6.11.4 RADIUS and TACACS+ Facts

A remote access server typically controls client access. Clients might be restricted to access resources only on the remote access server, or they might be allowed to access resources on other hosts on the private network.

- Remote access policies identify authorized users and other required connection parameters.
- In a small implementation, user accounts and remote access policies are defined on the remote access server. With this configuration, you must define user accounts and policies on each remote access server.
- For larger deployments with multiple remote access servers, you can centralize the administration of remote access policies by using an AAA (authentication, authorization, and accounting) server.
  - Connection requests from remote clients are received by the remote access server and forwarded to the AAA server to be approved or denied.
  - Policies defined on the AAA server apply to all clients connected to all remote access servers.

Two common AAA server solutions include:

Solution	Description
Remote Authentication Dial-in User Service (RADIUS)	RADIUS is used by Microsoft servers for centralized remote access administration. RADIUS: - Combines authentication, authorization, and accounting; all three must be implemented through the RADIUS system. - Allows for the separation of accounting to different servers. However, authentication and authorization remain combined on a single server. - Supports PPP, CHAP, and PAP. - Uses a challenge/response method for authentication. - Does not transmit passwords in cleartext between the RADIUS client and the RADIUS server. - A shared secret is used between the RADIUS server and the RADIUS client. - The password is hashed and the hash is added to the password before it is transmitted. - RADIUS encrypts only the password using MD5. - Uses UDP ports 1812 and 1813 and can be vulnerable to buffer overflow attacks. - Often uses vendor-specific extensions. RADIUS solutions from different vendors might not be compatible. When configuring a RADIUS solution, configure a server as a RADIUS *server* to provide AAA services. Then configure all remote access servers as RADIUS *clients*.
Terminal Access Controller Access-Control System Plus (TACACS+)	TACACS+ was originally developed by Cisco for centralized remote access administration. TACACS+: - Provides three protocols, one each for authentication, authorization, and accounting. This allows each service to be provided by a different server. - Uses TCP port 49. - Encrypts the entire packet contents, not just authentication packets; the client server dialogs are also encrypted. - Supports more protocol suites than RADIUS. - Remote access severs become TACACS+ clients to the backend TACACS+ server, similarly to a RADIUS solution. TACACS and XTACACS are older protocols developed before TACACS+. While they sound similar, they are different and less-secure protocols.

Points to consider when comparing RADIUS to TACACS+ are:

- TACACS+ and RADIUS have generally replaced earlier protocols in more recently built or updated networks, although TACACS and XTACACS are still running on many older systems.
- RADIUS is more interoperable because TACACS+ is Cisco proprietary.
- RADIUS performs better due to less encryption, less overhead, and more compatibility with other systems.
- TACACS+ is considered more reliable than RADIUS because of TCP.
- TACACS+ is more secure than RADIUS because RADIUS encrypts only the password; TACACS+ encrypts the entire session between the client and server.
- RADIUS is more secure than the original TACACS.
- PPTP does not work with RADIUS and TACACS+; L2TP can be used with RADIUS and TACACS+.
- Both solutions are vulnerable to buffer overflow attacks, birthday attacks, and packet sniffing.