Overview

Prime Access Registrar is a 3GPP-compliant, 64-bit carrier-class RADIUS (Remote Authentication Dial-In User Service)/Diameter server that enables multiple dial-in Network Access Server (NAS) devices to share a common authentication, authorization, and accounting database.

Prime Access Registrar handles the following tasks:

- Authentication—determines the identity of users and whether they can be allowed to access the network
- Authorization—determines the level of network services available to authenticated users after they are connected
- Accounting—keeps track of each user's network activity
- Session and resource management—tracks user sessions and allocates dynamic resources

This chapter contains the following sections:

Session Management

The Session Management feature requires the client (NAS or proxy) to send all RADIUS accounting requests to the Prime Access Registrar server performing session management. (The only exception is if the clients are USR/3Com Network Access Servers configured to use the USR/3Com RADIUS resource management feature.) This information is used to keep track of user sessions, and the resources allocated to those sessions.

When another accounting RADIUS server needs this accounting information, the Prime Access Registrar server performing session management might proxy it to this second server.

The **count-sessions /radius all** command helps to count the total sessions in Prime Access Registrar. The options are similar to the query-session command options. The query-session command displays cached attributes in addition to session details.

Table 1-1 describes how Prime Access Registrar handles session management.

Table 1-1 Session Management Processing

Action	Explanation
Determines whether to perform session management.	The session management defined in the Environment dictionary variable **Session-Manager**.
	The session management name referred to in **/Radius/DefaultSessionManager**.
Performs session management.	Selects Session Manager as defined in **/Radius/SessionManagers/**<*Name*>.

This section contains the following topics:

- Failover by the NAS and Session Management
- Cross Server Session and Resource Management

Failover by the NAS and Session Management

When a Network Access Server's primary RADIUS server is performing session management, and the NAS determines the server is not responding and begins sending requests to its secondary RADIUS server, the following occurs:

- The secondary server will not know about the current active sessions that are maintained on the primary server. Any resources managed by the secondary server must be distinct from those managed by the primary server, otherwise it will be possible to have two sessions with the same resources (for example, two sessions with the same IP address).
- The primary server will miss important information that allows it to maintain a correct model of what sessions are currently active (because the authentication and accounting requests are being sent to the secondary server). This means when the primary server comes back online and the NAS begins using it, its knowledge of what sessions are active will be out-of-date and the resources for those sessions are allocated even if they are free to allocate to someone else.

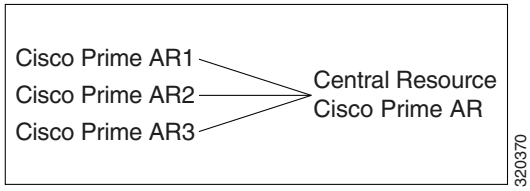
  For example, the user-session-limit resource might reject new sessions because the primary server does not know some of the users using the resource logged out while the primary server was offline. It might be necessary to release sessions manually using the **aregcmd** command **release-session**.

Note It might be possible to avoid this situation by having a disk drive shared between two systems with the second RADIUS server started up once the primary server has been determined to be offline. For more information on this setup, contact Technical Support.

Cross Server Session and Resource Management

Prime Access Registrar can manage sessions and resources across AAA Server boundaries. A session can be created by an Access-Request sent to Prime AR1, and it can be removed by an Accounting-Stop request sent to Prime AR2, as shown in Figure 1-1. This enables accurate tracking of User and Group session limits across multiple AAA Servers, and IP addresses allocated to sessions are managed in one place.

Figure 1-1 Multiple Prime Access Registrar Servers



All resources that must be shared cross multiple front line Prime Access Registrars are configured in the Central Resource Prime Access Registrar. Resources that are not shared can still be configured at each front line Prime Access Registrar.

When the front line Prime Access Registrar receives the access-request, it does the regular AA processing. If the packet is not rejected and a Central Resource Prime Access Registrar is also configured, the front line Prime Access Registrar will proxy the packet[1] to the configured Central Resource Prime Access Registrar. If the Central Resource Prime Access Registrar returns the requested resources, the process continues to the local session management (if local session manager is configured) for allocating any local resources. If the Central Resource Prime Access Registrar cannot allocate the requested resource, the packet is rejected.

When the Accounting-Stop packet arrives at the frontline Prime Access Registrar, Prime Access Registrar does the regular accounting processing. Then, if the front line Prime Access Registrar is configured to use Central Resource Prime Access Registrar, a proxy packet will be sent to Central Resource Prime Access Registrar for it to release all the allocated resources for this session. After that, any locally allocated resources are released by the local session manager.

Session-Service Service Step and Radius-Session Service

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.

Configure Front Line Cisco Prime Access Registrar

To use a Central Resource server, the DefaultSessionService property must be set or the Session-Service environment variable must be set through a script or the rule engine. The value in the Session-Service variable overrides the DefaultSessionService.

The configuration parameters for a Session-Service service type are the same as those for configuring a radius service type for proxy, except the service type is ***radius-session***.

The configuration for a Session-Service Remote Server is the same as configuring a proxy server.

```
[ //localhost/Radius ]
    Name = Radius
    Description =
    Version = 7.2
    IncomingScript =
    OutgoingScript =
    DefaultAuthenticationService = local-users
```

1. The proxy packet is actually a resource allocation request, not an Access Request.

```
    DefaultAuthorizationService = local-users
    DefaultAccountingService = local-file
    DefaultSessionService = Remote-Session-Service
    DefaultSessionManager = session-mgr-1

[ //localhost/Radius/Services ]
    Remote-Session-Service/
       Name = Remote-Session-Service
       Description =
       Type = radius-session
       IncomingScript =
       OutgoingScript =
       OutagePolicy = RejectAll
       OutageScript =
       MultipleServersPolicy = Failover
       RemoteServers/
        1. central-server

[ //localhost/Radius/RemoteServers ]
    central-server/
       Name = central-server
       Description =
       Protocol = RADIUS
       IPAddress = 209.165.200.224
       Port = 1812
       ReactivateTimerInterval = 300000
       SharedSecret = secret
       Vendor =
       IncomingScript =
       OutgoingScript =
       MaxTries = 3
       InitialTimeout = 2000
       AccountingPort = 1813
```

Configure Central Prime Access Registrar

Resources at the Central Resource server are configured the same way as local resources are configured. These resources are local resources from the Central Resource server's point of view.

Script Processing Hierarchy

For request packets, the script processing order is from the most general to the most specific. For response packets, the processing order is from the most specific to the most general.

Table 1-2, Table 1-3, and Table 1-4 show the overall processing order and flow:
(1-6) Incoming Scripts, (7-11) Authentication/Authorization Scripts, and (12-17) Outgoing Scripts.

Note The client and the NAS can be the same entity, except when the immediate client is acting as a proxy for the actual NAS.

Table 1-2 Prime Access Registrar Processing Hierarchy for Incoming Scripts

Overall Flow Sequence	Incoming Scripts
1)	Radius.
2)	Vendor of the immediate client.
3)	Immediate client.
4)	Vendor of the specific NAS.
5)	Specific NAS.
6)	Service.

Table 1-3 Prime Access Registrar Processing Hierarchy for Authentication/Authorization Scripts

Overall Flow Sequence	Authentication/Authorization Scripts
7)	Group Authentication.
8)	User Authentication.
9)	Group Authorization.
10)	User Authorization.
11)	Session Management.

Table 1-4 Prime Access Registrar Processing Hierarchy for Outgoing Script

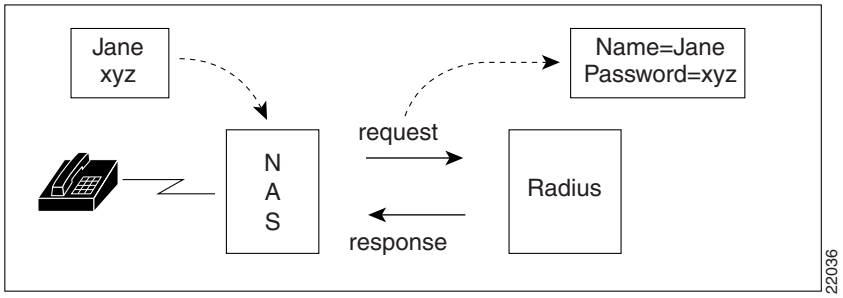
Overall Flow Sequence	Outgoing Scripts
12)	Service.
13)	Specific NAS.
14)	Vendor of the specific NAS.
15)	Immediate client.
16)	Vendor of the immediate client.
17)	Radius.

RADIUS Protocol

Prime Access Registrar is based on a client/server model, which supports AAA (authentication, authorization, and accounting). The *client* is the Network Access Server (NAS) and the *server* is Prime Access Registrar. The client passes user information on to the RADIUS server and acts on the response it receives. The *server*, on the other hand, is responsible for receiving user access requests, authenticating and authorizing users, and returning all of the necessary configuration information the client can then pass on to the user.

The protocol is a simple packet exchange in which the NAS sends a request packet to the Prime Access Registrar with a name and a password. Prime Access Registrar looks up the name and password to verify it is correct, determines for which dynamic resources the user is authorized, then returns an accept packet that contains configuration information for the user session (Figure 1-2).

Figure 1-2 Packet Exchange Between User, NAS, and RADIUS



Prime Access Registrar can also reject the packet if it needs to deny network access to the user. Or, Prime Access Registrar can issue a challenge that the NAS sends to the user, who then creates the proper response and returns it to the NAS, which forwards the challenge response to Prime Access Registrar in a second request packet.

In order to ensure network security, the client and server use a *shared secret*, which is a string they both know, but which is never sent over the network. User passwords are also encrypted between the client and the server to protect the network from unauthorized access.

This section contains the following topics:

Steps to Connection

Three participants exist in this interaction: the user, the NAS, and the RADIUS server.

Setting Up the Connection

To describe the receipt of an access request through the sending of an access response:

Step 1 The user, at a remote location such as a branch office or at home, dials into the NAS, and supplies a name and password.

Step 2 The NAS picks up the call and begins negotiating the session.

a. The NAS receives the name and password.

b. The NAS formats this information into an Access-Request packet.

c. The NAS sends the packet on to the Prime Access Registrar server.

Step 3 The Prime Access Registrar server determines what hardware sent the request (NAS) and parses the packet.

a. It sets up the Request dictionary based on the packet information.

b. It runs any incoming scripts, which are user-written extensions to Prime Access Registrar. An incoming script can examine and change the attributes of the request packet or the environment variables, which can affect subsequent processing.

c. Based on the scripts or the defaults, it chooses a service to authenticate and/or authorize the user.

Step 4 Prime Access Registrar's authentication service verifies the username and password is in its database. Or, Prime Access Registrar delegates the authentication (as a proxy) to another RADIUS server, an LDAP, or TACACS server.

Step 5 Prime Access Registrar's authorization service creates the response with the appropriate attributes for the user's session and puts it in the Response dictionary.

Step 6 If you are using Prime Access Registrar session management at your site, the Session Manager calls the appropriate Resource Managers that allocate dynamic resources for this session.

Step 7 Prime Access Registrar runs any outgoing scripts to change the attributes of the response packet.

Step 8 Prime Access Registrar formats the response based on the Response dictionary and sends it back to the client (NAS).

Step 9 The NAS receives the response and communicates with the user, which might include sending the user an IP address to indicate the connection has been successfully established.

Enhanced IP Allocation in Prime Access Registrar

In the previous versions of Prime Access Registrar, IP allocation happens internally based on a specific range of IPs configured. If there are multiple Prime Access Registrars in a deployment, each Prime Access Registrar server will have different range of IPs configured and can allocate/de-allocate IPs only within that specific range. Prime Access Registrar cannot allocate IPs from a common pool. This is addressed by the enhanced IP allocation feature.

For more information about the Enhanced IP Allocation feature, see Chapter 11, "Enhanced IP Allocation in Cisco Prime Access Registrar."

5G Data Network-AAA (DN-AAA) Compliance

Prime Access Registrar is 5G Data Network-AAA (DN-AAA) compliant based on the spec 3GPP TS 29.561 V15.1.0. Further enhancements are made to support this functionality. For more details, refer to the "Wireless" chapter of the *Cisco Prime Access Registrar 9.0 Reference Guide*.

Related Documentation

For a complete list of Cisco Prime Access Registrar documentation, see the *Cisco Prime Access Registrar Documentation Overview*.

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.

- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.