Cisco Prime Access Registrar Server Objects

This chapter describes the objects you use to configure and operate your Cisco Prime AR RADIUS server.

Cisco Prime Access Registrar (Cisco Prime AR) is configured and operated through a set of *objects*. These objects are arranged in a hierarchy, with some of the objects containing subobjects; just as in a UNIX file system, in which directories can contain subdirectories. All of the objects, except those that are merely lists, contain properties that define the attributes or behavior of the object.

This chapter describes the following Cisco Prime AR objects:

- Radius— root of the configuration hierarchy
- UserLists—contains individual UserLists, which in turn contain users
- UserGroups—contains individual UserGroups
- Policies—contains individual Policies
- Clients—contains individual Clients
- Vendors—contains individual Vendors
- Scripts—contains individual Scripts
- Services—contains individual Services
- Session Managers—contains individual Session Managers
- Resource Managers—contains individual Resource Managers
- Profiles—contains individual Profiles
- Rules—contains individual Rules
- Translations—contains individual Translations
- TranslationGroups—contains individual Translation Groups
- Remote Servers—contains individual RemoteServers
- Advanced—contains advanced properties, Ports, Interfaces, Reply Messages, and the Attribute dictionary

Radius

The **Radius** object is the root of the hierarchy. For each installation of the Cisco Prime AR server, there is one instance of the **Radius** object. You reach all other objects in the hierarchy from the **Radius**.

The following is a listing of the RADIUS server object:

```
[ //localhost/Radius ]
    Name = Radius
    Description =
    Version = 1.7R0
    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/
    Advanced/
    Replication/
```

Table 4-1 lists the **Radius** properties. You you can set or change Radius properties using the Cisco Prime AR **aregcmd** commands.

> **Note**   When a field is listed as required, it means a value must be supplied; that is, the value must be set. You can use the default (if it is supplied) or you can change it to something else, but you cannot unset it. You *must* supply values for the required fields and for which no defaults exist.

.

Table 4-1   Radius Properties

Property	Description
Name	Required; must be unique in the list of servers in the cluster
Description	Optional description of the server
Version	Required; the currently installed version of Cisco Prime AR
IncomingScript	Optional; if there is a script, it is the first script Cisco Prime AR runs when it receives a request from any client and/or for any service
OutgoingScript	Optional; if there is a script, it is the last script Cisco Prime AR runs before it sends a response to any client

Table 4-1   Radius Properties (continued)

Property	Description
DefaultAuthenticationService	Optional; Cisco Prime AR uses this property when none of the incoming scripts sets the environment dictionary variable **Authentication-Service**
DefaultAuthorizationService	Optional; Cisco Prime AR uses this property when none of the incoming scripts sets the environment dictionary variable **Authorization-Service**
DefaultAccountingService	Optional; Cisco Prime AR uses this property when none of the incoming scripts sets the environment dictionary variable **Accounting-Service**
DefaultSessionService	Optional; Cisco Prime AR uses this property when none of the incoming scripts sets the environment dictionary variable **Session-Service**.
DefaultSessionManager	Optional; Cisco Prime AR uses this property if none of the incoming scripts sets the environment dictionary variable **Session-Manager**.

The remaining Cisco Prime AR objects are sub-objects of the **Radius** object.

UserLists

The **UserLists** object contains all of the individual UserLists, which in turn, contain the specific users stored within Cisco Prime AR. Cisco Prime AR references each specific UserList by **name** from a Service whose type is set to **local**. When Cisco Prime AR receives a request, it directs it to a Service. When the Service has its type property set to **local**, the Service looks up the user's entry in the specific UserList and authenticates and/or authorizes the user against that entry.

Note   Usernames might not include the forward slash (**/**) character. If the Cisco Prime AR server receives an access request packet with a User-Name attribute containing a forward slash character and the Cisco Prime AR server uses an internal UserList to look up users, the server produces an error (AX_EINVAL) and might fail. If usernames require a forward slash, use a script to translate the slash to an acceptable, unused character.

You can have more than one UserList in the **UserLists** object. Therefore, use the **UserLists** object to divide your user community by organization. For example, you might have separate **UserLists** objects for Company A and B, or you might have separate **UserLists** objects for different departments within a company.

Using separate **UserLists** objects allows you to have the same name in different lists. For example, if your company has three people named `Bob` and they work in different departments, you could create a UserList for each department, and each Bob could use his own name. Using UserLists lets you avoid the problem of `Bob1`, `Bob2`, and so on.

If you have more than one UserList, you can have a script Cisco Prime AR can run in response to requests. The script chooses the Service, and the Service specifies the actual UserList which contains the user. The alternative is dynamic properties.

The subobjects are the Users listed by name. Table 4-2 lists the **UserLists** object properties.

Table 4-2   UserLists Properties

Property	Description
Name	Required; must be unique in UserLists.
Description	Optional description of the UserList.

Users

The **Users** object contains all of the information necessary to authenticate a user or authorize a user. Users in local UserLists can have multiple profiles. Table 4-3 lists the **Users** object properties.

Table 4-3   Users Properties

Property	Description
Name	Required; must be unique in the specific UserList.
Description	Optional description of the user.
Password	Required; length must be between 0-253 characters.
Enabled	Required; default is TRUE, which means the user is allowed access. Set to FALSE to cause Cisco Prime AR to deny the user access.
Group (Overridden by User-Group)	Optional; when you set this to the name of a UserGroup, Cisco Prime AR uses the properties specified in that UserGroup to authenticate and/or authorize the user.
BaseProfile (Overridden by User-Profile)	Optional; when you set this to the name of a Profile and the service-Type is not equal to Authenticate Only, Cisco Prime AR adds the properties in the Profile to the Response dictionary as part of the authorization.
AuthenticationScript	Optional; when you set this property to the name of a script, you can use the script to perform additional authentication checks to determine whether to accept or reject the user.
AuthorizationScript	Optional; when you set this property to the name of a script, you can use the script to add, delete, or modify the attributes of the Response dictionary.
UserDefined1	Optional; you can use this property to store notational information which you can then use to filter the UserList. This property also sets the environment variable for UserDefined1.

HiddenAttributes Property

The HiddenAttributes property in the user object provides a concatenation of all user-level reply attributes. The Cisco Prime AR server uses the HiddenAttributes property to construct and populate a virtual attributes directory.

The HiddenAttributes property is, in fact, hidden. It is not displayed and cannot be set or modified using **aregcmd**, but when an administrator issues a **save**, all values from the user's Attributes directory go into the HiddenAttributes property and the persistent storage.

The attributes are added in a replace-if-present-add-if-not manner as used in the UserGroup-Base-Profile and User-Base-Profile.

The order of application of the attributes is as follows:

- UserGroup Base Profile
- UserGroup Attributes
- User Base Profile
- User Attributes

UserGroups

The **UserGroups** objects allow you to maintain common authentication and authorization attributes in one location, and then have many users reference them. By having a central location for attributes, you can make modifications in one place instead of having to make individual changes throughout your user community.

For example, you can use several **UserGroups** to separate users by the services they use, such as a group specifying PPP and another for Telnet.

Table 4-4 lists the **UserGroups** properties.

Table 4-4   UserGroups Properties

Property	Description
Name	Required; must be unique in the **UserGroup** list.
Description	Optional description of the group.
BaseProfile	Optional; when you set this to the name of a Profile, Cisco Prime AR adds the properties in the Profile to the response dictionary as part of the authorization.
AuthenticationScript	Optional; when you set this property to the name of a Script, you can use the Script to perform additional authentication checks to determine whether to accept or reject the user.
AuthorizationScript	Optional; when you set this property to the name of a Script, you can use the Script to add, delete, or modify the attributes of the Response dictionary.

Policies

A Policy is a set of rules applied to an Access-Request. If you are using **Policies**, the first one that must be created is SelectPolicy.

Table 4-5 lists the properties required for a given **Policy**.

Table 4-5   Policies Properties

Property	Description
Name	Required; must be unique in the **Policies** list
Description	Optional description of the Policy
Grouping	Optional grouping of rules

Clients

All NASs and proxy clients that communicate directly with Cisco Prime AR must have an entry in the **Clients** list. This is required because NAS and proxy clients share a secret with the RADIUS server which is used to encrypt passwords and to sign responses. Table 4-6 lists the **Client** object properties.

Table 4-6   RADIUS Client Properties

Property	Description
Name	Required and should match the Client identifier specified in the standard RADIUS attribute, **NAS-Identifier**. The name must be unique within the Clients list.
Description	Optional description of the client.
Protocol	Required; specifies the client protocol which can be Radius, Diameter, or Tacacs-and-Radius.
IPAddress	Required; must be a valid IP address and unique in the Clients list. Cisco Prime AR uses this property to identify the Client that sent the request, either using the source IP address to identify the immediate sender or using the **NAS-IP-Address** or **NAS-IPv6-Address** attribute in the Request dictionary to identify the NAS sending the request through a proxy.
	When a range is configured for a Client's IPAddress property, any incoming requests whose source address belongs to the range specified, will be allowed for further processing by the server. Similarly when a wildcard (an asterisk '*' in this case) is specified, any incoming requests whose source address matches the wildcard specification will be allowed. In both the cases, the configured client properties like SharedSecret, and Vendor are used to process the requests.
	You can specify a range of IP addresses using a hyphen as in:
	100.1.2.11-20
	You can use an asterisk wildcard to match all numbers in an IP address octet as in:
	100.1.2.*
	You can specify an IPAddress and a subnet mask together using Classless Inter-Domain Routing (CIDR) notation as in:
	100.1.2.0/24
	You can use the IPAddress property to set a base address and use the NetMask property to specify the number of clients in the subnet range.
	The IP address format is enhanced to support IPv6 apart from IPv4.
	You can use an asterisk wildcard to match all numbers in an IP address octet as in:
	1124:1124:1124:1124:*:*:*:*
	Note The IPv6 address must be in standard notation.

Table 4-6   RADIUS Client Properties (continued)

Property	Description
SharedSecret	Required; must match the secret configured in the Client.
Type	Required; accept the default (NAS), or set it to ATM, Proxy, or NAS+Proxy.
Vendor	Optional; you can use this property when you need special processing for a specific vendor's NAS. To use this property, you must configure a **Vendor** object and include a Script. Cisco Prime AR provides five Scripts you can use: one for Ascend, Cisco, Cabletron, Altiga, and one for USR. You can also provide your own Script.
IncomingScript	Optional; you can use this property to specify a Script you can use to determine the services to use for authentication, authorization, and/or accounting.
OutgoingScript	Optional; you can use this property to specify a Script you can use to make any Client-specific modifications when responding to a particular Client.
EnableDynamicAuthorization	Optional; when set to TRUE, this property enables Change of Authorization and Packet of Disconnect features.
DynamicAuthorizationServer	This subdirectory is only present in a client with EnableDynamicAuthorization set to TRUE and contains properties required for CoA and PoD requests.
Port	Located under the DynamicAuthorizationServer subdirectory, the default port is 3799.
InitialTimeout	Located under the DynamicAuthorizationServer subdirectory, the default is 5000.
MaxTries	Located under the DynamicAuthorizationServer subdirectory, the default is 3.
DynamicAuthSharedSecret	Located under the DynamicAuthorizationServer subdirectory, this is the shared secret used for communicating CoA and PoD packets with the client.
PODAttributeGroup	This property is found under the DynamicAuthorizationServer subdirectory and points to a group of attributes to be included in a POD request sent to this client. These attribute groups are created and configured under the AttributeGroups subdirectory in **/Radius/Advanced**.
COAAttributeGroup	This property is found under the DynamicAuthorizationServer subdirectory and points to a group of attributes to be included in a CoA request sent to this client. These attribute groups are created and configured under the AttributeGroups subdirectory in **/Radius/Advanced**.

Table 4-6   RADIUS Client Properties (continued)

Property	Description
NetMask	Specifies the subnet mask used with the network address setting configured for the IPAdress property when configuring a range of IP addresses. This property is not used for a single client with an IP address only. The NetMask property is used to configure multiple clients when you configure a base IP address in the IPAddress property. You can set the NetMask property for a range of 256 clients using the following example: **set NetMask 255.255.255.0** When the NetMask property indicates a pool of 256 address (255.255.255.0), the range of addresses reserved for clients is 0-255, as in 100.1.1.0-100.1.1.255. **Note** If you set the NetMask property, validation will fail if you attempt to specify a subnet mask using CIDR notation with the IPAddress property (described above).
EnableNotifications	Required; the default value is FALSE and indicates the client is not capable of receiving Accounting-Stop notifications from the Cisco Prime AR server. When set to TRUE, the client can receive Accounting-Stop notifications from the Cisco Prime AR server and additional properties must be configured under a new sub-directory named NotificationProperties.
NotificationProperties	When the EnableNotifications property is set to TRUE, this subdirectory contains additional properties required to support the Query-Notify feature.
Port	Located under the NotificationProperties subdirectory, specifies the port used by the Cisco Prime AR server to receive Accounting-Stop packets. Required when EnableNotifications is set to TRUE; the default value is 1813.
InitialTimeout	Located under the NotificationProperties subdirectory, specifies the timeout value in milliseconds the Cisco Prime AR server waits for an Accounting-Response packet before attempting a retry (sending another Accounting-Stop packet to the client). Required when EnableNotifications is set to TRUE; the default value is 5000.
MaxTries	Located under the NotificationProperties subdirectory, specifies the number of times the Cisco Prime AR server sends an Accounting-Stop packet to a client. Required when EnableNotifications is set to TRUE; the default value is 3.

Table 4-6   RADIUS Client Properties (continued)

Property	Description
NotificationAttributeGroup	Located under the NotificationProperties subdirectory, specifies the name of an attribute group under **/Radius/Advanced/AttributeGroups** that contains the attributes to be included when sending an the Accounting-Stop packet to this client.
	Required when EnableNotifications is set to TRUE; there is no default value. You must provide the name of a valid AttributeGroup and the named AttributeGroup must contain at least one valid attribute, or validation will fail.
EnforceTrafficThrottling	Required; the default value is TRUE and indicates enforce traffic throttling for this client. This property is under **/Radius/Advanced/ MaximumOutstanding/IncomingRequests**.
	When set to FALSE, the traffic throttling for the packet coming from this client is bypassed.

Table 4-7 describes the Diameter client properties.

Table 4-7   Diameter Client Properties

Property	Description
Name	Required; must be unique in the client list.
Description	Optional; description of the client.
Protocol	Required; specifies the client protocol which can be Radius or Diameter.
HostName	Required; hostname or IP address of the Diameter client.
Vendor	Optional; you can use this property when you need special processing for a specific vendor's peer.
IncomingScript	Optional; specifies a script that you can use to make client-specific modifications when a request is received from a client.
OutgoingScript	Optional; specifies a script that you can use to make any client-specific modifications when responding to a particular client.
Port	Required; port on which the client connects with Cisco Prime AR server.
SCTP-Enabled	Required, default value is False. If set to TRUE, SCTP will be used to establish the connection with the peer else TCP will be used.

Vendors

The **Vendor** object provides a central location for specifying all of the request and response processing a particular NAS or Proxy vendor requires. Depending on the vendor, it might be necessary to map attributes in the request from one set to another, or to filter out certain attributes before sending the response to the client. For more information about standard RADIUS attributes, see Appendix C, "RADIUS Attributes."

> **Note** When you have also set **/Radius/IncomingScript**, Cisco Prime AR runs that script before the vendor's script. Conversely, when you have set a **/Radius/Outgoing** script, Cisco Prime AR runs the vendor's script before that script.

Table 4-8 lists the **Vendor** object properties.

Table 4-8   Vendor Properties

Property	Description
Name	Required; must be unique in the Vendors list.
Description	Optional description of the vendor.
IncomingScript	Optional; when you specify an IncomingScript, Cisco Prime AR runs the script on all requests from clients that specify that vendor.
OutgoingScript	Optional; when you specify an OutgoingScript, Cisco Prime AR runs the script on all responses to the Client.

Scripts

The **Script** objects define the function Cisco Prime AR invokes whenever the **Script** is referenced by name from other objects in the configuration.

You can write three types of scripts:

- REX (RADIUS EXtension) scripts are written in C or C++, and thus are compiled functions that reside in shared libraries
- Tcl scripts are written in Tcl, and are interpreted functions defined in source files.
- Java scripts

> **Note** For more information about how to write scripts and how to incorporate them into Cisco Prime AR, see Chapter 11, "Using Extension Points."

> **Note** Cisco is not liable for scripts developed by clients. See Client Scripting in Chapter 1, "Overview."

Table 4-9 lists the **Script** object properties.

Table 4-9   Script Object Properties

Property	Description
Name	Required; must be unique in the Scripts list.
Description	Optional description of the script.
Language	Required; specify either REX, Tcl, or Java.

Table 4-9   Script Object Properties (continued)

Property	Description
Filename	Required; specifies either a relative or absolute path. When you specify a relative path, the path must be relative to the **$INSTALL/scripts/radius/$Language** directory. When you specify an absolute path, the server must be able to reach it.
EntryPoint	Optional; when not set, Cisco Prime AR uses the value specified in the **Name** property.
InitEntryPoint	Optional; if set, it must be the name of the global symbol Cisco Prime AR should call when it initializes the shared library at system start up, and just before it unloads the shared library.
InitEntryPointArg	Optional; when set, it provides the arguments to be passed to the **InitEntryPoint** in the environmental variable **Arguments**.
ClassName	For Java language scripts, the name of the class that implements the extension interface; the **.class** file should be placed in **/cisco-ar/scripts/radius/java**
InitializeArg	Optional for Java language scripts; set to a string to be passed to the Initialize method if the class implements the optional ExtensionWithInitialization interface.

The **InitEntryPoint** properties allow you to perform initialization before processing and then cleanup before stopping the server. For example, when Cisco Prime AR unloads the script (when it stops the RADIUS server) it calls the **InitEntryPoint** again to allow it to perform any clean-up operations as a result of its initialization. One use of the function might be to allow the script to close an open Accounting log file before stopping the RADIUS server.

Note   When you use a Cisco Prime AR file service, Cisco Prime AR automatically closes any opened files. However, if you write scripts that manipulate files, you are responsible for closing them.

Note   If you have more than one extension point script (defined under **/Radius/Scripts**) using the same Java class, only one instance of the class is created and used for all the extension point scripts.

Services

Cisco Prime AR supports authentication, authorization, and accounting (AAA) services. In addition to the variety of built-in AAA services (specified in the **Type** property), Cisco Prime AR also enables you to add new AAA services through custom shared libraries.

Table 4-10 lists the common **Services** properties. There are additional properties depending on the type of service.

Table 4-10   Common Service Properties

Property	Description
Name	Required; must be unique in the Services list.
Description	Optional description of the service.
Type	Required, must set it to a valid Cisco Prime AR service.
OutagePolicy	Required; the default is **RejectAll**. This property defines how Cisco Prime AR handles requests if all servers listed in the **RemoteServers** properties are unavailable (that is, all remote RADIUS servers are not available). You must set it to one of the following: **AcceptAll**, **DropPacket**, or **RejectAll**.
OutageScript	Optional; if you set this property to the name of a script, Cisco Prime AR runs it when an outage occurs. This property allows you to create a script that notifies you when the RADIUS server detects a failure.

Note **OutagePolicy** also applies to Accounting-Requests. If an Accounting-Request is directed to an unavailable Service, then the values in Table 4-11 apply.

Table 4-11   OutagePolicy Request Packets

Property	Description	Accounting-Request Description
AcceptAll	Continues processing the packet as if the Service was successful.	The Accounting-Request will continue through the server and a response will be sent.
DropPacket	Immediately drops the packet, no further processing, and does not send any response to the client for this packet.	The packet will be discarded and it will not be processed any further.
RejectAll	Rejects the packet, but continues processing it and sends the client a reject response.	The request will be dropped and no more processing will be done.

Types of Services

This section lists the types of services available in Cisco Prime AR with their required and optional properties. The service you specify determines what additional information you must provide.

This section contains the following topics:

- Domain Authentication
- EAP Services
- File
- Group
- Java
- LDAP

- Local
- ODBC
- ODBC-Accounting
- Prepaid Services
- RADIUS
- Radius Query
- RADIUS-Session
- Rex
- WiMAX
- Diameter
- M3UA

Domain Authentication

The Domain Authentication service type, domain-auth, is used with a Remote Server of the same type to provide support for authentication against Windows Domain Controller/Active Directory (WDC/AD). The following example lists the default configuration for a domain-auth service which are all common service properties described in Table 4-10:

```
[ //localhost/Radius/Services/wdc ]
    Name = wdc
    Description =
    Type = domain-auth
    IncomingScript~ =
    OutgoingScript~ =
    OutagePolicy~ = RejectAll
    OutageScript~ =
    MultipleServersPolicy = Failover
    RemoteServers/
```

EAP Services

Cisco Prime AR supports Extensible Authentication Protocol (EAP) and Protected EAP (PEAP) to provide a common protocol for differing authentication mechanisms. EAP enables the dynamic selection of the authentication mechanism at authentication time based on information transmitted in the Access-Request. Cisco Prime AR provides the following EAP services:

- EAP-FAST
- EAP-GTC
- EAP-LEAP
- EAP-MD5
- EAP-MSChapV2
- EAP-Negotiate
- EAP-SIM
- EAP-Transport Level Security (TLS)
- EAP-Tunneled TLS (TTLS)

- PEAP Version 0 (Microsoft PEAP)

- PEAP Version 1 (Cisco PEAP)

See Chapter 9, "Extensible Authentication Protocols," for detailed information about properties used in EAP-type services.

File

Specify the **file** service when you want Cisco Prime AR's RADIUS Server to perform local accounting using a specific file. Every **file** Service in your configuration will cause a file with the configured name to be created when the server is started, even if the service is not being invoked by any request packets. Table 4-12 lists the properties used for a **file** service.

Table 4-12   File Service Properties

Property	Description
Type	Required; must be set to **group** for a group service.
IncomingScript	Name of script to run when the service starts.
OutgoingScript	Name of script to run when the service ends.
OutagePolicy	Required; the default is **RejectAll**. This property defines how Cisco Prime AR handles requests if all servers listed in the **RemoteServers** properties are unavailable (that is, all remote RADIUS servers are not available). You must set it to one of the following: **AcceptAll**, **DropPacket**, or **RejectAll**.
OutageScript	Optional; if you set this property to the name of a script, Cisco Prime AR runs it when an outage occurs. This property allows you to create a script that notifies you when the RADIUS server detects a failure.
FilenamePrefix	Required; a string that specifies where Cisco Prime AR writes the account records. It must be either a relative or absolute path. When you specify a relative path, it must be relative to the **$INSTALL/logs** directory. When you specify an absolute path, the server must be able to reach it. The default is **Accounting**.
MaxFileSize	Optional; stored as a string, but is composed of two parts, a number and a units indicator (<n> <units>) in which the unit is one of: K, Kilobyte, Kilobytes, M, Megabyte, Megabytes, G, Gigabyte, Gigabytes. The default is ten megabytes.
MaxFileAge	Optional; stored as a string, but is composed of two parts, a number and a units indicator (*<n> <units>*) in which the unit is one of: H, Hour, Hours, D, Day, Days, W, Week, Weeks. The default is one day.
RolloverSchedule	Indicates the exact time including the day of the month or day of the week, hour and minute to roll over the accounting log file.
UseLocalTimeZone	When set to TRUE, indicates the accounting records' TimeStamp is in local time. When set to FALSE, the default, accounting records' TimeStamp is in GMT.

Cisco Prime AR opens the file when it starts the RADIUS server and closes the file when you stop the server. You can depend on Cisco Prime AR flushes the accounting record to disk before it acknowledges the request.

Based on the maximum file size and age you have specified, Cisco Prime AR closes the accounting file, moves it to a new name, and reopens the file as a new file. The name Cisco Prime AR gives this accounting file depends on its creation and modification dates.

- If the file was created and modified on the same date, the filename is **FileNamePrefix-**<*yyyymmdd*>**-**<*n*>**.log**. The date is displayed as year, month, day, number.

- If the file was created on one day and modified on another, the filename is **FileNamePrefix-**<*yyyymmdd*>**-**<*yyyymmdd*>**-**<*n*>**.log**. The dates are creation, modification, and number.

Group

A group service contains a list of references to other services and specifies whether the responses from each of the services should be handled as a logical AND or a logical OR function. You specify AND or OR in the Result-Rule attribute of Group Services. The default value is AND.

Table 4-13 lists the properties used to configure a **group** service.

Table 4-13   Group Service Properties

Property	Description
Type	Required; must set it to group.
IncomingScript	Optional; name of script to run when the service starts.
OutgoingScript	Optional; name of script to run when the service ends.
ResultRule	When set to AND (the default), the response from the GroupService is positive if each of the services referenced return a positive result. The response is negative if any of the services reference return a negative result.
	When set to OR, the response from the GroupService is positive if any of the services referenced return a positive result. The response is negative if all the referenced services return a negative result.
	The settings parallel-AND or parallel-OR are similar to AND and OR settings, except that each referenced service processes requests simultaneously instead of asking each reference service sequentially to save processing time.
GroupServices	Use the GroupServices subdirectory to specify the subservices in an indexed list to provide specific ordering control of which services to apply first. Each subservice listed must be defined in the Services section of the Radius configuration and cannot be a of type *group*, eap-leap, or eap-md5.

If Result-Rule is set to AND, the response from the Group Service is positive if each of the services referenced return a positive result. The response is negative if any of the services reference return a negative result. If Result-Rule is set to OR, the response from the Group Service is positive if any of the services referenced return a positive result. The response is negative if all the referenced services return a negative result.

When the Result-Rule attribute is set to AND or OR, each referenced service is accessed sequentially, and the Group Service waits for a response from the first referenced service before moving on to the next service (if necessary). If a service takes a long time to respond, that causes a delay in sending the request to the next referenced server.

The ResultRule settings parallel-and and parallel-or are similar to the AND and OR settings except that they ask each referenced service to process the request simultaneously instead of asking each referenced server sequentially, thereby saving processing time.

A parallel-and setting might respond with its own reply as soon as it receives a negative response, but otherwise must wait for all responses before it can respond with a positive reply. Likewise, a parallel-or might respond as soon as it receives a positive response, but otherwise must wait for all responses before it can reply with a negative response.

If a service referenced from a Group Service is of type RADIUS and if Accounting-Requests are being processed by the Group Service, setting the AckAccounting property in the remote server will affect the behavior of the parallel-or Group Service. This is because if AckAccounting is set to FALSE, the RADIUS Remote Server will not wait for the response from the remote server but returns a response immediately. Since the Group Service is set to parallel-or, after it receives the response from the RADIUS service, it is free to send a response itself. This will have the effect that a response is sent very quickly from the Group Service acknowledging the Accounting-Request and responses from the other referenced services are handled as the arrive.

Note that since AckAccounting was set to FALSE, there is no guarantee that the Remote Server successfully processed the request. Since it is a RADIUS Remote Server, the Cisco Prime AR server attempts for MaxTries to send the request to the server and to get back an acknowledgement, but if that fails, there will be no indication to the client about that event. The acknowledgement to the client has been sent long before.

Java

Specify the **java** service type when you want to create a custom service and use a script for authentication, authorization, or accounting. Table 4-14 lists the properties required to configure a java service.

A java service uses an extension point script to provide the service's functionality and handles both RADIUS and TACACS requests for authentication, authorization, and accounting.

Table 4-14   Java Service Properties

Property	Description
Type	Required; must set it to java.
IncomingScript	Name of script to run when the service starts.
OutgoingScript	Name of script to run when the service ends.
OutagePolicy	Required; the default is **RejectAll**. This property defines how Cisco Prime AR handles requests if all servers listed in the **RemoteServers** properties are unavailable (that is, all remote RADIUS servers are not available). You must set it to one of the following: **AcceptAll**, **DropPacket**, or **RejectAll**.
OutageScript	Optional; if you set this property to the name of a script, Cisco Prime AR runs it when an outage occurs. This property allows you to create a script that notifies you when the RADIUS server detects a failure.
ClassName	Set to the name of a class that implements the Extension interface.
InitializeArg	Optional; set to a string to be passed to the Initialize method if the class implements the optional ExtensionWithInitialization interface.

LDAP

Specify the **ldap** service type when you want to use a particular LDAP remote server for authentication and/or authorization. Table 4-15 lists the properties used to configure an LDAP service.

When using LDAP for authentication and a local database for authorization, ensure that the usernames in both locations are identical with regard to case sensitivity.

Table 4-15   LDAP Service Properties

Property	Description
Type	Required, must set it to **ldap**
IncomingScript	Name of script to run when the service starts.
OutgoingScript	Name of script to run when the service ends.
OutagePolicy	Required; the default is **RejectAll**. This property defines how Cisco Prime AR handles requests if all servers listed in the **RemoteServers** properties are unavailable (that is, all remote RADIUS servers are not available). You must set it to one of the following: **AcceptAll**, **DropPacket**, or **RejectAll**.
OutageScript	Optional; if you set this property to the name of a script, Cisco Prime AR runs it when an outage occurs. This property allows you to create a script that notifies you when the RADIUS server detects a failure.
MultipleServersPolicy	Required; must be set to either **Failover** or **RoundRobin**.
	When you set it to **Failover**, Cisco Prime AR directs requests to the first server in the list until it determines the server is offline. At which time, Cisco Prime AR redirects all requests to the next server in the list until it finds a server that is online.
	When you set it to **RoundRobin**, Cisco Prime AR directs each request to the next server in the RemoteServers list to share the resource load across all of the servers listed in the RemoteServers list.
RemoteServers	Required; an indexed list from 1 to *<n>*. Each entry in the list is the name of a RemoteServer.

Local

Specify **local** when you want the Cisco Prime AR server to perform the authentication and authorization using a specific UserList. For more information, see the "UserLists" section on page 4-3. Table 4-16 lists the properties used to configure a **local** service.

Table 4-16   Local Service Properties

Property	Description
Type	Required, must set it to **local**.
IncomingScript	Optional; name of script to run when the service starts.
OutgoingScript	Optional; name of script to run when the service ends.

Table 4-16   *Local Service Properties (continued)*

Property	Description
OutagePolicy	Required; the default is **RejectAll**. This property defines how Cisco Prime AR handles requests if all servers listed in the **RemoteServers** properties are unavailable (that is, all remote RADIUS servers are not available). You must set it to one of the following: **AcceptAll**, **DropPacket**, or **RejectAll**.
OutageScript	Optional; if you set this property to the name of a script, Cisco Prime AR runs it when an outage occurs. This property allows you to create a script that notifies you when the RADIUS server detects a failure.
UserLists	Required; this object contains all of the individual UserLists, which in turn, contain the specific users stored within Cisco Prime AR. Cisco Prime AR references each specific UserList by **name** from a Service whose type is set to **local**.
	When Cisco Prime AR receives a request, it directs it to a Service. When the Service has its type property set to **local**, the Service looks up the user's entry in the specific UserList and authenticates and/or authorizes the user against that entry.

ODBC

Specify **odbc** when you want to use an ODBC service for authentication, authorization and accounting through an ODBC data store. Use an ODBC service to authenticate and authorize an access requests by querying user information through ODBC and to insert accounting records into a data store through ODBC. Table 4-17 lists the properties used to configure an ODBC service.

Table 4-17   *ODBC Service Properties*

Property	Description
Type	Required; must set it to **odbc**.
IncomingScript	Optional; name of script to run when the service starts.
OutgoingScript	Optional; name of script to run when the service ends.
OutagePolicy	Required; the default is **RejectAll**. This property defines how Cisco Prime AR handles requests if all servers listed in the **RemoteServers** properties are unavailable (that is, all remote RADIUS servers are not available). You must set it to one of the following: **AcceptAll**, **DropPacket**, or **RejectAll**.
OutageScript	Optional; if you set this property to the name of a script, Cisco Prime AR runs it when an outage occurs. This property allows you to create a script that notifies you when the RADIUS server detects a failure.

Table 4-17   ODBC Service Properties (continued)

Property	Description
MultipleServersPolicy	Required; must be set to either **Failover** or **RoundRobin**.
	When you set it to **Failover**, Cisco Prime AR directs requests to the first server in the list until it determines the server is offline. At which time, Cisco Prime AR redirects all requests to the next server in the list until it finds a server that is online.
	When you set it to **RoundRobin**, Cisco Prime AR directs each request to the next server in the RemoteServers list to share the resource load across all of the servers listed in the RemoteServers list.
RemoteServers	Required; an indexed list from 1 to *<n>*. Each entry in the list is the name of a RemoteServer.

ODBC-Accounting

If you use the Oracle Accounting feature, you must configure an ODBC-Accounting RemoteServer object. See Configuring an ODBC/OCI RemoteServer, page 21-7, for more information on ODBC-Accounting RemoteServer.

Prepaid Services

Cisco Prime Access Registrar (Cisco Prime AR) supports two types of prepaid billing, IS835C and Cisco Real-time Billing (CRB), a Cisco proprietary solution. See IS835C Prepaid Billing, page 16-2 for more information on Prepaid -IS835C. See CRB Prepaid Billing, page 16-7 for more information on Prepaid-CRB.

RADIUS

Specify the **radius** service type when you want to use a particular RADIUS remote server for authentication and authorization. Table 4-18 lists the properties used to configure a RADIUS service.

Table 4-18   RADIUS Service Properties

Property	Description
Type	Required; must set it to **radius**.
IncomingScript	Optional; name of script to run when the service starts.
OutgoingScript	Optional; name of script to run when the service ends.
OutagePolicy	Required; the default is **RejectAll**. This property defines how Cisco Prime AR handles requests if all servers listed in the **RemoteServers** properties are unavailable (that is, all remote RADIUS servers are not available). You must set it to one of the following: **AcceptAll**, **DropPacket**, or **RejectAll**.
OutageScript	Optional; if you set this property to the name of a script, Cisco Prime AR runs it when an outage occurs. This property allows you to create a script that notifies you when the RADIUS server detects a failure.

Table 4-18   RADIUS Service Properties (continued)

Property	Description
MultipleServersPolicy	Required; must be set to either **Failover** or **RoundRobin**.
	When you set it to **Failover**, Cisco Prime AR directs requests to the first server in the list until it determines the server is offline. At which time, Cisco Prime AR redirects all requests to the next server in the list until it finds a server that is online.
	When you set it to **RoundRobin**, Cisco Prime AR directs each request to the next server in the RemoteServers list to share the resource load across all of the servers listed in the RemoteServers list.
RemoteServers	Required; an indexed list from 1 to *<n>*. Each entry in the list is the name of a RemoteServer.

Radius Query

Cisco Prime AR supports a new service type called radius-query that can be used to query cached data through Radius packets. This radius-query service contains a list of session managers to be queried from and a list of (cached) attributes to be returned in the Access-Accept packet in response to a Radius Query request. Cisco Prime AR also supports caching and querying of multivalued attributes.

The Radius Query service should be selected through an extension point script or through the Rule and Policy Engine by setting it to a new environment variable named Query-Service. The reason for this is that the Radius Query request comes in as an Access-Request and the server has no way of knowing whether it is a Radius Query request or normal authentication request. Setting the Query-Service environment variable tells the Cisco Prime AR server that the request is a Radius Query request so the Cisco Prime AR server can process the request with the radius-query service set in the Query-Service environment variable.

When a Radius Query service is selected to process an Access-Request, it queries the configured list of Session Managers for a matching record using the QueryKey value configured in the session-cache Resource Manager referenced under these Session Managers as key. If a matching record is found, an Access-Accept containing a list of cached attributes present (based on the configuration) in the matched record is sent back to the client. If the session cache contains a multivalued attribute, all values of that attribute are returned in the response as a multivalued attribute. If there is no matching record, an Access-Reject packet is sent to the client.

Cisco Prime AR introduces scripting points at the Session Manager level along with automated programmable interfaces (APIs) to access cached information present in the session record. You can use these scripting points and APIs to write extension point scrips to modify the cached information.

The following example shows the default configuration of a radius-query service:

```
[ //localhost/Radius/Services/radius-query ]
   Name = radius-query
   Description =
   Type = radius-query
   IncomingScript~ =
   OutgoingScript~ =
   SessionManagersToBeQueried/
   AttributesToBeReturned/
```

Table 4-19 lists the properties used to configure a Radius Query service.

Table 4-19   Radius Query Service Properties

Property	Description
Type	Required; must set it to **radius query**.
IncomingScript	Optional; name of script to run before this service starts processing on the request.
OutgoingScript	Optional; name of script to run after this service completes processing on the request.
SessionManagersToBeQueried	Lists Session Managers to be queried for the target record. If this list is empty, all Session Managers having session-cache Resource Managers will be queried for the target record. Otherwise, only those SessionManagers configured under SessionManagerToBeQueried are queried. If the targeted record is found in a Session Manager, the query stops and the response is returned to the client.
AttributesToBeReturned	Lists attributes to be returned if present in a matched record. If this list is empty, all attributes cached in a matched session are returned. If a configured attribute is not present in the matched record, that attribute is ignored.
	Note The User-Password attribute will not be returned in query responses and cannot be configured under AttributesToBeReturned.

When an Access-Request packet is received by the Cisco Prime AR server, the session-cache Resource Manager caches the configured attributes in the session with the configured QueryKey as the key to the cached data. In the TAL solution, the QueryKey will usually be Framed-IP-Address. If an Accounting-Requestor Accounting-Start packet is received for the same session, the cached data is updated if necessary. If there is a multivalued attribute in the Access-Request packet or Accounting-Request packet, the Cisco Prime AR server caches all the values of that attributes.

In TAL, when the SSG receives an IP packet originating from a user unknown to the SSG, it sends an Access-Request packet to the Cisco Prime AR server in which the User-Name and Framed-IP-Address attributes both contain the user's source IP address, and the Service-Type is set to Outbound, among other attributes. These attributes and their values distinguish Radius Query requests from normal authentication requests in TAL.

Note   In solutions other than TAL, the criterion that distinguishes Radius Query requests from normal authentication requests might be different.

A new environment variable, Query-Service, can be set to the name of a radius-query service, in an extension point script, or through the Rule and Policy engine so the Cisco Prime AR server knows the current request is a Radius Query request and processes it with the radius-query service value set in the Query-Service environment variable.

API Calls

Cisco Prime AR provides several new API calls you can use to get, put, and delete the cached attributes present in the session record.

The entry point function changes slightly to take a fifth argument which is a pointer to a structure containing the new API calls:

```
typedef int (REXAPI * RexEntryPointFunction)
(
    int iScriptingPoint,
    rex_AttributeDictionary_t* pRequest,
    rex_AttributeDictionary_t* pResponse,
    rex_EnvironmentDictionary_t* pRadius,
    rex_SessionRecord_t* pSession
    );
```

However, you can continue to write extension point scripts with four arguments as well, for example without the pSession argument.

The following are API calls and their functionality. All these API calls fail gracefully when they are invoked from any scripting point other than the Session Manager scripting points.

const char* get

```
const char* get(
    rex_SessionRecord_t* pSession,
    const char* pszAttribute,
    int <iIndex>,
    abool_t* <pbMore>
    )
```

This API returns the value of the <iIndex>'d instance of the attribute cached in the session, represented as a string. When the session does not contain the attribute, an empty string is returned. When <pbMore> is non-zero, this method sets <pbMore> to TRUE when more instances of the same attribute exist after the one returned and to FALSE otherwise. This can be used to determine whether another call to get() method should be made to retrieve other instances of the same attribute.

abool_t put

```
abool_t put(
    rex_SessionRecord_t* pSession,
    const char* pszAttribute,
    const char* <pszValue>,
    int <iIndex>
    )
```

When <iIndex> equals the special value REX_REPLACE, this method replaces any existing instances of <pszAttribute> with a single value in the session. When <iIndex> equals the special value REX_APPEND, it appends a new instance of <pszAttribute> to the end of the list of existing instances of <pszAttribute>. When <iIndex> equals the special value REX_AUGMENT, this method only puts <pszAttribute> when it does not already exist. Otherwise, a new instance of <pszAttribute> is inserted/replaced at the position indicated. This method returns TRUE if it is able to cache the attribute successfully and FALSE otherwise.

abool_t remove

```
abool_t remove(
    rex_SessionRecord_t* pSession,
    const char* pszAttribute,
    int <iIndex>
    )
```

This method removes the <pszAttribute> from the session. When <iIndex> equals the special value REX_REMOVE_ALL, this method removes any existing instances of <pszAttribute>. Otherwise, it removes the instance of <pszAttribute> at the position indicated. It returns FALSE when <pszAttribute> is not present at any index in the session record and returns TRUE otherwise.

rex_SessionInfo_t*

rex_SessionInfo_t* getSessionInfo(rex_SessionRecord_t* pSession)

This method returns the pointer to a structure that contains the other session-related information, like Session Id, Session Start time, Session Last Accessed Time, present in the session record. The structure that holds this information will appear as follows:

```
typedef  struct rex_SessionInfo_s
{
    auint32_t iSessionId;
    auint32_t tSessionStartTime;
    auint32_t tSessionLastAccessedTime;
} rex_SessionInfo_t;
```

Tcl API calls

To use the extension point scripts written in Tcl, define the procedure at the session manager level as shown below:

```
proc test { request response environ session } {
}
```

There is a fourth argument *session* that needs to be passed to the Tcl procedure and the API calls that are intended to operate on the session record need to use this *session* dictionary.

API calls in Tcl have the same meaning with same number arguments and return values as described in Rex. The only difference is that the API getSessionInfo will not return a structure as in Rex but it will return the info as a string, as in the following example:

```
Session-ID=1, Session-Start-Time=1102099334, Session-Last-Accessed-Time=1102099334
```

Java API calls

There are two new interfaces ExtensionForSession and ExtensionForSessionWithInitialization and the customers whishing to use the extension point scripts written in Java at the session manager level needs to implement one of these interfaces.

The runExtension method of these interfaces will look as below:

```
public int runExtension
    ( int iExtensionPoint,
    AttributeDictionary request,
    AttributeDictionary response,
    EnvironmentDictionary environment,
    SessionRecord session
    );
```

API calls that are intended to operate on session record needs to use this 'session' dictionary.

API calls in Java have the same meaning with same number arguments and return values as described in Rex. The only difference is that the API getSessionInfo will not return a structure as in Rex but it will return the info as a string. For example:

Session-ID=1, Session-Start-Time=1102099334, Session-Last-Accessed-Time=1102099334

Existing scripts written in any of these three languages will not be affected with the introduction of the new 'session dictionary' argument. And the customers can use a script with any number of arguments (i.e with or without the last 'session dictionary' argument) at any extension point script. If there is no session to operate on, for example when the customer is trying to use session dictionary argument at an extension point other than session manager's, the Cisco Prime AR gracefully returns an error logging the appropriate message.

The simple *replace or add if it does not exist* model can still be used for simple modifications as before without the need to write a script. If the cached attributes are updated in the IncomingScript and if customers do not want them to be touched or updated again when the processing reaches session-cache resource manager, they can set the OverwriteAttributes property of the session-cache resource manager to FALSE so that the session-cache resource manager will not operate on this packet.

RADIUS-Session

A new Service step has been added in the processing of Access-Request and Accounting packets. This is an additional step after the AA processing for Access packet or Accounting processing for Accounting packet, but before the local session management processing. The Session-Service should have a service type of radius-session.

An environment variable Session-Service is introduced to determine the Session-Service dynamically. You can use a script or the rule engine to set the Session-Service environment variable. See Cross Server Session and Resource Management, page 1-9 for more information on RADIUS-Seesion.

Rex

Specify the **rex** service type when you want to create a custom service and use a script for authentication, authorization, or accounting. Table 4-20 lists the properties required to configure a **rex** service.

Table 4-20   rex Service Properties

Property	Description
Type	Required; must be set to **rex**.
IncomingScript	Optional; name of script to run when the service starts.
OutgoingScript	Optional; name of script to run when the service ends.
OutagePolicy	Required; the default is **RejectAll**. This property defines how Cisco Prime AR handles requests if all servers listed in the **RemoteServers** properties are unavailable (that is, all remote RADIUS servers are not available). You must set it to one of the following: **AcceptAll**, **DropPacket**, or **RejectAll**.
OutageScript	Optional; if you set this property to the name of a script, Cisco Prime AR runs it when an outage occurs. This property allows you to create a script that notifies you when the RADIUS server detects a failure.
Filename	Required; must be either a relative or an absolute path to the shared library containing the Service. When the pathname is relative, it must be relative to **$INSTALL/Scripts/Radius/rex**.
EntryPoint	Required; must be set to the function's global symbol.
InitEntryPoint	Required; must be the name of the global symbol Cisco Prime AR should call when it initializes the shared library and just before it unloads the shared library. **Note** A rex service must have an InitEntryPoint even if the service only returns REX_OK.
InitEntryPointArgs	Optional; when set, it provides the arguments to be passed to the **InitEntryPoint** in the environmental variable **Arguments**.

For more information about scripting, see Chapter 11, "Using Extension Points." For more information about using the REX Attribute dictionary, see Appendix A, "Cisco Prime Access Registrar Tcl, REX and Java Dictionaries."

WiMAX

Cisco Prime AR uses the Extensible Authentication Protocol (EAP) to enable the WiMAX feature. It also caches the IP attributes and Mobility Keys that are generated during network access authentication. To enable caching of the WiMAX attributes, you must configure the respective resource managers. See WiMAX in Cisco Prime Access Registrar, page 10-2, for more information on WiMAX.

Diameter

Diameter works with the rule policy engine to perform the routing for multiple peers. The following are the multiple peer policies supported with the proxy service to route the traffic:

- RoundRobin
- FailOver
- IMSI Range Based

For more information, refer Diameter Proxy Agent, page 8-22.

The following configuration is used to add Diameter proxy:

```
[ //localhost/Radius/Services/dia-proxy ]
Name = diameter-proxy
    Description =
    Type = diameter
    Realm = cisco.com
    Role = Proxy
    IncomingScript~ =
    OutgoingScript~ =
    Applications/
        Entries 1 to 1 from 1 total entries
        Current filter: <all>

NASREQ/
            Name = NASREQ
            Description =
            IsVendorSpecific = FALSE
            ApplicationID = 1
            StickySessionKey = Session-Id#1
            StickyCreationCmdList = 265||271::Accounting-Record-Type=2
            StickyDeletionCmdList = 275||271::Accounting-Record-Type=4
            DeMultiplexCCTerminateRequest = FALSE
            MultiplePeersPolicy = RoundRobin
            Peers/
                Entries 1 to 1 from 1 total entries
                Current filter: <all>

                hss1/
                    Name = hss1
                    HostName = gordon-ar1
                    Metric = 2
                    Weight = 0
                    IMSIRanges =
```

The following configuration is used to add Diameter local:

```
[ //localhost/Radius/Services/dia-local ]
    Name = dia-local
    Description =
    Type = diameter
    Realm = abc.com
    Role = Local
    IncomingScript~ =
    OutgoingScript~ =
    AuthenticationService = local-users
    AccountingService = local-file
    Peers/
        Entries 1 to 1 from 1 total entries
        Current filter: <all>

        murdcoh-ar1/
            Name = murdcoh-ar1
            HostName = murdoch-ar1
            IsVendorSpecific = FALSE
            ApplicationID = 1
            Metric = 2
```

The following configuration is used to add Diameter relay:

```
[ //localhost/Radius/Services/dia-relay ]
    Name = dia-relay
    Description =
    Type = diameter
    Realm = abc.com
    Role = relay
    Peers/
        Entries 1 to 1 from 1 total entries
        Current filter: <all>

        hss1/
            Name = hss1
            HostName = 10.77.240.69
            IsVendorSpecific = FALSE
            ApplicationID = 1
            Metric = 2
```

The following configuration is used to add Diameter redirect:

```
[ //localhost/Radius/Services/dia-redirect ]
    Name = dia-relay
    Description =
    Type = diameter
    Realm = abc.com
    Role = redirect
    Peers/
        Entries 1 to 1 from 1 total entries
        Current filter: <all>

        redirectserver/
            Name = redirectserver
            HostName = 10.77.240.69
            IsVendorSpecific = FALSE
            ApplicationID = 1
            Metric = 2
```

Table 4-21 describes the Diameter Service properties.

Table 4-21   Diameter Service Properties

Property	Description
Name	Required; name of the Diameter server.
Realm	Required; realm of the route. Must be unique for a route table.
Incoming Script	Optional; enabled when role is set to Proxy or Local. When set, must be the name of a known incoming script. Cisco Prime AR runs the IncomingScript before proxying the diameter packet to the remote diameter server.
Outgoing Script	Optional; enabled when role is set to Proxy or Local. When set, must be the name of a known outgoing script. Cisco Prime AR runs the OutgoingScript after it receives the response from the remote Diameter server.
Description	Optional; description of the Diameter server.
Role	Required; specifies the role that the diameter entity will play in resolving messages matching the realm.
	The role can be any one of the following:
	Relay - Application acting as a Relay Agent.
	Redirect - Application acting as a Redirect Agent.
	Proxy - Application acting as a Proxy Agent. When the role is set to Proxy, the IncomingScript and OutgoingScript points are enabled.
	Local - Application processes the requests locally. When the role is set to Local, the AuthenticationService and AccountingService are enabled.
	By default, the Proxy option is selected. However, you can select another option from the drop-down list.
AuthenticationService	Required; used when service is configured to process the diameter requests locally. Set to valid service of type (local/ldap/odbc) to authenticate the user. This field is displayed when you select the role type as 'Local' in the Role field.
AccountingService	Required; used when service is configured to process the accounting requests locally. Set to valid accounting service of type(file/odbc-accounting) to write the accounting records. This field is displayed when you select the role type as 'Local' in the Role field.
Type	Required; specifies the service type.The service type 'Diameter' is automatically displayed in this field.
Peer Definitions tab This tab is displayed when you select the 'Local', 'Relay', or 'Redirect'option in the Role field.	
Name	Required; name of the peer.
Host Name	Required; the hostname or IP address of the peer. The hostname must exist in the client list for the route to be active.
Metric	Required; metric value for the peer entry. The higher the value the lower the preference. The highest value of preference is 0.

Table 4-21   *Diameter Service Properties (continued)*

Property	Description
VendorSpecific	Required; the default is FALSE. If set to FALSE, the application is ordinary application and user is prompted to enter the ApplicationID. If set to TRUE, the application is a VendorSpecific Application. User is prompted to enter VendorSpecificApplicationID and VendorID.
VendorID	Required; specifies the VendorID for the application. Example: DIAMETER 3GPP Cx APPLICATION VendorSpecificApplicationID 16777216 VendorID 10415
VendorSpecificApplicationID	Required; specifies the integer value for the vendor specific application.
ApplicationID	Required; application used in the route. The application Id should be available in /Advanced/Diameter/Applications.

Applications tab

This tab is displayed when you select the 'Proxy' option in the Role field.

Name	Required; name of the application.
Description	The description of the application.
ApplicationID	Required; specifies the unique integer value for the application. It represents the applicationid of the Application used for load balancing the diameter messages.
EnableSticky	Required; default is FALSE. If set to True, the sticky entries for load balancing is enabled and the user is prompted to enter the values for StickySessionKey, StickyCreationCmdList, and StickyDeletionCmdList.
DeMultiplexCCTerminateRequest	Optional; default is FALSE. If set to True, Cisco Prime AR generates and sends multiple Credit Control Update (CCR-U) requests corresponding to an incoming diameter Credit Control Termination (CCR-T) request, while proxying Gy messages between the Gateway GPRS Support Node (GGSN) and Online charging system (OCS). The CCR-U requests are generated based on the number of RGs present in CCR-T message. For more information, see Configuring Cisco Prime AR to Demultiplex the Diameter CCR-T, page 8-26.
MultiplePeersPolicy	Required; must be set to RoundRobin, FailOver, or IMSIRangeBased. Policy used by the Cisco Prime AR server to load balance the peers.

Table 4-21   Diameter Service Properties (continued)

Property	Description
StickySessionKey	Required; used as the sticky key for mapping the sticky sessions. Set the value to a valid AVP in order to use the sticky key for maintaining diameter sessions. This ensures that Cisco Prime AR maps the request to the same server for all the subsequent messages using the sticky key. For example, set StickyAVP "Session-Id".
	When the Cisco Prime AR server receives the CCR-I request, Cisco Prime AR extracts the Session-Id from the request packet, maps the Session to the peer configured in the list, and forwards the request to the chosen peer. Cisco Prime AR chooses the same peer for all the subsequent messages(CCR-Update/CCR-Terminate) with same Session-Id.
StickyCreationCmdList	Required; specifies the command list to create the sticky entries.Specify the list of 'll' separated command code, AVP name, and its value to create the sticky sessions.
	The following is the StickyCreationCmdList format:
	```<commandcode1>::<AVPName1=Value1> || <commandcode2<::<AVPName2=Value2>||<commandcode3>```
	For example, if the sticky session entries need to created based on command code '265'or based on command code '271' with Accounting-Record-Type value as 2, use the format below:
	```Set StickyCreationCmdList "265||271:: Accounting-Record-Type=2"```
StickyDeletionCmdList	Required; specifies the command list to delete the sticky entries.Specify the list of 'll' separated command code, AVP name, and its value to delete the sticky sessions.
	The following is the StickyDeletionCmdList format:
	```<commandcode1>::<AVPName1=Value1> || <commandcode2<::<AVPName2=Value2>||<commandcode3>```
	For example, if the sticky session entries need to deleted based on command code '271' with Accounting-Record-Type value as 4, use the format below:
	```Set StickyDeletionCmdList "271:: Accounting-Record-Type=4"```
Peer Definitions Proxy tab	
Name	Required; name of the peer.
Host Name	Required; hostname or IP address of the peer. The HostName must exist in the client list for the route to be active.
Metric	Required; metric value for this peer entry. The higher the value the lower the preference. The highest value of preference is 0.

Cisco Prime Access Registrar 6.0 User Guide

Table 4-21   Diameter Service Properties (continued)

Property	Description
Weight	Required; default value is 0. Specifies the weight percentage for which the service needs to load balance the peer. **Note** When you set the weight to a value other than 0, the weight should be in multiples of 10 and the sum of the weights configured in the peer list should be equal to 100.
IMSIRanges	Required; used for load balancing. The value is set to comma separated values of IMSI Ranges. For example, set IMSIRanges "112156000000001-112156001000000,112156010000001-112156011000000" **Note** Cisco Prime AR uses the AVP configured in StickyAVP property to check whether the IMSI is in valid range.

M3UA

Cisco Prime AR supports the M3UA service, which is used to fetch MSISDN from IMSI through RADIUS Packets. The M3UA service sends a SendRoutingInfoForLCS(SRIForLCS) request that contains the IMSI information to the remote HLR. The HLR sends the MSISDN in response. To fetch the MSISDN information from IMSI, you need to configure the SIGTRAN-M3UA remote server where Cisco Prime AR is installed, see Configuring M3UA Service for more information.

The M3UA service checks for IMSI environment variable to fetch the MSISDN information. If there is no IMSI environment variable set, then the **User-Name** in the Radius **Access-Request** is used as IMSI to fetch the MSISDN information. The fetched MSISDN is copied to the AuthorizationInfo environment variable where you can write a script to copy the environment variable to any attribute of your choice.

Note   M3UA service supports fetching the MSISDN only through SIGTRAN-M3UA interface.

The following shows an example configuration of M3UA service:

```
[ //localhost/Radius/Services/FetchMSISDN ]
    Name = FetchMSISDN
    Description =
    Type = m3ua
    IncomingScript~ =
    OutgoingScript~ =
    OutageScript~ =
    OutagePolicy~ = RejectAll
    RemoteServers/
```

Table 4-22   M3UA Properties

Property	Description
Type	Required; must set to M3UA service.
IncomingScript	Optional; when set, must be the name of a known incoming script. Cisco Prime AR runs the IncomingScript after it receives the response.

Table 4-22   M3UA Properties (continued)

Property	Description
OutgoingScript	Optional; when set, must be the name of a known outgoing script. Cisco Prime AR runs the OutgoingScript just before it sends the proxy request to the remote server.
OutagePolicy	Required; the default is RejectAll. This property defines how Cisco Prime AR handles requests if all servers listed in the RemoteServers properties are unavailable (that is, all remote RADIUS servers are not available). You must set it to one of the following: AcceptAll, DropPacket, or RejectAll.
OutageScript	Optional; set this property to the name of a script. Cisco Prime AR runs the script when an outage occurs. It allows you to create a script that notifies you when the RADIUS server detects a failure.
RemoteServers	Required; an indexed list from 1 to <n>. Each entry in the list is the name of a RemoteServer of type SIGTRAN-M3UA.

Session Managers

You can use Session Managers to track user sessions. The Session Managers monitor the flow of requests from each NAS and detect the session state. When requests come through to the Session Manager, it creates sessions, allocates resources from appropriate Resource Managers, and frees and deletes sessions when users log out.

The Session Manager enables you to allocate dynamic resources to users for the lifetime of their session. You can define one or more Session Managers and have each one manage the sessions for a particular group or company.

Note   Session record size is limited by the operating system (OS) paging size (8 KB in Solaris and 4 KB in Linux). If a request triggers creation of a session that exceeds the OS paging size, the request will be dropped and the session will not be created.

Note   In this release of Cisco Prime AR, the memory capacity is enhanced to store more than 4 million active sessions by storing the active session records in database server instead of storing it in the main memory. The capacity is dependent on the number of attributes that are being captured for each session.

Note   If the disk partition where Cisco Prime AR stores session backing store data (usually the disk partition where Cisco Prime AR is installed, such as **/opt/CSCOar**) is full, the subsequent packets that try to create sessions will be dropped and no sessions will be created due to lack of disk space.

Session Managers use Resource Managers, which in turn, manage a pool of resources of a particular type. Table 4-23 lists the Session Manager properties.

Cisco Prime AR adds IncomingScript, OutGoingScript, and SessionKey properties. The IncomingScript is run as soon as the session is acquired. The OutGoingScript is run just before the session is written to backing store. The SessionKey property sets the session key value for the Session Manager.

Table 4-23   Session Manager Properties

Property	Description
Name	Required; must be unique in the Session Managers list.
Description	Optional description of the Session Manager.
Type	Set to local or remote. Local is the traditional session manager that maintains sessions in memory and has good performance. The remote session manager operates on a remote ODBC database, and its performance is highly dependent on the performance of the ODBC database.
IncomingScript	Optional; name of script to run when the service starts. This script is run as soon as the session is acquired in Cisco Prime AR.
OutgoingScript	Optional; script to be run just before the session is written to backing store.
SessionTimeOut	The SessionTimeOut property is optional; no value for this property means the session timeout feature is disabled. Used in conjunction with **/Radius/Advanced/SessionPurgeInterval** for the session timeout feature. Enables the session timeout feature for a Session Manager. If the SessionTimeOut property is set to a value under a session manager, all sessions that belong to that session manager will be checked for timeouts at each SessionPurgeInterval. If any sessions have timed out, they will be released, and all resources associated with those sessions are also released. The SessionTimeOut property determines the timeout for a session. If the time difference between the current time and the last update time is greater than this property's value, the session is considered to be stale. The last update time of the session is the time at which the session was created or updated. The SessionTimeOut value is comprised of a number and a units indicator, as in *n units*, where a unit is one of minutes, hours, days, or weeks. The default unit is 'days'.
AllowAccountingStartToCreateSession	Set to TRUE by default; start the session when the Cisco Prime AR server receives an Access Accept or an Accounting-Start. When set to FALSE, start the session when the Cisco Prime AR server receives an Access Accept.
Resource Managers	Ordered list of Resource Managers.

Table 4-23   Session Manager Properties (continued)

Property	Description
PhantomSessionTimeOut	Optional; no value for this property means the phantom session timeout feature is disabled.
	The PhantomSessionTimeOut property is used in conjunction with **/Radius/Advanced/SessionPurgeInterval** to enable the phantom session timeout feature for Session Manager.
	If the PhantomSessionTimeOut property is set to a value under a session manager, all sessions that belong to that session manager will be checked for receipt of an Accounting-Start packet. Sessions that do not receive an Accounting-Start packet from creation until its timeout will be released.
	The PhantomSessionTimeOut value comprises a number and a units indicator, as in *n* units, where a unit is one of minutes, hours, days, or weeks. The default unit is 'days'
MemoryLimitForRadiusProcess	This property is used to avoid crashing of the radius process. The default value is 3500 Megabytes. This property is under **/radius/advanced**. When the radius process uses memory more than the configured limit, further sessions are not created and Cisco Prime AR rejects further incoming requests.

Table 4-23   Session Manager Properties (continued)

Property	Description
MemorySizeCheckInterval	This property is used to avoid crashing of the radius process. This is used in conjunction with **MemoryLimitForRadiusProcess**. The default value is 5 minutes. **MemorySizeCheckInterval** is a hidden parameter in mcd database. To modify the default value, you need to export the mcd database. Typically, a separate thread is created to monitor the radius process memory usage for every 5 minutes.

SessionKey	SessionKey property is used to set the sessionkey value for the Session Manager.
	
	The SessionManager checks whether the environmental variable **Session-Key** is set or not. If the environmental variable is set, the server uses it as the sessionkey. If environmental variable **Session-Key** is not set then SessionManager gets the value configured in the SessionKey property under SessionManager.
	
	SessionKey can be a combination of attributes separated by colon. The values for those attributes are obtained from the RequestDictionary. If any one of the attribute that is configured for the sessionkey is not present in the RequestDictionary, Cisco Prime AR will drop the request.
	
	However, if **Session-Key** is not set, SessionManager uses NAS-Identifier and NAS-Port to create the sessionkey. An example configuration,
	
	`--> set SessionKey "User-Name:NAS-Port"`
	The following shows the sample configuration of sessionkey for Session Manager:
	
	`[ //localhost/Radius/SessionManagers/session-mgr-1 ]`
	`Name = session-mgr-1`
	`Description =`
	`IncomingScript =`
	`OutgoingScript =`
	`AllowAccountingStartToCreateSession = TRUE`
	`SessionTimeOut =`
	`PhantomSessionTimeOut =`
	`SessionKey =`
	`ResourceManagers/`

You can manage sessions with the two **aregcmd** session management commands: **query-sessions** and **release-sessions**. For more information about these two commands, see the query-sessions, page 2-9 and the release-sessions, page 2-9.

This section contains the following topics:

- Session Creation
- Session Notes
- Soft Group Session Limit
- Session Correlation Based on User-Defined Attributes

Session Creation

Cisco Prime AR Sessions can be created by two types of RADIUS packets:

- Access-Requests
- Accounting-Requests with an **Acct-Status-Type** attribute with a value of **Start**.

This allows Cisco Prime AR to monitor Sessions even when it is not allocating resources. For example, when Cisco Prime AR is being used as an "Accounting-Only" server (only receiving Accounting requests), it can create a Session for each Accounting "Start" packet it successfully processes. The corresponding Accounting "Stop" request will clean up the Session. Note, if a Session already exists for that NAS/NAS-Port/User (created by an Access-Request), Cisco Prime AR will not create a new one.

When you do not want Cisco Prime AR to create Sessions for Accounting "Start" requests, simply set the **AllowAccountingStartToCreateSession** property on the SessionManager to FALSE.

Session Notes

Session Notes are named text messages attached to a Session and are stored with the Session data, including resources allocated for a specific user session. This data, including Session Notes, can be retrieved and viewed using the **aregcmd** command **query-sessions**.

--> **query-sessions /Radius/SessionManagers/session-mgr-2**

```
sessions for /Radius/SessionManagers/session-mgr-2:
S257 NAS: localhost, NAS-Port:1, User-Name: user1, Time: 00:00:08,
   IPX 0x1, GSL 1, USL 1, NOTES: "Date" "Today is 12/14/98.", "Requested
   IP Address" "1.2.3.4", "Framed-IP-Address" "11.21.31.4"
```

Session Notes can be created by Scripts using the Environment dictionary passed into each or by the Cisco Prime AR server. When more than one Session Note is added, the **Session-Notes** entry should be a comma-separated list of entry names.

Performing a TCL Script

To perform a TCL script:

Step 1 The Script should create an Environment dictionary entry using the Session Note name as the entry name, and the Session Note text as the entry value. For example:

```
$environ put "Date" "Today is 12/15/08"
$environ put "Request IP Address" "1.2.3.4"
```

Step 2 The Script should create or set an Environment dictionary entry with the name **Session-Notes** with a value that contains the name of the entries created. For example:

```
$environ put "Session-Notes" "Date, Requested_IP_Address"
```

Performing a REX Script

To perform a REX script:

Step 1 The Script should create an Environment dictionary entry using the Session Note name as the entry name, and the Session Note text as the entry value. For example:

```
pEnviron-->put(pEnviron, Date, "Today is 12/15/08.");
pEnviron-->put(pEnviron, Request_IP_Address, "1.2.3.4");
```

Step 2   The Script should create/set an Environment dictionary entry with the name **Session-Notes** with a value that contains the name of the first entry created. For example:

```
pEnviron-->put(pEnviron, "Session-Notes", "Date, Requested_IP_Address");
```

> ✎ **Note**   Scripts creating Session Notes must be executed before the Session Management step takes place while processing a packet.

Cisco Prime AR will automatically create a Session Note if a packet is passed to a SessionManager and it already contains a **Framed-IP-Address** attribute in the packet's Response dictionary. This IP address could come from a Profile, RemoteServer response, or from a previously executed script. For example, a Session output containing Session Notes when using the **aregcmd** command **query-session** would be as follows:

```
sessions for /Radius/SessionManagers/session-mgr-2:
  S257 NAS: localhost, NAS-Port:1, User-Name: user1, Time: 00:00:08,
  IPX 0x1, GSL 1, USL 1, NOTES: "Date" "Today is 12/14/08.", "Requested
  IP Address" "1.2.3.4", "Framed-IP-Address" "11.21.31.4"
```

Session Notes are also copied into the Environment dictionary after Session Management. The **Session-Notes** Environment dictionary entry will contain the names of all the Environment dictionary entries containing Session Notes.

In Cisco Prime AR, a major command is introduced—count-sessions. The **count-session lr all** command helps to count the total sessions in Cisco Prime AR. The options are similar to the query-session command options. The query-session command displays cached attributes in addition to session details.

Soft Group Session Limit

Two new environment variables, **Group-Session-Limit** and **Current-Group-Count** (see rex.h), are set if the group session limit resource is allocated for a packet. These variables allow a script to see how close the group is to its session limit; one way to use this information is to implement a script-based soft limit. For example, you could use the Class attribute to mark sessions that have exceeded a soft limit of 80% -- as hard coded in the script (in a Tcl script called from /Radius/OutgoingScript):

```
set softlimit [ expr 0.8 * [ $environ get Group-Session-Limit ] ]
if { [ $environ get Current-Group-Count ] < $softlimit } {
$response put Class 0
} else {
$response put Class 1
}
```

> ✎ **Note**   The soft limit itself is hard coded in the script; soft limits are not directly supported in the server. The action to be taken when the soft limit is exceeded (for example, Class = 1, and then the accounting software branches on the value of Class) is also the responsibility of the script and/or external software.

Session Correlation Based on User-Defined Attributes

All the session objects are maintained in one dictionary keyed by a string. You can define the keying material to the session dictionary through a newly introduced environment variable, **Session-Key**.

If the **Session-Key** is presented at the time of session manager process, it will be used as the key to the session object for this session. The **Session-Key** is of type string. By default, the **Session-Key** is not set. Its value should come from attributes in the incoming packet and is typically set by scripts. For example, CLID can be used to set the value of **Session-Key**.

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

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

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

Resource Managers

Resource Managers allow you to allocate dynamic resources to user sessions. The following lists the different types of Resource Managers.

- **IP-Dynamic**—manages a pool of IP addresses that allows you to dynamically allocate IP addresses from a pool of addresses

- **IP-Per-NAS-Port**—allows you to associate ports to specific IP addresses, and thus ensure each NAS port always gets the same IP address

- **IPX-Dynamic**—manages a pool of IPX network addresses

- **Subnet-Dynamic**—manages a pool of subnet addresses

- **Group-Session-Limit**—manages concurrent sessions for a group of users; that is, it keeps track of how many sessions are active and denies new sessions after the configured limit has been reached

- **User-Session-Limit**—manages per-user concurrent sessions; that is, it keeps track of how many sessions each user has and denies the user a new session after the configured limit has been reached

- **Home-Agent**—manages a pool of on-demand IP addresses

- **USR-VPN**—manages Virtual Private Networks (VPNs) that use USR NAS Clients.

- **Home-Agent-IPv6**—manages a pool of on-demand IPv6 addresses

- **Remote-IP-Dynamic**—manages a pool of IP addresses that allows you to dynamically allocate IP addresses from a pool of addresses. It internally works with a remote ODBC database.

- **Remote-User-Session-Limit**—manages per-user concurrent sessions; that is, it keeps track of how many sessions each user has and denies the user a new session after the configured limit has been reached. It internally works with a remote ODBC database.

- **Remote-Group-Session-Limit**—manages concurrent sessions for a group of users; that is, it keeps track of how many sessions are active and denies new sessions after the configured limit has been reached. It internally works with a remote ODBC database.

Each Resource Manager is responsible for examining the request and deciding whether to allocate a resource for the user, do nothing, or cause Cisco Prime AR to reject the request.

Table 4-24 lists the Resource Manager properties.

Table 4-24   ***Resource Manager Properties***

Property	Description
Name	Required; must be unique in the Resource Managers list.
Description	Optional; description of the Resource Manager.
Type	Required; must be either **Dynamic-DNS**, **IP-Dynamic**, **IP-Per-NAS-Port**, **IPX-Dynamic**, **Session Cache, Subnet-Dynamic, Group-Session-Limit**, **Home-Agent**, **User-Session-Limit**, **USR-VPN, Home-Agent-IPv6, Remote-IP-Dynamic, Remote-User-Session-Limit, Remote-Group-Session-Limit** or **Remote-Session-Cache**.

Types of Resource Managers

A number of different types of Resource Managers exist that allow you to manage IP addresses dynamically or statically, limit sessions on a per group or per user basis, or manage a Virtual Private Network. See Appendix A, "Cisco Prime Access Registrar Tcl, REX and Java Dictionaries," for information on how to override these individual Resource Managers.

Note   Resource Manager supports the following remote type session managers: remote-ip-dynamic, remote-session-cache, home-agent, remote-user-session-limit, home-agent-ipv6 and remote-group-session-limit.

This section contains the following topics:

- Gateway Subobject
- Group-Session-Limit
- Home-Agent
- Home-Agent-IPv6
- IP-Dynamic
- IP-Per-NAS-Port
- IPX-Dynamic
- Session-Cache
- Subnet-Dynamic
- User-Session-Limit
- USR-VPN
- Dynamic-DNS
- Remote-IP-Dynamic
- Remote-User-Session-Limit
- Remote-Group-Session-Limit
- Remote-Session-Cache

Gateway Subobject

The **Gateway** subobject includes a list of names of the Frame Relay Gateways for which to encrypt the session key.

If you use this Resource Manager, supply the information listed in Table 4-25.

Table 4-25   Gateway Properties

Property	Description
Name	Required; must be unique in the Gateways list.
Description	Optional description of the gateway.
IPAddress	Required; IP address of the gateway.
SharedSecret	Required; must match the shared secret of the gateway.
TunnelRefresh	Optional; if specified it is the number of seconds the tunnel stays active before a secure "keepalive" is exchanged between the tunnel peers in order to maintain the tunnel open.
LocationID	Optional; if specified it is a string indicating the physical location of the gateway.

Group-Session-Limit

Group-Session-Limit allows you to manage concurrent sessions for a group of users; that is, it keeps track of how many sessions are active and denies new sessions after the configured limit has been reached.

When you use this Resource Manager, you must set the GroupSessionLimit property to the maximum number of concurrent sessions for all users.

Home-Agent

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

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

Detailed configuration information for the Home-Agent resource manager is found in Chapter 19, "Wireless Support." When you use this Resource Manager, you must set the Home-Agent-IPAddresses property to a single IP address or a range of IP addresses.

Home-Agent-IPv6

Home-Agent-Ipv6 is a new resource manager used to configure IPv6 address.

IP-Dynamic

IP-Dynamic allows you to manage a pool of IP addresses from which you dynamically allocate IP addresses.

When you use the IP-Dynamic Resource Manager, provide values for the properties listed in Table 4-26.

Table 4-26   IP-Dynamic Properties

Property	Description
NetMask	Required; must be set to a valid net mask.
IPAddresses	Required; must be a list of IP address ranges.
AllowOverlappedIPAddresses	When set to TRUE, this property supports overlapping IP addresses between session managers for VPN users. Default value is FALSE.
ReuseIPForSameSessionKeyAndUser	When set to FALSE, this property does not reuse IP address resources for a session. Default value is TRUE.

IP-Per-NAS-Port

IP-Per-NAS-Port allows you to associate specific IP addresses with specific NAS ports and thus ensures each NAS port always gets the same IP address.

When you use this Resource Manager, provide values for the properties listed in Table 4-27.

Note   You must have the same number of IP addresses and ports.

Table 4-27   IP-Per-NAS-Port Properties

Property	Description
NetMask	Required; if used, must be set to a valid net mask.
NAS	Required; must be the name of a known Client.This value must be the same as the NAS-Identifier attribute in the Access-Request packet.
IPAddresses	Required; must be a list of IP address ranges.
NASPorts	Required list of NAS ports.

IPX-Dynamic

An IPX-Dynamic Resource Manager allows you to dynamically manage a pool of IPX networks. When you use the IPX-Dynamic Resource Manager, you must set the Networks property to a valid set of numbers which correspond to your networks.

Note   You cannot use IPX network number 0x0. If you attempt to configure a Resource Manager with an IPX network number of 0x0, validation will fail.

Session-Cache

The **session-cache** Resource Manager supports the Identity Cache feature. You use session-cache Resource Managers to define the RADIUS attributes to store in cache. Set the QueryKey property to the XML attribute you want to key on such as XML-Address-format-IPv4 and list all attributes to be cached in the AttributesToBeCached subdirectory. Use the QueryMappings subdirectory to map XML attributes to RADIUS attributes.

Table 4-28   Session-Cache Resource Manager Properties

Property	Description
QueryKey	Required; set the QueryKey to the a RADIUS attribute you want to key on, such as Framed-IP-Address.
	A change made in Cisco Prime AR requires that this attribute not be an XML attribute, even if this session-cache resource manager is being used for an XML query.
	Note Any existing session-cache resource managers using an XML attribute for the Query Key must be changed to a RADIUS attribute that this XML attribute is mapped to under QueryMappings.
PendingRemovalDelay	Required; length of time information remains in the cache after the session ends (defaults to 10 seconds)
AttributesToBeCached	Required; use this subdirectory to provide a list of RADIUS attributes you want to store in cache
QueryMappings	Required; list of attribute pairs, mapping the XML attributes on the left-hand side to the RADIUS attribute on the right-hand side.

Note   Session record size is limited by the operating system (OS) paging size (8 KB in Solaris and 4 KB in Linux). If a request triggers creation of a session that exceeds the OS paging size, the request will be dropped and the session will not be created.

If the disk partition where Cisco Prime AR stores session backing store data (usually the disk partition where Cisco Prime AR is installed, such as **/opt/CSCOar**) is full, the subsequent packets that try to create sessions will be dropped and no sessions will be created due to lack of disk space.

Subnet-Dynamic

The **subnet-dynamic** Resource Manager supports the On Demand Address Pool feature. You use subnet-dynamic resource managers to provide pools of subnet addresses. Following is an example of the configuration of a subnet dynamic resource manager:

```
/Radius/ResourceManagers/newResourceMgr
Name = newResourceMgr
Description =
Type = subnet-dynamic
Subnet-Mask = 255.255.255.0
SubnetAddresses/
    10.1.0.0-10.1.10.0
    11.1.0.0-11.1.10.0
```

When you use the subnet-dynamic Resource Manager, provide values for the properties listed in Table 4-29.

Table 4-29   Subnet-Dynamic Properties

Property	Description
Type	Required
Subnet mask	Required; must be set to the size of the managed subnets
SubnetAddresses	Required; must be a valid range of IP addresses

User-Session-Limit

User-Session-Limit allows you to manage per-user concurrent sessions; that is, it keeps track of how many sessions each user has and denies the user a new session after the configured limit has been reached.

When you use the user-session-limit Resource Manager, set the user-session-limit property to the maximum number of concurrent sessions for a particular user.

USR-VPN

USR-VPN allows you to set up a Virtual Private Network (VPN) using a US Robotics NAS.

When you use this Resource Manager, provide values for the properties listed in Table 4-30.

Table 4-30   USR-VPN Properties

Property	Description
Identifier	Required; must be set to the VPN ID the USR NAS will use to identify a VPN.
Neighbor	Optional; if set, should be the IP address of the next hop router for the VPN.
FramedRouting	Optional; if set, should be **RIP V2 Off** or **RIP V2 On** if the USR NAS is to run RIP Version 2 for the user.
Gateways	Required to set up a tunnel between the NAS and the Gateways.

Dynamic-DNS

Cisco Prime AR supports the Dynamic DNS protocol providing the ability to update DNS servers.

When you use this Resource Manager, provide values for the properties listed in Table 4-31.

Table 4-31   DYNAMIC-DNS Properties

Fields	Description
Max DNS TTLS	Set the maximum TTL of the DNS record.
DNS Host bytes	Set the number of bytes to be used to construct the reverse zone entry.

Table 4-31   DYNAMIC-DNS Properties (continued)

Fields	Description
Forward Zone Name	Set the name of the forward zone. For a given Resource Manager you must decide which forward zone you will be updating for sessions the resource manager will manage.
Reverse Zone Name	Set the name of the reverse zone.
Forward Zone Server	Set the Server IP of the forward zone
Reverse Zone Server	Set the Server IP of the reverse zone
Forward Zone TSIG KeyS	Server-wide security key to process all forward zone dynamic DNS updates. This is used if a ForwardZoneTSIGKey was not specified on the Resource Manager.
Reverse Zone TSIG Keys	Server-wide security key to process all reverse zone dynamic DNS updates. This is used if a ReverseZoneTSIGKey was not specified on the Resource Manager

Remote-IP-Dynamic

The configuration is same as IP-Dynamic but internally it works with a remote ODBC database.

Remote-User-Session-Limit

The configuration is same as User-Session-Limit but internally it works with a remote ODBC database.

Remote-Group-Session-Limit

The configuration is same as Group-Session-Limit but internally it works with a remote ODBC database.

Remote-Session-Cache

The configuration is same as Session-Cache but it should be used with session manager of type remote.

Profiles

You use Profiles to group RADIUS attributes that belong together, such as attributes that are appropriate for a particular class of PPP or Telnet user. You can reference profiles by name from either the **UserGroup** or the **User** properties. Thus, if the specifications of a particular profile change, you can make the change in a single place and have it propagated throughout your user community.

Although you can use UserGroups or Profiles in a similar manner, choosing whether to use one rather than the other depends on your site. When you require some choice in determining how to authorize or authenticate a user session, then creating specific profiles, and creating a group that uses a script to choose among them is more flexible.

In such a situation, you might create a default group, and then write a script that selects the appropriate profile based on the specific request. The benefit to this technique is each user can have a single entry, and use the appropriate profile depending on the way they log in.

Table 4-32 lists the **Profile** properties.

Table 4-32   *Profile Properties*

Property	Description
Name	Required; must be unique in the Profiles list.
Description	Optional; description of the profile.
Attributes	Profiles include specific RADIUS attributes that Cisco Prime AR returns in the Access-Accept response.

Attributes

Attributes are specific RADIUS components of requests and responses defined in the Request and Response Attribute dictionaries. Use the **aregcmd** command **set** to assign values to attributes.

For a complete list of the attributes, see Appendix C, "RADIUS Attributes." When setting a value for a STRING-type attribute such as Connect-Info (which starts with an integer), you must use the hexadecimal representation of the integer. For example, to set the attribute Connect-Info to a value of 7:7, use a set command like the following:

    set Connect-Info 37:3A:37

Translations

Translations add new attributes to a packet or change an existing attribute from one value to another. The **Translations** subdirectory lists all definitions of **Translations** the RADIUS server can apply to certain packets.

Under the **/Radius/Translations** directory, any translation to insert, substitute, or translate attributes can be added. The following is a sample configuration under the **/Radius/Translations** directory:

```
cd /Radius/Translations
Add T1
cd T1
Set DeleAttrs Session-Timeout,Called-Station-Id
cd Attributes
Set Calling-Station-Id 18009998888
```

DeleAttrs is the set of attributes to be deleted from the packet. Each attribute is comma separated and no spaces are allowed between attributes. All attribute value pairs under the attributes subdirectory are the attributes and values that are going to be added or translated to the packet.

Under the **/Radius/Translations/T1/Attributes** directory, inserted or translated attribute value pairs can be set. These attribute value pairs are either added to the packet or replaced with the new value.

If a translation applies to an Access-Request packet, by referencing the definition of that translation, the Cisco Prime AR server modifies the Request dictionary and inserts, filters and substitutes the attributes accordingly. You can set many translations for one packet and the Cisco Prime AR server applies these translations sequentially.

Note   Later translations can overwrite previous translations.

Table 4-33 lists the Translation properties.

Table 4-33   Translations Properties

Property	Description
Name	Required; must be unique in the Translations list.
Description	Optional; description of the Translation
DeleteAttrs	Optional; lists attributes to be filtered out

TranslationGroups

You can add translation groups for different user groups under **TranslationGroups**. All Translations under the Translations subdirectory are applied to those packets that fall into the groups. The groups are integrated with the Cisco Prime AR Rule engine.

The Cisco Prime AR Administrator can use any RADIUS attribute to determine the **Translation Group**. The incoming and outgoing translation group can be different translation groups. For example, you can set one translation group for incoming translations and one for outgoing translations.

Under the **/Radius/TranslationGroups** directory, translations can be grouped and applied to certain sets of packets, which are referred to in a rule. The following is a sample configuration under the **/Radius/TranslationGroups** directory:

```
cd /Radius/TranslationGroups
Add CiscoIncoming
cd CiscoIncoming
cd Translations
Set 1 T1
```

The translation group is referenced through the Cisco Prime AR Policy Engine in the **/Radius/Rules/***<RuleName>***/Attributes** directory. **Incoming-Translation-Groups** are set to a translation group (for example `CiscoIncoming`) and **Outgoing-Translation-Groups** to another translation group (for example `CiscoOutgoing`). Table 4-34 lists the Translation Group properties.

Table 4-34   TranslationGroups Properties

Property	Description
Name	Required; must be unique in the Translations list.
Description	Optional; description of the Translation Group
Translations	Lists of translation

Remote Servers

You can use the **RemoteServers** object to specify the properties of the remote servers to which Services proxy requests. **RemoteServers** are referenced by name from the **RemoteServers** list in either the **radius**, **ldap** or **tacacs-udp** Services.

Table 4-35 lists the common **RemoteServers** properties.

Table 4-35   *Common RemoteServer Properties*

Property	Description
Name	Required; must be unique in the RemoteServers list.
Description	Optional; description of the remote server.
Protocol	Required; specifies the remote server protocol which can be **radius**, **ldap**, or **tacacs-udp**.
IPAddress	Required; this property specifies where to send the proxy request. It is the address of the remote server. You must set it to a valid IP address.
	The IP address format is enhanced to support IPv6 apart from IPv4 only for the RADIUS type remote server.
Port	Required; the port to which Cisco Prime AR sends proxy requests. You must specify a number greater than zero. If there is no default port number, you must supply the correct port number for your remote server.
	If you set a port to zero, Cisco Prime AR sets the port to the default value for the type of remote server being configured. For example, the following remote servers have these default port values:
	dynamic-dns—53
	radius—1645
	ldap—389
	accounting—1646
ReactivateTimerInterval	Required; the amount of time (in milliseconds) to wait before retrying a remote server that was offline. You must specify a number greater than zero. The default is 300,000 (5 minutes).

Types of Protocols

The Remote Server protocol you specify determines what additional information you must provide. The following are the protocols available in Cisco Prime AR with their required and optional fields.

Cisco Prime AR provides the following RemoteServer protocol types:

- Domain Authentication
- Dynamic DNS
- LDAP
- Map-Gateway
- Sigtran
- ODBC
- ODBC-Accounting
- OCI
- OCI-Accounting
- Prepaid-CRB

- Prepaid-IS835C
- RADIUS
- SIGTRAN-M3UA
- Rules

Domain Authentication

The domain-auth Remote Server is used with the Windows Domain Authentication feature. Cisco Prime AR supports the Windows Domain Controller/Active Directory (WDC/AD) and enables you to authenticate users present in a WDC/AD using the CiscoSecure Remote Agent (CSRA).

Note   To get the CiscoSecure Remote Agent software package, please send an email to ar-tme@cisco.com.

During authentication, the user credentials are sent to the CSRA, which authenticates the credentials with the WDC/AD. The user optionally can specify the domain name along with their UserID when they log in. If the domain is not specified, authentication is first performed with the local WDC/AD (default domain as specified in the remote server configuration), then with all the other trusted domain controllers, one by one until the user is found in any of the trusted WDC/ADs.

This *failover* to other domains is taken care by the local (default) WDC/AD. The local WDC/AD maintains a list of trusted domains and when the user is not found in the local AD, the WDC queries the trusted WDC/ADs, to see if any one those had the user in it. If any of the WDC/ADs has the user, those credentials would be used to authenticate the user.

The WDC/AD authentication stops at the first *hit* and does not check other domains even if the user credentials do not match (resulting in an authentication failure). When a domain is specified, authentication is performed only on that domain. This domain should be either the local WDC/AD or one of the trusted WDC/ADs.

A 128-bit Blowfish (variant) encryption algorithm secures the communication between the Cisco Prime AR and CSRA. The session key for this encryption is negotiated when the connection is established.

The following is the default configuration of a domain-auth Remote Server.

```
[ //localhost/Radius/RemoteServers/domain-auth ]
    Name = newone
    Description =
    Protocol = domain-auth
    HostName =
    Port = 2004
    ReactivateTimerInterval = 300000
    DefaultDomain =
    Timeout = 15
    AgentConnections = 15
    DefaultUserGroup =
    GroupMaps/
```

Table 4-36 lists and defines the domain-auth RemoteServer properties.

Table 4-36   Domain Authentication RemoteServer Properties

Property	Description
HostName	Required; hostname or IP address of the remote server.
Port	Required; port used for communication with WDC/AD; defaults to 2004.

Table 4-36   Domain Authentication RemoteServer Properties (continued)

Property	Description
ReactivateTimerInterval	Required; default is 300,000 milliseconds. Specifies the length of time to wait before attempting to reconnect if a thread is not connected to a data source.
DefaultDomain	Species the default domain for authentication if the user does not include a domain during log in. Otherwise, authentication is performed on the local domain.
Timeout	Required; defaults to 15.
AgentConnections	Required; default is 15. Represents the total number of connections Cisco Prime AR can open with the CSRA.
DefaultUserGroup	User group to be used when no mapping is found in the list of maps in the GroupMap property or when there is no hit in the groups listed in GroupMaps. The DefaultUserGroup is used to authorize users that are authenticated by this domain-auth RemoteServer.
GroupMaps	A list of groups to which the user belongs in the WDC/AD mapped to an internal group in the Cisco Prime AR server. Entries are of the form: 1. "InternalGroup1 = ExternalGroup1, ExternalGroup2, ..." 2. "InternalGroup2 = ExternalGroup3, ExternalGroup4, ..." To configure group mappings, use the following syntax: **set 1 "Group1 = ExternalGroup1,ExternalGroup2, ExternalGroup3"**

Users can optionally be authorized using WDC/AD using a list of groups the user belongs to in WDC/AD. This list of groups is mapped to an internal group in the Cisco Prime AR server using the GroupMaps property. An optional default group can also be configured using the DefaultUserGroup property.

When a hit is made, the corresponding group is taken, even if there might be a better match further down the list. For example, if the user is part of groups A, B, C, and D, and if a map for Groups A, B, and C is listed before a map for Groups A, B, C, and D, the map for Groups A, B, and C will be taken. This requires the administrator to configure more specific mapping before the general mapping.

The list of groups from the WDC/AD is copied to a new environment variable named Windows-Domain-Groups to permit mapping to a more appropriate group at the next relevant scripting point.

Dynamic DNS

The **dynamic-dns** RemoteServer is used with the Dynamic DNS feature. The following is the default configuration of a dynamic-dns RemoteServer.

```
[ //localhost/Radius/RemoteServers/ddns ]
    Name = ddns
    Description =
    Protocol = dynamic-dns
    IPAddress =
    Port = 53
    MaxTries = 3
    InitialTimeout = 2000
```

```
MaxDNSRenamingRetries = 3
TrimHostName = TRUE
ForwardZoneTSIGKey =
ReverseZoneTSIGKey =
```

Table 4-37 lists and defines the dynamic-dns RemoteServer properties.

Table 4-37   Dynamic-DNS RemoteServer Properties

Property	Description
IPAddress	The IPAddress address of the DNS server
Port	Port 53 is the port that most DNS servers will use as a default
MaxTries	Number of times the server tries to send dynamic updates to a DNS server
InitialTimeout	Time, in milliseconds, that the server waits for a response before retrying a dynamic DNS request
MaxRenamingRetries	Number of times that the dynamic-dns resource managers can try to add a host in DNS even if it detects that the host's name is already present. This controls the number of times Cisco Prime AR tries to modify a host's name to resolve a conflict on each failed update.
TrimHostName	Controls whether Cisco Prime AR trims the hostname string to the first period character (used to update dynamic DNS update records and to return the hostname option to clients). If this attribute is enabled, the hostname is truncated before the period. If disabled, the server retains the period characters in the hostname.
ForwardZoneTSIGKey	Server-wide security key to process all forward zone dynamic DNS updates. This is used if a ForwardZoneTSIGKey was not specified on the Resource Manager.
ForwardZoneTSIGKey	Server-wide security key to process all forward zone dynamic DNS updates. This is used if a ForwardZoneTSIGKey was not specified on the Resource Manager.
ReverseZoneTSIGKey	Server-wide security key to process all reverse zone dynamic DNS updates. This is used if a ReverseZoneTSIGKey was not specified on the Resource Manager.

LDAP

ldap specifies an LDAP server. When you specify the **ldap** protocol, provide the information listed in Table 4-38.

For any LDAP remote service, the server might perform the environment mappings at any time. This means that if the service is set to either authentication and authorization, authentication-only, or authorization-only, environment mappings will take place. RADIUS mappings will take place only if the service is set to perform authorization. Checkitem mappings will take place only if the service is set to perform authentication. Previously environment mappings only occurred when the service was set for both authentication and authorization. RADIUS mappings, environment mappings, and checkitem mappings will not take place, if bind-based authentication is enabled.

Table 4-38   ldap RemoteServer Properties

Property	Description
Port	Required; defaults to port 389.
Timeout	Required; the default is 15. The timeout property indicates how many seconds the RADIUS server will wait for a response from the LDAP server. **Note** Use InitialTimeout from above as a template, except this is timeout is specified in seconds.
HostName	Required; the LDAP server's hostname or IP address.
BindName	Optional; the distinguished name (dn) to use when establishing a connection between the LDAP and RADIUS servers.
BindPassword	Optional; the password associated with the **BindName**.
SearchPath (Overridden by Search-Path environment variable)	Required; the path that indicates where in the LDAP database to start the search for user information.
Filter	Required; this specifies the search filter Cisco Prime AR uses when querying the LDAP server for user information. When you configure this property, use the notation "%s" to indicate where the user ID should be inserted. For example, a typical value for this property is "(uid=%s)," which means that when querying for information about user joe, use the filter uid=joe.
UserPasswordAttribute	Required; this specifies which LDAP field the RADIUS server should check for the user's password.
LimitOutstandingRequests	Required; the default is FALSE. Cisco Prime AR uses this property in conjunction with the **MaxOutstandingRequests** property to tune the RADIUS server's use of the LDAP server. When you set this property to TRUE, the number of outstanding requests for this RemoteServer is limited to the value you specified in **MaxOutstandingRequests**. When the number of requests exceeds this number, Cisco Prime AR queues the remaining requests, and sends them as soon as the number of outstanding requests drops to this number.
MaxOutstandingRequests	Required when you have set the **LimitOutstandingRequests** to TRUE. The number you specify, which must be greater than zero, determines the maximum number of outstanding requests allowed for this remote server.

Table 4-38   ldap RemoteServer Properties (continued)

Property	Description
MaxReferrals	Required; must be a number equal to or greater than zero. This property indicates how many referrals are allowed when looking up user information. When you set this property to zero, no referrals are allowed.
	Cisco Prime AR manages referrals by allowing the RADIUS server's administrator to indicate an LDAP "referral attribute," which might or might not appear in the user information returned from an LDAP query. When this information is returned from a query, Cisco Prime AR assumes it is a referral and initiates another query based on the referral. Referrals can also contain referrals.
	Note This is an LDAP v2 referral property.
ReferralAttribute	Required when you have specified a **MaxReferrals** value. This property specifies which LDAP attribute, returned from an LDAP search, to check for referral information.
	Note This is an LDAP v2 referral property.
ReferralFilter	Required when you have specified a **MaxReferral** value. This is the filter Cisco Prime AR uses when processing referrals. When checking referrals, the information Cisco Prime AR finds in the referral itself is considered to be the search path and this property provides the filter. The syntax is the same as that of the **Filter** property.
	Note This is an LDAP v2 referral property.
PasswordEncryptionStyle	The default is **None**. You can also specify **crypt, dynamic, SHA-1, and SSHA-1**.
EscapeSpecialCharInUserName	FALSE by default
DNSLookupAndLDAPRebindInterval	Specifies the timeout period after which the Cisco Prime AR server will attempt to resolve the LDAP hostname to IP address (DNS resolution); 0 by default
DataSourceConnections	Specifies the number of concurrent connections to the LDAP server. The default value is 8.
SearchScope	Specifies how deep to search within a search path; default is *SubTree* which indicates a search of the base object and the entire subtree of which the base object distinguished name is the highest object.
	Base indicates a search of the base object only.
	OneLevel indicates a search of objects immediately subordinate to the base object, but does not include the base object.

Table 4-38   ldap RemoteServer Properties (continued)

Property	Description
LDAPToRadiusMappings	Optional; a list of name/value pairs in which the name is the name of the **ldap** attribute to retrieve from the user record, and the value is the name of the RADIUS attribute to set to the value of the **ldap** attribute retrieved.
	For example, when the **LDAPToRadiusMappings** has the entry: **FramedIPAddress = Framed-IP-Address**, the RemoteServer retrieves the **FramedIPAddress** attribute from the **ldap** user entry for the specified user, uses the value returned, and sets the Response variable **Framed-IP-Address** to that value.
LDAPToEnvironmentMappings	Optional; a list of name/value pairs in which the name is the name of the **ldap** attribute to retrieve from the user record, and the value is the name of the Environment variable to set to the value of the **ldap** attribute retrieved.
	For example, when the **LDAPToEnvironmentMappings** has the entry: **group = User-Group**, the RemoteServer retrieves the **group** attribute from the **ldap** user entry for the specified user, uses the value returned, and sets the Environment variable **User-Group** to that value.
LDAPToCheckItemMappings	Optional; a list of LDAP *attribute/value* pairs which must be present in the RADIUS access request and must match, both name and value, for the check to pass.
	For example, when the **LDAPToCheckItemMappings** has the entry: **group = User-Group**, the Access Request must contain the attribute **group**, and it must be set to **User-Group**.
UseSSL	A boolean field indicating whether you want Cisco Prime AR to use SSL (Secure Socket Layer) when communicating with this RemoteServer. When you set it to TRUE, be sure to specify the **CertificateDBPath** field in the **Advanced** section, and be sure the port you specified for this RemoteServer is the SSL port used by the LDAP server.
UseBinaryPasswordComparison	A boolean field that enables binary password comparison for authentication. This property when set to TRUE, enables binary password comparison. By default, this property is set to FALSE.
UseBindBasedAuthentication	A boolean field that enables bind-based authentication with LDAP server. This property when set to TRUE, enables bind-based authentication. By default, this property is set to FALSE. When set to FALSE, it uses existing legacy authentication method.

Map-Gateway

The following is the default configuration of a map gateway RemoteServer.

```
[ //localhost/Radius/RemoteServers/map-gateway ]
    Name = map-gateway
    Description =
    Protocol = map-gateway
    IPAddress =
    Port = 0
```

```
                  ReactivateTimerInterval = 300000
                  SharedSecret =
                  MaxTries = 3
                  InitialTimeout = 2000
```

Sigtran

The following is the default configuration of a Sigtran RemoteServer.

```
[ //localhost/Radius/RemoteServers/rs ]
    Name = rs
    Description =
    Protocol = sigtran
    HostName =
    LocalSubSystemNumber =
    CgPAGlobalTitleAddress =
    SetOPCInCgPA =
    GlobalTitleTranslationScript~ =
    SUAConfigurationFilename =
    ReactivateTimerInterval =
    Timeout = 5000
    LimitOutstandingRequests = FALSE
    MaxOutstandingRequests = 0
```

✎

Note   The RPM packages such as lksctp-tools-1.0.10-1, lksctp-tools-doc-1.0.10-1 and lksctp-tools-devel-1.0.10-1 should be installed in Linux 5.3 before configuring sigtran remote server which eventually adds the sctp libs (libsctp.so.1.0.10).

The following files can be downloaded from http://lksctp.sourceforge.net/

- lksctp-tools-1.0.10-1.i386.rpm
- lksctp-tools-devel-1.0.10-1.i386.rpm
- lksctp-tools-doc-1.0.10-1.i386.rpm

Cisco Prime AR supports only:

- one object of Remoteserver with protocol type "sigtran"
- MAP version 3 (3GPP TS 29.002 V6.4.0 (2003-12)) and ITU Q.773 TCAP

Only one Quintets is fetched from HLR. The ITU TCAP continue message is not supported.

Table 4-39 lists and defines the Sigtran RemoteServer properties.

Table 4-39   Sigtran RemoteServer Properties

Property	Description
HostName	Required; represents the IP address of remote Signalling Gateway specified in the SUAConfiguration file.
LocalSubSystemNumber	Required; the default value for this property is 0. This represents the subsystem number used by SUA user.
CgPAGlobalTitleAddress	Required; represents the Global Title Address of CallingPartyAddress.
SetOPCInCgPA	Required; if it is set to TRUE, OPC will be used in CallingPartyAddress.

Table 4-39   Sigtran RemoteServer Properties (continued)

Property	Description
GlobalTitleTranslationScript	This is used to specify the name of script which is responsible for translating IMSI to GTA.
SUAConfigurationFilename	Required; used to specify the name of configuration file for SUA stack initialization.
ReactivateTimerInterval	Required; represents the reactivate time interval to re-connect after failure.
Timeout	Required; represents the how long the remote server should wait before marking the request as timedout.
LimitOutstandingRequests	Limits the outstanding request to HLR when it is set to TRUE.
MaxOutstandingRequests	This represents the maximum outstanding request to HLR.

Note You should restart the Cisco Prime AR server, if you change any SIGTRAN related configuration.

ODBC

odbc specifies an ODBC server. Cisco Prime AR provides a RemoteServer object (and a service) to support Open Database Connectivity (ODBC), an open specification that provides application developers a vendor-independent API with which to access data sources. Table 4-40 lists the **odbc** server attributes.

For any ODBC remote service, the server might perform the environment mappings at any time. This means that if the service is set to either authentication and authorization, authentication-only, or authorization-only, environment mappings will take place. RADIUS mappings will take place only if the service is set to perform authorization. Checkitem mappings will take place only if the service is set to perform authentication. Previously environment mappings only occurred when the service was set for both authentication and authorization.

Table 4-40   odbc Properties

Property	Description
Timeout	Required; the default is 15. The timeout property indicates how many seconds the RADIUS server will wait for a response from the LDAP server. **Note** Use InitialTimeout from above as a template, except this is timeout is specified in seconds.
Protocol	Must be set to **odbc**.
ReactivateTimerInterval	Required; default is 300,000 milliseconds. Length of time to wait before attempting to reconnect if a thread is not connected to a data source.
Data Source Connections	Required; default is 8. This represents the total number of connections Cisco Prime AR can open with the ODBC server; total number of threads Cisco Prime AR can create for the ODBC server.

Table 4-40   odbc Properties (continued)

Property	Description
ODBCDataSource	Required; defines all items required for the **odbc.ini** file. The Cisco Prime AR server automatically creates the **odbc.ini** file based on these settings.
SQLDefinition	SQLDefinition properties define the SQL you want to execute. Type—**query** (Cisco Prime AR supports only type **query**). SQL—SQL query used to acquire the password UserPasswordAttribute—Defines the database column name for the user's password. MarkerList—Defines all markers for the query. MarkerList uses the format UserName/SQL_DATA_TYPE.
ODBCToRadiusMappings	Optional; a list of name/value pairs in which the name is the name of the **odbc** attribute to retrieve from the user record, and the value is the name of the RADIUS attribute to set to the value of the **odbc** attribute retrieved. For example, when the **ODBCToRadiusMappings** has the entry: **FramedIPAddress = Framed-IP-Address**, the RemoteServer retrieves the **FramedIPAddress** attribute from the **odbc** user entry for the specified user, uses the value returned, and sets the Response variable **Framed-IP-Address** to that value.
ODBCToEnvironmentMappings	Optional; a list of name/value pairs in which the name is the name of the **odbc** attribute to retrieve from the user record, and the value is the name of the Environment variable to set to the value of the **odbc** attribute retrieved. For example, when the **ODBCToEnvironmentMappings** has the entry: **group = User-Group**, the RemoteServer retrieves the **group** attribute from the **odbc** user entry for the specified user, uses the value returned, and sets the Environment variable **User-Group** to that value.
ODBCToCheckItemMappings	Optional; a list of ODBC *attribute/value* pairs which must be present in the RADIUS access request and must match, both name and value, for the check to pass. For example, when the **ODBCToCheckItemMappings** has the entry: **group = User-Group**, the Access Request must contain the attribute **group**, and it must be set to **User-Group**.

ODBC-Accounting

If you use the Oracle Accounting feature, you must configure an ODBC-Accounting RemoteServer object. Table 4-41 lists and defines the ODBC-Accounting RemoteServer properties.

Table 4-41   ODBC-Accounting RemoteServer Properties

Property	Description
Name	Name of the remote server; this property is mandatory, and there is no default
Description	Optional description of server
Protocol	Must be set to odbc-accounting
ReactivateTimerInterval	Mandatory time interval (in milliseconds) to activate an inactive server; defaults to 300000 ms.
Timeout	Mandatory time interval (in seconds) to wait for SQL operation to complete; defaults to 15 seconds
DataSourceConnections	Mandatory number of connections to be established; defaults to 8
ODBCDataSource	Name of the ODBCDataSource to use and must refer to one entry in the list of ODBC datasources configured under **/Radius/Advanced/ODBCDataSources**. Mandatory; no default
KeepAliveTimerInterval	Mandatory time interval (in milliseconds) to send a keepalive to keep the idle connection active; defaults to zero (0) meaning the option is disabled
BufferAccountingPackets	Mandatory, TRUE or FALSE, determines whether to buffer the accounting packets to local file, defaults to TRUE which means that packet buffering is enabled. **Note** When set to TRUE, a constant flow of incoming accounting packets can fill the buffer backing store files in **/cisco-ar/data/odbc** beyond the size configured in MaximumBufferFileSize. Configure BackingStoreDiscThreshold in **/Radius/Advanced** when using ODBC accounting. See Advanced, page 4-58 for information about how to configure BackingStoreDiscThreshold.
MaximumBufferFileSize	Mandatory if BufferAccountingPackets is set to TRUE, determines the maximum buffer file size, defaults to 10 Megabyte)
NumberOfRetriesForBufferdPacket	Mandatory if BufferAccountingPackets is set to TRUE. A number greater than zero determines the number of attempts to be made to insert the buffered packet into Oracle. Defaults to 3.

OCI

OCI service can be used to authenticate and authorize an access request by querying user information through OCI and to insert accounting records into a data store through OCI. For more information on OCI server properties, see ODBC/OCI, page 3-104.

OCI-Accounting

If you use the Oracle Accounting feature, you must configure an OCI-Accounting RemoteServer object. For more information, see ODBC/OCI-Accounting, page 3-107.

Prepaid-CRB

The following is the default configuration of a prepaid-crb RemoteServer. The Filename property is the name of the required shared library provided by the billing vendor. See CRB Prepaid Billing, page 16-7 for more information on Prepaid -CRB.

```
[ //localhost/Radius/RemoteServers/prepaid-crb ]
    Name = prepaid-crb
    Description =
    Protocol = prepaid-crb
    IPAddress =
    Port = 0
    Filename =
    Connections = 8
```

Prepaid-IS835C

The following is the default configuration of a prepaid-is835c RemoteServer. The Filename property is the name of the required shared library provided by the billing vendor. See IS835C Prepaid Billing, page 16-2 for more information on Prepaid -IS835C.

```
[ //localhost/Radius/RemoteServers/prepaid-is835c ]
    Name = prepaid-is835c
    Description =
    Protocol = prepaid-is835c
    IPAddress =
    Port = 0
    Filename =
    Connections = 8
```

RADIUS

radius specifies a RADIUS server. When you specify the **radius** protocol, supply the information in Table 4-42.

Table 4-42   RADIUS Properties

Property	Description
SharedSecret	Required; the secret shared between the remote server and the RADIUS server.
IncomingScript	Optional; when set, must be the name of a known incoming script. Cisco Prime AR runs the IncomingScript after it receives the response.
OutgoingScript	Optional; when set, must be the name of a known outgoing script. Cisco Prime AR runs the OutgoingScript just before it sends the proxy request to the remote server.
Vendor	Optional; when set, must be the name of a known Vendor.
MaxTries	Required; 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. The default is 3.

Table 4-42   RADIUS Properties (continued)

Property	Description
InitialTimeout	Required: represents the number of milliseconds used as a timeout for the first attempt to send a specific 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. The default value is 2000 (or 2 seconds).
ACKaccounting	When ACKAccounting is TRUE, the Cisco Prime AR server waits for the Accounting-Response from the remote RADIUS server before sending the corresponding Accounting-Response to the client. When ACKAccounting is FALSE, the Cisco Prime AR server does not wait for the Accounting-Response and immediately returns an Accounting-Response to the client.

SIGTRAN-M3UA

Cisco Prime AR supports SIGTRAN-M3UA to fetch the authentication vectors from HLR, which is required for EAP-AKA/EAP-SIM authentication. For more information on SIGTRAN-M3UA protocol, see Chapter 22, "SIGTRAN-M3UA".

Rules

A Rule is a function that selects services based on all input information used by the function.

Advanced

Advanced objects let you configure system-level properties and the Attribute dictionary. Under normal system operation, you should not need to change the system-level properties.

Note   The notation *required* means Cisco Prime AR needs a value for this property. For most of these properties, you can use system defaults.

Table 4-43 lists the **Advanced** properties.

Table 4-43   Advanced Object Properties

Property	Description
LogServerActivity	Required; the default is FALSE, which means Cisco Prime AR logs all responses except Access-Accepts and Access-Challenges. Accepting the default reduces the load on the server by reducing that amount of information it must log. Note, the client is probably sending accounting requests to an accounting server, so the Access-Accept requests are being indirectly logged. When you set it to TRUE, Cisco Prime AR logs all responses to the server log file.
MaximumNumberOfRadiusPackets	Required; the default is 8192. This is a critical property you should set high enough to allow for the maximum number of simultaneous requests. When more requests come in than there are packets allocated, Cisco Prime AR will drop those additional requests.
PerPacketHeapSize	Required; the default is 6500. This property sets the size of the initial heap for each packet. The heap is the dynamic memory a request can use during its lifetime. By preallocating the heap size at the beginning of request processing, we can minimize the cost of memory allocations. If PerPacketHeapSize is too low, Cisco Prime AR will ask the system for memory more often. If PerPacketHeapSize is too high, Cisco Prime AR will allocate too much memory for the request causing the system to use more memory than required.
UDPPacketSize	Required; the default is 4096. RFC 2138 specifies the maximum packet length can be 4096 bytes. Do not change this value.
RequireNASsBehindProxyBeInClientList	Required; the default is FALSE. If you accept the default, Cisco Prime AR only uses the source IP address to identify the immediate client that sent the request. Leaving it FALSE is useful when this RADIUS Server should only know about the proxy server and should treat requests as if they came from the proxy server. This might be the case with some environments that buy bulk dial service from a third party and thus do not need to, or are unable to, list all of the NASs behind the third party's proxy server. When you set it to TRUE, you must list all of the NASs behind the Proxy in the Clients list. For more information about this property, see Using the RequireNASsBehindProxyBeInClientList Property, page 4-71.

Table 4-43   Advanced Object Properties (continued)

Property	Description
AAAFileServiceSyncInterval	Required; specified in milliseconds, the default is 75. This property governs how often the file AAA service processes accounting requests and writes the accounting records to the file. You can lower the number to reduce the delay in acknowledging the **Account-Request** at the expense of more frequent flushing of the accounting file to disk. You can raise the number to reduce the cost of flushing to disk, at the expense of increasing the delays in acknowledging the **Accounting-Request**s. The default value was determined to provide a reasonable compromise between the two alternatives.
SessionBackingStoreSynchronizationInterval	Required; specified in milliseconds, the default is 100. If you change this value it must be a number greater than zero. This property governs how often the Session Manager backing store writes updated session information to disk. You can lower the number to reduce the delay in acknowledging requests at the expense of more frequent flushing of the file containing the session data to disk. You can raise the number to reduce the cost of flushing to disk at the expense of increasing delays in acknowledging requests. The default value was determined to provide a reasonable compromise between the two alternatives.
BackingStoreDiscThreshold	Required; the default is 10 gigabytes. The value of BackingStoreDisc-Threshold is made up of a number of units which can be K, kilobyte, or kilobytes, M, megabyte, or megabytes, or G, gigabyte, or gigabytes. BackingStoreDiscThreshold is used with session management and ODBC accounting and ensures that any data log files generated will not cross the BackingStoreDiscThreshold.
SessionBackingStorePruneInterval	Required; specifies the sleep time interval of the session backing store pruning thread. The recommended and default value is 6 hours, but you can modify this based on the traffic patterns you experience. With SessionBackingStorePruneInterval set to 6 hours, pruning will occur 6 hours after you restart or reload the Cisco Prime AR server and recur every 6 hours. You can set a very low value for this property to make pruning continuous, but there might not be enough data accumulated for the pruning to occur and pruning might be less effective compared to the default setting.

Table 4-43   Advanced Object Properties (continued)

Property	Description
PacketBackingStorePruneInterval	Required; specifies the sleep time interval of the packet backing store pruning thread. The recommended value is 6 hours, but you can modify this based on the traffic patterns you experience.
	When PacketBackingStorePruneInterval is set to 6 hours, pruning will occur 6 hours after you restart or reload the Cisco Prime AR server and recur every 6 hours.
	You can set a very low value for this property to make pruning continuous, but there might not be enough data accumulated for the pruning to occur and pruning might be less effective compared to the default setting.
RemoteLDAPServiceThreadTimerInterval	Required; specified in milliseconds, the default is 10. This property governs how often the **ldap** RemoteServer thread checks to see if any results have arrived from the remote LDAP server. You can modify it to improve the throughput of the server when it proxies requests to a remote LDAP server.
InitialBackgroundTimerSleepTime	Required; the default is 5. This property specifies the amount of time the time queue should initially sleep before beginning processing. This property is only used for initial synchronization and should not be changed.
MinimumSocketBufferSize	Required; the default is 65536 (64 K). This property governs how deep the system's buffer size is for queueing UDP datagrams until Cisco Prime AR can read and process them. The default is probably sufficient for most sites. You can, however, raise or lower it as necessary.
CertificateDBPath	Required if you are using an LDAP RemoteServer and you want Cisco Prime AR to use SSL when communicating with that LDAP RemoteServer. This property specifies the path to the directory containing the client certificates to be used when establishing an SSL connection to an LDAP RemoteServer. This directory must contain the **cert7.db** and **cert5.db** certificates and the **key3.db** and **key.db** files database used by Netscape Navigator 3.x (and above) or the **ServerCert.db** certificate database used by Netscape 2.x servers.

Table 4-43   Advanced Object Properties (continued)

Property	Description
LogFileSize	Required; the default is 1 Megabyte. This property specifies the maximum size of the RADIUS server log file. The value for the **LogFileSize** field is a string composed of two parts; a number, and a units indicator (<n> <units>) in which the unit is one of: K, kilobyte, kilobytes, M, megabyte, megabytes, G, gigabyte, or gigabytes.
	The **LogFileSize** property does not apply to the **config_mcd_1_log** or **agent_server_1_log** files. See Modifying File Sizes for Agent Server and MCD Server Logs, page 28-3 to configure these files.
	Note This does not apply to the trace log.
LogFileCount	Required; the default is 2. This property specifies the number of log files to be kept on the system. A new log file is created when the log file size reaches **LogFileCount**.
	The **LogFileCount** property does not apply to the **config_mcd_1_log** or **agent_server_1_log** files. See Modifying File Sizes for Agent Server and MCD Server Logs, page 28-3 to configure these files.
TraceFileSize	Required; the default is 1 GB. This property specifies the size of the trace files to be kept on the system. A new trace file is created when the trace file size reaches **TraceFileSize**. The value for the **TraceFileSize** field is a string composed of two parts; a number, and a units indicator (<n> <units>) in which the unit is one of: K, kilobyte, kilobytes, M, megabyte, megabytes, G, gigabyte, or gigabytes.
TraceFileCount	Required; this value can be set from 1-100, and the default is 2. This property specifies the number of trace files to maintain. A value of 1 indicates that no file rolling occurs.
UseAdvancedDuplicateDetection	Required; the default is FALSE. Set this property to TRUE when you want Cisco Prime AR to use a more robust duplicate request filtering algorithm. For more information on this property, see Advance Duplicate Detection Feature, page 4-72.
AdvancedDuplicateDetectionMemoryInterval	Required when the Advanced Duplicate Detection feature is enabled. This property specifies how long (in milliseconds) Cisco Prime AR should remember a request. You must specify a number greater than zero. The default is 10,000.

Table 4-43   Advanced Object Properties (continued)

Property	Description
DetectOutOfOrderAccountingPackets	Optional; used to detect accounting packets that arrive out of sequential order. The default is FALSE. This property is useful when using accounting and session management in a RADIUS proxy service.
	When the DetectOutOfOrderAccountingPacket property is enabled (set to TRUE), a new *Class* attribute is included in all outgoing Accept packets. The value for this Class attribute will contain the session magic number. The client will echo this value in the accounting packets, and this will be used for comparison.
	The session magic number is a unique number created for all sessions when the session is created or reused and the DetectOutOfOrderAccountingPacket property is set to TRUE. The DetectOutOfOrderAccountingPacket property is used to detect out-of-order Accounting-Stop packets in roaming scenarios by comparing the session magic number value in the session with the session magic number value contained in the Accounting packet.
	The value of 0xffffffff is considered by the Cisco Prime AR server to be a wild card magic number. If any accounting stop packets contain the value of 0xffffffff, it will pass the session magic validation even if the session's magic number is some thing else.
	The format of the class attribute is as follows:
	<4-byte Magic Prefix><4-byte server IP address><4-byte Magic value>
DefaultReturnedSubnetSizeIfNoMatch	Optional; used with the ODAP feature and reflects the returned size of the subnet if no matched subnet is found. There are three options to select if an exactly matched subnet does not exist: Bigger, Smaller, and Exact. The default is Bigger.
ClasspathForJavaExtensions	A string which is the classpath to be used to locate Java classes and jar files containing the classes required for loading the Java extensions, either Java extension points or services.
	Note The classpath will always contain the directory **$INSTALLDIR/scripts/radius/java** and all of the jar files in that directory.
JavaVMOptions	A string that can contain options to be passed to the JRE upon startup. JavaVMOptions should be used only when requested by Cisco TAC.
MaximumODBCResultSize	Specifies maximum size in bytes for an ODBC mapping. This parameter affects both ODBC result sizes and the trace log buffer for tracing script calls that access any of the dictionaries. (Default value is 256.)

Table 4-43   Advanced Object Properties (continued)

Property	Description
ARIsCaseInsensitive	When set to FALSE, requires that you provide exact pathnames with regard to upper and lower case for all objects, subobjects, and properties. The default setting, TRUE, allows you to enter paths such as **/rad/serv** instead of **/Rad/Serv**. **Note** Cisco Prime AR always authenticates the RADIUS attribute User-Name with regard to upper and lower case, regardless of the setting of this flag.
RemoteRadiusServerInterface	When set, specifies the local interface to bind to when creating the RemoteRadiusServer socket. If not set, the Cisco Prime AR binds to IPADDR_ANY.
ODBCEnvironmentMultiValueDelimiter	Optional; allows you to specify a character that separates multivalued attributes in the marker list when using Oracle (or ODBC) accounting
PacketBackingStoreSyncInterval	The minimum value is 1 and the maximum is a 32-bit unsigned integer. The default is 75.
ListenForDynamicAuthorizationRequests	Must be set to TRUE when using the Change of Authorization (CoA) feature or Packet of Disconnect (POD) feature. Default is FALSE.
MaximumNumberOfXMLPackets	Required when using identity caching. Indicates the maximum number of XML packets to be sent or received. The minimum value is 1 and the maximum is a 32-bit unsigned integer. The default is 1024.
XMLUDPPacketSize	Required when using identity caching. Indicates the maximum size of XML packets to be sent or received. The minimum value is 1 and the maximum is a 32-bit unsigned integer. The default is 4096.
RollingEncryptionKeyChangePeriod	Used in conjunction with the session-cache ResourceManager, this property specifies the length of time a given EncryptionKey will be used before a new one is created. When the session-cache ResourceManager caches User-Password attributes, Cisco Prime AR encrypts the User-Password so it is not stored in memory or persisted on disk in clear text. Cisco Prime AR uses up to 255 encryption keys, using a new one after each RollingEncryptionKeyChangePeriod expires. If RollingEncryptionKeyChangePeriod is set to *2 days*, Cisco Prime AR will create and begin using a new EncryptionKey every two days. The oldest key will be retired, and Cisco Prime AR will re-encrypt any User-Passwords that used the old key with the new key. This way, if the RollingEncryptionKeyChangePeriod is set to *1 day*, no key will be older than 255 days.

Table 4-43   Advanced Object Properties (continued)

Property	Description
SessionPurgeInterval	Optional; the SessionPurgeInterval property determines the time interval at which to check for timed-out sessions. If no value is set, the session timeout feature is disabled. The checks are performed in the background when system resources are available, so checks might not always occur at the exact time set.
	The minimum recommended value for SessionPurgeInterval is 60 minutes. The SessionPurgeInterval value is comprised of a number and a units indicator, as in n units, where a unit is one of minutes, hours, days, or weeks.
EapBadMessagePolicy	Set to one of two values: SilentDiscard (the default) or RejectFailure.
	When set to SilentDiscard, the Cisco Prime AR server silently discards and ignores bad EAP messages unless the protocol specification explicitly requires a failure message.
	When set to RejectFailure, the Cisco Prime AR server sends RADIUS Access-Rejects messages with embedded EAP-Failure in response to bad EAP messages as described in Internet RFC 3579.
StaleSessionTimeout	Required; the default value is "1 hour." Specifies the time interval to maintain a session when a client does not respond to Accounting-Stop notification.
	When the Cisco Prime AR server does not receive an Accounting-Response from a client after sending an Accounting-Stop packet, Cisco Prime AR maintains the session for the time interval configured in this property before releasing the session.
	This property is stored as a string composed of two parts: a number and a unit indicator (<n> <units>) similar to the MaxFileAge property where the unit is one of: M, Minute, Minutes, H, Hour, Hours, D, Day, Days, W, Week, or Weeks.
Ports/	Optional; allows you to use ports other than the default, 1645 and 1646. You can use this option to configure Cisco Prime AR to use other ports,. If you add additional ports, however, Cisco Prime AR will use the added ports and no longer use ports 1645 and 1646. These ports can still be used by adding them to the list of ports to use. For more information, see Ports, page 4-73.
Interfaces	Optional; see Interfaces, page 4-73
ReplyMessages	Optional; see Reply Messages, page 4-73.
AttributeDictionary	Optional; see Attribute Dictionary, page 4-75.
SNMP	Optional; see SNMP, page 4-76.

Table 4-43   Advanced Object Properties (continued)

Property	Description
RFC Compliance/	Optional; enables you to modify the Cisco Prime AR server to behave in a way that might deviate from RFC compliance in a special use case scenario.
	When AllowRejectAttrs is set to FALSE, Reply-Message attributes will not be passed in an Access Reject packet. When AllowRejectAttrs is set to TRUE, attributes will be allowed to pass in an Access Reject packet.
	When AllowEAPRejectAttrs is set to FALSE, Reply-Message attributes will not be passed in an Access Reject packet if the packet contains EAP-Message attribute. When AllowEAPRejectAttrs is set to TRUE, attributes will be allowed to pass in an Access Reject packet even if the packet contains EAP-Message attribute.
	Note Changing the state of either of these properties requires you to **reload** the Cisco Prime AR server.
DDNS	This subdirectory holds the SynthesizeReverseZone property and a list of Transaction Signatures (TSIG) keys.
SynthesizeReverseZone	This property exists under DDNS and controls whether Cisco Prime AR automatically generates the name of the reverse zone (**in-addr.arpa**) that is updated with PTR records. If this attribute is enabled and the resource manager does not have an explicit ReverseZoneName property configured, the server uses the IP address and DNSHostBytes property to generate the reverse zone name. The default value is TRUE.
ODBCDataSources	A list of ODBC data sets and their associated environments including operating system, DBMS, and network platform used to access the DBMS an application wants to access. Required when using Oracle (or ODBC) accounting.
AttributeGroups	Includes a Default subdirectory with an Attributes subdirectory that contains commonly-used attributes for Change of Authorization (CoA) and Packet of Disconnect (POD). You can add new attributes to the default group or create a new group as necessary.
KeyStores	Used to protect the security and integrity of the PACs it issues. • NumberOfKeys—Number (from 1-1024) that specifies the maximum number of keys stored for EAP-FAST. • RolloverPeriod—Specifies the amount of time between key updates.

Table 4-43   Advanced Object Properties (continued)

Property	Description
NumberOfRemoteUDPServerSockets	Required; the default value for this property is 4.
	The NumberOfRemoteUDPServerSockets property allows you to configure the number of source ports used while proxying requests to a remote radius server. If the NumberOfRemoteUDPServerSockets property is set to a value n, all remote servers share and use n sockets.
	The NumberOfRemoteUDPServerSockets value comprises a number, as in n, where n should be less than or equal to the current process file descriptor limit divided by 2.
	Note By default, the Radius process supports up to 1024 file descriptors. To increase the file descriptors, stop the arserver; in the arserver script, specify the required value to "NUMBER_OF_FILE_DESCRIPTORS" and restart the server. The value for "NUMBER_OF_FILE_DESCRIPTORS" should be in the range between 1024 to 65535.
NumberofRadiusIdentifiersPerSocket	This represents the number of RADIUS Identifiers that Cisco Prime AR can use per source port, while proxying requests to remote servers.
	To use a different source port for every request that is proxied, you need to set the value of this property to one.
MaximumIncomingRequestRate	Optional; the default value for this property is 0.
	The MaximumIncomingRequestRate property is used to limit the incoming traffic in terms of "allowed requests per second". Serves as a soft limit.
	The MaximumIncomingRequestRate property comprises a number n, where n can be any nonzero value.

Table 4-43   Advanced Object Properties (continued)

Property	Description
HideSharedSecretAndPrivateKeys	Required; the default value is TRUE.
	The HideSharedSecretAndPrivateKeys property hides:
	• The secret that is shared between a Radius Client and a Radius Server or between two radius servers in a radius proxy scenario.
	• The PrivateKeyPassword under the certificate-based EAP services.
	When this property is set to TRUE, the following properties are displayed as <encrypted>:
	• PrivateKeyPasswords in:
	– peap-v0 service
	– peap-v1 service
	– eap-tls service
	– eap-ttls service
	– eap-fast service
	• SharedSecret in:
	– RemoteServers of type radius
	– RemoteServers of type map-gateway
	– Clients object
	– Resource Manager of type usr-vpn under Gateway subobject
	• PseudonymSecret in eap-sim service
	• DynamicAuthSecret under DynamicAuthorizationServer subbject in Clients object
	• RepSecret under Replication
	• Secret in /radius/advanced/DDNS/TSIGKeys
	When the value for this property is set to FALSE, all the above properties are displayed in clear text.
MaximumOutstandingRequests	Optional; the default value for this property is 0.
	The MaximumOutstandingRequests property is used to limit the incoming traffic in terms of "requests processed". Serves as a hard limit.
	The MaximumOutstandingRequests property comprises a number n, where n can be any nonzero value.
Diameter	Required; See Diameter, page 4-77

Table 4-43   Advanced Object Properties (continued)

Property	Description
TPSSamplingPeriodInSecs	This represents the sampling period in seconds. The minimum sampling period is set to 5. The default is 30.
LogTPSActivity	When set to true this property enables to log in the TPS usage in a CSV file.The TPS is logged in the following format: *<mm-dd-yyyy>, <hh:mm:ss>, <tps-value>* For example, 04-01-2012, 12:00:01, 102 The default is False.
TPSLogFilenamePrefix	This represents the prefix of the CSV file which will be available in the logs directory of Cisco Prime AR. The following represents the CSV filename format: *<user-prefix>-<mm-dd-yyyy>*.csv tps-04-01-2012.csv
TPSLogFileCount	Configures the number of TPS Sampling log files to be maintained in the repository. The default value is 2.
AdditionalNativeOracleErrors	Optional; used to disconnect ODBC Remote Servers when configured native Oracle Error has occurred (which are not considered as connection errors). You must specify Native Errors as comma (,) separated integer values. For example, 04/14/2011 11:06:43.692: Log: ODBC client (DataSource 'CVOracleAcctDb', Connection 6): SQLExecute failed: SQLState:HY000 NativeError:12152 ErrorText:[Easysoft][Oracle]ORA-12152: TNS:unable to send break message 04/14/2011 10:44:59.388: Log: ODBC client (DataSource 'CVOracleAcctDb', Connection 3): SQLExecute failed: SQLState:HY000 NativeError:3114 ErrorText:[Easysoft][Oracle]ORA-03114: not connected to ORACLE For the above examples, the Native Errors need to be configured as follows: **--> set AdditionalNativeOracleErrors 12152,3114** When any one of the Native Errors 12152 or 3114 occurs, Cisco Prime AR disconnects the ODBC Remote Server.

This section contains the following topics:

- RemoteODBCSessionServer
- Using the RequireNASsBehindProxyBeInClientList Property
- Advance Duplicate Detection Feature
- Invalid EAP Packet Processing
- Ports
- Interfaces
- Reply Messages
- Attribute Dictionary
- SNMP
- Diameter

RemoteODBCSessionServer

The following is an example of theRemoteODBCSessionServer configuration:

--> cd /Radius/Advanced/RemoteODBCSessionServer/

```
[ //localhost/Radius/Advanced/RemoteODBCSessionServer ]
    ReactivateTimerInterval = 300000
    Timeout = 15
    DataSourceConnections = 8
    ODBCDataSource =
    KeepAliveTimerInterval = 0
    BufferAccountingPackets = TRUE
    MaximumBufferFileSize = "10 Megabytes"
    CacheLimit = 250000
    UseCacheIndex = 0
```

Table 4-44 lists and defines the RemoteODBCSessionServer properties.

Table 4-44   *RemoteODBCSesionServer Properties*

Property	Description
ReactivateTimerInterval	Mandatory time interval (in milliseconds) to activate an inactive server; defaults to 300000 ms
Timeout	Mandatory time interval (in seconds) to wait for SQL operation to complete; defaults to 15 seconds
DataSourceConnections	Mandatory number of connections to be established; defaults to 8
ODBCDataSource	Name of the ODBCDataSource to use and must refer to one entry in the list of ODBC datasources configured under **/Radius/Advanced/ODBCDataSources**. Mandatory; no default
KeepAliveTimerInterval	Mandatory time interval (in milliseconds) to send a keepalive to keep the idle connection active; defaults to zero (0) meaning the option is disabled

Table 4-44   RemoteODBCSesionServer Properties (continued)

Property	Description
BufferAccountingPackets	Mandatory, TRUE or FALSE, determines whether to buffer the accounting packets to local file, defaults to TRUE which means that packet buffering is enabled.
	Note When set to TRUE, a constant flow of incoming accounting packets can fill the buffer backing store files in **/cisco-ar/data/odbc** beyond the size configured in MaximumBufferFileSize. Configure BackingStoreDiscThreshold in **/Radius/Advanced** when using ODBC accounting. See Advanced, page 4-58 for information about how to configure BackingStoreDiscThreshold.
MaximumBufferFileSize	Mandatory if BufferAccountingPackets is set to TRUE, determines the maximum buffer file size, defaults to 10 Megabyte)
CacheLimit	Default is 250000; This represents the overall limit on cache of all 'remote' session managers. This value is interpreted as the maximum number of packets that can be present in cache. When the number of sessions hits this limit, sessions will be 'cached out'. This cache out operation will continue, until the cache is at least 20% free.
UseCacheIndex	If set to 1, it enables a fast cache based lookup index for the items in the database. This optimizes the number of queries to the database hence will improve performance, but limits the number of sessions that can be scaled.
	If set to 0, it disables fast cache based lookup index.

Note   Remote session manager will work only with Oracle database.

Using the RequireNASsBehindProxyBeInClientList Property

You can use the property **RequireNASsBehindProxyBeInClientList** to require NASs that send requests indirectly through a proxy to be listed in the Clients list or to allow the proxy to represent them all.

- When you want to ensure the proxy is only sending requests from NASs known to this server, set the property to TRUE, and list all of the NASs using this proxy. This increases memory usage.

- When it is impossible to know all of the NASs using this proxy or when you do not care, set the property to FALSE. Cisco Prime AR will use the proxy's IP address to identify the origin of the request.

Advance Duplicate Detection Feature

Cisco Prime AR automatically detects and handles duplicate requests it is currently working on. It also provides an optional, more complex mechanism to handle duplicate requests that can be received by the server after it has completed processing the original request. These duplicate requests can consume extra processing power, and, if received out of order (as RADIUS is a UDP-based protocol) might cause Session Management problems.

One solution is the Advanced Duplicate Detection feature which causes Cisco Prime AR to *remember* requests it has seen, as well as the response sent to that request, for a configurable amount of time.

To enable this feature, perform the following:

- Set the **UseAdvancedDuplicateDetection** property in the **/Radius/Advanced** section of the configuration to **TRUE**.

- Set the **AdvancedDuplicateDetectionMemoryInterval** in the **/Radius/Advanced** section to specify how long (in milliseconds) Cisco Prime AR should remember a request.

> **Note** Enabling this feature causes Cisco Prime AR to keep more of its preallocated packet buffers in use for a longer period of time. The number of preallocated buffers is controlled by the **MaximumNumberOfRadiusPackets** property in the **/Radius/Advanced** section of the configuration. This property might need to be increased (which will increase the amount of memory used by Cisco Prime AR) when the Advanced Duplicate Detection feature is enabled.

Invalid EAP Packet Processing

Cisco Prime AR has been enhanced to implement *fatal error* packet handling for Extensible Authentication Protocol (EAP) messages as described in section 2.2 of Internet RFC 3579 which states the following:

> A RADIUS server determining that a fatal error has occurred must send an Access-Reject containing an EAP-Message attribute encapsulating EAP-Failure.

Because this enhancement is a deviation from various EAP specifications, you must explicitly enable this feature through a new configuration property in **/Radius/Advanced** named *EapBadMessagePolicy.*

You can set the EapBadMessagePolicy property to one of two values: SilentDiscard (the default) or RejectFailure. When set to SilentDiscard, the Cisco Prime AR server silently discards and ignores bad EAP messages unless the protocol specification explicitly requires a failure message. When set to RejectFailure, the Cisco Prime AR server sends RADIUS Access-Rejects messages with embedded EAP-Failure in response to bad EAP messages as described in Internet RFC 3579.

The implementation of EAP authentication methods in Cisco Prime AR behaves as described in Internet RFC 2284 (EAP) and related EAP method specifications. These specify *silent discard* as the standard way to handle all EAP error conditions. Any EAP response message from the client that contains an error or is received in an invalid authenticator state is discarded and there is no error response.

In a configuration where EAP requests are proxied between RADIUS servers using RADIUS messages (EAP over RADIUS), the silent discard of an EAP message means that no RADIUS response message is sent back to the originating RADIUS server. Because of this, the RADIUS server originating the request eventually declares the destination RADIUS server *dead* and fails over to a backup server (if so configured).

Ports

The Ports list specifies which ports to listen to for requests. When you specify a port, Cisco Prime AR makes no distinction between the port used to receive Access-Requests and the port used to receive Accounting-Requests. Either request can come in on either port.

Most NASs send Access-Requests to port 1645 and Accounting-Requests to 1646, however, Cisco Prime AR does not check.

When you do not specify any ports, Cisco Prime AR reads the **/etc/services** file for the ports to use for access and accounting requests. If none are defined, Cisco Prime AR uses the standard ports (1645 and 1646).

Interfaces

The Interfaces list specifies the interfaces on which the RADIUS server receives and sends requests. You specify an interface by its IP address.

- When you list an IP address, Cisco Prime AR uses that interface to send and receive Access-Requests.

- When no interfaces are listed, the server performs an interface discover and uses all interfaces of the server, physical and logical (virtual).

Note   The IP address format is enhanced to support both IPv4 and IPv6.

Reply Messages

The Reply Messages list allows you to choose the reply message based on the reason the request was rejected. Each of the following properties (except **Default**) corresponds to a reason why the packet was rejected. The Reply Message properties allows you to substitute your own text string for the defined errors. After you set the property (with the **set** command) and the reason occurs, Cisco Prime AR sends the NAS that message in the Access-Reject packet as a **Reply-Message** attribute.

You might want to substitute your own messages to prevent users from getting too much information about why their requests failed. For example, you might not want users to know the password was invalid to prevent hackers from accessing your system. In such a case, you might specify the text string "unauthorized access" for the property **UserPasswordInvalid**.

Table 4-45 lists the **Reply Message** properties.

Table 4-45   Reply Message Properties

Property	Description
Default	Optional; when you set this property, Cisco Prime AR sends this value when the property corresponding to the reject reason is not set.
UnknownUser	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever Cisco Prime AR cannot find the user specified by **User-Name**.

Table 4-45   Reply Message Properties (continued)

Property	Description
UserNotEnabled	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever the user account is disabled.
UserPasswordInvalid	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever the password in the Access-Request packet did not match the password in the database.
UnableToAcquireResource	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever one of the Resource Managers was unable to allocate the resource for this request.
ServiceUnavailable	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever a service the request needs (such as a RemoteServer) is unavailable.
InternalError	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever an internal error caused the request to be rejected.
MalformedRequest	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever a required attribute (such as **User-Name**) is missing from the request.
ConfigurationError	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever the request is rejected due to a configuration error. For example, if a script sets an environment variable to the name of an object such as **Authentication-Service**, and that object does not exist in the configuration, the reason reported is ConfigurationError.
IncomingScriptFailed	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever one of the **IncomingScripts** fails to execute.
OutgoingScriptFailed	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever one of the **OutgoingScripts** fails to execute.
IncomingScriptRejectedRequest	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever one of the **IncomingScripts** rejects the Access-Request.
OutgoingScriptRejectedRequest	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever one of the **OutgoingScripts** rejects the Access-Request.
TerminationAction	Optional; when you set this property, Cisco Prime AR sends back this value in the **Reply-Message** attribute whenever Cisco Prime AR processes the Access-Request as a Termination-Action and is being rejected as a safety precaution.

Attribute Dictionary

The Attribute dictionary allows you to specify the attributes to the RADIUS server. Cisco Prime AR comes with the standard RADIUS attributes (as defined by the RFC 2865) as well as the attributes required to support the major NASs. For more information about the standard attributes, see Appendix C, "RADIUS Attributes."

All RADIUS requests and responses consist of one or more *attributes*, such as the user's name, the user's password, the type of service the NAS should provide to the user, or the IP address the user should use for the session.

In the request and response packets, an attribute is composed of a number (between 1-255) that specifies the type of attribute to use, a length that specifies the entire attribute length, and a value. How the value is interpreted depends on its type. When it is a username, the value is a string. When it is the NAS's IP address, the value is an IP address, and so on.

Table 4-46 lists the Attribute dictionary properties.

Table 4-46   Attribute Dictionary Properties

Property	Description
Name	Required; must be unique in the Attribute dictionary list within the same context. Although it should be an attribute defined in the RFC, the name can be any attribute defined by your client. The NAS typically comes with a list of attributes it uses. Attributes are referenced in the Profile and by Scripts by this name. The accounting file service also uses this name when printing the attribute.
Description	Optional description of the attribute.
Attribute	Required; must be a number between 1-255. It must be unique within the Attribute dictionary list.
Type	Required; must be set to one of the types listed in Table 4-47. The type governs how the value is interpreted and printed.

Types

Types are required and must be one of the following listed in Table 4-47.

Table 4-47   Types Attributes

Property	Description
UNDEFINED	Treated as a sting of binary bytes.
UINT32	Unsigned 32-bit integer.
STRING	Character string.
IPADDR	A valid IP address in dotted-decimal format.
CHAP_PASSWORD	17-byte value representing the password.

Table 4-47   Types Attributes (continued)

Property	Description
ENUM	Enums allow you to specify the mapping between the value and the strings. After you have established this mapping, Cisco Prime AR then replaces the number with the appropriate string. The min/max properties represent the lowest to highest values of the enumeration.
VENDOR_SPECIFIC	Vendor Specific Attribute (VSAs) are a special class of attribute. VSAs were created to extend the standard 256 attributes to include attributes required by specific manufacturers. VSAs add new capabilities for the value field in an attribute. Rather than being a simple integer string, or IP address, the value of a VSA can be one or more subattributes whose meaning depends on the vendor's definition. The Vendors list allows you to add, delete, or modify the definitions of the vendors and the subattributes they specify.

Vendor Attributes

Table 4-48 lists the **Vendor** properties.

Table 4-48   Vendor Properties

Property	Description
Name	Required; must be unique in the Vendors attribute list.
Description	Optional; description of the subattribute list.
VendorID	Required; must be a valid number and unique within the entire attribute dictionary.
Type	Required; must be one of the following: UNDEFINED, UINT32, STRING, IPADDR, CHAP_PASSWORD, ENUM, or SUB_ATTRIBUTES.

SNMP

Table 4-49 lists the five properties of the SNMP directory.

Table 4-49   SNMP Properties

Property	Description
Enabled	Either TRUE or FALSE; default is FALSE
TracingEnabled	Either TRUE or FALSE; default is FALSE
InputQueueHighThreshold	An integer; default is 90
InputQueueLowThreshold	An integer; default is 60
MasterAgentEnabled	Either TRUE or FALSE; default is TRUE

If Enabled and MasterAgentEnabled are both TRUE, **arservagt** will start and stop the SNMP daemon (**snmpd**). If either of these properties is FALSE, if the Cisco Prime AR server is not using SNMP or if your site uses a different master agent, **arservagt** will not start your master agent.

Diameter

This section explains how to configure Diameter general configuration and transport managment.

Change the directory to **/Radius/Advanced/Diameter**.

```
//localhost/Radius/Advanced/Diameter
    General/
    TransportManagement/
```

The following configuration is used to configure Diameter general configuration like Product name and Version.

```
[ //localhost/Radius/Advanced/Diameter/General ]
    Product = Cisco Prime Access Registrar
    Version = 6.0
    AuthApplicationIdList = 1
    AcctApplicationIdList = 3
```

Table 4-50 describes the Diameter general properties.

Table 4-50   Diameter General Properties

Property	Description
Product	Optional; name of the product.
Version	Optional; version number.

Table 4-50   Diameter General Properties (continued)

Property	Description
AuthApplicationIdList	Specifies the list of AuthApplications that the Cisco Prime AR server registers to Diameter Base stack during start up. It is a combination of Auth ApplicationId's separated by colon.
	For example:
	For Registering NASREQApplication,
	--> set AuthApplicationIdList 1
	For Registering applications with id's 1 and 5,
	--> set AuthApplicationIdList 1:5
	Note The Auth ApplicationIds that are configured should be present in **/Radius/Advanced/Diameter/Applications** section.
AcctApplicationIdList	Specifies the list of AcctApplications that the Cisco Prime AR server registers to Diameter Base stack during start up. It is a combination of Acct ApplicationId's separated by colon.
	For example:
	For Registering BaseAccountingApplication,
	--> set AcctApplicationIdList 3
	Note TheAcctApplicationId'sthatareconfiguredshouldbepresentin /Radius/Advanced/Diameter/Applications section.

Configuring Diameter TransportManagement Properties

The following example shows the Diameter transport management configuration:

```
[ //localhost/Radius/Advanced/Diameter/TransportManagement ]
    Identity = toby-ar1.cisco.com
    Realm = cisco.com
    TCPListenPort = 3868
    SCTPListenPort = 3868
    EnableIPV6 = FALSE
    WatchdogTimeout = 500
    ReconnectInterval = 500
    MaxReconnections = 3
    RequestRetransmissionInterval = 100
    MaxRequestRetransmissionCount = 3
    ReceiveBufferSize = 2048
    AdvertisedHostNames = toby-ar1.cisco.com
```

Table 4-51 describes the Diameter transport management properties.

Table 4-51   Diameter TransportManagement Properties

Property	Description
Identity	Required; identity of the system on which Diameter application is running. Must be set to a valid resolvable string.
Realm	Required; must be set to a valid Realm in the domain.
TCPListenPort	Required; port number on which Cisco Prime AR server listens for TCP peer connections.
SCTPListenPort	Required; port number on which Cisco Prime AR server listens for SCTP peer connections.
EnableIPv6	Required; if set to TRUE it enables IPV6 for the Diameter application.
WatchdogTimeout	Required; specifies the time interval between watch dog messages.
ReconnectInterval	Required; specifies the time interval between which Cisco Prime AR server attempts to connect to a disconnected peer. If set to 0, then no attempt will be made to connect to a disconnected peer.
MaxReconnections	Required; specifies the number of times Cisco Prime AR server tries to Make a reconnection attempt. If set to 0, then no attempt will be made to reconnect.
RequestRetransmissionInterval	Required; the time for which retransmission of pending requests will be done. If set to 0, then no attempt will be made to retransmit.
MaxRequestRetransmissionCount	Required, maximum number of times Cisco Prime ARserver tries to retransmit a pending request. If set to 0, then no attempt will be made to retransmit.
ReceiveBufferSize	Required; intial size of buffer that is preallocated for message reception.
AdvertisedHostNames	Optional; specifies the local hostname address that will be advertised by the Cisco Prime AR server to other peers during CER/CEA exchange. For example: AdvertisedHostNames = toby-ar1.cisco.com

Configuring Diameter SessionManagement

The following example shows the Diameter session management configuration:

```
//localhost/Radius/Advanced/Diameter/SessionManagement ]
    MaxSessions = 10000
    AuthSessions/
    AcctSessions/
    AuthSessions/
    EnableStatefulSessions = TRUE
    AuthSessionTimeout = 5
    LifeTimeTimeout = 360
    GracePeriodTimeout = 30
    AbortRetryTimeout = 20
    AcctSessions/
    AcctSessionTimeOut = 30
    InterimInterval = 5
    RealTime = 0
```

Table 4-52 describes the Diameter SessionManagement properties.

Table 4-52   Diameter SessionManagement Properties

Property	Description
MaxSessions	Required; specifies the maximum number of concurrent Diameter sessions Cisco Prime AR server will maintain. These sessions include both Auth and Acct sessions.
AuthSessions/EnableStatefulSessions	If set to TRUE, the server will enforce stateful sessions and the client will hint for stateful sessions. Default Value is TRUE. Set the property to FALSE to disable stateful sessions.
AuthSessionTimeout	Required; specifies the timeout in seconds before a session requires reauthentication.
LifeTimeTimeout	Required; specifies the timeout in seconds before a session is terminated regardless of whether the session has been reauthenticated.
GracePeriodTimeout	Required; specifies the grace period after the life timeout and before the full termination of the session.
AbortRetryTimeout	Required; specifies the timeout between the subsequent Abort Session Request (ASR) messages if the initial attempt fails.
AcctSessions/AcctSessionTimeOut	Required; specifies the the timeout in seconds before a session requires reauthentication.
InterimInterval	Required; specifies the interim interval dictated to the client if the entity is a server or hint to the server if the entity is a client.
RealTime	Required; RealTime value dictated to the client.

Configuring Diameter Application

Table 4-53 describes the Diameter Application properties.

Table 4-53   Diameter Application Properties

Property	Description
Name	Required; name of the application.
Description	Optional; description of the application.
IsVendorSpecific	Required; the default is FALSE. If set to FALSE, the application is ordinary application. If set to TRUE, the application is a VendorSpecific Application.
IsAuthApplication	Required; if set to TRUE the application represents AuthApplication else it represents Accounting Application.
Application ID	Required; specifies the unique integer value for the application. The following are examples of Diameter application: NASREQ 1 Mobile-IP 2 Diameter Base Accounting 3 **Note** ApplicationId property must be set to 0 for Base Protocol.
VendorSpecificApplicationID	Required; specifies the integer value for the vendor specific application.
VendorID	Required; specifies the VendorID for the application. Example: DIAMETER 3GPP Cx APPLICATION VendorSpecificApplicationID 16777216 VendorID 10415
ApplicationURI	Optional; specifies the URI of the Application. Eg: "ftp://ftp.ietf.org/internet-drafts/draft-ietf-aaa-diameter-nasreq-12.txt"
Commands	Required; an indexed list from 1 to <n>. Each entry in the list is the name of the command. It specifies the list of commands associated with the application.

Configuring the Diameter Application

To configure the Diameter application:

Step 1   Move to **//localhost/Radius/Advanced/Diameter/Applications** directory:

Step 2   Add the application you want to add (eg: NASREQ).

add NASREQ

```
Added NASREQ
```

cd NASREQ

```
[ //localhost/Radius/Advanced/Diameter/Applications/NASREQ ]
        Name = NASREQ
        Description =
        IsAuthApplication = TRUE
        IsVendorSpecific = FALSE
        ApplicationID =
        ApplicationURI =
        Commands/
```

Step 3   Set the ApplicationId and ApplicationURI .

set ApplicationId 1

```
Set ApplicationId 1
```

set ApplicationURL "ftp://ftp.ietf.org/internet-drafts/draft-ietf-aaa-diameter-nasreq-12.txt"

Step 4   Add the list of commands for this application.

cd commands/

```
Set 1  AA
```

Configuring Diameter Commands

Table 4-54 describes the Diameter Application properties.

Table 4-54   *Diameter Command Properties*

Property	Description
Name	Required; name of the command.
CommandCode	Required; specifies the integer code of the command.
EnableProxyBit	Required; default is TRUE . When enabled it represents the message is proxiable.

Table 4-54   Diameter Command Properties (continued)

Property	Description
RequestMsgAVPs /	The RequestMsgAVPs define the placement of AVPs within the request command. This contains three sub directories: Fixed, Required and Optional.
	Fixed - Defines the fixed position of AVP in a request message
	Required - The AVP must be present and can appear anywhere in the request message.
	Optional - The AVP name in optional cannot evaluate to any avp name which is included in a fixed or required directory. The avp can appear anywhere in the request message.
	For example: ``` cd Fixed/ Add Session-Id cd Session-Id/ Name = Session-Id Description = Min = 0 Max = 1 ``` where:
	Min is the minimum number of times AVP element may be present in a request. The default value is 0.
	Max is the maximum number of times the element may present in a request. A value of zero implies AVP is not present in the request.
AnswerMsgAVPs/	The AnswerMsgAVPs define the placement of AVP's within the answer command. This contains three sub directories: Fixed, Required and Optional.
	Fixed - Defines the fixed position of AVP in the answer message.
	Required - The AVP must present and can appear anywhere in the answer message.
	Optional - The AVP name in optional cannot evaluate to any avp name which is included in a fixed or required directory. The avp can appear anywhere in the answer message.

Configuring the Diameter Commands

To configure the Diameter commands:

Step 1   Change to **/Radius/Advanced/Diameter/Commands**.

Step 2   Add AA command.

> **add AA**

```
[ //localhost/Radius/Advanced/Diameter/Commands ]
```

> **cd AA/**

```
cd AA/
```

Step 3   Set the properties for AA command.

```
[ //localhost/Radius/Advanced/Diameter/Commands/AA ]
    Name = AA
    Description =
    CommandCode =
    EnableProxyBit = TRUE
    RequestMsgAVPs/
    AnswerMsgAVPs/
```

set CommandCode 265

```
Set CommandCode 265
```

set EnableProxyBit TRUE

```
Set EnableProxyBit TRUE
```

Step 4   Configure the RequestMsgAVP's for the command.

cd RequestMsgAVPs/

```
[ //localhost/Radius/Advanced/Diameter/Commands/AA/RequestMsgAVPs ]
    Fixed/
    Required/
    Optional/
```

Add Fixed AVP's for the request message.

Add Fixed AVP's

```
cd Fixed/
```

add Session-Id

```
Added Session-Id
```

cd Session-Id/

```
[ //localhost/Radius/Advanced/Diameter/Commands/AA/RequestMsgAVPs/Fixed/Session-Id ]
    Name = Session-Id
    Description =
     Min = 0
     Max =
```

Maximum and Minimum property specifies the multiplicity of the AVP Inside a request (or response). Similarly add the required and Optional AVP's.

Step 5   Configure AnswerMsgAVP's similar to step 3.

cd AnswerMsgAVPs/

```
[ //localhost/Radius/Advanced/Diameter/Commands/AA/AnswerMsgAVPs ]
    Fixed/
    Required/
    Optional/
```

The following shows an example of NASREQ application configuration:

```
[ //localhost/Radius/Advanced/Diameter/Applications/NASREQ ]
    Name = NASREQ
    Description =
    IsAuthApplication = TRUE
    IsVendorSpecific = FALSE
    ApplicationID = 1
    ApplicationURI =
    ftp://ftp.ietf.org/internet-drafts/draft-ietf-aaa-diameter-nasreq-12.txt
    Commands/
    1. AA
```

The following shows an example of the AA command configuration:

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

[ //localhost/Radius/Advanced/Diameter/Commands/AA ]
    Name = AA
    Description =
    CommandCode = 265
    EnableProxyBit = TRUE
    RequestMsgAVPs/
        Fixed/
            Entries 1 to 1 from 1 total entries
            Current filter: <all>

            Session-Id/
                Name = Session-Id
                Description =
                Min = 1
                Max = 1
        Required/
            Entries 1 to 7 from 7 total entries
            Current filter: <all>

            Auth-Application-Id/
                Name = Auth-Application-Id
                Description =
                Min = 1
                Max = 1
            Auth-Request-Type/
                Name = Auth-Request-Type
                Description =
                Min = 1
                Max = 1
            Destination-Realm/
                Name = Destination-Realm
                Description =
                Min = 1
                Max = 1
            Origin-Host/
                Name = Origin-Host
                Description =
                Min = 1
                Max = 1
            Origin-Realm/
                Name = Origin-Realm
                Description =
                Min = 1
                Max = 1
            User-Name/
                Name = User-Name
```

```
                            Description =
                            Min = 0
                            Max = 1
                        User-Password/
                            Name = User-Password
                            Description =
                            Min = 0
                            Max = 1
                    Optional/
                        Entries 1 to 42 from 42 total entries
                        Current filter: <all>

                        ARAP-Password/
                            Name = ARAP-Password
                            Description =
                            Min = 0
                            Max = 1
                        ARAP-Security/
                            Name = ARAP-Security
                            Description =
                            Min = 0
                            Max = 1
                        ARAP-Security-Data/
                            Name = ARAP-Security-Data
                            Description =
                            Min = 0
                            Max = 100
                        Auth-Grace-Period/
                            Name = Auth-Grace-Period
                            Description =
                            Min = 0
                            Max = 1
                        Auth-Session-State/
                            Name = Auth-Session-State
                            Description =
                            Min = 0
                            Max = 1
                        Authorization-Lifetime/
                            Name = Authorization-Lifetime
                            Description =
                            Min = 0
                            Max = 1
            AnswerMsgAVPs/
                Fixed/
                    Entries 1 to 1 from 1 total entries
                    Current filter: <all>

                    Session-Id/
                        Name = Session-Id
                        Description =
                        Min = 1
                        Max = 1
                Required/
                    Entries 1 to 5 from 5 total entries
                    Current filter: <all>

                    Auth-Application-Id/
                        Name = Auth-Application-Id
                        Description =
                        Min = 1
                        Max = 1
                    Auth-Request-Type/
                        Name = Auth-Request-Type
                        Description =
```

```
                            Min = 1
                            Max = 1
                        Origin-Host/
                            Name = Origin-Host
                            Description =
                            Min = 1
                            Max = 1
                        Origin-Realm/
                            Name = Origin-Realm
                            Description =
                            Min = 1
                            Max = 1
                        Result-Code/
                            Name = Result-Code
                            Description =
                            Min = 1
                            Max = 1
                Optional/
                        Entries 1 to 59 from 59 total entries
                        Current filter: <all>

                        Acct-Interim-Interval/
                            Name = Acct-Interim-Interval
                            Description =
                            Min = 0
                            Max = 1
                        ARAP-Challenge-Response/
                            Name = ARAP-Challenge-Response
                            Description =
                            Min = 0
                            Max = 1
                        ARAP-Features/
                            Name = ARAP-Features
                            Description =
                            Min = 0
                            Max = 1
                        ARAP-Security/
                            Name = ARAP-Security
                            Description =
                            Min = 0
                            Max = 1
                        ARAP-Security-Data/
                            Name = ARAP-Security-Data
                            Description =
                            Min = 0
                            Max = 100
                        ARAP-Zone-Access/
                            Name = ARAP-Zone-Access
                            Description =
                            Min = 0
                            Max = 1
                        Auth-Grace-Period/
                            Name = Auth-Grace-Period
                            Description =
                            Min = 0
                            Max = 1
```

```
Auth-Session-State/
    Name = Auth-Session-State
    Description =
    Min = 0
    Max = 1
Authorization-Lifetime/
    Name = Authorization-Lifetime
    Description =
    Min = 0
    Max = 1
```

Configuring Diameter Dictionary

The Diameter dictionary contains a list of application specific AVPs.

Table 4-55 describes the Diameter BaseProtocol AVP Properties.

Table 4-55   Diameter BaseProtocol AVP Properties

Property	Description
Name	Required; name of the application specifc AVPs.
Description	Optional; description of the application specifc AVPs.
IsVendorSpecific	Required; default is FALSE. If set to FALSE, the application is ordinary application and user is prompted to enter ApplicationID. If set to TRUE, the application is a VendorSpecific Application. User is prompted to enter VendorSpecificApplicationID and VendorID.
ApplicationID	Required; specifies the unique integer value for the application. **Note** The Application ID must be set to 0 for BaseProtocol AVPs.
VendorSpecificApplicationID	Required, Specifies the integer value for the vendor specific application.
VendorID	Required, specifies the VendorID for the application.
AVPS/	Specifies the list of application specific avps. Example: ```\nAccounting-Realtime-Required/\nName = Accounting-Realtime-Required\nDescription =\nAttribute = 483\nMandatory = Must\nMay-Encrypt = Yes\nProtected = MustNot\nType = UINT32\nMin = 0\nMax = 253\n``` Refer Table 4-56 for the description of AVP properties.

Table 4-56 lists the application specific AVP properties.

Table 4-56 **AVP Properties**

Property	Description
Attribute	Specifies the integer value for the AVP.
Mandatory	Specifies whether the mandatory bit of this AVP should or should not be set.
May-Encrypt	If set to 'yes' then theAVP will be sent encrypted if the connection uses CMS security.
Protected	Specifies whether the protected bit of this AVP should or should not be set.
Type	Specifies the type of the Diameter AVP.

Configure the Diameter Dictionary

To configure the Diameter Dictionary:

Step 1   Change to **/Radius/Advanced/Diameter/Diameter Dictionary**.

Step 2   Add BaseProtocolAVPs.

add BaseProtocolAVPs

```
[ //localhost/Radius/Advanced/Diameter/Diameter Dictionary ]
```

cd BaseProtocolAVPs/

Step 3   Set the porperties for BaseProtocolAVPs.

```
[ //localhost/Radius/Advanced/Diameter/Diameter Dictionary/BaseProtocolAVPs ]
    Name = BaseProtocolAVPs
    Description =
    IsVendorSpecific = FALSE
    ApplicationID = 0
    AVPs/
```

set IsVendorSpecific "FALSE"

```
set IsVendorSpecific   "FALSE"
```

set ApplicationID 0

```
set ApplicationID   0
```

Step 4   Configure the application specific AVPs.

cd AVPs/

add User-Name

Step 5   Configure User-Name AVP type and number

--> cd User-Name/

```
[ //localhost/Radius/Advanced/Diameter/Diameter Dictionary/BaseProtocolAVPs/AVPs/User-Name
]
    Name = User-Name
    Description =
    Attribute = 1
    Mandatory = MustNot
    May-Encrypt = No
    Protected = MustNot
    Type = UTF8_STRING
    Min = 0
    Max = 253
```

set Attribute 1

```
set Attribute  1
```

set Type UTF8_STRING

```
set Type UTF8_STRING
```

The following is an example of Diameter BaseProtocol AVPs:

```
[ //localhost/Radius/Advanced/Diameter/Diameter Dictionary/BaseProtocolAVPs ]
        Name = BaseProtocolAVPs
        Description =
        IsVendorSpecific = FALSE
        ApplicationID = 0
        AVPs/
            Entries 1 to 55 from 55 total entries
            Current filter: <all>

            Accounting-Realtime-Required/
                Name = Accounting-Realtime-Required
                Description =
                Attribute = 483
                Mandatory = Must
                May-Encrypt = Yes
                Protected = MustNot
                Type = UINT32
                Min = 0
                Max = 253
            Accounting-Record-Number/
                Name = Accounting-Record-Number
                Description =
                Attribute = 485
                Mandatory = Must
                May-Encrypt = Yes
                Protected = MustNot
                Type = UINT32
                Min = 0
                Max = 253
            Accounting-Record-Type/
                Name = Accounting-Record-Type
                Description =
                Attribute = 480
                Mandatory = Must
                May-Encrypt = Yes
                Protected = MustNot
                Type = ENUM
```

```
                          Min = 0
                          Max = 253
                          Enums/
                                1 = "Event Record"
                                2 = "Start Record"
                                3 = "Interim Record"
                                4 = "Stop Record"
           Accounting-Session-Id/
                          Name = Accounting-Session-Id
                          Description =
                          Attribute = 44
                          Mandatory = Must
                          May-Encrypt = Yes
                          Protected = May
                          Type = STRING
                          Min = 0
                          Max = 253
           Accounting-Sub-Session-Id/
                          Name = Accounting-Sub-Session-Id
                          Description =
                          Attribute = 287
                          Mandatory = Must
                          May-Encrypt = Yes
                          Protected = May
                          Type = UINT64
                          Min = 0
                          Max = 253
```