**Remote Authentication Dial-In User Service** (**RADIUS**) is a networking protocol, operating on port 1812, that provides centralized Authentication, Authorization, and Accounting ([AAA](https://en.wikipedia.org/wiki/AAA_(computer_security)) or Triple A) management for users who connect and use a network service. RADIUS was developed by Livingston Enterprises, Inc. in 1991 as an access server authentication and accounting protocol and later brought into the Internet Engineering Task Force (IETF) standards.

RADIUS is a [client/server](https://en.wikipedia.org/wiki/Client/server) protocol that runs in the [application layer](https://en.wikipedia.org/wiki/Application_layer), and can use either [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) or [UDP](https://en.wikipedia.org/wiki/User_Datagram_Protocol) as [transport](https://en.wikipedia.org/wiki/Transport_Layer). [Network access servers](https://en.wikipedia.org/wiki/Network_access_server), the gateways that control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server.[[1]](https://en.wikipedia.org/wiki/RADIUS#cite_note-ciscohow-1) RADIUS is often the [back-end](https://en.wikipedia.org/wiki/Back-end_database) of choice for [802.1X](https://en.wikipedia.org/wiki/802.1X) authentication as well.[[2]](https://en.wikipedia.org/wiki/RADIUS#cite_note-Brown2006-2)

The RADIUS server is usually a [background process](https://en.wikipedia.org/wiki/Background_process) running on a UNIX or Microsoft Windows server.[[1]](https://en.wikipedia.org/wiki/RADIUS#cite_note-ciscohow-1)



**Contents**

* [1Protocol components](https://en.wikipedia.org/wiki/RADIUS#Protocol_components)
  + [1.1Authentication and authorization](https://en.wikipedia.org/wiki/RADIUS#Authentication_and_authorization)
  + [1.2Accounting](https://en.wikipedia.org/wiki/RADIUS#Accounting)
* [2Roaming](https://en.wikipedia.org/wiki/RADIUS#Roaming)
  + [2.1Realms](https://en.wikipedia.org/wiki/RADIUS#Realms)
  + [2.2Proxy operations](https://en.wikipedia.org/wiki/RADIUS#Proxy_operations)
  + [2.3Security](https://en.wikipedia.org/wiki/RADIUS#Security)
* [3Packet structure](https://en.wikipedia.org/wiki/RADIUS#Packet_structure)
  + [3.1Attribute value pairs](https://en.wikipedia.org/wiki/RADIUS#Attribute_value_pairs)
* [4Vendor-specific attributes](https://en.wikipedia.org/wiki/RADIUS#Vendor-specific_attributes)
* [5Security](https://en.wikipedia.org/wiki/RADIUS#Security_2)
* [6History](https://en.wikipedia.org/wiki/RADIUS#History)
* [7Standards documentation](https://en.wikipedia.org/wiki/RADIUS#Standards_documentation)
* [8See also](https://en.wikipedia.org/wiki/RADIUS#See_also)
* [9References](https://en.wikipedia.org/wiki/RADIUS#References)
* [10Bibliography](https://en.wikipedia.org/wiki/RADIUS#Bibliography)
* [11External links](https://en.wikipedia.org/wiki/RADIUS#External_links)

Protocol components[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=1)]

RADIUS is an AAA protocol that manages network access. AAA stands for Authentication, Authorization and Accounting. RADIUS uses two packet types to manage the full AAA process: Access-Request, which manages authentication and authorization; and Accounting-Request, which manages accounting. [Authentication](https://en.wikipedia.org/wiki/Authentication) and [authorization](https://en.wikipedia.org/wiki/Authorization) are defined in [RFC 2865](https://tools.ietf.org/html/rfc2865) while [accounting](https://en.wikipedia.org/wiki/Accounting) is described by [RFC 2866](https://tools.ietf.org/html/rfc2866).

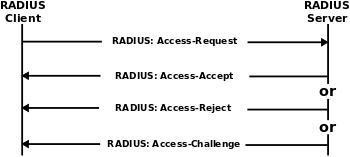
**Authentication and authorization**[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=2)]

The user or machine sends a request to a [Network Access Server](https://en.wikipedia.org/wiki/Network_Access_Server) (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS device via the [link-layer](https://en.wikipedia.org/wiki/Link-layer) protocol—for example, [Point-to-Point Protocol](https://en.wikipedia.org/wiki/Point-to-Point_Protocol) (PPP) in the case of many [dialup](https://en.wikipedia.org/wiki/Dialup) or [DSL](https://en.wikipedia.org/wiki/DSL) providers or posted in an [HTTPS](https://en.wikipedia.org/wiki/HTTPS) secure web form.

In turn, the NAS sends a RADIUS *Access Request* message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol.[[3]](https://en.wikipedia.org/wiki/RADIUS#cite_note-rfc2865-3)

This request includes access credentials, typically in the form of [username](https://en.wikipedia.org/wiki/Username) and [password](https://en.wikipedia.org/wiki/Password) or security certificate provided by the user. Additionally, the request may contain other information which the NAS knows about the user, such as its [network address](https://en.wikipedia.org/wiki/Network_address) or phone number, and information regarding the user's physical point of attachment to the NAS.

The RADIUS server checks that the information is correct using authentication schemes such as [PAP](https://en.wikipedia.org/wiki/Password_authentication_protocol), [CHAP](https://en.wikipedia.org/wiki/Challenge-handshake_authentication_protocol) or [EAP](https://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](https://en.wikipedia.org/wiki/SQL), [Kerberos](https://en.wikipedia.org/wiki/Kerberos_(protocol)), [LDAP](https://en.wikipedia.org/wiki/LDAP), or [Active Directory](https://en.wikipedia.org/wiki/Active_Directory) servers—to verify the user's credentials.

[](https://en.wikipedia.org/wiki/File:Drawing_RADIUS_1812.svg)

RADIUS Authentication and Authorization Flow

The RADIUS server then returns one of three responses to the NAS: 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 NAS.

**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. Again, this information may be stored locally on the RADIUS server, or may be 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.

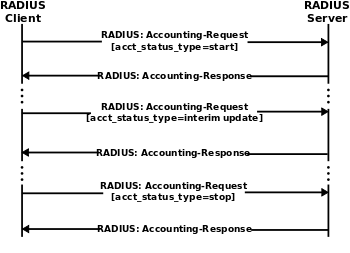
Authorization [attributes](https://en.wikipedia.org/wiki/Radius_Values) are conveyed to the NAS stipulating terms of access to be granted. For example, the following authorization attributes may be included in an Access-Accept:

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

When a client is configured to use RADIUS, any user of the client presents authentication information to the client. This might be with a customizable login prompt, where the user is expected to enter their username and password. Alternatively, the user might use a link framing protocol such as the Point-to-Point Protocol (PPP), which has authentication packets which carry this information.

Once the client has obtained such information, it may choose to authenticate using RADIUS. To do so, the client creates an "Access- Request" containing such Attributes as the user's name, the user's password, the ID of the client and the Port ID which the user is accessing. When a password is present, it is hidden using a method based on the RSA Message Digest Algorithm MD5.

**Accounting**[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=3)]

[](https://en.wikipedia.org/wiki/File:Drawing_RADIUS_1813.svg)

RADIUS Accounting Flow

Accounting is described in [RFC 2866](https://tools.ietf.org/html/rfc2866).

When network access is granted to the user by the [NAS](https://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.[[4]](https://en.wikipedia.org/wiki/RADIUS#cite_note-4)

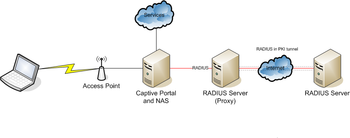
Periodically, *Interim Update* records (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value "interim-update") may be sent by the NAS to the RADIUS server, to update it on the status of an active session. "Interim" records typically convey the current session duration 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](https://en.wikipedia.org/wiki/Bill_(payment)) accordingly; the data is also commonly used for [statistical](https://en.wikipedia.org/wiki/Statistical) purposes and for general network monitoring.

Roaming[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=4)]

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

Roaming using a proxy RADIUS AAA server.

RADIUS is commonly used to facilitate [roaming](https://en.wikipedia.org/wiki/Roaming) between [ISPs](https://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](https://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**[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=5)]

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.

Realms can also be compounded using both prefix and postfix notation, to allow for complicated roaming scenarios; for example, somedomain.com\username@anotherdomain.com could be a valid username with two realms.

Although realms often resemble domains, it is important to note that realms are in fact arbitrary text and need not contain real domain names. Realm formats are standardized in [RFC 4282](https://tools.ietf.org/html/rfc4282), which defines a Network Access Identifier (NAI) in the form of 'user@realm'. In that specification, the 'realm' portion is required to be a domain name. However, this practice is not always followed. [RFC 7542](https://tools.ietf.org/html/rfc7542)[[5]](https://en.wikipedia.org/wiki/RADIUS#cite_note-5) replaced [RFC 4282](https://tools.ietf.org/html/rfc4282) in May 2015.

**Proxy operations**[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=6)]

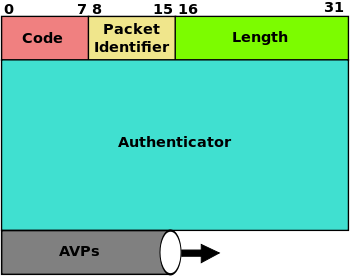
When a RADIUS server receives an AAA request for a user name containing a realm, the server will reference a table of configured realms. If the realm is known, the server will then *proxy* the request to the configured home server for that domain. The behavior of the proxying server regarding the removal 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 over time again.

Proxy Chaining is possible in RADIUS and authentication/authorization and accounting packets are usually routed between a NAS Device and a Home server through a series of proxies. Some of advantages of using Proxy chains include scalability improvements, policy implementations and capability adjustments. But in roaming scenarios, the NAS, Proxies and Home Server could be typically managed by different administrative entities. Hence, the trust factor among the proxies gains more significance under such Inter-domain applications. Further, the absence of end to end security in RADIUS adds to the criticality of trust among the Proxies involved. Proxy Chains are explained in [RFC 2607](https://tools.ietf.org/html/rfc2607).

**Security**[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=7)]

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]](https://en.wikipedia.org/wiki/RADIUS#cite_note-6)

Packet structure[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=8)]

[](https://en.wikipedia.org/wiki/File:RADIUS_packet_format.svg)

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.

RADIUS Codes (decimal) are assigned as follows:

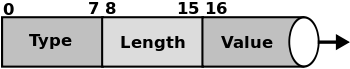
|  |  |
| --- | --- |
| **Code** | **Assignment** |
| 1 | Access-Request |
| 2 | Access-Accept |
| 3 | Access-Reject |
| 4 | Accounting-Request |
| 5 | Accounting-Response |
| 11 | Access-Challenge |
| 12 | Status-Server (experimental) |
| 13 | Status-Client (experimental) |
| 40 | Disconnect-Request |
| 41 | Disconnect-ACK |
| 42 | Disconnect-NAK |
| 43 | CoA-Request |
| 44 | CoA-ACK |
| 45 | CoA-NAK |
| 255 | Reserved |

The Identifier field aids in matching requests and replies.

The Length field indicates the length of the entire RADIUS packet including the Code, Identifier, Length, Authenticator and optional Attribute fields.

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**[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=9)]

[](https://en.wikipedia.org/wiki/File:RADIUS_AVP_layout.svg)

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.

|  |  |
| --- | --- |
| show**AVP type** | **Assignment** |

Vendor-specific attributes[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=10)]

RADIUS is extensible; many vendors of RADIUS hardware and software implement their own variants using Vendor-Specific Attributes (VSAs). Microsoft has published some of their VSAs.[[7]](https://en.wikipedia.org/wiki/RADIUS#cite_note-7) VSA definitions from many other companies remain proprietary and/or ad-hoc, nonetheless many VSA dictionaries can be found by downloading the source code of open source RADIUS implementations, for example [FreeRADIUS](https://en.wikipedia.org/wiki/FreeRADIUS) or openRADIUS.

Security[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=11)]

The RADIUS protocol transmits obfuscated passwords using a [shared secret](https://en.wikipedia.org/wiki/Shared_secret) and the [MD5](https://en.wikipedia.org/wiki/MD5) hashing algorithm. As this particular implementation provides only weak protection of the user's credentials,[[8]](https://en.wikipedia.org/wiki/RADIUS#cite_note-8) additional protection, such as [IPsec](https://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. Additionally, the user's security credentials are the only part protected by RADIUS itself, yet other user-specific attributes such as tunnel-group IDs or vlan memberships passed over RADIUS may be considered sensitive (helpful to an attacker) or private (sufficient to identify the individual client) information as well.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] The [RadSec](https://en.wikipedia.org/wiki/RadSec) protocol claims to solve aforementioned security issues.

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

As more dial-up customers used the [NSFnet](https://en.wikipedia.org/wiki/NSFnet) a [request for proposal](https://en.wikipedia.org/wiki/Request_for_proposal) was sent out by [Merit Network](https://en.wikipedia.org/wiki/Merit_Network) in 1991 to consolidate their various proprietary authentication, authorization and accounting systems. Among the early respondents was Livingston Enterprises and an early version of the RADIUS was written after a meeting. The early RADIUS server was installed on a [UNIX](https://en.wikipedia.org/wiki/UNIX) [operating system](https://en.wikipedia.org/wiki/Operating_system). Livingston Enterprises was acquired by [Lucent](https://en.wikipedia.org/wiki/Lucent) and together with Merit steps were taken to gain industry acceptance for RADIUS as a protocol. Both companies offered a RADIUS server at no charge.[[9]](https://en.wikipedia.org/wiki/RADIUS#cite_note-9) RADIUS was in 1997 published as [RFC 2058](https://tools.ietf.org/html/rfc2058) and [RFC 2059](https://tools.ietf.org/html/rfc2059), current versions are [RFC 2865](https://tools.ietf.org/html/rfc2865) and [RFC 2866](https://tools.ietf.org/html/rfc2866).[[10]](https://en.wikipedia.org/wiki/RADIUS#cite_note-Vollbrecht2006-10)

The original RADIUS standard specified that RADIUS is [stateless](https://en.wikipedia.org/wiki/Stateless_protocol) and should run over the [User Datagram Protocol](https://en.wikipedia.org/wiki/User_Datagram_Protocol) (UDP). For authentication it was envisaged that RADIUS should support the [Password Authentication Protocol](https://en.wikipedia.org/wiki/Password_Authentication_Protocol) (PAP) and the [Challenge-Handshake Authentication Protocol](https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol) (CHAP) over the [Point-to-Point Protocol](https://en.wikipedia.org/wiki/Point-to-Point_Protocol). Passwords are hidden by taking the [MD5](https://en.wikipedia.org/wiki/MD5) hash of the packet and a shared secret, and then XORing that hash with the password. The original RADIUS also provided more than 50 attribute or value pairs, with the possibility for vendors to configure their own pairs.[[11]](https://en.wikipedia.org/wiki/RADIUS#cite_note-11)

The choice of the hop-by-hop security model, rather than [end-to-end encryption](https://en.wikipedia.org/wiki/End-to-end_encryption), meant that if several proxy RADIUS servers are in use, every server must examine, perform logic on and pass on all data in a request. This exposes data such as passwords and certificates at every hop. RADIUS servers also did not have the ability to stop access to resources once an authorisation had been issued. Subsequent standards such as [RFC 3576](https://tools.ietf.org/html/rfc3576) and its successor [RFC 5176](https://tools.ietf.org/html/rfc5176) allowed for RADIUS servers to dynamically change a users authorization, or to disconnect a user entirely.

Now, several commercial and open-source RADIUS servers exist. Features can vary, but most can look up the users in text files, [LDAP](https://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](https://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](https://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](https://en.wikipedia.org/wiki/Diameter_(protocol)) protocol was intended as the replacement for RADIUS. While both are Authentication, Authorization, and Accounting (AAA) protocols, the use-cases for the two protocols have since diverged. Diameter is largely used in the [3G](https://en.wikipedia.org/wiki/3G) space. RADIUS is used elsewhere. One of the largest barriers to having Diameter replace RADIUS is that [switches](https://en.wikipedia.org/wiki/Network_Switch) and [Access Points](https://en.wikipedia.org/wiki/Wireless_Access_Point) typically implement RADIUS, but not Diameter. Diameter uses [SCTP](https://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol) or [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) while RADIUS typically uses [UDP](https://en.wikipedia.org/wiki/User_Datagram_Protocol) as the [transport layer](https://en.wikipedia.org/wiki/Transport_layer). As of 2012, RADIUS can also use TCP as the transport layer with [TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security) for security.

Standards documentation[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=13)]

The RADIUS protocol is currently defined in the following [IETF](https://en.wikipedia.org/wiki/IETF) RFC documents.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **RFC** | **Title** | **Date published** | **Related article** | **Related RFCs** | **Notes** |
| [RFC 2058](https://tools.ietf.org/html/rfc2058) | Remote Authentication Dial In User Service (RADIUS) | January 1997 | RADIUS | Obsoleted by [RFC 2138](https://tools.ietf.org/html/rfc2138) |  |
| [RFC 2059](https://tools.ietf.org/html/rfc2059) | RADIUS Accounting | January 1997 | RADIUS | Obsoleted by [RFC 2139](https://tools.ietf.org/html/rfc2139) |  |
| [RFC 2138](https://tools.ietf.org/html/rfc2138) | Remote Authentication Dial In User Service (RADIUS) | April 1997 | RADIUS | Obsoleted by [RFC 2865](https://tools.ietf.org/html/rfc2865) |  |
| [RFC 2139](https://tools.ietf.org/html/rfc2139) | RADIUS Accounting | April 1997 | RADIUS | Obsoleted by [RFC 2866](https://tools.ietf.org/html/rfc2866) |  |
| [RFC 2548](https://tools.ietf.org/html/rfc2548) | Microsoft Vendor-specific RADIUS Attributes | March 1999 | RADIUS |  |  |
| [RFC 2607](https://tools.ietf.org/html/rfc2607) | Proxy Chaining and Policy Implementation in Roaming | June 1999 |  |  |  |
| [RFC 2618](https://tools.ietf.org/html/rfc2618) | RADIUS Authentication Client MIB |  | [Management information base](https://en.wikipedia.org/wiki/Management_information_base) | Obsoleted by [RFC 4668](https://tools.ietf.org/html/rfc4668) |  |
| [RFC 2619](https://tools.ietf.org/html/rfc2619) | RADIUS Authentication Server MIB |  | [Management information base](https://en.wikipedia.org/wiki/Management_information_base) | Obsoleted by [RFC 4669](https://tools.ietf.org/html/rfc4669) |  |
| [RFC 2620](https://tools.ietf.org/html/rfc2620) | RADIUS Accounting Client MIB | June 1999 | [Management information base](https://en.wikipedia.org/wiki/Management_information_base) | Obsoleted by [RFC 4670](https://tools.ietf.org/html/rfc4670) |  |
| [RFC 2621](https://tools.ietf.org/html/rfc2621) | RADIUS Accounting Server MIB | June 1999 | [Management information base](https://en.wikipedia.org/wiki/Management_information_base) | Obsoleted by [RFC 4671](https://tools.ietf.org/html/rfc4671) |  |
| [RFC 2809](https://tools.ietf.org/html/rfc2809) | Implementation of [L2TP](https://en.wikipedia.org/wiki/L2TP) Compulsory Tunneling via RADIUS | April 2000 |  |  |  |
| [RFC 2865](https://tools.ietf.org/html/rfc2865) | Remote Authentication Dial In User Service (RADIUS) | June 2000 | RADIUS | Updated by [RFC 2868](https://tools.ietf.org/html/rfc2868), [RFC 3575](https://tools.ietf.org/html/rfc3575), [RFC 5080](https://tools.ietf.org/html/rfc5080) | This standard describes RADIUS authentication and authorization between a Network Access Server (NAS) and a shared RADIUS authentication server. This protocol is also used to carry configuration information from the RADIUS server to the NAS. |
| [RFC 2866](https://tools.ietf.org/html/rfc2866) | RADIUS Accounting | June 2000 | RADIUS |  | This standard describes how accounting information is carried from the NAS to a shared RADIUS accounting server. |
| [RFC 2867](https://tools.ietf.org/html/rfc2867) | RADIUS Accounting Modifications for Tunnel Protocol Support | June 2000 | RADIUS | Updates [RFC 2866](https://tools.ietf.org/html/rfc2866) |  |
| [RFC 2868](https://tools.ietf.org/html/rfc2868) | RADIUS Attributes for Tunnel Protocol Support | June 2000 |  | Updates [RFC 2865](https://tools.ietf.org/html/rfc2865) |  |
| [RFC 2869](https://tools.ietf.org/html/rfc2869) | RADIUS Extensions | June 2000 |  | Updated by [RFC 3579](https://tools.ietf.org/html/rfc3579), [RFC 5080](https://tools.ietf.org/html/rfc5080) |  |
| [RFC 2882](https://tools.ietf.org/html/rfc2882) | Network Access Servers Requirements: Extended RADIUS Practices | July 2000 |  |  |  |
| [RFC 3162](https://tools.ietf.org/html/rfc3162) | RADIUS and [IPv6](https://en.wikipedia.org/wiki/IPv6) | August 2001 |  |  |  |
| [RFC 3575](https://tools.ietf.org/html/rfc3575) | IANA Considerations for RADIUS | July 2003 |  |  |  |
| [RFC 3576](https://tools.ietf.org/html/rfc3576) | Dynamic Authorization Extensions to RADIUS | July 2003 |  | Obsoleted by [RFC 5176](https://tools.ietf.org/html/rfc5176) |  |
| [RFC 3579](https://tools.ietf.org/html/rfc3579) | RADIUS Support for EAP | September 2003 | [Extensible Authentication Protocol](https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol) | Updates [RFC 2869](https://tools.ietf.org/html/rfc2869) |  |
| [RFC 3580](https://tools.ietf.org/html/rfc3580) | IEEE 802.1X RADIUS Usage Guidelines | September 2003 | [802.1X](https://en.wikipedia.org/wiki/802.1X) |  |  |
| [RFC 4014](https://tools.ietf.org/html/rfc4014) | RADIUS Attributes Suboption for the DHCP Relay Agent Information Option | February 2005 |  |  |  |
| [RFC 4372](https://tools.ietf.org/html/rfc4372) | Chargeable User Identity | January 2006 |  |  |  |
| [RFC 4590](https://tools.ietf.org/html/rfc4590) | RADIUS Extension for Digest Authentication | July 2006 |  | Obsoleted by [RFC 5090](https://tools.ietf.org/html/rfc5090) |  |
| [RFC 4668](https://tools.ietf.org/html/rfc4668) | RADIUS Authentication Client MIB for IPv6 | August 2006 | [Management information base](https://en.wikipedia.org/wiki/Management_information_base) |  |  |
| [RFC 4669](https://tools.ietf.org/html/rfc4669) | RADIUS Authentication Server MIB for IPv6 | August 2006 | [Management information base](https://en.wikipedia.org/wiki/Management_information_base) |  |  |
| [RFC 4670](https://tools.ietf.org/html/rfc4670) | RADIUS Accounting Client MIB for IPv6 | August 2006 | [Management information base](https://en.wikipedia.org/wiki/Management_information_base) |  |  |
| [RFC 4671](https://tools.ietf.org/html/rfc4671) | RADIUS Accounting Server MIB for IPv6 | August 2006 | [Management information base](https://en.wikipedia.org/wiki/Management_information_base) |  |  |
| [RFC 4675](https://tools.ietf.org/html/rfc4675) | RADIUS Attributes for Virtual LAN and Priority Support | September 2006 |  |  |  |
| [RFC 4679](https://tools.ietf.org/html/rfc4679) | DSL Forum Vendor-Specific RADIUS Attributes | September 2006 |  |  |  |
| [RFC 4818](https://tools.ietf.org/html/rfc4818) | RADIUS Delegated-IPv6-Prefix Attribute | April 2007 |  |  |  |
| [RFC 4849](https://tools.ietf.org/html/rfc4849) | RADIUS Filter Rule Attribute | April 2007 |  |  |  |
| [RFC 5080](https://tools.ietf.org/html/rfc5080) | Common RADIUS Implementation Issues and Suggested Fixes | December 2007 |  | Updates [RFC 3579](https://tools.ietf.org/html/rfc3579) |  |
| [RFC 5090](https://tools.ietf.org/html/rfc5090) | RADIUS Extension for Digest Authentication | February 2008 |  |  |  |
| [RFC 5176](https://tools.ietf.org/html/rfc5176) | Dynamic Authorization Extensions to RADIUS | January 2008 |  |  |  |
| [RFC 5607](https://tools.ietf.org/html/rfc5607) | RADIUS Authorization for NAS Management | July 2009 |  |  |  |
| [RFC 5997](https://tools.ietf.org/html/rfc5997) | Use of Status-Server Packets in the RADIUS Protocol | August 2010 |  | Updates [RFC 2866](https://tools.ietf.org/html/rfc2866) |  |
| [RFC 6158](https://tools.ietf.org/html/rfc6158) | RADIUS Design Guidelines | March 2011 |  |  |  |
| [RFC 6218](https://tools.ietf.org/html/rfc6218) | Cisco Vendor-Specific RADIUS Attributes for the Delivery of Keying Material | April 2011 |  |  |  |
| [RFC 6421](https://tools.ietf.org/html/rfc6421) | Crypto-Agility Requirements for Remote Authentication Dial-In User Service (RADIUS) | November 2011 |  |  |  |
| [RFC 6613](https://tools.ietf.org/html/rfc6613) | RADIUS over TCP | May 2012 |  | Experimental |  |
| [RFC 6614](https://tools.ietf.org/html/rfc6614) | Transport Layer Security (TLS) Encryption for RADIUS | May 2012 |  | Experimental |  |
| [RFC 6911](https://tools.ietf.org/html/rfc6911) | RADIUS Attributes for IPv6 Access Networks | April 2013 |  | Standards track |  |
| [RFC 6929](https://tools.ietf.org/html/rfc6929) | Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions | April 2013 |  | Updates [RFC 2865](https://tools.ietf.org/html/rfc2865), [RFC 3575](https://tools.ietf.org/html/rfc3575), [RFC 6158](https://tools.ietf.org/html/rfc6158) |  |
| [RFC 7360](https://tools.ietf.org/html/rfc7360) | Datagram Transport Layer Security (DTLS) as a Transport Layer for RADIUS | September 2014 |  | Experimental |  |
| [RFC 7585](https://tools.ietf.org/html/rfc7585) | Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI) | Oct 2015 |  | Experimental |  |
| [RFC 8044](https://tools.ietf.org/html/rfc8044) | Data Types in RADIUS | January 2017 |  | Updates: 2865, 3162, 4072, 6158, 6572, 7268 |  |

See also[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=14)]

* [802.1X](https://en.wikipedia.org/wiki/802.1X)
* [Diameter (protocol)](https://en.wikipedia.org/wiki/Diameter_(protocol))
* [Kerberos (protocol)](https://en.wikipedia.org/wiki/Kerberos_(protocol))
* [Security Assertion Markup Language](https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language)
* [TACACS](https://en.wikipedia.org/wiki/TACACS)
* [TACACS+](https://en.wikipedia.org/wiki/TACACS%2B)

References[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=15)]

* 1. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/RADIUS#cite_ref-ciscohow_1-0) [***b***](https://en.wikipedia.org/wiki/RADIUS#cite_ref-ciscohow_1-1) [*"How Does RADIUS Work?"*](http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml)*.*[*Cisco*](https://en.wikipedia.org/wiki/Cisco)*. 2006-01-19. Retrieved 2009-04-15.*
  2. [**^**](https://en.wikipedia.org/wiki/RADIUS#cite_ref-Brown2006_2-0) *Edwin Lyle Brown (2006).*[*802.1X Port-Based Authentication*](https://books.google.com/books?id=nlbrC3KLvCAC&pg=PA17)*. Taylor & Francis. p. 17.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-1-4200-4465-2*](https://en.wikipedia.org/wiki/Special:BookSources/978-1-4200-4465-2)*.*
  3. [**^**](https://en.wikipedia.org/wiki/RADIUS#cite_ref-rfc2865_3-0) [RFC 2865](https://tools.ietf.org/html/rfc2865) Remote Authentication Dial In User Service (RADIUS)
  4. [**^**](https://en.wikipedia.org/wiki/RADIUS#cite_ref-4) [RFC 2866](https://tools.ietf.org/html/rfc2866) RADIUS Accounting
  5. [**^**](https://en.wikipedia.org/wiki/RADIUS#cite_ref-5) <https://tools.ietf.org/html/rfc7542>
  6. [**^**](https://en.wikipedia.org/wiki/RADIUS#cite_ref-6) *Alexander Sotirov; Marc Stevens; Jacob Appelbaum; Arjen Lenstra; David Molnar; Dag Arne Osvik; Benne de Weger (2008-12-08).*[*"MD5 considered harmful today - Creating a rogue CA certificate"*](http://www.win.tue.nl/hashclash/rogue-ca/)*.*[*Technische Universiteit Eindhoven*](https://en.wikipedia.org/wiki/Technische_Universiteit_Eindhoven)*. Retrieved 2009-04-19.*
  7. [**^**](https://en.wikipedia.org/wiki/RADIUS#cite_ref-7) [RFC 2548](https://tools.ietf.org/html/rfc2548)
  8. [**^**](https://en.wikipedia.org/wiki/RADIUS#cite_ref-8) [An Analysis of the RADIUS Authentication Protocol](http://www.untruth.org/~josh/security/radius/radius-auth.html)
  9. [**^**](https://en.wikipedia.org/wiki/RADIUS#cite_ref-9) *Jonathan Hassell (2003). RADIUS: Securing Public Access to Private Resources. O'Reilly Media. pp. 15–16.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*9780596003227*](https://en.wikipedia.org/wiki/Special:BookSources/9780596003227)*.*
  10. [**^**](https://en.wikipedia.org/wiki/RADIUS#cite_ref-Vollbrecht2006_10-0) *John Vollbrecht (2006).*[*"The Beginnings and History of RADIUS"*](http://www.interlinknetworks.com/app_notes/History%20of%20RADIUS.pdf)*(PDF). Interlink Networks. Retrieved 2009-04-15.*
  11. [**^**](https://en.wikipedia.org/wiki/RADIUS#cite_ref-11) *Jonathan Hassell (2003). RADIUS: Securing Public Access to Private Resources. O'Reilly Media. p. 16.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*9780596003227*](https://en.wikipedia.org/wiki/Special:BookSources/9780596003227)*.*

Bibliography[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=16)]

* *Hassell, Jonathan (2002).*[*RADIUS - Securing Public Access to Private Resources*](http://oreilly.com/catalog/9780596003227/)*. O'Reilly & Associates.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*0-596-00322-6*](https://en.wikipedia.org/wiki/Special:BookSources/0-596-00322-6)*. Retrieved 2009-04-17.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=RADIUS&action=edit&section=17)]

* [Radius Types](http://www.iana.org/assignments/radius-types/radius-types.xhtml)
* [An Analysis of the RADIUS Authentication Protocol](http://www.untruth.org/~josh/security/radius/radius-auth.html)
* [Decoding a Sniffer-trace of RADIUS Transaction](http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080093f42.shtml)
* [Using Wireshark to debug RADIUS](https://wiki.wireshark.org/Radius)