6.5.4 TCP/IP Protocol Facts

A *protocol* is a rule that identifies some aspect of how computers communicate on a network. For two computers to communicate, they must be using the same protocols. Protocols are grouped into protocol *suites*, or sets of related protocols, that are meant to be used together.

Common protocol suites include:

Protocol	Description
TCP/IP	TCP/IP is the protocol suite used on the internet and on most networks. Nearly all computers today use TCP/IP for communication. The Internet Protocol (IP) is a key component of the TCP/IP protocol suite. The IP protocol is responsible for determining how to deliver data from the sending host to the destination host. However, it does not provide a mechanism for segmenting and sequencing packets in a communication. To accomplish this, IP is used in conjunction with another transport protocol: ▪ Transmission Control Protocol (TCP) - TCP is a connection-oriented protocol. To ensure reliable delivery of data, TCP requires the recipient of a network transmission to send an acknowledgement of each and every IP packet it receives to the sender. Packets that don't make it are retransmitted. This ensures that the data is delivered reliably. ▪ User Datagram Protocol (UDP) - UDP is a connectionless protocol. Unlike TCP, UDP does not require acknowledgements. One of the key drawbacks of using TCP is the fact that its reliability introduces latency. For small data transmissions, such as sending an email, moderate latency is not a problem. However, for large data transmissions, such as video or audio streaming, the latency associated with TCP is unacceptable. By using UDP instead, the latency of the transmission is significantly reduced, with the assumption that an occasional lost packet won't be detrimental.
NetBIOS	NetBIOS is the term used to describe the combination of two protocols: NetBEUI and NetBIOS. NetBIOS was used in early Windows networks. Because NetBIOS is a non-routable protocol, it was often combined with IP to enable internetwork communications. NetBIOS over TCP/IP, or NetBT, is used to allow older computers and applications that rely on NetBIOS to communicate on a TCP/IP network.

Be aware of the following facts regarding protocol suite support and features:

- Virtually all operating systems today provide native (built-in) support for TCP/IP.
- Most older versions of some operating systems used a different protocol as the default protocol suite. For example, older NetWare servers used IPX/SPX, while older Mac OS systems used AppleTalk.
- Older operating systems without native TCP/IP support enabled IP communications by either installing the protocol stack or through a process known as encapsulation or tunneling. With this process, non-IP packets are re-packaged as IP packets at the sending device. The receiving device strips off the IP headers to reveal the original packets.

The following table lists several protocols in the TCP/IP protocol suite:

Protocol	Default Port(s)	Description
Hypertext Transfer Protocol (HTTP)	80	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.
Hypertext Transfer Protocol over Secure Socket Layer or HTTP over SSL (HTTPS)	443	HTTPS is a secure form of HTTP that uses SSL as a sublayer for security. 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.
File Transfer Protocol (FTP)	21	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://* followed by the DNS name of the FTP server. To log into an FTP server, use: ftp://username@servername.
Simple Mail Transfer Protocol (SMTP)	25	SMTP is used to route electronic mail through the internetwork. Email applications provide the interface to communicate with SMTP or mail servers.
Internet Message	143	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

Access Protocol (IMAP)		server and are not automatically downloaded to a client system.
Post Office Protocol 3 (POP3)	110	POP3 is part of the IP protocol suite and used to retrieve email from a remote server to a local client over an IP connection. With POP3, email messages are downloaded to the client.
Remote Terminal Emulation (Telnet)	23	Telnet allows an attached computer to act as a dumb terminal, with data processing taking place on the IP host computer. It is still widely used to provide connectivity between dissimilar systems. Telnet can also be used to test a service by the use of HTTP commands. You should avoid using Telnet as it transmits all data (e.g., usernames and passwords) clear text.
Secure Shell (SSH)	22	SSH allows for secure interactive control of remote systems. SSH is a much more secure alternative to Telnet.
Secure FTP (SFTP)	22	SFTP addresses one of the key weaknesses of FTP; namely, FTP doesn't use encryption. All data, including usernames and passwords, is sent clear text. SFTP provides the same functionality as FTP, but secures the data transmissions using the SSH protocol.
Domain Name System (DNS)	53	DNS is a system that is distributed throughout the internetwork to provide address/name resolution. For example, the name www.mydomain.com would be identified with a specific IP address.
Remote Desktop Protocol (RDP)	3389	RDP allows you to view and use the graphical desktop of a remote computer system as if you were sitting in front of it.
Dynamic Host Configuration Protocol (DHCP)	67, 68	DHCP is used to dynamically assign IP addressing information to network hosts when they come online. The client system, when it connects to the network, broadcasts a DHCPDISCOVER message on the network, looking for a DHCP server. The DHCP server responds with a DHCPOFFER message containing proposed IP addressing configuration information. The client then responds with a DHCPREQUEST message to the DHCP server indicating it wants to use the proposed configuration. The DHCP server makes the assignment with a DHCPACK message.
Lightweight Directory Access Protocol (LDAP)	389, 636	LDAP is a protocol used to access information about network resources stored by a directory service, such as Active Directory or eDirectory. LDAP uses port 389 for clear text transmissions and port 636 for secure transmissions.
Simple Network Management Protocol (SNMP)	161, 162	SNMP is used to monitor and manage network devices. SNMP agents can be installed on network devices such as PCs, switches, and routers. These agents send data to an SNMP manager application running on an administrative workstation, which aggregates the information and displays an overview of the current network status. Thresholds can be configured which trigger alerts if exceeded.
Server Message Block (SMB)	445	SMB enables the sharing of folders and printers on the network. Using SMB, remote users can access files in a shared folder on a server or workstation. Likewise, a remote user can send print jobs to a shared printer. SMB is also known as *Common Internet File System* (CIFS). SMB running directly over TCP uses port 445. SMB running on "NetBIOS over TCP/IP" uses UDP ports 137 & 138 and TCP ports 137 & 139.
Service Location Protocol (SLP)	427	SLP is a protocol that is able to organize and locate various network devices and services, such as printers, shared disk drives, directories, etc.
Apple Filing Protocol (AFP)	548	AFP is the protocol used by systems running Mac OS X or newer to support file sharing on the network. AFP replaced AppleTalk and has gone through several revisions.