13.12.3 VPN Facts

A virtual private network (VPN) is a type of network that uses encryption to allow IP traffic to travel securely over the TCP/IP network. A VPN is used primarily to support secure communications over an untrusted network.

- VPNs work by using a tunneling protocol that encrypts packet contents and wraps them in an unencrypted packet.
- Tunnel endpoints are devices that can encrypt and decrypt packets. When you create a VPN, you establish a security association between the two tunnel endpoints. The endpoints create a secure, virtual communication channel. Only the destination tunnel endpoint can unwrap packets and decrypt the packet contents.
- Routers use the unencrypted packet headers to deliver the packet to the destination device. Intermediate routers along the path cannot read the encrypted packet contents.
- A VPN can be used over a local area network, across a WAN connection, over the internet, and even over a dial-up connection.
- VPNs can be implemented in the following ways:
  - With a *host-to-host* VPN, two hosts establish a secure channel and communicate directly. With this configuration, both devices must be capable of creating the VPN connection.
  - With a *site-to-site* VPN, routers on the edge of each site establish a VPN with the router at the other location. Data from hosts within the site are encrypted before being sent to the other site. With this configuration, individual hosts are unaware of the VPN.
  - With a *remote access* VPN, a server on the edge of a network (called a VPN *concentrator*) is configured to accept VPN connections from individual hosts in a *client-to-site* configuration. Hosts that are allowed to connect using the VPN connection are granted access to resources on the VPN server or the private network.

The following table describes the most common VPN tunneling protocols:

Protocol	Description
Point-to-Point Tunneling Protocol (PPTP)	PPTP was developed by Microsoft as one of the first VPN protocols. PPTP: - Uses standard authentication protocols, such as CHAP and PAP - Supports TCP/IP only - Is supported by most operating systems and servers - Uses TCP port 1723
Layer Two Tunneling Protocol (L2TP)	L2TP is an open standard for secure multiprotocol routing. L2TP: - Supports multiple protocols (not just IP) - Uses IPsec for encryption - Is not supported by older operating systems - Uses TCP port 1701 and UDP port 500
Internet Protocol Security (IPsec)	IPsec provides authentication and encryption, and it can be used in conjunction with L2TP or by itself as a VPN solution. IPsec includes the following three protocols for authentication, data encryption, and connection negotiation: - Authentication Header (AH) enables authentication with IPsec. - Encapsulating Security Payload (ESP) provides data encryption. - Internet Key Exchange (IKE) negotiates the connection. IPsec can be used to secure the following types of communications: - Host-to-host communications within a LAN - VPN communications through the internet, either by itself or in conjunction with the L2TP VPN protocol - Any traffic supported by the IP protocol, including web, email, Telnet, file transfer, SNMP traffic, as well as countless others IPsec uses either digital certificates or pre-shared keys
Secure Sockets Layer (SSL)	The SSL protocol has long been used to secure traffic generated by IP protocols such as HTTP, FTP, and email. SSL can also be used as a VPN solution, typically in a remote access scenario. SSL: - Authenticates the server to the client using public key cryptography and digital certificates

	▪ Encrypts the entire communication session ▪ Uses port 443, which is already open on most firewalls Implementations that use SSL for VPN tunneling include Microsoft's SSTP and Cisco's SSL VPN.
Generic Routing Encapsulation (GRE)	GRE is a tunneling protocol that was developed by Cisco. GRE can be used to route any Layer 3 protocol across an IP network. GRE: ▪ Creates a tunnel between two routers. ▪ Encapsulates packets by adding a GRE header and a new IP header to the original packet. ▪ Does not offer any type of encryption. ▪ Can be paired with other protocols, such as IPsec or PPTP, to create a secure VPN connection.

Ports must be open in firewalls to allow VPN protocols. For this reason, using SSL for the VPN often works through firewalls when other solutions do not. Additionally, some NAT solutions do not work well with VPN connections.
