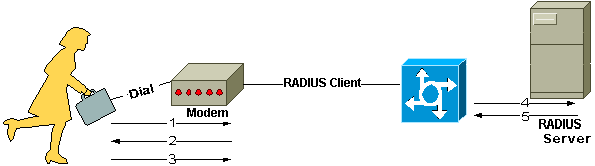
Describe the idea of the RADIUS Protocol. Provide details and different scenarious.

Remote Authentication Dial-In User Service (RADIUS) 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 allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics. Created by Livingston (now owned by Lucent), RADIUS is a de facto industry standard used by a number of network product companies and is a proposed IETF standard.

This figure shows the interaction between a dial-in user and the RADIUS client and server.



* User initiates PPP authentication to the NAS.
* NAS prompts for username and password (if Password Authentication Protocol [PAP]) or challenge (if Challenge Handshake Authentication Protocol [CHAP]).
* User replies.
* RADIUS client sends username and encrypted password to the RADIUS server.
* RADIUS server responds with Accept, Reject, or Challenge.
* The RADIUS client acts upon services and services parameters bundled with Accept or Reject.

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, user passwords are sent encrypted between the client and RADIUS server to eliminate the possibility that someone snooping on an insecure network could determine a user's password.