**遠端用戶撥入驗證服務**(**RADIUS**, **Remote Authentication Dial In User Service**)是一個[AAA](http://en.wikipedia.org/wiki/AAA_protocol" \o "en:AAA protocol)協議，同時兼顧[驗證](http://zh.wikipedia.org/w/index.php?title=%E9%A9%97%E8%AD%89&action=edit&redlink=1)(authentication)、授權(authorization)及計費(accounting)三種服務的[協議](http://zh.wikipedia.org/w/index.php?title=%E5%8D%94%E8%AE%AE&action=edit&redlink=1" \o "協議（頁面不存在）)(protocol)，通常用於網路存取、或流動IP服務，適用於[局域網](http://zh.wikipedia.org/wiki/%E5%B1%80%E5%9F%9F%E7%BD%91" \o "區域網)及[漫遊](http://zh.wikipedia.org/wiki/%E6%BC%AB%E9%81%8A)服務。

**Remote Authentication Dial In User Service** (**RADIUS**) is a networking [protocol](http://en.wikipedia.org/wiki/Communications_protocol) that provides centralized Authentication, Authorization, and Accounting ([AAA](http://en.wikipedia.org/wiki/AAA_protocol)) 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).

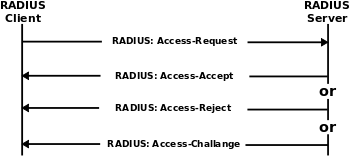
### Authentication and authorization

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 credentials are passed to the RAS device via the [link-layer](http://en.wikipedia.org/wiki/Link_Layer) protocol - for example, [Point-to-Point Protocol](http://en.wikipedia.org/wiki/Point-to-Point_Protocol) (PPP) in the case of many [dialup](http://en.wikipedia.org/wiki/Dialup) or [DSL](http://en.wikipedia.org/wiki/Digital_subscriber_line) providers or posted in an [HTTPS](http://en.wikipedia.org/wiki/HTTPS) secure web form.

In turn, 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 [EAP](http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol). The user's proof of identification is verified, along with, optionally, other information related to the request, such as the user's network address or phone number, account status, and specific network service access privileges. Historically, RADIUS servers checked the user's information against a locally stored flat file database. Modern RADIUS servers can do this, or can refer to external sources — commonly [SQL](http://en.wikipedia.org/wiki/SQL), [Kerberos](http://en.wikipedia.org/wiki/Kerberos_(protocol)), [LDAP](http://en.wikipedia.org/wiki/LDAP), or [Active Directory](http://en.wikipedia.org/wiki/Active_Directory) servers — to verify the user's credentials.

[](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.

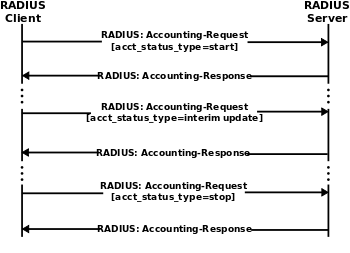
* *Access Reject* - The user is unconditionally denied access to all requested network resources. Reasons may include failure to provide proof of identification or an unknown or inactive user account.
* *Access Challenge* - Requests additional information from the user such as a secondary password, PIN, 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

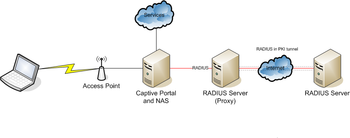
When network access is granted to the user by the [NAS](http://en.wikipedia.org/wiki/Network_access_server), an *Accounting Start* (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value "start") is sent by the NAS to the RADIUS server to signal the start of the user's network access. "Start" records typically contain the user's identification, network address, point of attachment and a unique session identifier.

Periodically, *Interim Update* records (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value "interim-update") may be sent by the NAS to the RADIUS server, to update it on the status of an active session. "Interim" records typically convey the current session duration and information on current data usage.

Finally, when the user's network access is closed, the NAS issues a final *Accounting Stop* record (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value "stop") to the RADIUS server, providing information on the final usage in terms of time, packets transferred, data transferred, reason for disconnect and other information related to 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.

## Roaming

[](http://en.wikipedia.org/wiki/File:Drawing_Roaming_RADIUS.png)

Roaming using a proxy RADIUS AAA server.

RADIUS is commonly used to facilitate [roaming](http://en.wikipedia.org/wiki/Roaming) between [ISPs](http://en.wikipedia.org/wiki/Internet_service_provider), for example:

* by companies which provide a single global set of credentials that are usable on many public networks;
* by independent, but collaborating, institutions issuing their own credentials to their own users, that allow a visitor from one to another to be authenticated by their home institution, such as in [eduroam](http://en.wikipedia.org/wiki/Eduroam).

RADIUS facilitates this by the use of *realms*, which identify where the RADIUS server should forward the AAA requests for processing.

### Realms

A realm is commonly appended to a user's user name and delimited with an '@' sign, resembling an email address domain name. This is known as *postfix* notation for the realm. Another common usage is *prefix* notation, which involves prepending the realm to the username and using '\' as a delimiter. Modern RADIUS servers allow any character to be used as a realm delimiter, although in practice '@' and '\' are usually used.

Although realms often resemble domains, it is important to note that realms are in fact arbitrary text and need not contain real domain names.

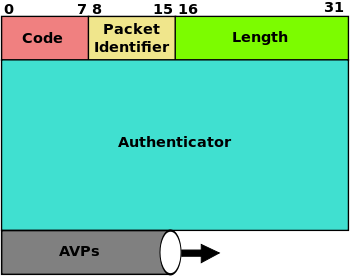
### Proxy operations

When a RADIUS server receives an AAA request for a user name containing a realm, the server will reference a table of configured realms. If the realm is known, the server will then *proxy* the request to the configured home server for that domain. The behaviour of the proxying server regarding the removal of the realm from the request ("stripping") is configuration-dependent on most servers. In addition, the proxying server can be configured to add, remove or rewrite AAA requests when they are proxied.

### Security

Roaming with RADIUS exposes the users to various security and privacy concerns. More generally, some roaming partners establish a secure tunnel between the RADIUS servers to ensure that users' credentials cannot be intercepted while being proxied across the internet. This is a concern as the MD5 hash built into RADIUS is considered insecure.[[6]](http://en.wikipedia.org/wiki/RADIUS#cite_note-5)

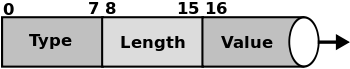
## Packet structure

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

RADIUS packet data format: The RADIUS packet data format is shown to the right. 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 by the [Internet Assigned Numbers Authority](http://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority) (IANA). However, prior to IANA allocation of ports 1812 and 1813, ports 1645 and 1646 (authentication and accounting, respectively) were used unofficially and became the default ports assigned by many RADIUS Client/Server implementations of the time. The tradition of using 1645 and 1646 for backwards compatibility continues to this day. For this reason many RADIUS Server implementations monitor both sets of UDP ports for RADIUS requests. [Microsoft](http://en.wikipedia.org/wiki/Microsoft) RADIUS servers default to 1812 and 1813. [Cisco](http://en.wikipedia.org/wiki/Cisco) RADIUS servers listen on RADIUS ports UDP 1645 and UDP 1812 for authentication; on ports 1646 and 1813 for accounting and can be configured with non-standard ports. [Juniper Networks](http://en.wikipedia.org/wiki/Juniper_Networks)' RADIUS servers listen on both unofficial and official ports 1645, 1812, 1646 and 1813 by default but can be configured with arbitrary ports.[SBR](https://download.juniper.net/software/aaa_802/public/sbr/docs/ref_61.pdf). [Cloudessa](http://en.wikipedia.org/w/index.php?title=Cloudessa&action=edit&redlink=1) and [Avaya](http://en.wikipedia.org/wiki/Avaya) virtual RADIUS solutions assign a pair of unique authentication and accounting ports to each virtual RADIUS server.

## [[edit](http://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=12)] Security

The RADIUS protocol does not transmit passwords in [cleartext](http://en.wikipedia.org/wiki/Cleartext) between the NAS and RADIUS server (not even with PAP protocol). Rather, a [shared secret](http://en.wikipedia.org/wiki/Shared_secret) is used along with the [MD5](http://en.wikipedia.org/wiki/MD5) hashing algorithm to obfuscate passwords. Because this particular implementation is not considered to be a very strong protection of the user's credentials,[[8]](http://en.wikipedia.org/wiki/RADIUS" \l "cite_note-7) additional protection, such as [IPsec](http://en.wikipedia.org/wiki/IPsec) tunnels or physically secured data-center networks, should be used to further protect the RADIUS traffic between the NAS device and the RADIUS server.

## [[edit](http://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=13)] RADIUS history

Several commercial and open-source RADIUS servers exist. Features can vary, but most can look up the users in text files, [LDAP](http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol) servers, various databases, etc. Accounting records can be written to text files, various databases, forwarded to external servers, etc. [SNMP](http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol) is often used for remote monitoring and keep-alive checking of a RADIUS server. RADIUS [proxy servers](http://en.wikipedia.org/wiki/Proxy_server) are used for centralized administration and can rewrite RADIUS packets on the fly (for security reasons, or to convert between vendor dialects).

The [Diameter](http://en.wikipedia.org/wiki/Diameter_(protocol)) protocol is the planned replacement for RADIUS. Diameter uses [SCTP](http://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol) or [TCP](http://en.wikipedia.org/wiki/Transmission_Control_Protocol) while RADIUS uses [UDP](http://en.wikipedia.org/wiki/User_Datagram_Protocol) as the [transport layer](http://en.wikipedia.org/wiki/Transport_layer).

**How Does RADIUS Work**?

## Introduction

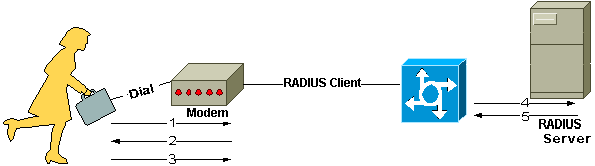
The Remote Authentication Dial-In User Service (RADIUS) protocol was developed by Livingston Enterprises, Inc., as an access server authentication and accounting protocol. leavingcisco.comobsoletes RFC 2139.

## 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. 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.



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.

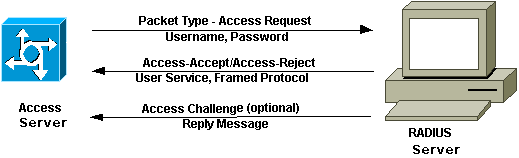
## Authentication and Authorization

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.

Typically, 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. The early deployment of RADIUS was done using UDP port number 1645, which conflicts with the "datametrics" 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 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. The figure below illustrates the 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, 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. 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](http://www.ietf.org/rfc/rfc2139.txt?number=2139) leavingcisco.com).

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