**Remote Authentication Dial In User Service** (**RADIUS, 遠端用戶撥入驗證服務**) is a networking [protocol](http://en.wikipedia.org/wiki/Communications_protocol) that provides centralized [AAA](http://en.wikipedia.org/wiki/AAA_protocol): Authentication ([驗證](http://zh.wikipedia.org/w/index.php?title=%E9%A9%97%E8%AD%89&action=edit&redlink=1)), Authorization (授權), and Accounting (計費) management for computers to connect and use a network service.

RADIUS is a client/server protocol that runs in the [application layer](http://en.wikipedia.org/wiki/Application_Layer), using [UDP](http://en.wikipedia.org/wiki/User_Datagram_Protocol) as transport. The [Remote Access Server](http://en.wikipedia.org/wiki/Remote_Access_Server), the [Virtual Private Network server](http://en.wikipedia.org/wiki/Virtual_Private_Network_server), the [Network switch](http://en.wikipedia.org/wiki/Network_switch) with port-based authentication, and the [Network Access Server (NAS)](http://en.wikipedia.org/wiki/Network_Access_Server), are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server. The RADIUS server is usually a background process running on a UNIX or Microsoft Windows server.RADIUS serves three functions:

1. To authenticate users or devices before granting them access to a network,
2. To authorize those users or devices for certain network services and
3. To account for usage of those services.

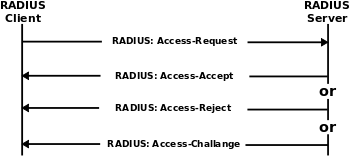
## AAA

RADIUS servers use the [AAA](http://en.wikipedia.org/wiki/AAA_protocol) concept to manage network access in the following two-step process, also known as an "AAA transaction". AAA stands for “authentication, authorization and accounting”. [Authentication](http://en.wikipedia.org/wiki/Authentication) and [Authorization](http://en.wikipedia.org/wiki/Authorization) characteristics in RADIUS are described in [RFC 2865](http://tools.ietf.org/html/rfc2865) while [Accounting](http://en.wikipedia.org/wiki/Accounting) is described by [RFC 2866](http://tools.ietf.org/html/rfc2866).

### Authentication and authorization

The user or machine sends a request to a [Remote Access Server](http://en.wikipedia.org/wiki/Remote_Access_Server) (RAS) to gain access to a particular network resource using access credentials. The RAS sends a RADIUS *Access Request* message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol. This request includes access credentials, typically in the form of [username](http://en.wikipedia.org/wiki/Username) and [password](http://en.wikipedia.org/wiki/Password) or security certificate provided by the user. Additionally, the request may contain other information which the RAS knows about the user, such as its network address or phone number, and information regarding the user's physical point of attachment to the RAS.

The RADIUS server checks that the information is correct using authentication schemes such as [PAP](http://en.wikipedia.org/wiki/Password_authentication_protocol), [CHAP](http://en.wikipedia.org/wiki/Challenge-handshake_authentication_protocol) or **RADIUS Authentication and Authorization Flow**

[](http://en.wikipedia.org/w/index.php?title=File:Drawing_RADIUS_1812.svg&page=1)

RADIUS Authentication and Authorization Flow

The RADIUS server then returns one of three responses to the RAS : 1) Access Reject, 2) Access Challenge, or 3) Access Accept.

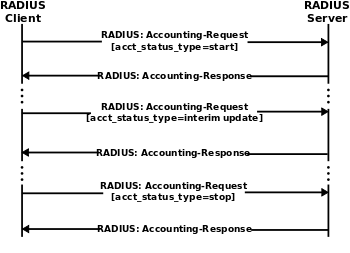
* *Access Reject* - The user is unconditionally denied access to all requested network resources. Reasons may include failure to provide proof of identification or an unknown or inactive user account.
* *Access Challenge* - Requests additional information from the user such as a secondary password, PIN, token, or card. Access Challenge is also used in more complex authentication dialogs where a secure tunnel is established between the user machine and the Radius Server in a way that the access credentials are hidden from the RAS.
* *Access Accept* - The user is granted access. Once the user is authenticated, the RADIUS server will often check that the user is authorized to use the network service requested. A given user may be allowed to use a company's wireless network, but not its VPN service, for example. This information may be stored locally on the RADIUS server, or looked up in an external source such as LDAP or Active Directory.

Each of these three RADIUS responses may include a Reply-Message attribute which may give a reason for the rejection, the prompt for the challenge, or a welcome message for the accept. The text in the attribute can be passed on to the user in a return web page.

Authorization [attributes](http://en.wikipedia.org/wiki/Radius_Values) are conveyed to the RAS stipulating terms of access to be granted. For example, the following authorization attributes may be included in an Access-Accept:

* The specific [IP address](http://en.wikipedia.org/wiki/IP_address) to be assigned to the user
* The address pool from which the user's IP should be chosen
* The maximum length that the user may remain connected
* An access list, priority queue or other restrictions on a user's access
* [L2TP](http://en.wikipedia.org/wiki/L2TP) parameters
* VLAN parameters
* Quality of Service (QoS) parameters

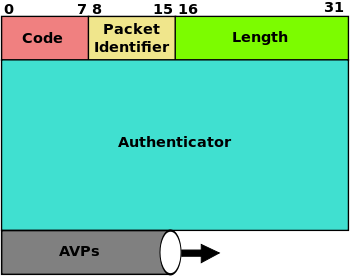
### Accounting

[](http://en.wikipedia.org/w/index.php?title=File:Drawing_RADIUS_1813.svg&page=1)

RADIUS Accounting Flow

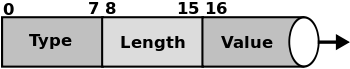
When network access is granted to the user by the [NAS](http://en.wikipedia.org/wiki/Network_access_server), an *Accounting Start* (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value "start") is sent by the NAS to the RADIUS server to signal the start of the user's network access. Typically, the client sends Accounting-Request packets until it receives an Accounting-Response acknowledgement, using some retry interval. The primary purpose of this data is that the user can be [billed](http://en.wikipedia.org/wiki/Bill_(payment)) accordingly; the data is also commonly used for [statistical](http://en.wikipedia.org/wiki/Statistical) purposes and for general network monitoring.

## Packet structure

[](http://en.wikipedia.org/w/index.php?title=File:RADIUS_packet_format.svg&page=1)

RADIUS packet data format: The fields are transmitted from left to right, starting with the code, the identifier, the length, the authenticator and the attributes. The Authenticator is used to authenticate the reply from the RADIUS server, and is used in encrypting passwords; its length is 16 bytes.

### Attribute value pairs

[](http://en.wikipedia.org/w/index.php?title=File:RADIUS_AVP_layout.svg&page=1)

RADIUS AVP layout: The RADIUS Attribute Value Pairs (AVP) carry data in both the request and the response for the authentication, authorization, and accounting transactions. The length of the radius packet is used to determine the end of the AVPs.

## UDP port numbers

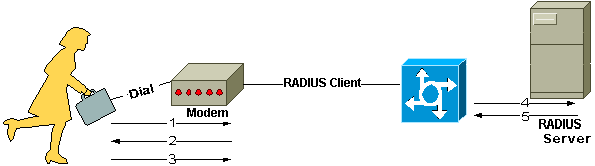
RADIUS has been officially assigned UDP ports 1812 for RADIUS Authentication and 1813 for RADIUS Accounting.

**How Does RADIUS Work**?

## Background Information

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 running on a UNIX or Windows NT machine. The client passes user information to designated RADIUS servers and acts on the response that is returned. 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. This figure shows the interaction between a 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 login, and other authentication mechanisms.

A user login 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.

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 indicating 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, including 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 will be installed on the NAS.

## 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, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use RADIUS access control and accounting software to meet special security and billing needs.

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's password