CHAPTER 1

Overview

The chapter provides an overview of the RADIUS server, including connection steps, RADIUS message types, and using Cisco Access Registrar as a proxy server.

Cisco Access Registrar is a RADIUS (Remote Authentication Dial-In User Service) server that allows multiple dial-in Network Access Server (NAS) devices to share a common authentication, authorization, and accounting database.

Cisco Access Registrar handles the following tasks:

- Authentication—determines the identity of users and whether they may 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

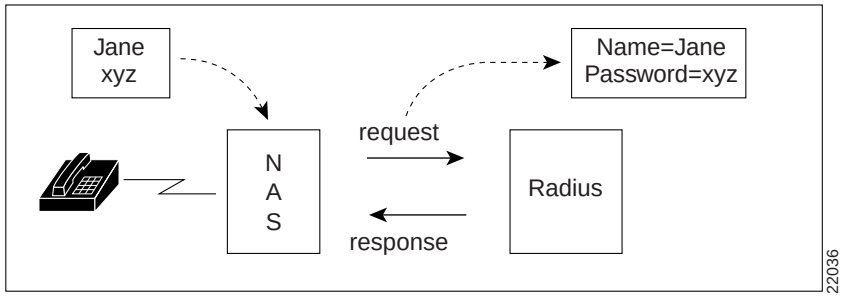
Using a RADIUS server allows you to better manage the access to your network, as it allows you to store all security information in a single, centralized database instead of distributing the information around the network in many different devices. You can make changes to that single database instead of making changes to every network access server in your network.

RADIUS Protocol

Cisco 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 Cisco 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 Cisco Access Registrar with a name and a password. Cisco AR 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 1-1).

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



Cisco AR can also reject the packet if it needs to deny network access to the user. Or, Cisco AR might 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 Cisco 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.

Steps to Connection

Three participants exist in this interaction: the user, the NAS, and the RADIUS server. The following steps 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 Cisco Access Registrar server.

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

- **d.** It sets up the Request dictionary based on the packet information.
- **e.** It runs any incoming scripts, which are user-written extensions to Cisco Access Registrar. An incoming script can examine and change the attributes of the request packet or the environment variables, which can affect subsequent processing.
- **f.** Based on the scripts or the defaults, it chooses a service to authenticate and/or authorize the user.

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

Step 5 Cisco 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 Cisco Access Registrar session management at your site, the Session Manager calls the appropriate Resource Managers that allocate dynamic resources for this session.

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

Step 8 Cisco 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 may include sending the user an IP address to indicate the connection has been successfully established.

Types of RADIUS Messages

The client/server packet exchange consists primarily of the following types of RADIUS messages:

- Access-Request—sent by the client (NAS) requesting access
- Access-Reject—sent by the RADIUS server rejecting access
- Access-Accept—sent by the RADIUS server allowing access
- Access-Challenge—sent by the RADIUS server requesting more information in order to allow access. The NAS, after communicating with the user, responds with another Access-Request.

When you use RADIUS accounting, the client and server can also exchange the following two types of messages:

- Accounting-Request—sent by the client (NAS) requesting accounting
- Accounting-Response—sent by the RADIUS server acknowledging accounting

Packet Contents

The information in each RADIUS message is encapsulated in a UDP (User Datagram Protocol) data packet. A packet is a block of data in a standard format for transmission. It is accompanied by other information such as the origin and destination of the data.

lists each message packet which contains the following five fields:

Table 1-1 ***RADIUS Packet Fields***

Fields	Description
Code	Indicates what type of message it is: Access-Request, Access-Accept, Access-Reject, Access-Challenge, Accounting-Request, or Accounting-Response.
Identifier	Contains a value that is copied into the server's response so the client can correctly associate its requests and the server's responses when multiple users are being authenticated simultaneously.
Length	Provides a simple error-checking device. The server silently drops a packet if it is shorter than the value specified in the length field, and ignores the octets beyond the value of the length field.

Table 1-1 *RADIUS Packet Fields* (continued)

Fields	Description
Authenticator	Contains a value for a Request Authenticator or a Response Authenticator. The Request Authenticator is included in a client's Access-Request. The value is unpredictable and unique, and is added to the client/server shared secret so the combination can be run through a one-way algorithm. The NAS then uses the result in conjunction with the shared secret to encrypt the user's password.
Attribute(s)	Depends on the type of message being sent. The number of attribute/value pairs included in the packet's attribute field is variable, including those required or optional for the type of service requested.

The Attribute Dictionary

The Attribute dictionary contains a list of preconfigured authentication, authorization, and accounting attributes that can be part of a client's or user's configuration. The dictionary entries translate an attribute into a value Cisco Access Registrar uses to parse incoming requests and generate responses. Attributes have a human-readable name and an enumerated equivalent from 1-255.

Sixty three standard attributes exist, which are defined in RFCs 2865, 2866, 2867, 2868, and 2869. There also are additional vendor-specific attributes that depend on the particular NAS you are using.

Some sample attributes include:

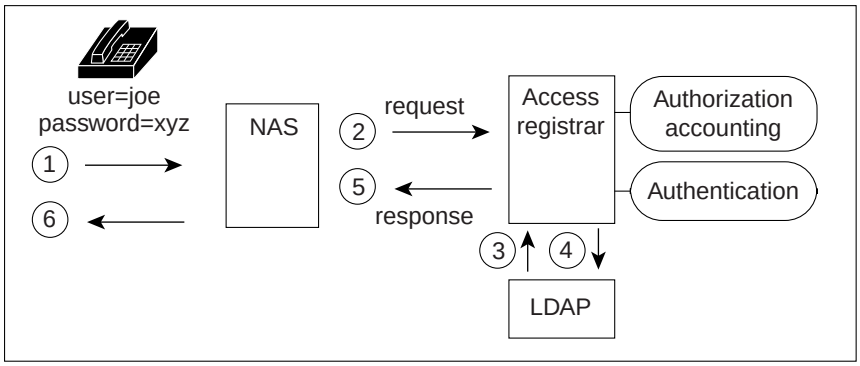
- User-Name—the name of the user
- User-Password—the user's password
- NAS-IP-Address—the IP address of the NAS
- NAS-Port—the NAS port the user is dialed in to
- Framed Protocol—such as SLIP or PPP
- Framed-IP-Address—the IP address the client uses for the session
- Filter-ID—vendor-specific; identifies a set of filters configured in the NAS
- Callback-Number—the actual callback number.

Proxy Servers

Any one or all of the RADIUS server's three functions: authentication, authorization, or accounting can be subcontracted to another RADIUS server. Cisco AR then becomes a *proxy server*. Proxying to other servers enables you to delegate some of the RADIUS server's functions to other servers.

You can use Cisco AR to "proxy" to an LDAP server for access to directory information about users in order to authenticate them. Figure 1-2 shows user `joe` initiating a request, the Cisco AR server proxying the authentication to the LDAP server, and then performing the authorization and accounting processing in order to enable `joe` to log in.

Figure 1-2 Proxying to an LDAP Server for Authentication



Basic Authentication and Authorization

This section provides basic information about how Cisco Access Registrar performs the basic RADIUS functions of authentication and authorization as defined in Internet RFC 2865.

- Authentication—determining the identity of a user of a client NAS through user identification and password validation and deciding whether to grant access
- Authorization—determining the level of network services available to authenticated users after a connection has been established

The Cisco Access Registrar (AR) server provides authentication and authorization service to clients which are network access servers (NAS). The following paragraphs describe the steps to a connection.

1. The process begins when user dials into the NAS and enters a user name and a password. The NAS creates an Access-Request containing attributes such as the user's name, the user's password, the ID of the client, and the Port ID the user is accessing.
2. The Cisco AR server determines which hardware (client NAS) sent the request, parses the packet, and determines whether to accept the request.

   The Cisco AR server checks to see if the client's IP address is listed in **/Radius/Clients/<Name>/<IPAddress>**.
3. After accepting the request, the Cisco AR server does the following:
   - Sets up the Request Dictionary based on the packet information
   - Runs any incoming scripts (user-written extensions to Cisco Access Registrar)

     An incoming script can examine and change the attributes of the request packet or the environmental variables which can affect subsequent processing.
   - Based on default values or scripts, it chooses a service to authenticate and authorize the user.

     The Cisco AR server directs the request to the appropriate service, which then performs authentication and/or authorization according to the type specified in **/Radius/Services/<Name>/<Type>**.
   - Performs session management, directing the request to the appropriate Session Manager.

- Performs resource management for each Resource Manager in the Session Manager. The Cisco AR server directs the request to the appropriate resource manager listed in **/Radius/SessionManagers/<Name>/<ResourceManagers>/<Name>**. The resource manager then allocates or checks the resource according to the type listed in **/Radius/<ResourceManagers>/<Name>/<Type>**.

4. The Cisco AR server finally creates and formats an Access-Accept, Access Reject, or Access Challenge response, then sends it to the client (NAS).