

Remote Authentication Dial-In User Service (RADIUS) Protocol

Simulate Hundreds of Thousands of RADIUS Authentications with Blended Applications and Security

The Remote Authentication Dial-In User Service (RADIUS) is a collection of two individually specified protocols defined originally by Livingston Enterprises, Inc. The Internet Engineering Task Force (IETF) officially adopted these two protocols in 1997, originally producing RFC 2058 and RFC 2059, which defined RADIUS Access and RADIUS Accounting, respectively.

The RADIUS protocol is considered an Authentication, Authorization, and Accounting mechanism that allows computers to access a network and various services within that network. RADIUS utilizes the User Datagram Protocol (UDP) as its transport layer. The Internet Assigned Numbers Authority (IANA) has officially reserved ports 1812 and 1813 for RADIUS Authentication and Accounting, respectively. Due to the gap between the original development of RADIUS and the IETF's adoption of the protocol, various other UDP ports are actively in use in live deployments. Some implementations of RADIUS servers have historically used 1645 and 1646 for RADIUS Authentication and Accounting, and many server implementations continue that tradition. According to Cisco's website, their RADIUS implementations default to the historical 1645 and 1646, while Microsoft's website indicates that while it defaults to 1812 and 1813, it does acknowledge that 1645 and 1646 may also be used.

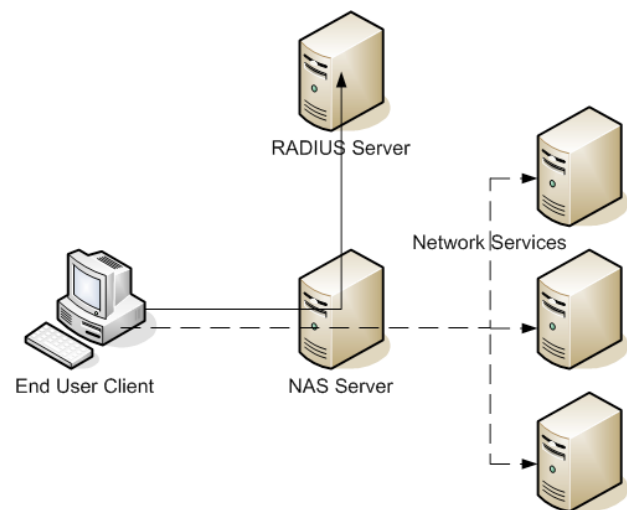
How RADIUS Works

A Network Access Server (NAS) attempting to secure access to a network with RADIUS authentication must start by sending an "Access-Request" message. This message contains client identification information such as username and password (encoded using an MD5 algorithm), as well as a list of additional services that are being requested. Upon receipt of the "Access-Request" message, the RADIUS server verifies the information provided by the client and issues one of the following messages: "Access-Reject", "Access-Accept", or "Access-Challenge". If configured to do so, the server may issue a challenge that prompts the client to provide additional information. Once the client satisfies the "Access-Challenge", the server issues an "Access-Accept" message, containing the type of service and additional information necessary to access the desired service.

BreakingPoint Testing Tools Simulate the RADIUS Protocol:

- BreakingPoint is able to generate thousands of RADIUS authentications per second using a single, easy-to-use test product.
- Utilizing blended applications and security, users can fully test their network infrastructure to ensure RADIUS authentication and accounting are handled properly under full network load.
- Users can infer the number of RADIUS-authenticated users from the detailed reporting of the BreakingPoint Elite.

Figure 1 - A Typical RADIUS Flow Test Bed



A typical RADIUS flow consists of a client PC requesting authentication from the network access server (NAS). The NAS in turn makes a RADIUS Access request to the RADIUS server to authenticate the user. Once the NAS has received permission to grant access, the end user will be permitted to access network resources.

Once the client has been authenticated and authorized, the NAS server will send an "Accounting-Request" Start packet, which describes the service being delivered and lets the RADIUS server know which user will be using the service. The RADIUS server should then respond with the "Accounting-Response" packet acknowledging the request. Finally, to stop the accounting process, the NAS will send an "Accounting-Request" Stop packet, which will indicate that the service should no longer be made available.

The Transmission Control Protocol (TCP) transport layer is not supported with RADIUS. RFC 2865 details four key reasons why UDP was chosen as the exclusive transport for RADIUS. In general, the most important reason for selecting UDP is that TCP retransmission timers are overly aggressive for RADIUS users and the overhead associated with TCP acknowledgements does not support the incremental benefit.

Realistic testing of devices that must handle RADIUS traffic must take into consideration all of the elements described above for this protocol. BreakingPoint has built the RADIUS protocol into their testing scenarios, allowing users to easily add fully stateful RADIUS traffic into their network simulation during testing.