5.7.7 VPN Protocol Facts

A VPN uses a tunneling protocol that encrypts packet contents and wraps them in an unencrypted packet. The tunneling protocol (also referred to as the VPN protocol) identifies the methods that devices use to establish the VPN connection and encrypt the data. The three types of protocols used by VPNs are:

- A carrier protocol (such as IP).
- A tunneling protocol (such as PPTP or L2TP).
- A passenger protocol for the data being transmitted.

Many networks make use of a piece of hardware called a VPN concentrator. VPN concentrators are advanced routers that can create and maintain many secure connections to the network through VPN tunnels.

The following table compares the common VPN tunneling protocols.

Protocol	Description
Point-to-Point Tunneling Protocol	Point-to-Point Tunneling Protocol (PPTP) was one of the first VPN protocols and was developed by Microsoft. PPTP: - Uses standard authentication protocols, such as Challenge-Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP). - Supports TCP/IP only. - Encapsulates other LAN protocols and carries the data securely over an IP network. - Uses Microsoft's MPPE for data encryption. - Is supported by most operating systems and servers. - Uses TCP port 1723.
Layer 2 Forwarding	Layer 2 Forwarding (L2F) is a VPN technology developed by Cisco that: - Operates at the data link layer (layer 2). - Offers mutual authentication. - Does not encrypt data. - Merged with PPTP to create L2TP.

Layer 2 Tunneling Protocol	Layer 2 Tunneling Protocol (L2TP) is an open standard for secure multi-protocol routing. L2TP:
	- Operates at the data link layer (layer 2).
	- Supports multiple protocols (not just IP).
	- Uses IPsec for encryption. Combining L2TP with IPsec (called L2TP/IPsec) provides:
	  - Per packet data origin authentication (nonrepudiation)
	  - Replay protection
	  - Data confidentiality
	- Is not supported by older operating systems.
	- Uses TCP port 1701 and UDP port 500.

Internet Protocol Security	Internet Protocol Security (IPsec) provides authentication and encryption, and can be used in conjunction with L2TP or by itself as a VPN solution. IPsec includes two protocols that provide different features. - Authentication Header (AH) provides authentication features. Use AH to enable authentication with IPsec. - Encapsulating Security Payload (ESP) provides data encryption. Use ESP to encrypt data. If you use AH alone, data is *not* encrypted. IPsec has two modes of operation, based on the relationship of the communicating devices to each other. - Transport mode is used for end-to-end encryption of data. The packet data is protected, but the header is left intact, allowing intermediary devices (such as routers) to examine the packet header and use the information in routing packets. - Tunnel mode is used for link-to-link communications. Both the packet contents and the header are encrypted. IPsec can be used to secure communications such as: - 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. Be aware of the following additional characteristics of IPsec:

	▪ It functions at the network layer (layer 3) of the OSI model. ▪ It uses either digital certificates or pre-shared keys. ▪ It generally can't be used when a NAT proxy is deployed.
Secure Sockets Layer	The Secure Sockets Layer (SSL) protocol has long been used to secure traffic generated by other 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, a port that is often already open in most firewalls. Implementations that use SSL for VPN tunneling include Microsoft's SSTP and Cisco's SSL VPN.
Transport Layer Security	The Transport Layer Security (TLS) protocol works in a similar way to SSL, even though they are not interoperable. When securing a connection with a VPN, TLS: ▪ Authenticates the server to the client, using public key cryptography and digital certificates. ▪ Encrypts the entire communication session. ▪ Uses port 443 or port 30.