ABOUT NETWORK ACCESS CONTROL / MANAGEMENT

RADIUS

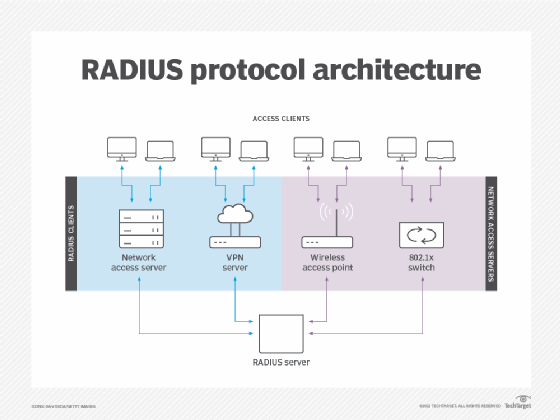
It stands for Remote Authentication Dial-In User Service; is a client-server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

RADIUS was originally designed to support large numbers of users connecting remotely to internet service providers (ISPs) or corporate networks via modem pools or other point-to-point serial line links. RADIUS is now commonly used for remote access across different types of networks, including wireless networks, Ethernet networks and other types of remote user access through the internet. (Thus RADIUS may help with your finishing project)

How does RADIUS work?

In the RADIUS protocol, remote network user connects to their networks through a network access server (NAS). Because unlike other client-server concepts, where the client is often an individual user; RADIUS clients are the NAS systems used to access a network and the authentication server is the RADIUS Server.

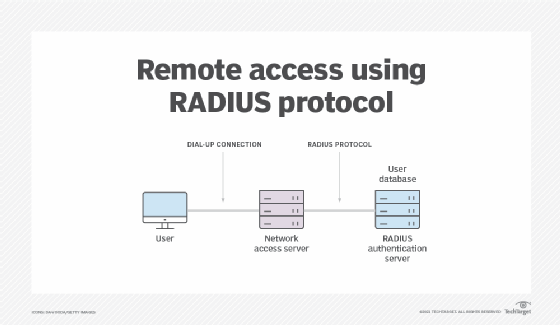
The NAS queries the authentication server to get authentication, authorization and configuration information about the remote user.



In the RADIUS protocol; access servers, access points, routers, l3 switches (in other words network devices) act as clients of the RADIUS server while in an active Directory and an IPA, the users themselves (individual) / domains (user groups) are the clients and this differentiates the RADIUS from Active Directory (Domain Controller) solution for Windows or IPA (Integrated Identity and Authentication) solution for Linux.

The RADIUS protocol provides centralized authentication services to the servers through which remote users connect to the network. Types of remote user access authentication servers can include:

* **Dial-in servers**, which mediate access to corporate or ISP networks through modem pools.
* **Virtual private network servers**, which accept requests from remote users to [set up secure connections](https://www.techtarget.com/searchsecurity/Ultimate-guide-to-secure-remote-access) to a private network.
* **Wireless access points**, which accept requests from wireless clients to connect to a network.
* **Managed network access switches** that implement the 802.1x authenticated access protocol to mediate access to networks by remote users.



End users interact only indirectly, through a network access server, with the RADIUS server when authenticating with a remote network.

Microsoft Active Directory / DC

IPA

LDAP

The Lightweight Directory Access Protocol is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol network.

EXAMPLE: Integrating ClearPass with Active Directory

