prime Access Registrar:

- **Re-Authentication-Service**

When the Re-Authentication-Service is set, the server directs the request to the specified reauthentication service for processing.

- **Re-Authorization-Service**

When the Re-Authorization-Service is set, the server directs the request to the specified reauthorization service for processing.

- **Re-Accounting-Service**

When the Re-Accounting-Service is set, the server directs the request to the specified reaccounting service for processing.

You can set the environmental variable by using scripts. See for more information.



Note

When using the same service for reauthentication and reauthorization, a loop can occur in these services. The loop count, by default is 10. You can change the loop count using the **Dynamic-Service-Loop-Limit** environment variable.

Following is a sample procedure for setting the environment variable:

```
proc dynamicService { request response environ } {
  $environ put Re-Authentication-Service "local-users"
  $environ put Re-Authorization-Service "local-users"
}
```

You can append this procedure by copying it into **tclscript.tcl** that is located in **/opt/CSCOar/scripts/radius/tcl directory**, or to the location that you chose when you installed Prime Access Registrar. You can also use this procedure as a separate script file and configure the script accordingly. See for more information on configuring the TCL script.

Configuring the Script for the Dynamic Service Authorization

To configure the script for the dynamic service authorization:

-
- Step 1** Launch **aregcmd**.
aregcmd
 - Step 2** Change directory to **/Radius/Scripts**.
cd /Radius/Scripts
 - Step 3** Enter **dynamicService**.
 - Step 4** Change the directory to **dynamicService**.
cd dynamicService

You get the following output:

```
[ //localhost/Radius/Scripts/dynamicService ]
Name = dynamicService
Description =
Language =
```

- Step 5** Set the Language property to TCL.

Set Language TCL

Step 6 Set the filename property to **tclscript.tcl**.

Set Filename tclscript.tcl

Step 7 Set the EntryPoint property to **dynamicservice**.

Set EntryPoint dynamicservice

The following is an example of the script configuration:

```
cd /Radius
set IncomingScript dynamicservice
[ //localhost/Radius ]
  IncomingScript~ = dynamicservice
  DefaultAuthenticationService~ = local-users
  DefaultAuthorizationService~ = local-users
```

Step 8 Enter **Save** to save the configuration.

The following shows a sample trace:

```
10/30/2013 12:32:02.258: P577: Packet received from 127.0.0.1
10/30/2013 12:32:02.259: P577: Packet successfully added
10/30/2013 12:32:02.259: P577: Trace of Access-Request packet
10/30/2013 12:32:02.259: P577:   identifier = 9
10/30/2013 12:32:02.259: P577:   length = 61
10/30/2013 12:32:02.259: P577:   reqauth =
b6:89:41:52:6e:d4:86:37:4a:aa:9b:27:1f:74:ff:05
10/30/2013 12:32:02.259: P577:   User-Name = bob
10/30/2013 12:32:02.259: P577:   User-Password =
2b:4a:f0:c8:95:f1:ad:e5:52:d4:83:0f:45:2b:2b:70
10/30/2013 12:32:02.259: P577:   NAS-Port = 2
10/30/2013 12:32:02.260: P577:   NAS-Identifier = localhost
10/30/2013 12:32:02.260: P577: Running Server's IncomingScript: dynamicservice
10/30/2013 12:32:02.261: P577:   Tcl: environ put Re-Authentication-Service local-users
-> OK
10/30/2013 12:32:02.261: P577:   Tcl: environ put Re-Authorization-Service local-users
-> OK
10/30/2013 12:32:02.261: P577: Using Client: localhost
10/30/2013 12:32:02.262: P577: Using NAS: localhost (127.0.0.1)
10/30/2013 12:32:02.262: P577: Request is directly from a NAS: TRUE
10/30/2013 12:32:02.262: P577: Authenticating and Authorizing with Service local-users
10/30/2013 12:32:02.262: P577: Getting User bob's UserRecord from UserList Default
10/30/2013 12:32:02.263: P577: user list user bob's password matches
10/30/2013 12:32:02.263: P577: Processing UserGroup PPP-users's check items
10/30/2013 12:32:02.263: P577: User bob is part of UserGroup PPP-users
10/30/2013 12:32:02.263: P577: Merging UserGroup PPP-users's BaseProfiles into response
dictionary
10/30/2013 12:32:02.264: P577: Merging BaseProfile default-PPP-users into response
dictionary
10/30/2013 12:32:02.264: P577: Merging attributes into the Response Dictionary:
10/30/2013 12:32:02.264: P577:   Adding attribute Service-Type, value = Framed
10/30/2013 12:32:02.264: P577:   Adding attribute Framed-Protocol, value = PPP
10/30/2013 12:32:02.264: P577:   Adding attribute Framed-Routing, value = None
10/30/2013 12:32:02.264: P577:   Adding attribute Framed-MTU, value = 1500
10/30/2013 12:32:02.264: P577:   Adding attribute Framed-Compression, value = VJ TCP/IP
header compression
10/30/2013 12:32:02.264: P577:   Adding attribute Ascend-Idle-Limit, value = 1800
10/30/2013 12:32:02.265: P577: Merging UserGroup PPP-users's Attributes into response
Dictionary
10/30/2013 12:32:02.265: P577: Merging attributes into the Response Dictionary:
10/30/2013 12:32:02.265: P577: Authenticating and Authorizing with Service local-users
10/30/2013 12:32:02.265: P577: Getting User bob's UserRecord from UserList Default
10/30/2013 12:32:02.266: P577: user list user bob's password matches
```

```

10/30/2013 12:32:02.266: P577: Processing UserGroup PPP-users's check items
10/30/2013 12:32:02.266: P577: User bob is part of UserGroup PPP-users
10/30/2013 12:32:02.266: P577: Merging UserGroup PPP-users's BaseProfiles into response
dictionary
10/30/2013 12:32:02.266: P577: Merging BaseProfile default-PPP-users into response
dictionary
10/30/2013 12:32:02.266: P577: Merging attributes into the Response Dictionary:
10/30/2013 12:32:02.266: P577:   Replacing attribute Service-Type, new value = Framed
10/30/2013 12:32:02.267: P577:   Replacing attribute Framed-Protocol, new value = PPP
10/30/2013 12:32:02.267: P577:   Replacing attribute Framed-Routing, new value = None
10/30/2013 12:32:02.267: P577:   Replacing attribute Framed-MTU, new value = 1500

```

Remote Session Management

Prime Access Registrar sessions can also be stored on a remote database. This improves the overall scalability of the number of sessions that Prime Access Registrar can simultaneously handle. The remote session manager internally uses two ODBC remote servers, Internal-ODBC-Read-Server and Internal-ODBC-Write-Server. Configurations pertaining to these internal remoteservers can be done under **/Radius/Advanced/RemoteODBCSessionServer**

For more information on how to configure the Remote ODBC Session Server, refer to .



Note

Ensure that the length of fields such as Username, Session/Resource Manager name Session-Key, Query-Key and so on are limited to the value specified in the [Table 9-8](#) while it is configured. Although the field length of entire session record is 3KB it is limited to 2KB. This is practically sufficient to hold all the session parameters as well as the cached attributes (if any).

Table 9-8 **Schema Details**

Field	Type
ID	NUMBER(10)
SESSION_KEY	VARCHAR2(20)
NAME	VARCHAR2(20)
PER_USER_RM	VARCHAR2(20)
PER_GROUP_RM	VARCHAR2(20)
IP_RM	VARCHAR2(20)
IP	VARCHAR2(20)
SESSION_MANAGER	VARCHAR2(20)
AC	NUMBER(10)
NAS	VARCHAR2(20)
CACHE_RM	VARCHAR2(20)
Q_VALUE	VARCHAR2(20)
TS	NUMBER(15)
SESSION_RECORD	VARCHAR2(3072)



Note Remote session manager will work only with Oracle database.



Note In remote-session-manager, query-session with the 'with-age' option will not work.

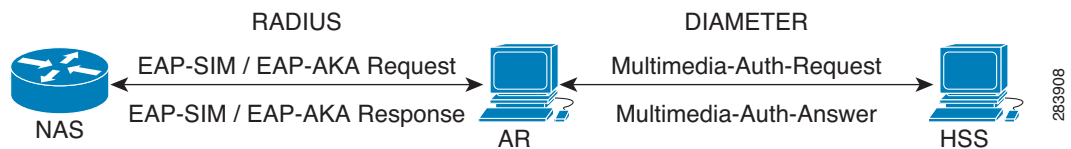
Wx Interface Support for SubscriberDB Lookup

Prime Access Registrar supports Diameter Wx interface to fetch the authentication vectors from HSS required for EAP-SIM/EAP-AKA authentication.

The EAP-SIM and EAP-AKA authentication service is extended to generate a Diameter message Multimedia-Authentication-Request (MAR), with the subscriber identity (IMSI), to the HSS when it requires the authentication vectors. The HSS sends a Diameter Multimedia-Authentication-Answer (MAA) back containing the number of triplets/quintuplets.

The PreRequestTranslationScript, PostRequestTranslationScript, PreResponseTranslationScript, and PostResponseTranslationScript are the available scripting points to modify the RADIUS and Diameter packets while sending and receiving the packets to or from the HSS. For more information, see [Table 5-1](#) for EAP-AKA and for EAP-SIM details.

Figure 9-1 Wx Interface Support for SubscriberDB lookup



For more information on Wx interface, see the [3GPP TS 29.124](#) and [TS 29.229](#) specifications.

Configuration Examples

The following shows an example configuration for EAP-AKA:

```
[ //localhost/Radius/Services/eap-aka-wx ]
  Name = eap-aka-wx
  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
SubscriberDBLookup = Diameter
DestinationRealm = mpc.com
PreRequestTranslationScript~ =
PostRequestTranslationScript~ =
PreResponseTranslationScript~ =
PostResponseTranslationScript~ =

```

The following shows an example configuration for EAP-SIM:

```

[ //localhost/Radius/Services/eap-sim-wx ]
Name = eap-sim-wx
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 = 120
AuthenticationTimeout = 120
UseProtectedResults = False
SendReAuthIDInAccept = False
SubscriberDBLookup = Diameter
DestinationRealm = hss.com
PreRequestTranslationScript~ =
PostRequestTranslationScript~ =
PreResponseTranslationScript~ =
PostResponseTranslationScript~ =

```

Smart Grid Solution Management

Prime Access Registrar provides identity and access management for the smart grid solutions on IPv6 (and IPv4) networks. This is achieved using the Elliptic Curve Cryptographic (ECC) based certificate validation and SNMP support for TACACS+.

For EAP services, in addition to RSA certificates, Prime Access Registrar supports verification of ECC certificates. ECC uses elliptic curves to encrypt data when creating keys which enables you to create shorter and stronger keys for better efficiency. This is achieved using the Cisco SSL library APIs.

TACACS+ supports ASCII,PAP, and CHAP Authentication type, login and enable services, and LDAP, OCI, and ODBC services in addition to Local service.

The client certificate files and RSA or ECC key file are available in `/cisco-ar/pki` as **client-cert.pem** and **client-key.pem** respectively. Both the files must be in “.PEM” format, since the certificate validation is done based on the extension of the files.

ECC certificate validation is used in the following authentication methods:

- [EAP-FAST](#)
- [EAP-Transport Level Security \(TLS\)](#)
- [EAP-TTLS](#)
- [Protected EAP](#)

Lawful Interception (LI) Support in Prime Access Registrar

Lawful Interception (LI) is a requirement placed upon service providers to provide legally sanctioned official access to private communications. With the existing Public Switched Telephone Network (PSTN), LI is performed by applying a physical tap on the telephone line of the target in response to a warrant from a Law Enforcement Agency (LEA). However, Voice over IP (VoIP) technology has enabled the mobility of the end-user, so it is no longer possible to guarantee the interception of calls based on tapping a physical line.

When a Law Interception Server (LIS) of the LEA requests the LI server to start monitoring a particular target, LI server sends the corresponding request to the Prime Access Registrar server. XML schema definition files are shared between Prime Access Registrar and Mediation Partner device for request and response messages. A local web service, which runs on the Prime Access Registrar server listens to the messages from the LI server.

Prime Access Registrar provides support for Intercept Access Point (IAP) for receiving the intercept/monitoring request for the subscriber whose “Access Associated” Communications Identifying Information (AA CmII) is to be intercepted and delivered to the LIS.

[Table 9-9](#) provides the list of supported RADIUS and Diameter intercept requests from the LIS.

Table 9-9 Intercept Requests Supported

Intercept Request (RADIUS)	Intercept Request (Diameter)	Purpose
ProvisionTargetRequest	DiaProvisionTargetRequest	To start monitoring the target user
DeprovisionTargetRequest	DiaDeProvisionTargetRequest	To stop monitoring the target user

Table 9-9 Intercept Requests Supported

Intercept Request (RADIUS)	Intercept Request (Diameter)	Purpose
LinkUpdateRequest	DiaLinkUpdateRequest	To query the target user in the monitored list
ListTargetRequest	DiaListTargetRequest	To list all the users that are currently being monitored

Initiating Monitoring Process

When the ProvisionTarget/DiaProvisionTarget request is received from the LIS, Prime Access Registrar adds the respective user in the monitoring list and starts monitoring the user events.

Table 9-10 lists the events of the target user that are reported to LIS:

Table 9-10 Targeted User Events

Events	Attributes (RADIUS)	Attributes (Diameter)
Access Attempt (for RADIUS) / DiameterAccess Attempt (for Diameter)	<ul style="list-style-type: none"> • CaseIdentity (M) • IAPSystemIdentity (M) • TimeStamp (M) • SubscriberIdentity (M) • AccessMethod (C) • NetworkAccessNodeIdentity (C) • ProtocolSignal (O) 	<ul style="list-style-type: none"> • CaseIdentity (M) • IAPSystemIdentity (M) • TimeStamp (M) • SubscriberIdentity (M) • OriginHost (C) • AuthRequestType (C) • SessionIdentity (C) • AuthApplID (C) • ProtocolSignal (O) • OriginRealm (C) • TargetNetwork (O)
Access-Accept (for RADIUS) / DiameterAccess-Accept (for Diameter)	<ul style="list-style-type: none"> • CaseIdentity (M) • IAPSystemIdentity (M) • TimeStamp (M) • SubscriberIdentity (M) • AccessMethod (C) • NetworkAccessNodeIdentity (C) • IPaddress (C) • AccessSessionIdentity (M) • AccessSessionCharacteristics (C) • Locationinformation (C) • ProtocolSignal (O) 	<ul style="list-style-type: none"> • CaseIdentity (M) • IAPSystemIdentity (M) • TimeStamp (M) • SubscriberIdentity (M) • OriginHost (C) • AuthRequestType (C) • SessionIdentity (C) • AuthApplID (C) • ProtocolSignal (O) • OriginRealm (C) • TargetNetwork (O) • ResultCode (C)

Table 9-10 Targeted User Events (continued)

Events	Attributes (RADIUS)	Attributes (Diameter)
Access-Failed (for RADIUS) / DiameterAccess-Failed (for Diameter)	<ul style="list-style-type: none"> • CaseIdentity (M) • IAPSystemIdentity (M) • TimeStamp (M) • SubscriberIdentity (M) • IPAddress (C) • ReasonForTermination (C) • ProtocolSignal (O) 	<ul style="list-style-type: none"> • CaseIdentity (M) • IAPSystemIdentity (M) • TimeStamp (M) • SubscriberIdentity (M) • OriginHost (C) • AuthRequestType (C) • SessionIdentity (C) • AuthApplID (C) • ProtocolSignal (O) • OriginRealm (C) • TargetNetwork (O) • ResultCode (C) • ReasonForTermination (C)
Access-Session-Start (for RADIUS) / DiameterAccess-Session-Start (for Diameter)	<ul style="list-style-type: none"> • CaseIdentity (M) • IAPSystemIdentity (M) • TimeStamp (M) • SubscriberIdentity (M) • AccessSessionIdentity (M) • IPAddress (C) • ProtocolSignal (O) 	<ul style="list-style-type: none"> • CaseIdentity (M) • IAPSystemIdentity (M) • TimeStamp (M) • SubscriberIdentity (M) • OriginHost (C) • AuthApplID (C) • SessionIdentity (M) • AuthRecNo (C) • ProtocolSignal (O) • OriginRealm (C) • TargetNetwork (O)

Table 9-10 Targeted User Events (continued)

Events	Attributes (RADIUS)	Attributes (Diameter)
Access-Session-End (for RADIUS) / DiameterAccess-Session-End (for Diameter)	<ul style="list-style-type: none"> • CaseIdentity (M) • IAPSystemIdentity (M) • TimeStamp (M) • SubscriberIdentity (M) • AccessSessionIdentity (M) • IPAddress (C) • ReasonforTermination (C) • ProtocolSignal (O) 	<ul style="list-style-type: none"> • CaseIdentity (M) • IAPSystemIdentity (M) • TimeStamp (M) • SubscriberIdentity (M) • OriginHost (C) • AuthApplID (C) • SessionIdentity (M) • AuthRecNo (C) • ProtocolSignal (O) • OriginRealm (C) • TargetNetwork (O) • ReasonForTermination (C)
Access-Rejected (for RADIUS) / DiameterAccess-Rejected (for Diameter)	<ul style="list-style-type: none"> • CaseIdentity (M) • IAPSystemIdentity (M) • TimeStamp (M) • SubscriberIdentity (M) • IPAddress (C) • ReasonforTermination (C) • ProtocolSignal (O) 	<ul style="list-style-type: none"> • CaseIdentity (M) • IAPSystemIdentity (M) • TimeStamp (M) • SubscriberIdentity (M) • OriginHost (C) • AuthRequestType (C) • SessionIdentity (C) • AuthApplID (C) • ProtocolSignal (O) • OriginRealm (C) • TargetNetwork (O) • ResultCode (C) • ReasonForTermination (C)

**Note**

The attribute with (M) represents mandatory, (O) represents optional, (C) represents conditionally available.

If 3GPP-IMSI is present in the incoming request packet, the following 3GPP-related attributes are also reported to the LI server:

- 3GPP-IMSI
- Called-Station-Id
- Calling-Station-Id
- 3GPP-PDP-Type
- SGSN-Address

- GGSN-Address
- 3GPP-IMSI-MCC-MNC
- 3GPP-NSAPI
- 3GPP-SGSN-MCC-MNC
- 3GPP-IMEISV

Stopping Monitoring Process

On receiving the DeprovisionTarget request from LIS, the target user is removed from the monitoring list.

Querying Target User Events

On receiving the LinkUpdate request on target user from LIS, the target user details are checked in the monitoring list and message is sent to LIS as listed below:

- If the specified user is not currently being monitored, a reply with reason-code indicating that the user is currently not targeted is sent.
- If the specified user is currently being targeted and is not logged into the network, a reply with status stating that the user is “inactive” in the network is sent.
- If the specified user is currently being targeted and is logged into the network, a reply with the following attributes is sent:
 - Case Identity (M)
 - IAP System Identity (M)
 - Time Stamp (M)
 - Subscriber Identity (M)
 - Access Method (C)
 - Network Access Node Identity (C)
 - IP address (C)
 - Access Session Identity (M)
 - Access Session Characteristics (C)
 - Location information (C)
 - Protocol Signal (O)

Viewing Monitored Users

On receiving the ListTarget request from LIS, a list of users that are currently being monitored are sent to LIS. The reply will contain a surveillance-target-count attribute indicating the count of the number of users being targeted and multiple instances of surveillance-target-identifier attribute having the real identifiers.

Intercept Response

Each request from the LIS contains a transaction-id which is copied on to the reply from Prime Access Registrar. For each request type there is an appropriate response type with appropriate return data.

[Table 9-9](#) provides the list of Intercept results for RADIUS and Diameter.

Table 9-11 Intercept Results for RADIUS and Diameter

Intercept Response (RADIUS)	Intercept Response (Diameter)	Description
ProvisionTargetResult	DiaProvisionTargetResult	An acknowledgment for the request with the same transaction ID. For information on the request, see Initiating Monitoring Process, page 9-52 .
DeprovisionTargetResult	DiaDeProvisionTargetResult	An acknowledgment for the request with the same transaction ID. For information of the request, see Stopping Monitoring Process, page 9-55 .
LinkUpdateResult	DiaLinkUpdateResult	For LinkUpdate, see Querying Target User Events, page 9-55 .
ListTargetResult	DiaListTargetResult	For ListTarget, see Viewing Monitored Users, page 9-55 .

Configuring Lawful Intercept

Two scripts which are LawfulIntercept and RexLiScript are to be configured to run LawfulIntercept service in Prime Access Registrar. LawfulIntercept script should be configured in the server's incoming scripting point which is used to check the provisioned status of the user in the incoming access request. If the user is provisioned in the data store, Virtual-Server-Outgoing-Script will be executed after the server's incoming point.

InitEntryPoint of LawfulIntercept script writes the targeted list of users to a file while the server is stopping and reads the targeted users back to data store while the server is starting.

RexLiScript is configured in Virtual-Server-Outgoing-Script that sends events of the provisioned users to the LI service client.

Configuring the Lawful Intercept

To configure Lawful Intercept:

- Step 1** Create the RexLiScript script object that will be set in Virtual-Server-Outgoing-Script point.

```
[ //localhost/Radius/Scripts/virtual ]
  Name = virtual
  Description =
  Language = rex
  Filename = libLiScript.so
  EntryPoint = RexLiScript
  InitEntryPoint = InitRexLiScript
  InitEntryPointArgs =
```

- Step 2** Create the LawfulIntercept script object.

```
[ //localhost/Radius/Scripts/LiScript ]
  Name = LiScript
  Description =
  Language = Rex
  Filename = libLiScript.so
  EntryPoint = LawfulIntercept
  InitEntryPoint = RexInitialize
  InitEntryPointArgs = virtual
```


Step 3 set LawfulIntercept script object to ServerIncoming scripting point;

```
[ //localhost/Radius ]
  IncomingScript~ = LiScript
```



Note The file 'libLiScript.so' comes up with Prime Access Registrar kit. You have to copy it into /cisco-ar/scripts/radius/rex/ path.

Step 4 Save the configuration:

```
save
```

Step 5 Reload the configuration:

```
reload
```

TACACS+ Support for AAA

TACACS+ (Terminal Access Controller Access-Control System Plus) is a terminal access control protocol for routers, switches, network access servers and other networked computing devices. The main goal of TACACS+ is to provide separate authentication, authorization and accounting services.

In Prime Access Registrar, TACACS+ supports authentication, command authorization, and accounting. The authentication support is available for login services with PAP, CHAP, and ASCII authentication types. It also tracks and maintains the executed command details in the command accounting database. Configuration is supported through the CLI/GUI and statistics are provided through CLI, GUI, and SNMP. TACACS+ supports the following Prime Access Registrar services:

- Local-users and Local-file service
- OCI
- ODBC
- LDAP

The following shows an example configuration for TACACS+:

```
[ /Radius/Clients/mytac ]
  Name = mytac
  Description =
  Protocol = tacacs-and-radius
  IPAddress = 10.77.123.57
  SharedSecret = <encrypted>
  Type = NAS
  Vendor =
  IncomingScript~ =
  OutgoingScript~ =
  EnableDynamicAuthorization = FALSE
  NetMask =
  EnableNotifications = FALSE
  EnforceTrafficThrottling = TRUE
```

Prime Access Registrar provides command authorization support to authorize the cmd mode commands. Command authorization is based on device access rules and the decision to authorize is based on command sets and conditions or expressions defined for the access rules. They determine whether to authorize a set of commands for the user or not.

If you enable TACACS+ command authorization for a service, you must define the following:

- Command sets—You must configure the list of commands with the arguments and the action to perform: permit or deny.
- Device access rules—You must configure the conditions or expressions and the command sets that are applicable to the access rule if the conditions are met.
- Service—You must enable the device access and associate the device access rules for the service.

When a packet enters the service, it selects the first device access rule and evaluates the condition. If the condition is met, then the service applies the device access rule for the request. If the command that is processed matches a command listed in the command set, the service decides on whether to permit the command for the user or not based on the permissions set up. See the example below.

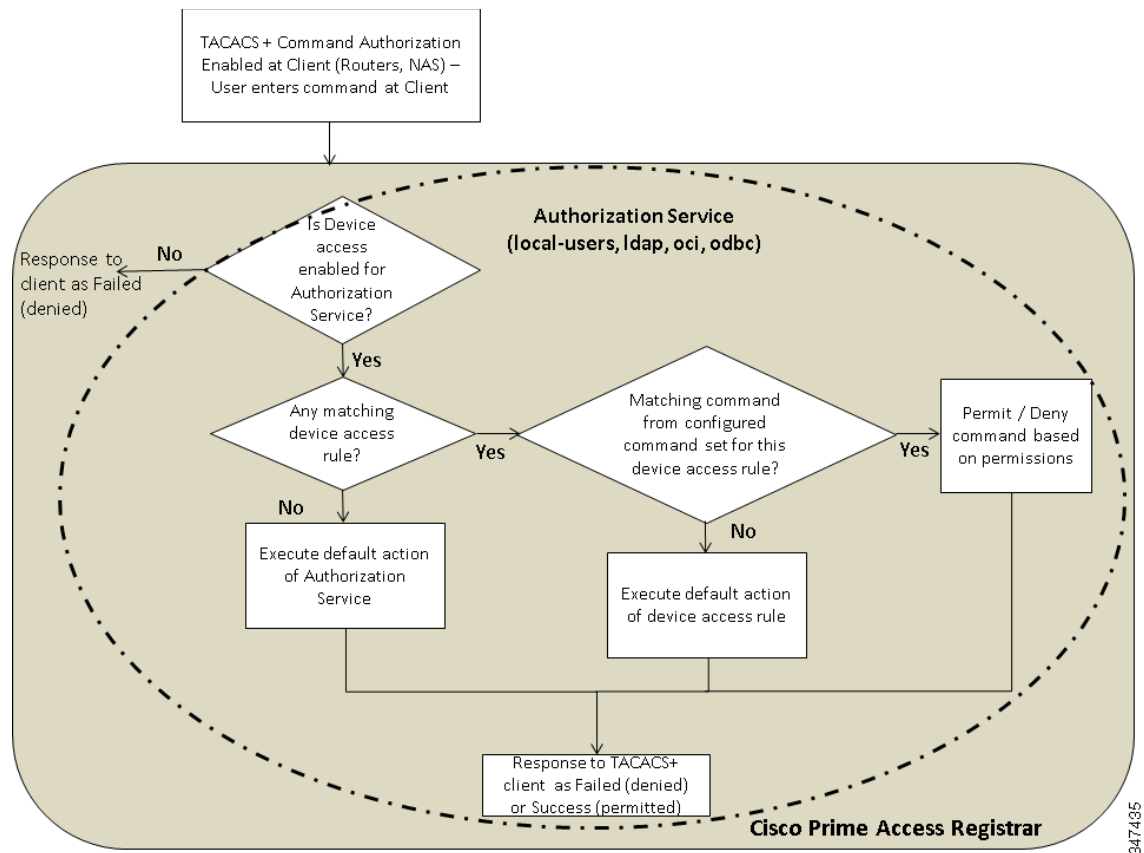
Device Access Rule	Condition	Command Set	Command	Arguments	Action
NewAccessRule	Expr1 OR Expr2 Where: Expr1 = user-name=bob Expr2 = nas-identifier=~PGW*/ OR = Conditional operator	cmdset1	show	*	permit
			enable	~/serial*/	deny

In the above example, if one of the conditions user-name = bob or nas-identifier = ~/PGW*/ is met, then the service applies the device access rule. If the processed command with its arguments matches one of the commands listed above, then the service permits or denies the command according to the setup.

Note Prime Access Registrar supports POSIX Extended Regular Expression (ERE) for command arguments and condition expressions value property.

Figure 9-2 shows the transaction flow for TACACS+ command authorization.

Figure 9-2 TACACS+ Command Authorization Flow



The following is an example configuration of device access rules and command sets configured for a local-users service:

```

[ //localhost/Radius ]
  Name = Radius
  Description =
  Version = 7.2.0.0
  IncomingScript~ =
  OutgoingScript~ =
  DefaultAuthenticationService~ = local-users
  DefaultAuthorizationService~ = local-users
  DefaultAccountingService~ = local-file
  DefaultSessionService~ =
  DefaultSessionManager~ = session-mgr-1
  UserLists/
  UserGroups/
  Policies/
  Clients/
  Vendors/
  Scripts/
  Services/
  SessionManagers/
  ResourceManagers/
  Profiles/
  Rules/
  Translations/
  TranslationGroups/
  RemoteServers/
  CommandSets/

```

```

DeviceAccessRules/
FastRules/
Advanced/
Replication/

--> cd /r/DeviceAccessRules/

[ //localhost/Radius/DeviceAccessRules ]
  Entries 0 to 0 from 0 total entries
  Current filter: <all>

--> add d2

Added d2

--> cd d2

[ //localhost/Radius/DeviceAccessRules/d2 ]
  Name = d2
  Description =
  CommandSetNames =
  Conditions =
  DefaultDeviceAction = PermitAll
  ConditionExpressions/

--> set Conditions "A1 and A2"

Set Conditions "A1 and A2"

--> SET CommandSetNames "cm1, CM2"

Set CommandSetNames "cm1, CM2"

--> CD ConditionExpressions/

[ //localhost/Radius/DeviceAccessRules/d2/ConditionExpressions ]
  Entries 0 to 0 from 0 total entries
  Current filter: <all>

--> add a1

Added a1

--> add a2

Added a2

--> cd a1

[ //localhost/Radius/DeviceAccessRules/d2/ConditionExpressions/a1 ]
  Name = a1
  Description =
  Attribute =
  Value =

--> Set Attribute user-name

Set Attribute user-name

--> Set Value user*

Set Value user*

```

```
--> cd ..

[ //localhost/Radius/DeviceAccessRules/d2/ConditionExpressions ]
  Entries 1 to 2 from 2 total entries
  Current filter: <all>

  a1/
  a2/

--> cd a2

[ //localhost/Radius/DeviceAccessRules/d2/ConditionExpressions/a2 ]
  Name = a2
  Description =
  Attribute =
  Value =

--> Set Attribute user-group

Set Attribute user-group

--> Set Value ABC

Set Value ABC

--> cd /r/CommandSets/

[ //localhost/Radius/CommandSets ]
  Entries 0 to 0 from 0 total entries
  Current filter: <all>

--> add cm1

Added cm1

--> cd cm1

[ //localhost/Radius/CommandSets/cm1 ]
  Name = cm1
  Description =
  Commands/

--> cd Commands/

[ //localhost/Radius/CommandSets/cm1/Commands ]

--> Set 1 "permit show *"

Set 1 "permit show *"

--> cd ..

[ //localhost/Radius/CommandSets/cm1 ]
  Name = cm1
  Description =
  Commands/

--> cd ..

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

```
cm1/
--> add cm2

Added cm2

--> cd cm2

[ //localhost/Radius/CommandSets/cm2 ]
  Name = cm2
  Description =
  Commands/

--> cd commands/

[ //localhost/Radius/CommandSets/cm2/Commands ]

--> Set 1 "deny show all"

Set 1 "deny show all"
--> sav

Validating //localhost...
Saving //localhost...
```

For more information on configuring the command sets and device access rules in the GUI, see the [CommandSets, page 2-57](#) and [DeviceAccessRules, page 2-58](#) sections in [Chapter 2, “Using the Graphical User Interface.”](#)