11.4.2 Remote Access Facts

Remote access allows a host to remotely connect to a private server or a network. Remote access connections are typically used to connect to an office network, but they are very similar to internet service provider (ISP) connections. A remote access server is used for remote access connections.

Establish a Remote Access Connection

Use the following process to establish a remote access connection.

Process	Description
Physical Connection	Clients must establish a physical connection to the remote access server. ▪ If you are using a broadband connection, just connect the device to the network and turn it on. ▪ If you are using a dial-up connection, the device dials the number of the remote access server, and the remote access server answers the incoming call.
Connection Parameters	After the physical connection is set up, a Data Link layer connection is established. During this phase, additional parameters that will be used during the connection are decided. For example, the devices identify the upper layer protocols that they will use during the connection. Protocols negotiated at this phase control the following parameters: ▪ Upper layer protocol suite (such as IP) ▪ Network layer addressing ▪ Compression (if any) ▪ Encryption (if any) ▪ Authentication method Two common protocols are used during this phase. ▪ The point-to-point protocol (PPP) is used for dial-up connections. ▪ PPP over Ethernet (PPPoE) is used for broadband connections, such as DSL, cable, or fiber optic running Ethernet. PPPoE is a modification of PPP that is able to negotiate additional parameters that are not present on regular Ethernet networks. ISPs usually implement PPPoE to control and monitor internet access over broadband links. During this phase, the remote client is assigned an IP address. The IP address can be assigned from a range configured on the remote access server or even from a DHCP server on the private network. ▪ If the IP address for the remote client is on the same subnet as the private network, the remote access server uses a process called proxy ARP to forward packets from the private network to the remote access client. Proxy ARP associates the MAC address of the remote access server with the IP address of the remote client. The remote access server receives the frames addressed to the remote access client and forwards the packets to the remote access client. ▪ If the IP address for the remote client is on a different subnet (such as a special subnet defined for remote access clients), then the remote access server acts as a router, sending packets between the remote client and the public network. In this configuration, the remote access server must be configured with routing enabled.
Authentication	*Authentication* is the process of proving identity. The authentication protocol is negotiated during the connection parameter phase. After devices agree on the authentication protocol to use, the logon credentials are exchanged, and logon is allowed or denied. Extensible authentication protocol (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. Authorization can restrict access based on the following parameters: ▪ Time of day ▪ Type of connection (such as PPP or PPPoE, wired or wireless) ▪ Location of the resource (allowing you to restrict access to specific servers)
Accounting	*Accounting* is an activity that tracks or logs the use of the remote access connection. Accounting is often used by ISPs to bill for services based on time spent or the amount of data downloaded.

Remote Access Facts

It's important to know a few things about remote access.

- Remote Access Service (RAS) is used by a remote access server to control access for remote access clients. Clients might be granted access to resources on only the remote access server, or they might be allowed to access resources on other hosts on the private network.

- Both the remote access server and the client computer must be configured to use or accept the same connection parameters. During the connection phase, the devices negotiate the protocols that will be used. If the allowed protocols do not match, the connection will be refused.
- Remote access policies identify allowed users and other required connection parameters.
- In a small implementation, user accounts and remote access policies are defined on the remote access server.
- When using a directory service, you can configure the remote access server to look up user account information on the directory service server.
- If you have multiple remote access servers, you must define user accounts and policies on each remote access server.
- Use an AAA server to centralize authentication, authorization, and accounting for multiple remote access servers. Connection requests from remote clients are received by the remote access server and are 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.
- The following table explains two commonly used AAA server solutions.

Solution	Description
Remote Authentication Dial-In User Service (RADIUS)	RADIUS is used by Microsoft servers for centralized remote access administration. RADIUS: ▪ Combines authentication and authorization using policies to grant access. ▪ Uses UDP. ▪ Encrypts only the password. ▪ Often uses vendor-specific extensions. RADIUS solutions from different vendors might not be compatible. When implementing a RADIUS solution, configure a single server as a RADIUS server and 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 for authentication, one for authorization, and one for accounting. This allows each service to be provided by a different server. ▪ Uses TCP port 49. ▪ Encrypts the entire packet contents. ▪ Supports more protocol suites than RADIUS.