12.1.2 IP Protocol Facts

This lesson covers the following topics:

- Protocols
- Protocols in the IP protocol suite

Protocols

A protocol is a set of standards for communication between network hosts. Protocols often provide services, such as email or file transfer. Most protocols are not intended to be used alone, but, instead, rely on and interact with other dependent or complimentary protocols. A group of protocols intended to be used together is called a protocol suite.

Protocols in the IP Protocol Suite

The Internet Protocol (IP) protocol suite (commonly referred to as TCP/IP) is the most widely used protocol suite today. The following table describes several protocols in the IP protocol suite.

Protocol	Description
Internet Protocol (IP)	IP is the main protocol used on the internet. It is a connectionless protocol that makes routing path decisions. It also handles logical addressing issues through the use of IP addresses.
Transmission Control Protocol (TCP)	TCP provides services that ensure accurate and timely delivery of network communications between two hosts. TCP is a connection-oriented protocol. TCP provides the following services to ensure message delivery: ▪ Sequencing of data packets ▪ Flow control ▪ Error checking
User Datagram Protocol (UDP)	UDP is a connectionless protocol. UDP is a host-to-host protocol like TCP. However, it does not include mechanisms for ensuring timely and accurate delivery. Because it has less overhead, it offers fast communications, but at the expense of possible errors or data loss.
Internet Control Message Protocol (ICMP)	ICMP works closely with IP to provide error and control information by allowing hosts to exchange packet status information, which helps move the packets through the internetwork. Two common management utilities, **ping** and **traceroute**, use ICMP messages to check network connectivity. ICMP also works with IP to send notices when destinations are unreachable, when devices' buffers overflow, and whether devices can communicate across the network. It also relays information about the route and hops packets take through the network.
Internet Group Membership Protocol (IGMP)	IGMP is a protocol for defining host groups. All group members can receive broadcast messages intended for the group (called multicasts). Multicast groups can be composed of devices within the same network or across networks (connected with a router).
HyperText Transfer Protocol (HTTP)	HTTP is used by web browsers and web servers to exchange files (such as web pages) through the World Wide Web and intranets. HTTP can be described as an information requesting and responding protocol. It is typically used to request and send web documents, but is also used as the protocol for communication between agents using different IP protocols.
HTTP over SSL (HTTPS)	HTTPS is a secure form of HTTP that uses SSL to encrypt data before it is transmitted.
Secure Sockets Layer (SSL)	SSL secures messages being transmitted on the internet. It uses RSA for authentication and encryption. Web browsers use SSL (Secure Sockets Layer) to ensure safe web transactions. URLs that begin with https:// trigger your web browser to use SSL.
Transport Layer Security (TLS)	TLS is an improved version of SSL. It ensures that messages being transmitted on the internet are private and tamper proof. TLS is implemented through two protocols: ▪ TLS Record provides connection security with encryption (e.g., with DES). ▪ TLS Handshake provides mutual authentication and choice of the encryption method.
File Transfer Protocol (FTP)	FTP provides a generic method of transferring files. It can include file security through usernames and passwords, and it allows file transfer between dissimilar computer systems. FTP can transfer both binary and text files, including HTML, to another host. FTP URLs are preceded by ftp://. To log in to an FTP server, use ftp://*username@servername*.

Trivial File Transfer Protocol (TFTP)	TFTP is similar to FTP. It lets you transfer files between a host and an FTP server. However, it provides no user authentication and no error detection. Because it does not perform error detection, TFTP is faster than FTP, but might be subject to transmission errors.
Secure File Transfer Protocol (SFTP)	SFTP is a secure version of FTP that uses Secure Shell (SSH) to encrypt data transfers. SSH ensures that SFTP transmissions use encrypted commands and data, which prevent data from being transmitted over the network in clear text.
Secure Copy Protocol (SCP)	SCP is used to copy files between systems. Like SFTP, SCP relies on SSH to ensure that data and passwords are not transmitted over the network in cleartext.
Simple Mail Transfer Protocol (SMTP)	SMTP is used to route electronic mail through the internetwork. SMTP is used: ▪ Between mail servers for sending and relaying mail. ▪ By all email clients to send mail.
Internet Message Access Protocol (IMAP)	IMAP is an email retrieval protocol designed to enable users to access their email from various locations without the need to transfer messages or files back and forth between computers. Messages remain on the remote mail server and are not automatically downloaded to a client system. An email client that uses IMAP for receiving mail uses SMTP for sending mail.
Post Office Protocol 3 (POP3)	POP3 is used to retrieve email from a remote server to a local client over a TCP/IP connection. With POP3, email messages are downloaded to the client. An email client that uses POP3 for receiving mail uses SMTP for sending mail.
Dynamic Host Configuration Protocol (DHCP)	DHCP is a protocol that automatically assigns addresses and other configuration parameters to network hosts. Using a DHCP server, hosts receive configuration information at startup, reducing the amount of manual configuration required on each host.
Domain Name System (DNS)	DNS is a system that is distributed throughout the internetwork to provide address and name resolution. For example, the name **www.mydomain.com** would be identified with a specific IP address.
Network Time Protocol (NTP)	NTP is used to communicate time synchronization information between systems on a network.
Lightweight Directory Access Protocol (LDAP)	LDAP is used to allow searching and updating of a directory service. The LDAP directory service follows a client/server model. One or more LDAP servers contain the directory data. The LDAP client connects to an LDAP server to make a directory service request.
Simple Network Management Protocol (SNMP)	SNMP is a protocol designed for managing complex networks. SNMP lets network hosts exchange configuration and status information. This information can be gathered by management software and used to monitor and manage the network.
Remote Terminal Emulation (Telnet)	Telnet allows an attached computer to act as a dumb terminal with data processing taking place on the TCP/IP host computer. Telnet uses insecure data transmissions and should be avoided. SSH provides the same functionality, but does so securely using encryption.
Secure Shell (SSH)	SSH allows secure interactive control of remote systems. SSH is a secure and acceptable alternative to Telnet. SSH uses public key cryptography for both connection and authentication.