Protocols

TCP and UDP

The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are used to transmit network data to and from server and client applications. The main difference between the two protocols is that TCP uses a connection-oriented transport, while UDP uses a connectionless type of communication. When the TCP protocol is used, a special connection is opened up between two network devices, and the channel remains open to transmit data until it is closed.

On the other hand, a UDP transmission does not make a proper connection and merely broadcasts its data to the specified network address without any verification of receipt. For certain types of applications and services, a TCP connection makes more sense, while other types are more efficiently provided by UDP communication. The advantage of TCP is that the transmission is much more reliable because it uses acknowledgement packets to ensure delivery. The advantage of UDP is that there is no connection, so it is much faster without all the checks and acknowledgements going on, but is also less reliable. In Table some common TCP/IP applications are shown with the type of protocol they use.

Protocol	Common Po
FTP (File Transfer Protocol)	20, 21
SSH (Secure Shell)	22
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name Service)	53
TFTP (Trivial File Transfer Protocol)	69
HTTP (Hypertext Transfer Protocol)	80
POP3 (Post Office Protocol version 3)	110
NNTP (Network News Transport Protocol)	119
NTP (Network Time Protocol)	123
IMAP4 (Internet Message Access Protocol version 4)	143
HTTPS (Hypertext Transfer Protocol Secure)	443

DNS

TCP/IP networks communicate with hosts using their IP addresses. It would be very difficult for someone to have to memorize the different IP addresses for the hosts they want to connect to on the network. A Domain Name Service (DNS) makes it easier to identify a host by a domain name. A domain name uses words rather than numbers to identify Internet hosts. Suppose you want to connect to the CompTIA Web site by using your Web browser. You would enter

```
http://www.comptia.org
```

In the address bar to go to the Comp TIA Web page. www.comptia.org would be a common name used for a numerical IP address. You could use 216.119.103.72 instead, but www.comptia.org is easier to remember. A DNS server translates these addresses. Your Web browser asks the TCP/IP protocol to ask the DNS server for the IP address of www.comptia.org. When the browser receives the address, it connects to the Web site. Remember that DNS stands for Domain Name System (or Domain Name Service) and that a DNS server translates domain names into their IP addresses.

NAT (Network Address Translation)

NAT translates one IP address to another. This can be a source address or a destination address. Two basic implementations of NAT can be used: static and dynamic

Static NAT

With static NAT, a manual translation is performed by an address translation device, translating one IP address to a different one. Typically, static NAT is used to translate destination IP addresses in packets as they come into your network, but you can translate source addresses also.

Dynamic NAT

With static address translation, you need to build the translations manually. If you have 1000 devices, you need to create 1000 static entries in the address translation table, which is a lot of work. Typically, static translation is done for inside resources that outside people want to access. When inside users access outside resources, dynamic translation is typically used. In this situation, the global address assigned to the internal user isn't that important, since outside devices don't directly connect to your internal users—they just return traffic to them that the inside user requested.

ICS (Internet Connection Sharing)

ICS (Internet Connection Sharing) is a built-in feature of Windows 98 Second Edition, Windows 2000, Windows Me, and Windows Xp. ICS provides networked computers with the capability to share a single connection to the Internet. Multiple users can use ICS to gain access to the Internet through a single connection by using Dial-Up Networking or local networking.

WINS (Windows Internet Name Service)

While DNS resolves host names to IP addresses, WINS resolves NetBIOS names to IP addresses. Windows Internet Name Service provides a dynamic database of IP address to NetBIOS name resolution mappings. WINS, determines the IP address associated with a particular network computer. This is called name resolution. WINS supports network client and server computers running Windows. WINS uses a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one. DNS is an alternative for name resolution suitable for network computers with fixed IP addresses.

SNMP (Simple Network Management Protocol)

Simple Network Management Protocol, is a TCP/IP protocol for monitoring networks and network components. SNMP uses small utility programs called agents to monitor behavior and traffic on the

network, in order to gather statistical data. These agents can be loaded onto managed devices such as hubs, NIC's, servers, routers, and bridges. The gathered data is stored in a MIB (management information base). To collect the information in a usable form, a management program console polls these agents and downloads the information from their MIB's, which then can be displayed as graphs, charts and sent to a database program to be analyzed.

NFS (Network File System)

Network File System (NFS) is a distributed file system that allows users to access files and directories located on remote computers and treat those files and directories as if they were local.

Zeroconf (Zero configuration)

Zero Configuration Networking is a set of techniques that automatically create a usable IP network without configuration or special servers. This allows unknowledgeable users to connect computers, networked printers, and other items together and expect them to work automatically. Without Zeroconf or something similar, a knowledgeable user must either set up special servers, like DHCP and DNS, or set up each computer's network settings manualy.

Zeroconf currently solves three problems :

- Choose numeric network addresses for networked items
- Figure out which computer has a certain name
- Figure out where to get services, like printing.

SMB (Server Message Block)

A file-sharing protocol designed to allow networked computers to transparently access files that reside on remote systems over a variety of networks. The SMB protocol defines a series of commands that pass information between computers. SMB uses four message types: session control, file, printer, and message. It is mainly used by Microsoft Windows equipped computers. SMB works through a client-server approach, where a client makes specific requests and the server responds accordingly. One section of the SMB protocol is specifically for filesystem access, such that clients may make requests to a file server. The SMB protocol was optimised for local subnet usage, but one could use it to access different subnets across the Internet on which MS Windows file-and-print sharing exploits usually focus. Client computers may have their own hard disks, which are not publicly shared, yet also want access to the shared file systems and printers on the server, and it is for this primary purpose that SMB is best known and most heavily used.

AFP (Apple File Protocol)

The file sharing protocol used in an AppleTalk network. In order for non-Apple networks to access data in an AppleShare server, their protocols must translate into the AFP language. AFP versions 3.0 and greater rely exclusively on TCP/IP (port 548 or 427) for establishing communication, supporting AppleTalk only as a service discovery protocol. The AFP 2.x family supports both TCP/IP and AppleTalk for communication and service discovery.

LPD (Line Printer Daemon) and Samba)

LPD is the primary UNIX printing protocol used to submit jobs to the printer. The LPR component initiates commands such as "print waiting jobs," "receive job," and "send queue state," and the LPD component in the print server responds to them. The most common implementations of **LPD** are in the official BSD UNIX operating system and the LPRng project. The Common Unix Printing System (or CUPS), which is more common on modern Linux distributions, borrows heavily from LPD. Unix and Mac OS X Servers use the Open Source **SAMBA** to provide Windows users with Server Message Block (SMB) file sharing.

WAN (Wide Area Networks) technologies:

Circuit-switched

services provide a temporary connection across a phone circuit. In networking, these are typically used for backup of primary circuits and for temporary boosts of bandwidth.

dedicated circuit

dedicated circuit is a permanent connection between two sites in which the bandwidth is dedicated to that company's use. These circuits are common when a variety of services, such as voice, video, and data, must traverse the connection and you are concerned about delay issues with the traffic and guaranteed bandwidth.

Cell-switched

cell-switched services can provide the same features that dedicated circuits offer. Their advantage over dedicated circuits is that a single device can connect to multiple devices on the same interface. The downside of these services is that they are not available at all locations, they are difficult to set up and troubleshoot, and the equipment is expensive when compared to equipment used for dedicated circuits.

Packet switching

Packet-switched services are similar to cell-switched services. Whereas cell-switched services switch fixed-length packets called cells, packet-switched services switch variable-length packets. This feature makes them better suited for data services, but they can nonetheless provide some of the QoS features that cell-switched services provide. Packet switching offers more efficient use of a telecommunication provider's network bandwidth. With packet switching, the switching mechanisms on the network route each data packet from switch to switch individually over the network using the best-available path. Any one physical link in a packet-switched network can carry packets from many different senders and for many different destinations. Where as in a circuit switched connection, the bandwidth is dedicated to one sender and receiver only.

ISDN (Integrated Services Digital Network)

Integrated Services Digital Network adapters can be used to send voice, data, audio, or video over standard telephone cabling. ISDN adapters must be connected directly to a digital telephone network. ISDN adapters are not actually modems, since they neither modulate nor demodulate the digital ISDN signal. Like standard modems, ISDN adapters are available both as internal devices that connect directly to a computer's expansion bus and as external devices that connect to one of a computer's serial or parallel ports. ISDN can provide data throughput rates from 56 Kbps to 1.544 Mbps using a T1 service.

ISDN hardware requires a NT (network termination) device, which converts network data signals into the signaling protocols used by ISDN. Some times, the NT interface is included, or integrated, with ISDN adapters and ISDN-compatible routers. In other cases, an NT device separate from the adapter or router must be implemented. ISDN works at the physical, data link, network, and transport layers of the OSI Model.

FDDI (Fiber Distributed Data Interface)

Fiber Distributed Data Interface, shares many of the same features as token ring, such as a token passing, and the continuous network loop configuration. But FDDI has better fault tolerance because of its use of a dual, counter-rotating ring that enables the ring to reconfigure itself in case of a link failure. FDDI also has higher transfer speeds, 100 Mbps for FDDI, compared to 4 - 16 Mbps for Token Ring. Unlike Token Ring, which uses a star topology, FDDI uses a physical ring. Each device in the ring attaches to the adjacent device using a two stranded fiber optic cable. Data travels in one direction on the outer strand and in the other direction on the inner strand. When all devices attached to the dual ring are functioning properly, data travels on only one ring. FDDI transmits data on the second ring only in the event of a link failure.

Media	MAC Method	Signal Propagation Method	Speed	Topologies	Maxim Conne
Fiber-optic	Token passing	Forwarded from device to device (or port to port on a hub) in a closed loop	100 Mbps	Double ring Star	500 no

T1 (T Carrier level 1)

A 1.544 Mbps point to point dedicated, digital circuit provided by the telephone companies. T1 lines are widely used for private networks as well as interconnections between an organizations LAN and the telco. A T1 line uses two pairs of wire one to transmit, and one to receive. and time division multiplexing (TDM) to interleave 24 64-Kbps voice or data channels. The standard T1 frame is 193 bits long, which holds 24 8-bit voice samples and one synchronization bit with 8,000 frames transmitted per second. T1 is not restricted to digital voice or to 64 Kbps data streams. Channels may be combined and the total 1.544 Mbps capacity can be broken up as required.

T3 (T Carrier level 3)

A T3 line is a super high-speed connection capable of transmitting data at a rate of 45 Mbps. A T3 line represents a bandwidth equal to about 672 regular voice-grade telephone lines, which is wide enough to transmit real time video, and very large databases over a busy network. A T3 line is typically installed as a major networking artery for large corporations, universities with high-volume network traffic and for the backbones of the major Internet service providers.

OCx (Optical Carrier)

Optical Carrier, designations are used to specify the speed of fiber optic networks that conforms to the SONET standard.

Level	Speed
OC-1	51.85 Mbps
OC-3	155.52 Mbps
OC-12	622.08 Mbps
OC-24	1.244 Gbps
OC-48	2.488 Gbps

X.25

X.25 is a network layer protocol that runs across both synchronous and asynchronous physical circuits, providing a lot of flexibility for your connection options. X.25 was actually developed to run across unreliable medium. It provides error detection and correction, as well as flow control, at both the data link layer (by LAPB) and the network layer (by X.25). In this sense, it performs a function similar to what TCP, at the transport layer, provides for IP. Because of its overhead, X.25 is best delegated to asynchronous, unreliable connections. If you have a synchronous digital connection, another protocol, such as Frame Relay or ATM, is much more efficient. An X.25 network transmits data with a packet-switching protocol, bypassing noisy telephone lines. This protocol relies on an elaborate worldwide network of packet-forwarding nodes that can participate in delivering an X.25 packet to its designated address.

Internet access technologies:

xDSL (Digital Subscriber Line)

xDSL is a term referring to a variety of new Digital Subscriber Line technologies. Some of these varieties are asymmetric with different data rates in the downstream and upstream directions. Others are symmetric. Downstream speeds range from 384 Kbps (or "SDSL") to 1.5-8 Mbps (or "ADSL").

Asymmetric Digital Subscriber Line (ADSL)

A high-bandwidth digital transmission technology that uses existing phone lines and also allows voice transmissions over the same lines. Most of the traffic is transmitted downstream to the user, generally at rates of 512 Kbps to about 6 Mbps.

Broadband Cable (Cable modem)

Cable modems use a broadband connection to the Internet through cable television infrastructure. These modems use frequencies that do not interfere with television transmission.

POTS / PSTN

(Plain Old Telephone Service / Public Switched Telephone Network) **POTS / PSTN** use modem's, which is a device that makes it possible for computers to communicate over telephone lines. The word modem comes from Modulate and Demodulate. Because standard telephone lines use analog signals, and computers digital signals, a sending modem must modulate its digital signals into analog signals. The computers modem on the receiving end must then demodulate the analog signals into digital signals. Modems can be external, connected to the computers serial port by an RS-232 cable or internal in one of the computers expansion slots. Modems connect to the phone line using standard telephone RJ-11 connectors.

Wireless

A wireless network consists of wireless NICs and access points. NICs come in different models including PC Card, ISA, PCI, etc. Access points act as wireless hubs to link multiple wireless NICs into a single subnet. Access points also have at least one fixed Ethernet port to allow the wireless network to be bridged to a traditional wired Ethernet network, such as the organization's network infrastructure. Wireless and wired devices can coexist on the same network.

- **WLAN (Wireless Local Area Network)** A group of computers and associated devices that communicate with each other wirelessly.
- **WPA (Wi-Fi Protected Access)** A security protocol for wireless networks that builds on the basic foundations of WEP. It secures wireless data transmission by using a key similar to WEP, but the added strength of WPA is that the key changes dynamically. The changing key makes it much more difficult for a hacker to learn the key and gain access to the network.
- **WPA2 (Wi-Fi Protected Access 2)** WPA2 is the second generation of WPA security and provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some government users.
- **WPA-Personal** A version of WPA that uses long and constantly changing encryption keys to make them difficult to decode.
- **WPA-Enterprise** A version of WPA that uses the same dynamic keys as WPA-Personal and also requires each wireless device to be authorized according to a master list held in a special authentication server.

A MAC address is 48 bits long and is represented as a hexadecimal number. Represented in hex, it is 12 characters in length, where each character is 4 bits. To make it easier to read, the MAC address is represented in a dotted hexadecimal format, like this: **FFFF. FFFF.FFFF**.

Some formats use a colon (:) instead; and in Some cases, the colon separator is spaced after every two hexadecimal digits, like this: **FF:FF:FF:FF:FF:FF.** the first six digits of a MAC address are associated with the vendor, or maker, of the NIC.

Each vendor has one or more unique sets of six digits. These first six digits are commonly called the ***organizationally unique identifier (OUI)***. The last six digits are used to represent the NIC uniquely within the OUI value. In theory, each NIC has a unique MAC address. In reality however, this is probably not true. What is important for your purposes is that each of your NICs has a unique MAC address within the same physical or logical segment.

A logical segment is a virtual LAN (VLAN) and is referred to as a broadcast domain .

Some devices, such as Cisco routers, might allow you to change the MAC address for a NIC, while others won't.

Every data link layer frame has two MAC addresses: a **source MAC address** of the host creating the frame and a **destination MAC address** for the device (or devices, in the cast of a broadcast or multicast) intended to receive the frame.

If only one device is to receive the frame, a unicast destination MAC address is used. If all devices need to receive the frame, a destination broadcast address is used.

When all the binary bits are enabled for a MAC address, this is referred to as a **local broadcast address**: FFFF.FFFF.FFFF.

Network protocols in terms of routing, addressing schemes, interoperability and naming conventions:

TCP/IP

Transmission Control Protocol, A connection based Internet protocol responsible for breaking data into packets, which the IP protocol sends over the network. IP is located at the TCP/IP Internet layer which corresponds to the network layer of the OSI Model. IP is responsible for routing packets by their IP address.

IP is a connectionless protocol. which means, IP does not establish a connection between source and destination before transmitting data, thus packet delivery is not guaranteed by IP. Instead, this must be provided by TCP. TCP is a connection based protocol and, is designed to guarantee delivery by monitoring the connection between source and destination before data is transmitted. TCP places packets in sequential order and requires acknowledgment from the receiving node that they arrived properly before any new data is sent.

TCP/IP model

Application layer	DHCP - DNS - FTP - HTTP - IMAP4 - IRC - NNTP - XMPP - MIME - POP3 - SIP - SMTP - SNMP - SSH - TELNET - E RTP - RTCP - TLS/SSL - SDP - SOAP - L2TP - PPTP
Transport layer	This layer deals with opening and maintaining connections, ensuring that packets are in fact received. This flow-control and connection protocols exist, such as: TCP - UDP - DCCP - SCTP - GTP
Network layer	IP (IPv4 - IPv6) - ARP - RARP - ICMP - IGMP - RSVP - IPSec - IPX/SPX
Data link layer	ATM - DTM - Ethernet - FDDI - Frame Relay - GPRS - PPP
Physical layer	Ethernet physical layer - ISDN - Modems - PLC - RS232 - SONET/SDH - G.709 - Wi-Fi

IPX/SPX

IPX/SPX is the primary protocol of Novell NetWare (in particular, versions 4.0 and earlier, though it can be used on all versions). Internetwork Packet Exchange/Sequenced Packet Exchange developed by Novell and is used primarily on networks that use the Novell NetWare network operating system. The IPX and SPX protocols provide services similar to those offered by IP and TCP. Like IP, IPX is a connectionless network layer protocol. SPX runs on top of IPX at the transport layer and, like TCP, provides connection oriented, guaranteed delivery. IPX/SPX provides many of the same features as TCP/IP, and is a routable transport protocol that allows networks to be segmented. However, network segmentation with IPX/SPX is done with network numbers and not with subnet masks. IPX/SPX is also similar to TCP/IP because IPX/SPX relies on internal protocols for network communication.

IPX

IPX is similar to the operation of UDP of TCP/IP. IPX is a connectionless datagram transfer service. Because it is connectionless, like UDP, it does not require any preliminary connection setup to transmit the data packets. A disadvantage to connectionless communication is that flow control and error correction are not provided during network communication. In addition, packet delivery is not guaranteed. IPX also provides addressing and routing of packets within and between network segments.

SPX

SPX is similar to the operation of TCP of TCP/IP. SPX is connection-oriented data transfer over IPX. Because SPX is connection oriented, flow control and error correction are provided along with packet delivery acknowledgments. SPX allows a single packet to remain unacknowledged at one time. If a packet is unacknowledged, the packet is retransmitted a total of 8 times. If there's no acknowledgment, SPX considers the connection failed.

SPXII

SPXII is an enhancement to SPX. SPXII has several improvements over SPX. SPXII allows more than one packet to remain unacknowledged. SPXII also allows for a larger packet size, which improves network performance by reducing the number of acknowledgment packets placed on the network.

NetBEUI

NetBIOS Enhanced User Interface was designed as a small, efficient protocol for use in department-sized LANs of 20-200 computers that do not need to be routed to other subnets. NetBEUI is used almost exclusively on small, non-routed networks. A LAN-only (non-routable) protocol used in early Windows networks based on the NetBIOS API, NetBEUI is a Windows protocol that even Microsoft doesn't recommend for any but the most isolated networks. NetBEUI isn't required for NetBIOS functionality. As an extension of NetBIOS, NetBEUI is not routable, therefore networks supporting NetBEUI must be connected with bridges, rather than routers, like NetBIOS, the NetBEUI interface must be adapted to routable protocols like TCP/IP for communication over WANs.

AppleTalk

The AppleTalk routing protocol is, amazing as it may sound, used by Macintosh networks. There are two important factors to understand about the AppleTalk protocol: zones and network numbers. AppleTalk network numbers assign AppleTalk networks unique numerical values that identify them as segments. Clients and servers can be part of only one network number. Because AppleTalk is routable, clients can access servers from any network number. AppleTalk also uses zones to aid clients in browsing an AppleTalk network. Zones allow servers, printers, and clients to be grouped logically for the purpose of resource access. Unlike network numbers, servers, printers, and clients can be part of more than one zone. Having membership in more than one zone allows clients easier access to network resources. Clients need not use the Chooser to view the resources of multiple zones.

TCP (Transmission Control Protocol)

Transmission Control Protocol uses a reliable delivery system to deliver layer 4 segments to the destination. This would be analogous to using a certified, priority, or next-day service with the Indian Speed Post;Service.

For example, with a certified letter, the receiver must sign for it, indicating the destination actually received the letter: proof of the delivery is provided. **TCP** operates under a similar premise: it can detect whether or not the destination received a sent segment. With the postal example, if the certified letter got lost, it would be up to you to resend it; with TCP, you don't have to worry about what was or wasn't received—TCP will take care of all the tracking and any necessary resending of lost data for you.

TCP's main responsibility is to provide a reliable full-duplex, connection-oriented, logical service between two devices.

TCP goes through a three-way handshake to establish a session before data can be sent. Both the source and destination can simultaneously send data across the session. It uses windowing to implement flow control so that a source device doesn't overwhelm a destination with too many segments. It supports data recovery, where any missed or corrupted information can be re-sent by the source. Any packets that arrive out of order, because the segments traveled different paths to reach the destination, can easily be reordered, since segments use sequence numbers to keep track of the ordering.

UDP (User Datagram Protocol)

UDP uses a best-effort delivery system, similar to how first class and lower postal services of the Indian Postal Service work. With a first class letter (post card), you place the destination address and put it in your mailbox, and hope that it arrives at the destination.

With this type of service, nothing guarantees that the letter will actually arrive at the destination, but in most instances, it does. If, however, the letter doesn't arrive at the destination, it's up to you, the letter writer, to resend the letter: the post office isn't going to perform this task for you.

UDP operates under the same premise: it does not guarantee the delivery of the transport layer segments. While TCP provides a reliable connection, UDP provides an unreliable connection.

UDP doesn't go through a three-way handshake to set up a connection—it simply begins sending the data. Likewise, UDP doesn't check to see whether sent segments were received by a destination; in other words, it doesn't use an acknowledgment

Some commonly used ports

Port Number	Service
80	HTTP
21	FTP
110	POP3
25	SMTP
23	Telnet

FTP (File Transfer Protocol)

One of the earliest uses of the Internet, long before Web browsing came along, was transferring files between computers. The **File Transfer Protocol (FTP)** is used to connect to remote computers, list shared files, and either upload or download files between local and remote computers.

FTP runs over TCP, which provides a connection-oriented, guaranteed data-delivery service. **FTP** is a character-based command interface, although many FTP applications have graphical interfaces. **FTP** is still used for file transfer purposes, most commonly as a central FTP server with files available for download. Web browsers can make FTP requests to download programs from links selected on a Web page.

You should become familiar with the basic commands available in an FTP session. To begin a characterbased command session on a Windows computer, follow these steps.

- Open a Command prompt window, type ***ftp*** at the prompt, and press Enter.
- This will begin an FTP session on the local machine but will not initialize a connection to another machine.
- Without a connection to another machine, you will not be able to do anything. To connect, type ***open example.com*** or ***open 10.10.10.1***, in which exmple.com or 10.10.10.1 is the name or IP address of a host that is available as an FTP server. Most FTP servers require a logon id and password, or they will accept anonymous connections. At this point you will be prompted for a logon ID and password.
- Once you are connected, you can list the files on the remote server by typing ***dir***.
- If you have create privileges on the remote server, you can create a new directory by typing ***mkdir***.
- To download a file, type ***get filename.txt*** where filename.txt is the name of the file you are downloading.
  To upload a file, type***put filename.txt***.

SFTP (Secure File Transfer Protocol)

SSH File Transfer Protocol or SFTP is a network protocol that provides file transfer and manipulation functionality over any reliable data stream.

TFTP (Trivial File Transfer Protocol)

TFTP is used when a file transfer does not require an acknowledgment packet during file transfer. TFTP is used often in router configuration. TFTP is similar in operation to FTP. TFTP is also a command-line-based utility.

One of the two primary differences between TFTP and FTP is ***speed*** and ***authentication***. Because TFTP is used without acknowledgment packets, it is usually faster than FTP. TFTP does not provide user authentication like FTP and therefore the user must be logged on to the client and the files on the remote computer must be writable. TFTP supports only unidirectional data transfer (unlike FTP, which supports bi-directional transfer). TFTP is operated over port 69.

SMTP (Simple Mail Transfer Protocol)

SMTP is a standard electronic-mail protocol that handles the sending of mail from one SMTP to another SMTP server. To accomplish the transport, the SMTP server has its own MX (mail exchanger) record in the DNS database that corresponds to the domain for which it is configured to receive mail.

When equipped for two-way communication, mail clients are configured with the address of a POP3 server to receive mail and the address of an SMTP server to send mail. The clients can configure server parameters in the properties sheets of the mail client, basing the choices on an FQDN or an IP address.

SMTP uses TCP for communication and operates on port 25. Simple Mail Transfer Protocol (SMTP) is the application-layer protocol used for transmitting e-mail messages. SMTP is capable of receiving e-mail messages, but it's limited in its capabilities. The most common implementations of SMTP are in conjunction with either POP3 or IMAP4. For example, users download an e-mail message from a POP3 server, and then transmit messages via an SMTP server

HTTP (Hypertext Transfer Protocol)

HTTP is often called the protocol of the Internet. HTTP received this designation because most Internet traffic is based on HTTP. When a user requests a Web resource, it is requested using HTTP. The following is a Web request:

http://www.example.com

When a client enters this address into a Web browser, DNS is called to resolve the Fully Qualified Domain Name (FQDN) to an IP address. When the address is resolved, an HTTP get request is sent to the Web server. The Web server responds with an HTTP send response. Such communication is done several times throughout a single session to a Web site. HTTP uses TCP for communication between clients and servers. HTTP operates on port 80.

HTTPS (Hypertext Transfer Protocol Secure)

HTTP is for Web sites using additional security features such as certificates. HTTPS is used when Web transactions are required to be secure. HTTPS uses a certificatebased technology such as VeriSign.

Certificate-based transactions offer a mutual authentication between the client and the server. Mutual authentication ensures the server of the client identity, and ensures the client of the server identity. HTTPS, in addition to using certificate-based authentication, encrypts all data packets sent during a session.

Because of the encryption, confidential user information cannot be compromised. To use HTTPS, a Web site must purchase a certificate from a third-party vendor such as VeriSign, CertCo, United States Postal Service, or other certificate providers. When the certificate is issued to a Web site from a third-party vendor, the Web site is using trusted communication with the client. The communication is trusted because the third party is not biased toward either the Web site or the client. To view a certificate during a HTTPS session, simply double-click the lock icon in the lower-right area of the Web browser. HTTPS operates on port 443 and uses TCP for communication.

POP3 / IMAP4 (Post Office Protocol version 3 / Internet Message Access Protocol version 4)

Post Office Protocol 3 (POP3) and Internet Message Access Protocol 4 (IMAP4) are two application-layer protocols used for electronic messaging across the Internet. POP3 is a protocol that involves both a server and a client. A POP3 server receives an e-mail message and holds it for the user. A POP3 client application periodically checks the mailbox on the server to download mail. POP3 does not allow a client to send mail, only to receive it. POP3 transfers e-mail messages over TCP port 110.

IMAP4 is an alternate e-mail protocol. IMAP4 works in the same way as POP3, in that an e-mail message is held on a server and then downloaded to an e-mail client application. Users can read their e-mail

message locally in their e-mail client application, but they can't send an e-mail message using IMAP4. When users access e-mail messages via IMAP4, they have the option to view just the message header, including its title and the sender's name, before downloading the body of the message. Users can create, change, or delete folders on the server, as well as search for messages and delete them from the server.

To perform these functions, users must have continued access to the IMAP server while they are working with e-mail messages. With IMAP4, an e-mail message is copied from the server to the e-mail client. When a user deletes a message in the e-mail client, the message remains on the server until it is deleted on the server. POP3 works differently in that an e-mail message is downloaded and not maintained on the server, unless configured otherwise. Therefore, the difference between POP3 and IMAP4 is that IMAP4 acts like a remote file server, while POP3 acts in a store-and-forward manner in its default configuration. (You can configure POP3 clients to leave copies of messages on the server, if you prefer.)

Both Microsoft and Netscape Web browsers have incorporated POP3. In addition, the Eudora and Microsoft Outlook Express e-mail client applications support both POP3 and IMAP4.

Telnet

Short for Telecommunication Network, a virtual terminal protocol allowing a user logged on to one TCP/IP host to access other hosts on the network. Many people use remote control applications to access computers at their workplace from outside the network. In remote control, a session appears in which the user is able to manage the files on the remote computer, although the session appears to be functioning locally. Telnet is an early version of a remote control application.

Telnet is very basic; it offers solely character-based access to another computer. If you want to see a person's graphical desktop, you would need a different type of protocol, such as Remote Desktop Protocol (RDP), Independent Computing Architecture (ICA), or X Windows. Telnet acts as a user command with an underlying Transmission Control Protocol/Internet Protocol (TCP/IP) protocol that handles the establishment, maintenance, and termination of a remote session. The difference between using Telnet and a protocol such as File Transfer Protocol (FTP), is that Telnet logs you directly on to the remote host, and you see a window into that session on your local computer. A typical Telnet command might be as follows:

```
telnet example.com
```

Because this particular host is invalid, this command will have no result. However, if it were a valid host the remote computer would ask you to log on with a user ID and password. A correct ID and password would allow you to log on and execute Telnet commands.

You can often use Telnet to manage equipment that lacks a monitor. For example, most routers have Telnet enabled so that the administrator can log in and manage the router. Telnet also provides a quick check to make certain that network connectivity is functioning. Because Telnet sits at the application layer, if it can connect to a remote host, you can be certain that network connectivity between the two hosts is operational, as well as all lower-layer protocols.

SSH (Secure Shell)

is a program for logging in to and executing commands on a remote machine. It provides secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. When SSH connects and logs in to a specified computer, the user must prove his/her identity to the remote machine which is transmitted across the connection using one of three forms of data encryption. This process makes SSH impervious to Internet eavesdroppers who might otherwise steal account information.

ICMP (Internet Control Message Protocol)

ICMP provides network diagnostic functions and error reporting. One of the most used IP commands is the Packet Internet Grouper (PING) command. When a host PINGS another client, it sends an ICMP ECHO request, and the receiving host responds with an ICMP ECHO REPLY. PING checks network connectivity on clients and routers. ICMP also provides a little network help for routers. When a router is being overloaded with route requests, the router sends a source quench message to all clients on the network, instructing them to slow their data requests to the router.

ARP / RARP (Address Resolution Protocol / Reverse Address Resolution Protocol)

The Address Resolution Protocol (ARP) is an Internet layer protocol that helps TCP/IP network components find other devices in the same broadcast domain. ARP uses a local broadcast (255.255.255.255) at layer 3 and FF:FF:FF:FF:FF:FF at layer 2 to discover neighboring devices. Basically stated, you have the IP address you want to reach, but you need a physical (MAC) address to send the frame to the destination at layer 2.

ARP resolves an IP address of a destination to the MAC address of the destination on the same data link layer medium, such as Ethernet. Remember that for two devices to talk to each other in Ethernet (as with most layer 2 technologies), the data link layer uses a physical address (MAC) to differentiate the machines on the segment. When Ethernet devices talk to each other at the data link layer, they need to know each other's MAC addresses.

RARP is sort of the reverse of an ARP. In an ARP, the device knows the layer 3 address, but not the data link layer address. With a RARP, the device doesn't have an IP address and wants to acquire one. The only address that this device has is a MAC address. Common protocols that use RARP are BOOTP and DHCP

NTP (Network Time Protocol)

The Network Time Protocol is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver or modem. It provides accuracy's typically within a millisecond on LANs and up to a few tens of milliseconds on WANs.

SNMP

SNMP is a two-way network management protocol. SNMP consists of two components, the SNMP Agent, and the SNMP Management Console. The SNMP Management Console is the server side for SNMP. The management console sends requests to the SNMP Agents as get commands that call for information about the client.

The SNMP Agent responds to the Management Console's get request with a trap message. The trap message has the requested information for the Management Console to evaluate. Security can be provided in many ways with SNMP; however, the most common form of security for SNMP is the use of community names, associations that link SNMP Agents to their Management Consoles:

- Agents, by default, respond only to Management Consoles that are part of the same community name.
- If an SNMP Agent receives a request from a Management Console that is not part of the same community name, then the request for information is denied.

Because SNMP is an industry-standard protocol, heterogeneous environments are common. Many vendors provide versions of SNMP Management Consoles. Hewlett Packard, for example provides HP Open View (one of the most popular Management Consoles on the market); Microsoft provides SNMP Server with the Windows NT and 2000 Resource Kits and Systems Management Server. SNMP Management Consoles request information according to a Management Information Base (MIB) format. An MIB is a numeric value that specifies the type of request, and to which layer of the OSI model the request is being sent.

SCP (Secure Copy Protocol)

Secure Copy or SCP is a means of securely transferring computer files between a local and a remote host or between two remote hosts, using the Secure Shell (SSH) protocol. The protocol itself does not provide authentication and security; it expects the underlying protocol, SSH, to secure this.

The SCP protocol implements file transfers only. It does so by connecting to the host using SSH and there executes an SCP server (scp). The SCP server program is typically the very same program as the SCP client.

LDAP (Lightweight Directory Access Protocol)

Lightweight Directory Access Protocol, or LDAP, is a networking protocol for querying and modifying directory services running over TCP/IP.

A directory is a set of information with similar attributes organized in a logical and hierarchical manner. The most common example is the telephone directory, which consists of a series of names organized alphabetically, with an address and phone number attached.

An LDAP directory often reflects various political, geographic, and/or organizational boundaries, depending on the model chosen. LDAP deployments today tend to use Domain Name System (DNS) names for structuring the topmost levels of the hierarchy. Deeper inside the directory might appear entries representing people, organizational units, printers, documents, groups of people or anything else which represents a given tree entry.

IGMP (Internet Group Multicast Protocol)

The Internet Group Management Protocol is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

LPR (Line Printer Remote)

The Line Printer Daemon protocol/Line Printer Remote protocol (or LPD, LPR) also known as the Berkeley printing system, is a set of programs that provide printer spooling and network print server functionality for Unix-like systems.

The most common implementations of LPD are the official BSD UNIX operating system and the LPRng project. The Common Unix Printing System (or CUPS), which is more common on modern Linux distributions, borrows heavily from LPD.

A printer that supports LPD/LPR is sometimes referred to as a "TCP/IP printer" (TCP/IP is used to establish connections between printers and workstations on a network), although that term seems equally applicable to a printer that supports CUPS.