6.11.2 Remote Access Facts

Remote access allows a host to connect to a server or even a private network and access resources as if they were connected to the LAN locally. Remote access connections are typically used by business users to connect to the office from home or while traveling.

Remote access includes the following:

Concept	Description
PSTN	Public Switch Telephone Network (PSTN) used modems to connect to a remote access server. This, however, is an outdated method because of slow connection speeds.
PPP/PPPoE	- Point-to-Point Protocol (PPP) and Point-to-Point Protocol over Ethernet (PPPoE) is used at the data link layer. PPP is less common because it was usually used in dial-up connections. - PPPoE normally requires a static IP from the ISP and sometimes a user name and a password to authenticate with the ISP.
Proxy ARP	A proxy ARP is used when a host fakes the identity of other machines in order to receive the packets intended for those other machines and takes responsibility for routing the packets to the intended machine.
CHAP, MS-CHAP, and EAP	- Challenge Handshake Authentication Protocol (CHAP) uses a challenge/response (three-way handshake) mechanism to protect passwords. CHAP is the only remote access authentication protocol that ensures that the same client or system exists throughout a communication session by repeatedly and randomly re-testing the validated system. - Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is Microsoft's version of CHAP. - MS-CHAP encrypts the shared secret on each system so that it is not saved in cleartext. - MS-CHAP v2 allows for mutual authentication, in which the server authenticates to the client. Mutual authentication helps to prevent man-in-the-middle attacks and server impersonation. - Extensible Authentication Protocol (EAP) allows the client and server to negotiate the characteristics of authentication. When a connection is established, the client and server negotiate the authentication type that will be used based on the allowed or required authentication types configured on each device. Both CHAP and MS-CHAP provide user name and password authentication, while EAP allows authentication using a variety of methods, including passwords, certificates, and smart cards.
Authorization	*Authorization* is the process of identifying the resources that a user can access over the remote access connection. *Remote access policies* are commonly used to restrict access. Authorization can restrict access based on: - Time of day - Type of connection (for example, PPP or PPPoE, wired or wireless) - Location of the resource (restrict access to specific servers) Authorization is controlled through the use of network policies (remote access policies) as well as access control lists.
AAA Server/Accounting	AAA stands for three parts of this remote access process; Authentication, Authorization and Accounting. Accounting is the process of keeping track of what was done during a connection.
Radius Server	A Radius server is used as an authentication and authorization mechanism that uses UDP for authorization. It is used in Microsoft implementations. It provides a single solution for authentication and authorization.
TACACS and TACACS+	TACACS+ is the updated version of TACACS. They both: - Separate authentication, authorization, and accounting into different services. - Can all be on the same server or split betweens different servers. - Use TCP instead of UDP.