Examine how the RADIUS Works

Contents

Introduction

This document describes what a RADIUS server is and how it works.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Background Information

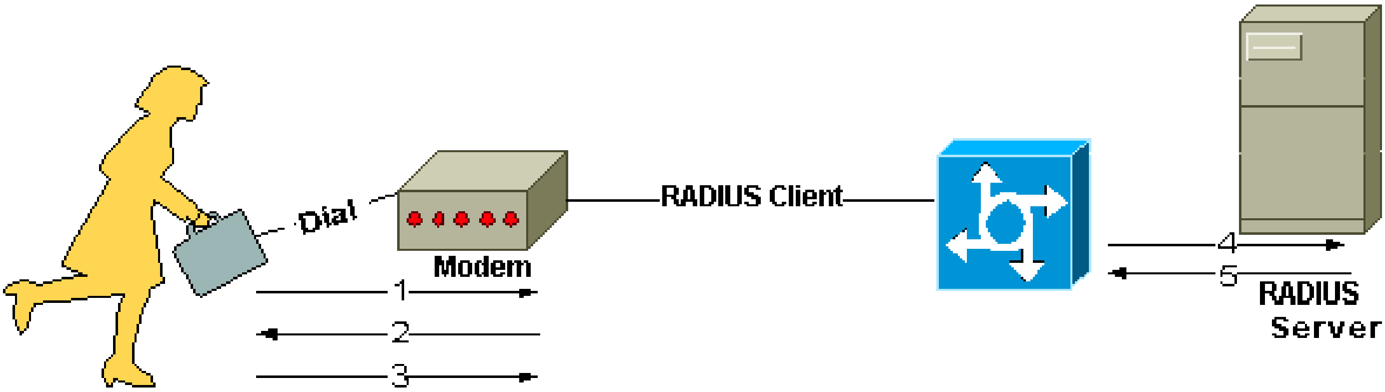
The Remote Authentication Dial-In User Service (RADIUS) protocol was developed by Livingston Enterprises, Inc., as an access server authentication and accounting protocol. The RADIUS specification RFC 2865 obsoletes RFC 2138. The RADIUS accounting standard RFC 2866 obsoletes RFC 2139.

Communication between a network access server (NAS) and a RADIUS server is based on the User Datagram Protocol (UDP). Generally, the RADIUS protocol is considered a connectionless service. Issues related to server availability, retransmission, and timeouts are handled by the RADIUS-enabled devices rather than the transmission protocol.

RADIUS is a Client/Server Protocol

The RADIUS client is typically a NAS, and the RADIUS server is usually a daemon process that runs on a UNIX or Windows NT machine. The client passes user information to designated RADIUS servers and acts on the returned response. RADIUS servers receive user connection requests, authenticate the user, and then return the configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

This figure shows the interaction between a dial-in user and the RADIUS client and server.



Interaction between Dial-in User and the RADIUS Client and Server

1. User initiates PPP authentication to the NAS.
2. NAS prompts for username and password (if Password Authentication Protocol [PAP]) or challenge (if Challenge Handshake Authentication Protocol [CHAP]).
3. User replies.
4. RADIUS client sends username and encrypted password to the RADIUS server.
5. RADIUS server responds with Accept, Reject, or Challenge.
6. The RADIUS client acts upon services and services parameters bundled with Accept or Reject.

Authentication and Authorization

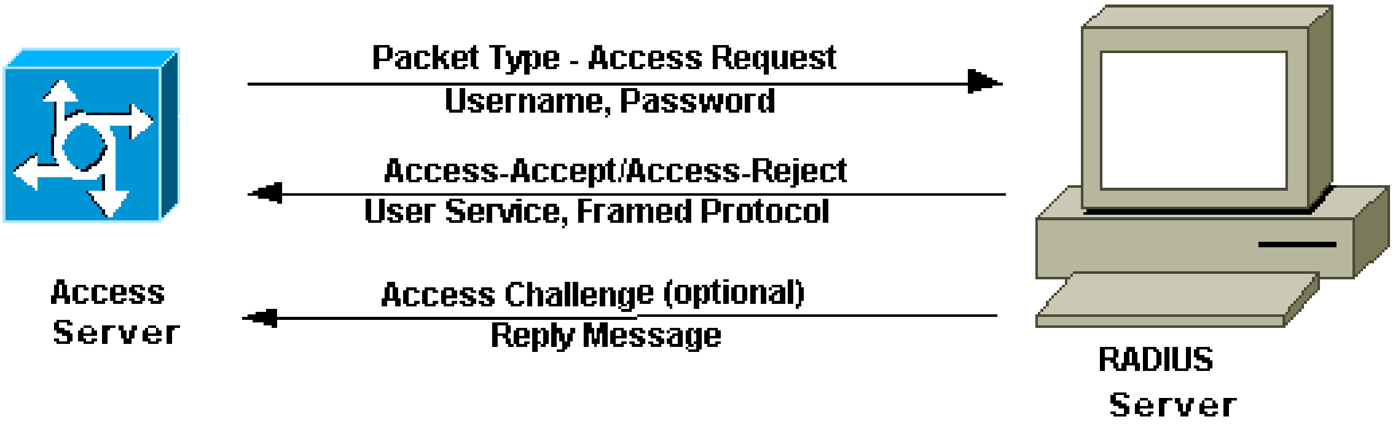
The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX log in, and other authentication mechanisms.

Typically, a user log in consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server. The Access-Request packet contains the username, encrypted password, NAS IP address, and port. The early deployment of RADIUS was done with UDP port number 1645, which conflicts with the "data metrics" service. Because of this conflict, RFC 2865 officially assigned port number 1812 for RADIUS. Most Cisco devices and applications offer support for either set of port numbers. The format of the request also provides information about the type of session that the user wants to initiate. For example, if the query is presented in character mode, the inference is **Service-Type = Exec-User**, but if the request is presented in PPP packet mode, the inference is **Service Type = Framed User** and **Framed Type = PPP**.

When the RADIUS server receives the Access-Request from the NAS, it searches a database for the username listed. If the username does not exist in the database, either a default profile is loaded, or the

RADIUS server immediately sends an Access-Reject message. This Access-Reject message can be accompanied by a text message that indicates the reason for the refusal.

In RADIUS, authentication and authorization are coupled together. If the username is found and the password is correct, the RADIUS server returns an Access-Accept response, that includes a list of attribute-value pairs that describe the parameters to be used for this session. Typical parameters include service type (shell or framed), protocol type, IP address to assign the user (static or dynamic), access list to apply, or a static route to install in the NAS routing table. The configuration information in the RADIUS server defines what can be installed on the NAS. The next figure illustrates the RADIUS authentication and authorization sequence.


Packet Type - Access Request
Username, Password
Access-Accept/Access-Reject
User Service, Framed Protocol
Access Challenge (optional)
Reply Message
Access Server
RADIUS Server

RADIUS Authentication and Authorization Sequence

Accounting

The accounting features of the RADIUS protocol can be used independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of sessions, that indicates the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) can use RADIUS access control and accounting software to meet special security and billing needs. The accounting port for RADIUS for most Cisco devices is 1646, but it can also be 1813 (because of the change in ports as specified in RFC 2139).

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, user passwords are sent encrypted between the client and RADIUS server to eliminate the possibility that someone snooping on an insecure network could determine a user password.

Related Information

- **Authentication Protocols**
- **Requests for Comments (RFCs)**
- **Cisco Technical Support & Downloads**