

Clarinet Systems® RADIUS Security Function

What is RADIUS and why

RADIUS, specified in RFC2865 (<http://www.ietf.org/rfc/rfc2865.txt>), is “A protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server”.

A Network Access Server (NAS) operates as a client of RADIUS (Authentication Server). It is responsible for passing user information to designated RADIUS servers, and then acting on the response returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. RADIUS was designed largely for authenticating and managing large number of users dialing-up for WAN access.

Typical WAN-access is a laptop computer dialing up to an ISP and connecting to the Internet; user name and password are required for dialing up to the ISP. The ISP acts as a “Network Access Server” that receives the user name and password and sends them to an “Authentication Server”. After Authentication Server verifies the user name and password, network access is granted to the dial-up user.

All the PDAs today use PPP dial-up connection, either through IR or external modem, to access the network. The term “network” could be LAN, WAN or the Internet. Clarinet Systems provides PDA network access using IR. Today anyone with a PDA can connect to network through Clarinet Systems, user name and password are not required. With more and more concerns about not letting just any PDA accessing the network, Clarinet Systems will support RADIUS in its EthIR LAN™ product line so that PDA user will need to have the correct user name and password in order to access the network. In this case, EthIR LAN acts as a Network Access Server between the PDA and an Authentication Server. EthIR LAN passes the user name and password from the PDA to the Authentication Server for verification and grant network access if user name and password are verified.

What do you need to do on EthIR LAN and your environment

RADIUS is a widely used protocol and is supported by most servers, for example, Win2000 and Linux. Clarinet Systems supports MS-CHAP, CHAP and PAP in its RADIUS implementation.

For existing EthIR LAN customers, you need to update the firmware, which will be available on our website soon, and purchase the RADIUS option key (part number

“RAD-KEY-1-8”) from authorized sales channels. Every EthIR LAN system needs to order one Key (one key for one EthIR LAN.)

For new EthIR LAN purchases, you need to purchase the RADIUS option (part number “RADIUS-1” for single port and “RADIUS-8” for multi-port EthIR LAN) and it will be available out-of-box, otherwise RADIUS will not be enabled.

What do users need to do on their PDAs

For PalmOS users, you need to select a network service and connection to use IR. You need to enter user name and password for the selected network service. For those PalmOS devices that have been configured by using ClarinetIR, “ClarinetIR” network service would be the one to choose. You only need to enter the user name and password once.

For PocketPC devices, you need to create a modem connection by using IR. When making an IR connection, you will be asked for user name and password. You have a choice of letting PocketPC to remember the password or not. If yes, then you don’t have to enter password the next time you make an IR connection. Otherwise, you would have to enter the password the next time.

After receiving the user name and password from the PDA, EthIR LAN verifies them with a pre-configured RADIUS server. If verified, the PDA is connected to the network. Otherwise, an error message will be displayed to the user indicating authentication failed.

What about security

Keep in mind that nothing is 100% secure, so is RADIUS. There is no protection on lost user name and password.

A common question is “what if the PDA with the user name and password is lost”. The answer is simple; you should do as if you lost your credit card by reporting to the system admin to change your password. Also, the system admin could setup the RADIUS server so that user would have to change its password every so often, although this could be very annoying.

The benefit of having RADIUS is not to let any PDA or laptop computer access your network without a user name and password. Also, a central database of users is much easier to support and manage for IT department.