

Authentication via Radius Servers

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service. It is a client/server protocol that runs in the application layer, using UDP as transport. RADIUS protocol is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services.

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.

AAA

Authentication and Authorization

The user or machine sends a request to a **Remote Access Server (RAS)**, also called a **RADIUS client** (in wireless networks typically access point), to gain access to a particular network resource using access credentials.

In turn, the RAS sends a *RADIUS Access Request* message to the **RADIUS server**, requesting authorization to grant access via the RADIUS protocol.

The RADIUS server checks that the information against a trusted database and then returns one of three responses to the RAS:

- *Access Reject* - The user is unconditionally denied access to all requested network resources.
- *Access Challenge* - Requests additional information from the user such as a secondary password, PIN, token, or card.
- *Access Accept* - The user is granted access. Once the user is authenticated, the RADIUS server will often check whether the user is authorized to use the network service requested.

Accounting

If network access is granted to the user by the RAS, the RAS issues records to the RADIUS server, providing information on the usage in terms of time, packets transferred, data transferred and other information related to the user's network access.

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.

Security

The RADIUS protocol does not transmit passwords in cleartext between the RAS and RADIUS server. A shared secret is used along with the MD5 hashing algorithm to obfuscate passwords. Because this particular implementation is not considered to be a very strong protection, additional protection, such as IPsec tunnels or physically secured data-center networks, should be used.