RADIUS

Remote Authentication Dial-In User Service (**RADIUS**) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service. RADIUS was developed by Livingston Enterprises in 1991 as an access server authentication and accounting protocol. It was later brought into IEEE 802 and IETF standards.

RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP. Network access servers, which control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server.[1] RADIUS is often the back-end of choice for 802.1X authentication.[2] A RADIUS server is usually a background process running on UNIX or Microsoft Windows.[1]

Protocol components

RADIUS is an AAA (authentication, authorization, and accounting) protocol that manages network access. RADIUS uses two types of packets to manage the full AAA process: Access-Request, which manages authentication and authorization; and Accounting-Request, which manages accounting. Authentication and authorization are defined in RFC 2865 while accounting is described by RFC 2866.

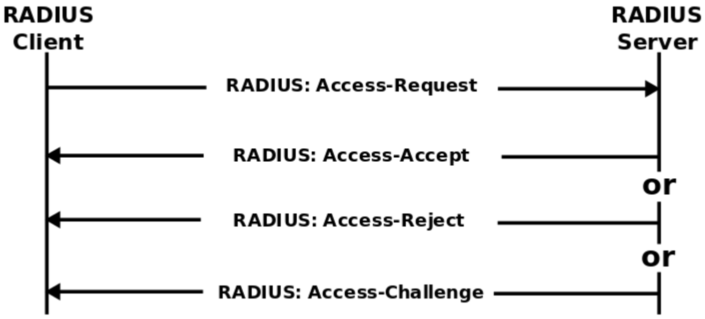
Authentication and authorization

The user or machine sends a request to a 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 protocol—for example, Point-to-Point Protocol (PPP) in the case of many dialup or DSL providers or posted in an 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]

This request includes access credentials, typically in the form of username and 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 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, CHAP or EAP. 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, Kerberos, LDAP, or Active Directory servers—to verify the user's credentials.



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.

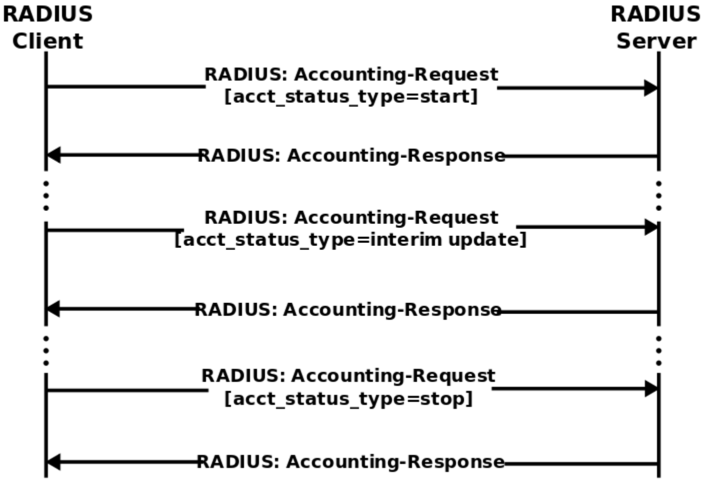
Authorization attributes are conveyed to the NAS stipulating terms of access to be granted. For example, the following authorization attributes may be included in an Access-Accept:

- The specific IP address 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 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


RADIUS Client
RADIUS Server
RADIUS: Accounting-Request [acct_status_type=start]
RADIUS: Accounting-Response
RADIUS: Accounting-Request [acct_status_type=interim update]
RADIUS: Accounting-Response
RADIUS: Accounting-Request [acct_status_type=stop]
RADIUS: Accounting-Response

RADIUS Accounting Flow

Accounting is described in RFC 2866.

When network access is granted to the user by the NAS, 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]

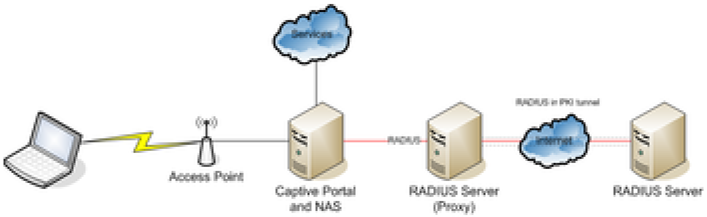
Periodically, *Interim Update* records (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value "interim-update") may be sent by the NAS to the RADIUS server, to update it on the status of an active session. "Interim" records typically convey the current session duration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

Roaming



Roaming using a proxy RADIUS AAA server.

RADIUS is commonly used to facilitate roaming between ISPs, including by:

- Companies which provide a single global set of credentials that are usable on many public networks;
- 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.

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.

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, 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[5] replaced RFC 4282 in May 2015.

Proxy operations

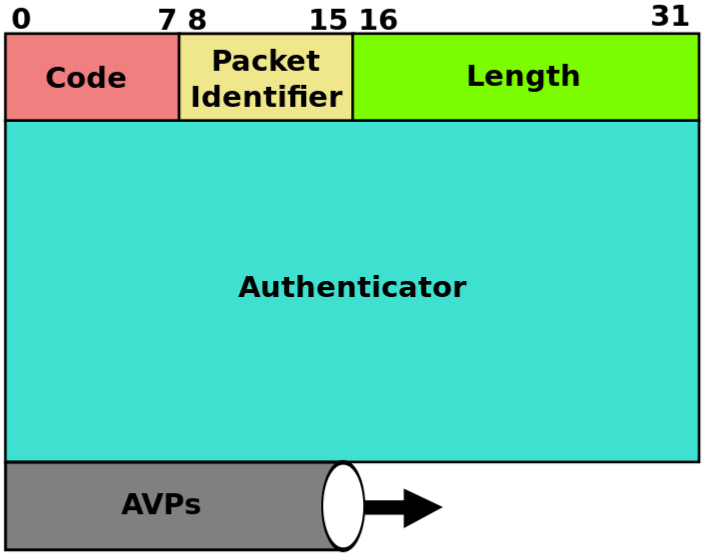
When a RADIUS server receives an AAA request for a user name containing a realm, the server will reference a table of configured realms. If the realm is known, the server will then *proxy* the request to the configured home server for that domain. The behavior of the proxying server regarding the removal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

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]

Packet structure



RADIUS packet data format.

RADIUS is transported over UDP/IP on ports 1812 and 1813.[7]

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.

Assigned RADIUS Codes (decimal) include the following:[8]

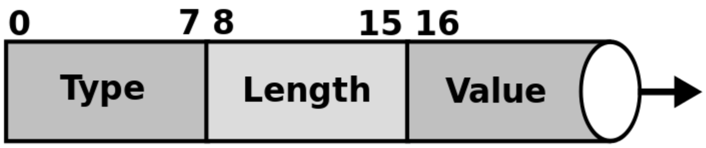
Code	Assignment
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
40	Disconnect-Request
41	Disconnect-ACK
42	Disconnect-NAK
43	CoA-Request
44	CoA-ACK
45	CoA-NAK
255	Reserved

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



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.

AVP type	Assignment
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
9	Framed-IP-Netmask
10	Framed-Routing
11	Filter-Id
12	Framed-MTU
13	Framed-Compression
14	Login-IP-Host
15	Login-Service
16	Login-TCP-Port
18	Reply-Message
19	Callback-Number
20	Callback-Id
22	Framed-Route
23	Framed-IPX-Network
24	State
25	Class
26	Vendor-Specific
27	Session-Timeout
28	Idle-Timeout
29	Termination-Action
30	Called-Station-Id

31	Calling-Station-Id
32	NAS-Identifier
33	Proxy-State
34	Login-LAT-Service
35	Login-LAT-Node
36	Login-LAT-Group
37	Framed-AppleTalk-Link
38	Framed-AppleTalk-Network
39	Framed-AppleTalk-Zone
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
50	Acct-Multi-Session-Id
51	Acct-Link-Count
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
55	Event-Timestamp
56	Egress-VLANID
57	Ingress-Filters
58	Egress-VLAN-Name
59	User-Priority-Table
60	CHAP-Challenge

61	NAS-Port-Type
62	Port-Limit
63	Login-LAT-Port
64	Tunnel-Type
65	Tunnel-Medium-Type
66	Tunnel-Client-Endpoint
67	Tunnel-Server-Endpoint
68	Acct-Tunnel-Connection
69	Tunnel-Password
70	ARAP-Password
71	ARAP-Features
72	ARAP-Zone-Access
73	ARAP-Security
74	ARAP-Security-Data
75	Password-Retry
76	Prompt
77	Connect-Info
78	Configuration-Token
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
82	Tunnel-Assignment-ID
83	Tunnel-Preference
84	ARAP-Challenge-Response
85	Acct-Interim-Interval
86	Acct-Tunnel-Packets-Lost
87	NAS-Port-Id
88	Framed-Pool

89	CUI
90	Tunnel-Client-Auth-ID
91	Tunnel-Server-Auth-ID
92	NAS-Filter-Rule
94	Originating-Line-Info
95	NAS-IPv6-Address
96	Framed-Interface-Id
97	Framed-IPv6-Prefix
98	Login-IPv6-Host
99	Framed-IPv6-Route
100	Framed-IPv6-Pool
101	Error-Cause Attribute
102	EAP-Key-Name
103	Digest-Response
104	Digest-Realm
105	Digest-Nonce
106	Digest-Response-Auth
107	Digest-Nextnonce
108	Digest-Method
109	Digest-URI
110	Digest-Qop
111	Digest-Algorithm
112	Digest-Entity-Body-Hash
113	Digest-CNonce
114	Digest-Nonce-Count
115	Digest-Username
116	Digest-Opaque
117	Digest-Auth-Param
118	Digest-AKA-Auts

119	Digest-Domain
120	Digest-Stale
121	Digest-HA1
122	SIP-AOR
123	Delegated-IPv6-Prefix
124	MIP6-Feature-Vector
125	MIP6-Home-Link-Prefix
126	Operator-Name
127	Location-Information
128	Location-Data
129	Basic-Location-Policy-Rules
130	Extended-Location-Policy-Rules
131	Location-Capable
132	Requested-Location-Info
133	Framed-Management-Protocol
134	Management-Transport-Protection
135	Management-Policy-Id
136	Management-Privilege-Level
137	PKM-SS-Cert
138	PKM-CA-Cert
139	PKM-Config-Settings
140	PKM-Cryptosuite-List
141	PKM-SAID
142	PKM-SA-Descriptor
143	PKM-Auth-Key
144	DS-Lite-Tunnel-Name
145	Mobile-Node-Identifier
146	Service-Selection
147	PMIP6-Home-LMA-IPv6-Address

148	PMIP6-Visited-LMA-IPv6-Address
149	PMIP6-Home-LMA-IPv4-Address
150	PMIP6-Visited-LMA-IPv4-Address
151	PMIP6-Home-HN-Prefix
152	PMIP6-Visited-HN-Prefix
153	PMIP6-Home-Interface-ID
154	PMIP6-Visited-Interface-ID
155	PMIP6-Home-IPv4-HoA
156	PMIP6-Visited-IPv4-HoA
157	PMIP6-Home-DHCP4-Server-Address
158	PMIP6-Visited-DHCP4-Server-Address
159	PMIP6-Home-DHCP6-Server-Address
160	PMIP6-Visited-DHCP6-Server-Address
161	PMIP6-Home-IPv4-Gateway
162	PMIP6-Visited-IPv4-Gateway
163	EAP-Lower-Layer
164	GSS-Acceptor-Service-Name
165	GSS-Acceptor-Host-Name
166	GSS-Acceptor-Service-Specifics
167	GSS-Acceptor-Realm-Name
168	Framed-IPv6-Address
169	DNS-Server-IPv6-Address
170	Route-IPv6-Information
171	Delegated-IPv6-Prefix-Pool
172	Stateful-IPv6-Address-Pool
173	IPv6-6rd-Configuration
174	Allowed-Called-Station-Id
175	EAP-Peer-Id
176	EAP-Server-Id

177	Mobility-Domain-Id
178	Preauth-Timeout
179	Network-Id-Name
180	EAPoL-Announcement
181	WLAN-HESSID
182	WLAN-Venue-Info
183	WLAN-Venue-Language
184	WLAN-Venue-Name
185	WLAN-Reason-Code
186	WLAN-Pairwise-Cipher
187	WLAN-Group-Cipher
188	WLAN-AKM-Suite
189	WLAN-Group-Mgmt-Cipher
190	WLAN-RF-Band

Vendor-specific attributes

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.[9] 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.

Security

The RADIUS protocol transmits obfuscated passwords using a shared secret and the MD5 hashing algorithm. As this particular implementation provides only weak protection of the user's credentials,[10] additional protection, such as 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. The RadSec protocol claims to solve aforementioned security issues.

History

As more dial-up customers used the NSFNET a request for proposal was sent out by 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 operating system. Livingston Enterprises was acquired by 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.[11] In 1997 RADIUS was published as RFC 2058 and RFC 2059, current versions are RFC 2865 and RFC 2866.[12]

The original RADIUS standard specified that RADIUS is stateless and should run over the User Datagram Protocol (UDP). For authentication it was envisaged that RADIUS should support the Password Authentication Protocol (PAP) and the Challenge-Handshake Authentication Protocol (CHAP) over the Point-to-Point Protocol. Passwords are hidden by taking the 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-value pairs, with the possibility for vendors to configure their own pairs.[13]

The choice of the hop-by-hop security model, rather than 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 and its successor RFC 5176 allowed for RADIUS servers to dynamically change a users authorization, or to disconnect a user entirely.[14]

Now, several commercial and open-source RADIUS servers exist. Features can vary, but most can look up the users in text files, LDAP servers, various databases, etc. Accounting records can be written to text files, various databases, forwarded to external servers, etc. SNMP is often used for remote monitoring and keep-alive checking of a RADIUS server. RADIUS proxy servers are used for centralized administration and can rewrite RADIUS packets on the fly for security reasons, or to convert between vendor dialects.

The Diameter 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 space. RADIUS is used elsewhere. One of the largest barriers to having Diameter replace RADIUS is that switches and Access Points typically implement RADIUS, but not Diameter. Diameter uses SCTP or TCP while RADIUS typically uses UDP as the transport layer. As of 2012, RADIUS can also use TCP as the transport layer with TLS for security.

Standards documentation

The RADIUS protocol is currently defined in the following IETF RFC documents.

RFC	Title	Date published	Related article	Related RFCs	Note
RFC 2058	Remote Authentication Dial In User Service (RADIUS)	January 1997	RADIUS	Obsoleted by RFC 2138	
RFC 2059	RADIUS Accounting	January 1997	RADIUS	Obsoleted by RFC 2139	
RFC 2138	Remote Authentication Dial In User Service (RADIUS)	April 1997	RADIUS	Obsoleted by RFC 2865	
RFC 2139	RADIUS Accounting	April 1997	RADIUS	Obsoleted by RFC 2866	
RFC 2548	Microsoft Vendor-specific RADIUS Attributes	March 1999	RADIUS		
RFC 2607	Proxy Chaining and Policy Implementation in Roaming	June 1999			
RFC 2618	RADIUS Authentication Client MIB		Management information base	Obsoleted by RFC 4668	
RFC 2619	RADIUS Authentication Server MIB		Management information base	Obsoleted by RFC 4669	
RFC 2620	RADIUS Accounting Client MIB	June 1999	Management information base	Obsoleted by RFC 4670	
RFC 2621	RADIUS Accounting Server MIB	June 1999	Management information base	Obsoleted by RFC 4671	

RFC 2809	Implementation of L2TP Compulsory Tunneling via RADIUS	April 2000			
RFC 2865	Remote Authentication Dial In User Service (RADIUS)	June 2000	RADIUS	Updated by RFC 2868, RFC 3575, RFC 5080	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	RADIUS Accounting	June 2000	RADIUS		This standard describes how accounting information is carried from the NAS to a shared RADIUS accounting server.
RFC 2867	RADIUS Accounting Modifications for	June 2000	RADIUS	Updates RFC 2866	

	Tunnel Protocol Support				
RFC 2868	RADIUS Attributes for Tunnel Protocol Support	June 2000		Updates RFC 2865	
RFC 2869	RADIUS Extensions	June 2000		Updated by RFC 3579, RFC 5080	
RFC 2882	Network Access Servers Requirements: Extended RADIUS Practices	July 2000			
RFC 3162	RADIUS and IPv6	August 2001			
RFC 3575	IANA Considerations for RADIUS	July 2003			
RFC 3576	Dynamic Authorization Extensions to RADIUS	July 2003		Obsoleted by RFC 5176	
RFC 3579	RADIUS Support for EAP	September 2003	Extensible Authentication Protocol	Updates RFC 2869	
RFC 3580	IEEE 802.1X RADIUS Usage Guidelines	September 2003	802.1X		
RFC 4014	RADIUS Attributes Suboption for the DHCP Relay Agent Information Option	February 2005			
RFC 4372	Chargeable User Identity	January 2006			
RFC 4590	RADIUS Extension	July 2006		Obsoleted by	

	for Digest Authentication			RFC 5090	
RFC 4668	RADIUS Authentication Client MIB for IPv6	August 2006	Management information base		
RFC 4669	RADIUS Authentication Server MIB for IPv6	August 2006	Management information base		
RFC 4670	RADIUS Accounting Client MIB for IPv6	August 2006	Management information base		
RFC 4671	RADIUS Accounting Server MIB for IPv6	August 2006	Management information base		
RFC 4675	RADIUS Attributes for Virtual LAN and Priority Support	September 2006			
RFC 4679	DSL Forum Vendor-Specific RADIUS Attributes	September 2006			
RFC 4818	RADIUS Delegated-IPv6-Prefix Attribute	April 2007			
RFC 4849	RADIUS Filter Rule Attribute	April 2007			
RFC 5080	Common RADIUS Implementation Issues and Suggested Fixes	December 2007		Updates RFC 3579	
RFC 5090	RADIUS Extension for Digest Authentication	February 2008			
RFC 5176	Dynamic Authorization	January 2008			

	Extensions to RADIUS				
RFC 5607	RADIUS Authorization for NAS Management	July 2009			
RFC 5997	Use of Status-Server Packets in the RADIUS Protocol	August 2010		Updates RFC 2866	
RFC 6158	RADIUS Design Guidelines	March 2011			
RFC 6218	Cisco Vendor-Specific RADIUS Attributes for the Delivery of Keying Material	April 2011			
RFC 6421	Crypto-Agility Requirements for Remote Authentication Dial-In User Service (RADIUS)	November 2011			
RFC 6613	RADIUS over TCP	May 2012		Experimental	
RFC 6614	Transport Layer Security (TLS) Encryption for RADIUS	May 2012		Experimental	
RFC 6911	RADIUS Attributes for IPv6 Access Networks	April 2013		Standards track	
RFC 6929	Remote Authentication Dial-In User Service	April 2013		Updates RFC 2865, RFC 3575, RFC 6158	

	(RADIUS) Protocol Extensions				
RFC 7360	Datagram Transport Layer Security (DTLS) as a Transport Layer for RADIUS	September 2014		Experimental	
RFC 7585	Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)	Oct 2015		Experimental	
RFC 8044	Data Types in RADIUS	January 2017		Updates: 2865, 3162, 4072, 6158, 6572, 7268	
RFC 8559	Dynamic Authorization Proxying in the RADIUS Protocol	April 2019		Standards track	

See also

- Security Assertion Markup Language
- TACACS

References

1. *"How Does RADIUS Work?" (http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml) . Cisco. 2006-01-19. Retrieved 2009-04-15.*

2. *Edwin Lyle Brown (2006). 802.1X Port-Based Authentication (https://books.google.com/books?id=nlbrC3KLvCAC&pg=PA17) . Taylor & Francis. p. 17. ISBN 978-1-4200-4465-2.*

3. *RFC 2865 Remote Authentication Dial In User Service (RADIUS)*

4. *RFC 2866 RADIUS Accounting*

5. *"The Network Access Identifier" (https://tools.ietf.org/html/rfc7542) . Internet Engineering Task Force (IETF). May 2015. Retrieved 8 May 2021.*

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. Retrieved 2009-04-19.*

7. *"Configure NPS UDP Port Information" (https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-udp-ports-configure) . Microsoft. 2020-08-07. Retrieved 2021-06-20.*

8. *"IANA Considerations for RADIUS (Remote Authentication Dial In User Service)" (https://datatracker.ietf.org/doc/html/rfc3575) . Internet Engineering Task Force (IETF). July 2003. Retrieved 8 May 2021.*

9. *RFC 2548*

10. *An Analysis of the RADIUS Authentication Protocol (http://www.untruth.org/~josh/security/radius/radius-auth.html)*

11. *Jonathan Hassell (2003). RADIUS: Securing Public Access to Private Resources. O'Reilly Media. pp. 15–16. ISBN 9780596003227.*

12. *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.*

13. *Jonathan Hassell (2003). RADIUS: Securing Public Access to Private Resources. O'Reilly Media. p. 16. ISBN 9780596003227.*

14. *"Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)" (https://datatracker.ietf.org/doc/html/rfc5176) . Internet Engineering Task Force. January 2008. Retrieved 8 May 2021.*

Bibliography

- Hassell, Jonathan (2002). *RADIUS - Securing Public Access to Private Resources* (http://oreilly.com/catalog/9780596003227/) . O'Reilly & Associates. ISBN 0-596-00322-6. Retrieved 2009-04-17.

External links

- Radius Types (https://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)

Retrieved from "https://en.wikipedia.org/w/index.php?title=RADIUS&oldid=1097719401"