

The Test

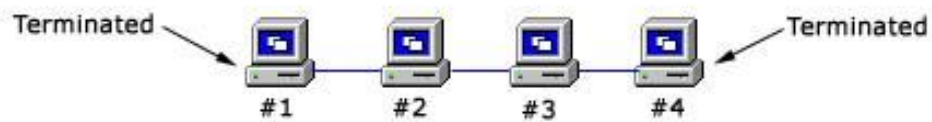
- 80 Questions
- 90 Minutes
- The exam is graded on a scale of 100 - 900 and 554 is the minimum passing score

Network Models

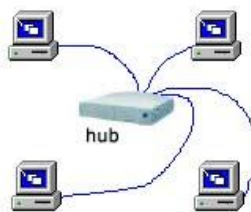
- Peer to Peer
- Client/Server
- Centralized
- Mixed Mode

Topologies

Bus



Star



Hybrid



Mesh

In a true mesh topology every node has a connection to every other node in the network. A full mesh network can be very expensive, but provides redundancy in case of a failure between links.

Differentiate logical and physical topologies

Network Categories

- LAN
- CAN
- MAN
- WAN
- Internet
- Intranet
- Extranet

Transmission Types

- Unicast – data is transferred from specific source to specific destination
- Broadcast -data goes from a source to all other nodes on a network
- Multicast- data is transferred from a source to specific nodes that are members of a multicast group.

Media Access Methods

- Multiplexed –central device combines signals from multiple nodes and transmits the combined signal. Often uses a time division multiplexing device (TDM) or frequency division multiplexing device (FDM)
- Polling – central device contacts each node to see if it has data
- Demand priority – each node signals it is ready to send.
- Token based- like a token ring
- CSMA/CD – Carrier Sense Multiple Access/Collision Detection- IEEE 802 standard
- CSMA/CA – Carrier Sense Multiple Access/Collision Avoidance

Transmissions

- Serial data transmissions are sent on per clock cycle across a single transmission medium.
- Parallel transmissions are transmitted across multiple transmission lines.
- Baseband transmissions are digital signaling sending data over a single transmission medium using the entire bandwidth of the medium.
- Broadband transmissions have analog signaling used to send data over a medium using a portion of the bandwidth.

Hardware

- ▶ **Network Interface Card:** - A Network Interface Card, often abbreviated as NIC, is an expansion board you insert into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network, protocol and media, although some can serve multiple networks.
- ▶ **Hub:** - A hub is used to connect computers on an Ethernet network.
- ▶ **Repeater:** - Boosts signals in order to allow a signal to travel farther and prevent attenuation. Attenuation is the degradation of a signal as it travels farther from its origination. Repeaters do not filter packets and will forward broadcasts. Both segments must use the same access method, which means that you can't connect a token ring segment to an Ethernet segment. Repeaters can connect different cable types.

Bridges

- ▶ Functions the same as a repeater, but can also divide a network in order to reduce traffic problems. A bridge can also connect unlike network segments (ie. token ring and ethernet). Bridges create routing tables based on the source address. If the bridge can't find the source address it will forward the packets to all segments.
Bridging methods:
 - Transparent - Only one bridge is used.
 - Source-Route - Bridging address tables are stored on each PC on the network
 - Spanning Tree - Prevents looping where there exists more than one path between segments
- Bridges listen to traffic and capture the source address for each packet. Then use that data to build a bridge routing table of all MAC addresses on each of its interfaces.
- Transparent Bridges are bridges with the same type of network.
- Source route Bridges are designed for Token Ring networks.

- Translational Bridges are used for two different types of networks to exchange data.

Gateway - Often used as a connection to a mainframe or the internet. Gateways enable communications between different protocols, data types and environments. This is achieved via protocol conversion, whereby the gateway strips the protocol stack off of the packet and adds the appropriate stack for the other side.

Router

A router is similar to a switch, but it can also connect different logical networks or subnets and enable traffic that is destined for the networks on the other side of the router to pass through. Routers can connect networks that use dissimilar protocols. Routers also typically provide improved security functions over a switch. Unroutable protocols can't be forwarded.

Switches

A switch prevents traffic jams by ensuring that data goes straight from its origin to its proper destination, with no wandering in between. Switches remember the address of every node on the network, and anticipate where data needs to go. It only operates with the computers on the same LAN. It isn't smart enough to send data out to the internet, or across a WAN. These functions require a router.

- Cut Through Switch-is a switching method for packet switching systems, wherein the switch starts forwarding a frame (or packet) before the whole frame has been received, normally as soon as the destination address is processed. This technique reduces latency through the switch, but decreases reliability
- Store and forward switch – sends the entire packet

Modems

- ▶ The modem is a device that converts digital information to analog by MODulating it on the sending end and DEModulating the analog information into digital information at the receiving end. Most modern modems are internal, however, they can be internal or external. External modems are connected to the back of the system board via a RS-232 serial connection. Internal modems are installed in one of the motherboard's PCI or ISA expansion slots depending on the modem. The modem contains an RJ-11 connection that is used to plug in the telephone line. Modems have different transmission modes as follows:
 - Simplex - Signals can be passed in one direction only.
 - Half Duplex - Half duplex means that signals can be passed in either direction, but not in both simultaneously. Half-duplex modems can work in full-duplex mode.
 - Full Duplex - Full duplex means that signals can be passed in either direction simultaneously.
- ▶ Modems can also be classified by their speed which is measured by the BAUD rate. One baud is one electronic state change per second. Since a single state change can involve more

than a single bit of data, the Bits Per Second(BPS) unit of measurement has replaced it as a better expression of data transmission speed. Common modem speeds are V.34 at 28.8 kbps, V.34+ at 33.6 kbps and V.90 at 56 Kbps.

- ▶ **Proxy** - A proxy server acts as a middle-man between clients and the Internet providing security, administrative control, and caching services. When a user makes a request for an internet service and it passes filtering requirements, the proxy server looks in its local cache of previously downloaded web pages. If the item is found in cache, the proxy server forwards it to the client. This reduces bandwidth through the gateway. If the page is not in the cache, the proxy server uses Network Address Translation (NAT) to use one of its own IP addresses to request the page from the appropriate server. In recent years NAT capability is simply included with the firewall rather than in a separate device/service.
- ▶ **Firewall** - Either a hardware or software entity that protects a network by stopping network traffic from passing through it. In most cases, a firewall is placed on the network to allow all internal traffic to leave the network (emails to the outside world, web access, etc.), but stop unwanted traffic from the outside world from entering the internal network.

Cabling

UTP

Cat 1 Low speed analog, less than 1 MHz. Telephone, door bell, etc.

Cat 2 Analog line less than 10 MHz Telephone

Cat 3 Up to 16 MHz or 100 Mbps (Mega bits per second) Voice transmissions

Cat 4 Up to 20 MHz/ 100 MBPS Used in data lines, Ethernet networks

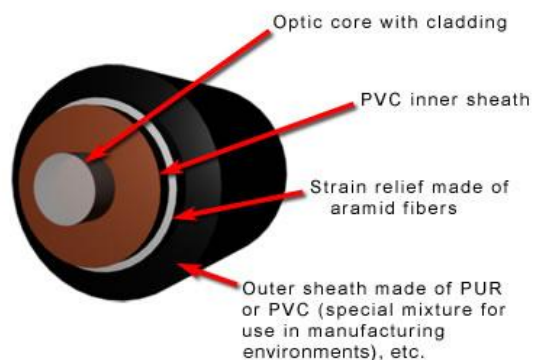
Cat 5 100 MHz / 100 MBPS The most common type of network cable found.

This type of cable is also often referred to as UTP or Unshielded Twisted Pair cable. This literally means that the wires in the cable are in pairs, twisted together without any additional shielding. As you can see each category cable is somewhat faster and more robust than the last. It should be noted that although category 4 can be used for networks, it almost never is. You will usually see category 5 cable, and increasingly category 6. There is also a category 7 but as of 4th quarter 2008 it is not widely seen in use.

- Unshielded Twisted Pair (100 meters up to 1 Gbps)
- Shielded Twisted Pair (100 meters. Most common in token ring networking)
- 8 wire RJ 45 connector (as opposed to the 4 wire RJ 11 phone connector)

Name	Standard	Cable Type	Connector	Maximum Length	Speed
10Base-T	802.3i	Category 3 or better UTP cable	RJ-45	100 meters (328 ft)	10 mbps
10Base-FL	802.3j	Fiber optic cable	ST	2000 meters	10 mbps
100Base-TX	802.3u	Cat 5 twisted pair	RJ-45	100 meters (328 ft)	100 mbps
100Base-FX	802.3u	Fiber Optic	ST, SC	2000 meters	100 mbps
1000Base-T	802.3ab	CAT5e or higher	RJ-45	100 meters (328 ft)	1 gbps
1000Base-LX	802.3z	Laser over fiber	SC	Up to 5000 meters	1 gbps
1000Base-SX	802.3z	Short wavelength laser over fiber	SC	Up to 550 meters	1 gbps
1000Base-CX	802.3z	Twinax or short haul copper	9-Pin shielded D-subminiature connector, or 8-pin ANSI fiber channel type 2 (HSSC) connector.	25 meters	1 gbps

Fiber Optic



There are many types of plugs and sockets available to connect optical fibers; the most common connector used with fiber optic cable are:

- **ST (Straight Tip) connector:** It is barrel shaped and is similar to a BNC connector.

- **SC (Subscriber Connector or Standard Connector):** Easier to connect in a confined space and it is squared faced.

Single Mode

- The Single-mode Fiber (SMF) is a single strand of glass fiber with core diameter less than 10 microns and has one mode of transmission.
- It carries higher bandwidth of data, approximately 50 times more than Multimode Fiber and has speeds up to 25,000 Gbps on paper.
- The SMF is more expensive than the Multimode Fiber Optic Cables and requires a light source with a narrow spectral width for propagation.
- These are normally used for local area networks

Multi Mode

- Multi-mode fiber (MMF) is made of glass fibers with core diameter in the range of 50 to 100 microns and can carry data of more than 5 Gbps, which equals a million megabits.
- It meets the bandwidth needs of the new high performance applications such as Streaming Audio/video, Multimedia, and Networking.
- The industry has come up with next generation of fiber optic patch cable, 10 Gigabit (10GigE). The 10 Gigabit fiber which has a 50um fiber core and provides nearly 3 times more bandwidth than the conventional 62.5um fiber optic patch cables. It is typically used in installations up to 2000 meters in length.
- These are normally used for wide area networks.

Network Connection Types

DS0-64 kilobits per second Standard phone line

ISDN-128 kilobits per second. 2 DS0 lines working together to provide a high speed data connection.

T1-1.54 megabits per second. 24 DS0 lines working as one. 23 carry data, and one carries information about the other lines. This type of connection is becoming quite common for schools and businesses.

T3-43.2 megabits per second. 672 DS0 lines working together. This is the equivalent of 28 T1 lines.

OC3 -155 megabits per second

All OC lines are optical and do not use traditional phone lines. These are quite fast and quite expensive. They are often found at telecommunications companies.

OC12- 622 megabits per second . The equivalent of 336 T1 lines or 8064 phone lines.

OC48 -2.5 gigabits per second. The equivalent of 4 OC 12 lines

Cable - While cable modem technology can theoretically support up to about 30 Mbps, most providers offer service with between 1 Mbps and 6 Mbps bandwidth for downloads, and bandwidth between 128 Kbps and 768 Kbps for uploads.

DSL - Service providers advertise DSL speed in terms of bandwidth ratings. Bandwidth numbers advertised for residential DSL service range from 128 Kbps to 3 Mbps (3000 Kbps).

Fiber Optic – increasingly fiber optic connections for home and small business are becoming common. These get much faster speeds than cable or dsl. Up to 50 mbps download and 15 mbps upload (as of October 2008)

Transmissions

- ▶ Serial data transmissions are sent on per clock cycle across a single transmission medium.
- ▶ Parallel transmissions are transmitted across multiple transmission lines.
- ▶ Baseband transmissions are digital signaling sending data over a single transmission medium using the entire bandwidth of the medium.
- ▶ Broadband transmissions have analog signaling used to send data over a medium using a portion of the bandwidth.

Protocols

21- FTP (File Transfer Protocol) For transferring files between computers.

23-TelnetUsed to remotely log on to a system. You can then use a command prompt or shell to execute commands on that system. Popular with network administrators.

25 SMTP (Simple Mail Transfer Protocol) Send email.

43-WhoIS A command that queries a target IP address for information.

53-DNS (Domain Name Service) Translates URL's into Web Addresses

80-HTTP (Hyper Text Transfer Protocol) Display web pages

110-POP3 (Post Office Protocol Version 3)Retrieve email.

194-IRC (Internet Relay Chat)Chat Rooms

ICMP (Internet Control Message Protocol) These are simply packets that contain error message, informational messages, and control messages no specific port

You should note that this list is not complete. There are dozens of other protocols, but for now these will suffice. All of these protocols are part of a suite of protocols referred to as TCP/IP, or Transmission Control Protocol/Internet Protocol. The most important thing for you to realize is that the communication on networks takes place via packets, and those packets are transmitted according to certain protocols, depending on the type of communication occurring **For a full list check**
<http://www.protocols.com/protocols.htm>

Network Utilities to KNOW

- Ipconfig
- Ping
- Tracert
- Netstat
- Nslookup
- nbtstat

7 Layers of the OSI Model

- **Application Layer:** This layer interfaces directly to and performs common application services for the application processes.
- **Presentation Layer:** The Presentation layer relieves the Application layer of concern regarding syntactical differences in data representation within the end-user systems.-POP, SMTP, DNS, FTP, Telnet
- **Session Layer:** The Session layer provides the mechanism for managing the dialogue between end-user application processes.-NetBIOS
- **Transport Layer:** This layer provides end to end communication control.-TCP
- **Network Layer:** This layer routes the information in the network.-IP, ARP, ICMP
- **Data Link-**This layer describes the logical organization of data bits transmitted on a particular medium. It is also divided into two sub layers: the Media Access Control layer (MAC) and the Logical Link Control layer (LLC).-SLIP, PPP
- **Physical**
 - This layer describes the physical properties of the various communications media, as well as the electrical properties and interpretation of the exchanged signals. In other words this is the actual NIC, Ethernet Cable, etc.

DHCP

DHCP stands for Dynamic Host Configuration Protocol and provides a solution that automatically assigns IP addresses to computers on a network

- Discover (client to server)
- Offer (server to client)
- Request (client to server)

BootP is a local broadcast that cannot be sent through routers. So you either have a DHCP server on every subnet, or a DHCP relay agent

DNS

DNS Record Entries

- ▶ **A** - The A-record is used for hosts on a network. It is used to translate human friendly domain names such as "www.mcmce.com" into an IP-addresses such as 206.67.72.48.
- ▶ **CNAME** - CNAME (canonical name) records are used to create aliases. Often computers on the Internet have multiple functions such as web server, FTP server, mail server etc. To mask this, CNAME-records can be used to give a single computer multiple names (aliases). For example computer "xyz.com" may be both a web-server and an ftp-server, so two CNAME-records are defined: "www.xyz.com" = "xyz.com" and "ftp.xyz.com" = "xyz.com".
- ▶ **MX** - MX (mail exchanger) records identify mail server(s) responsible for a domain name. When sending an e-mail to "user@xyz.com", your mail server must first look up the MX record for "xyz.com" to see which mail server actually handles mail for "xyz.com".
- ▶ **NS** - NS (name server) records identify DNS servers responsible (authoritative) for a zone.
- ▶ **PTR** - PTR (pointer) records map IP addresses to domain names which is the reverse of A-records.

HOSTS File

- Plain Text on the client
- Provides alternative method of name resolution
- Look in C:\Windows\System32\drivers\etc

NetBIOS

- Must be resolved to MAC Addresses
- The original NetBios name resolution method was to broadcast a name and wait for a response from the device with the name.
- LMHosts file (like host file but for NetBios)

NetBios

- ⦿ There are several different methods of resolving names to IP addresses. Before getting into the different methods, it is important to understand the role of NetBIOS. When talking about NetBIOS, we typically refer to the concept of NetBIOS name which is the name assigned to your computer. NetBIOS allows applications to talk to each other using protocols such as TCP/IP that support NetBIOS. NetBIOS is typically seen in other forms such as Netbeui and NetBT. These are the main functions that NetBIOS serves: Starting and stopping sessions.
- ⦿ Name registration
- ⦿ Session layer data transfer(reliable)
- ⦿ Datagram data transfer(unreliable)

Protocol driver and network adapter management functions

A NetBIOS name is either a unique name or a group name, the difference being that a unique name is used for communication with a specific process on a computer, whereas a group name is for communication with multiple clients. NetBIOS name resolution resolves a computer's NetBIOS name to an IP address. Microsoft offers several different ways to resolve Netbios names and each will be discussed below. **Local Broadcast** - If the destination host is local, then first the NetBIOS name cache is checked and a broadcast is not sent. If it is not found here, then a name query broadcast is sent out that includes the destination NetBIOS name. Each computer that receives the broadcast checks to see if it belongs to the name requested. The computer that owns the name then uses ARP to determine the MAC address of the source host. Once obtained a name query response is sent. NOTE: Some routers do not support the forwarding of these broadcasts as they use UDP ports 137 and 138.

WINS

Microsoft's definition of WINS is "An enhanced NetBIOS Name Server(NBNS) designed by Microsoft to eliminate broadcast traffic associated with the B-node implementation of NetBIOS over TCP/IP. It is used to register NetBIOS names and resolve them to IP addresses for both local and remote hosts." If a WINS server is configured, then name resolution requests are sent directly to it and in turn the WINS server will send the IP address to the requesting client. If the WINS server can't resolve the name for some reason, then it will use a broadcast to try to resolve the name. A secondary WINS server can be configured to prevent such situations. WINS is dynamically updated which gets rid of the need for lmhosts files. If a client is configured to use WINS then it will register it's name and IP address with the WINS server. When the computer is turned off, it

releases its lease on that name which may be used by a different computer. With Windows 2000, Microsoft has introduced Dynamic DNS (DDNS) which may be the beginning of the end for WINS and NETBIOS.

Frame Types

Frame Types

A frame type is the format of the packet that your Operating System will use to communicate over your network. Below is a table of the different types:

802.1	Internetworking
802.2	Logical link control - LLC adds header information that identifies the upper layer protocols sending the frame.
802.3	Ethernet - Media Access Control (MAC) sub-layer uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
802.4	Token bus LAN
802.5	Token Ring BUS
802.6	Metropolitan Area network (MAN)
802.7	Broadband
802.8	Fiber optic
802.9	Integrated voice/Data
802.10	Network Security
802.11	Wireless Networks
802.12	Demand Priority. Like 100VG-Any LAN

Wireless

- Ad-Hoc mode - **ad-hoc** mode is a method for wireless devices to directly communicate with each other. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicate in peer-to-peer fashion without involving central access points
- Infrastructure Mode - wireless networking bridges (joins) a wireless network to a wired Ethernet network. Infrastructure mode wireless also supports central connection points for WLAN clients. A wireless access point (AP) is required for infrastructure mode wireless networking.

- **802.11b** - WiFi 2.4 Ghz Wireless networking commonly used in homes and SOHO environments. Being replaced by the faster 802.11g standard. Uses a wireless access point (WAP) to connect to other wireless computers. 150+ feet 11 mbps
- **802.11g** - WiFi 2.4 Ghz Wireless networking commonly used in homes and SOHO environments. Uses a wireless access point (WAP) to connect to other wireless computers. Backward compatible with 802.11b 150+ feet 54 mbps . The newer 802.11n standard has better range than the g standard.
- **Infrared - IrDA** Uses light, not radio frequencies Uses line of sight connections making it useful for sharing data between personal devices. 150+ feet Usually 16mbps - high powered beams can reach 10Gbps
- **Bluetooth** 2.4 Ghz See below Up to 30 feet 721 kbps
- **Microwave** is also on the test but with no details other than it is a directional unbounded media type.

TCP Handshake Process

- The "SYN" flags are requests
- The ACK flags acknowledges earlier packets in this session
- **SYN**chronize and **ACK**nowledge messages are indicated by a bit inside the TCP header of the segment.
 - Host A **sends** a TCP **SYN**chronize packet to Host B
 - Host B receives A's **SYN**
 - Host B **sends** a **SYN**chronize-**ACK**nowledgement
 - Host A receives B's **SYN-ACK**
 - Host A **sends ACK**nowledge
 - Host B receives **ACK**. TCP connection is ESTABLISHED.

IP Addresses

32 bit longs made up of 4 -8 bit numbers(Called OCTETS) between 0 and 255

127.0.0.1 Your workstation

255.255.255.255 Broadcast

IP addresses are assigned by classes.

Class A IP address is one that begins with 0.__.__. up to 126.__.__. These can have approximately 16 million hosts.

Class B Are from 128.0.__. to 191.255.__. and can have 65,000 hosts

Class C are from 192.0.0._ to 223.255.255._ and can have 127 hosts

Class E are from 224-247 These are reserved for multicasting.

Class F 248-255 Reserved for experimental use.

- Each device that connects to the network must have a unique IP address.
- Each subnet must have its own unique network ID
- All devices on a given subnet must have the same subnet mask.
- RFC 1918 defines the non-routable private IP address ranges:
 - 10.0.0.10 to 10.255.255.255
 - 172.16.0.0 to 172.31.255.255
 - 192.168.0.0 to 192.168.255.255
- Automatic Private Addressing (APIPA) 169.254.0.1 to 169.254.255.255

Subnetting

- The subnet mask is a 32 bit number that is assigned to each host to divide the 32 bit binary IP address into network and node portions.
- The first number of a subnet mask must be 255 the remaining 3 numbers can be 255, 254, 252, 248, 240, 224.
- To apply a subnet mask you convert both IP and subnet to binary and AND The two.
- Custom subnet masks are used to separate block for IP addresses into multiple subnets.
- Classfull addresses are ones that belong to one of the classes (A, B, C, etc.) with default subnet masks.
- Classless addresses do NOT use the default subnet masks.

- Variable Length Subnet Masks can be used to create subnets containing different numbers of nodes.
- Classless Inter Domain Routing (CIDR) is a subnetting method that treats a VLSM as a 32 bit binary word.

IPX/SPX

- Internetwork Packet Exchange/Sequenced Packet Exchange
- Developed by Novell for use in versions 3 and 4 of Netware.
- IPX is a connectionless network layer protocol that provides best effort data delivery.
- SPC is a connection oriented transport layer protocol.
- NWLink is Microsoft's version of IPX/SPX for compatibility with Novell Networks.
- Service Advertisement Protocol (SAP) – Servers Broadcast what services they have available.
- IPX/SPX addresses have an IPX external network number a node number and a socket number all in a 12 byte IPX internetwork number that is represented by 24 hexadecimal digits.

AppleTalk

- A routable protocol found on Macintosh Networks
- Works with various physical topologies such as TokenTalk, EtherTalk, and FDDITalk
- Nodes – randomly generate their own 8 bit address and confirm its availability by broadcasting a request.
- Zones with a zone administrator. Descriptive names assigned to nodes.
- Non extended network – A single cable segment assigned a unique 10 bit network ID ranging from 1 to 1023.
- Extended network 0 combination of logical networks assigned to the same cable segment. This circumvents AppleTalks 254 node limit.
- AFP – AppleTalk Filing Protocol (AFP) application and presentation layer protocol used to exchange data.
- ADSP – AppleTalk Data Stream Protocol a session layer protocol that establishes and maintains full duplex connections between nodes.
- ZIP – Zone Information Protocol session layer protocol that provides a node with information about the zone.

- ASP – AppleTalk Session Protocol is a session layer protocol that maintains communication sessions between network nodes.
- PAP – Printer Access Protocol used by clients to send data to print servers.
- ATP – AppleTalk Transaction Protocol is a transport level protocol used to manage transactions between 2 sockets
- AEP AppleTalk Echo Protocol is the equivalent of Ping.
- DDP – Datagram Delivery Protocol is the main routing protocol and provides connectionless data delivery.
- AARP Appletalk Address Resolution Protocol is the equivalent of ARP.
- Data Link Access Protocol – A data link level access protocol: EtherTalk Link Access, LocalTalk Link Access, TokenTalk Link Access, and FDDITalk Link Access Protocols.

FDDI

Fiber Distributed Data Interface (FDDI) is an appealing choice for high-speed data networking. Essentially, it is a very high-speed token ring network connected by optical fibers. With a data transfer rate of 100Mbps, the ring can support up to 500 nodes with as much as 2 km of spacing between adjacent nodes.

ATM

ATM stands for Asynchronous Transfer Mode and is a high-speed, packet-switching technique that uses short fixed length packets called cells. ATM can transmit voice, video, and data over a variable-speed LAN and WAN connections at speeds ranging from 1.544Mbps to as high as 622Mbps. ATM is capable of supporting a wide range of traffic types such as voice, video, image and data. This technology is not as commonly used as it was in the mid to late 1990's.

Frame Relay

Frame relay is a secure, private network that utilizes a logical path or “virtual circuit” to allocate bandwidth for high performance transmissions. Frame relay is the premier high-speed packet-switching protocol communicating data, imaging, and voice between multiple locations. Frame relay is available in a range of bandwidths from 56 Kbps to full T1 (1.54 Mbps).

IP V 6.0

The previous information on TCP/IP has referred to IPv4, however, this addressing scheme has run out of available IP addresses due to the large influx of internet users and expanding networks. As a result, the powers that be had to create a new addressing scheme to deal with this situation and developed IPv6. This new addressing scheme utilizes a 128 bit address (instead of 32) and utilizes a hex numbering method in order to avoid long addresses such as 132.64.34.26.64.156.143.57.1.3.7.44.122.111.201.5. The hex address format will appear in the form of **3FFE:B00:800:2::C** for example.

More On TCP Protocols

- Line Printer Remote (LPR) sends print request to the IP address of LPD print server
- Line Printer Daemon (LPD)
- Network File System (NFS)
- Secure Shell (SSH)
- Secure Copy Protocol (SCP) – uses SSH to copy.
- Server Message Block – used for sharing resources.
- LDAP – defines how a client can access information and share directory data.
- SNMP – application layer service used to collect information from network devices for diagnostic purposes.
 - SNMP traps – when an SNP agent sends data to the management system without first being queried.
 - SNMP MIB (Management Information Base) – custom database containing system information

Zero Configuration Networking – proposed set of standards that provides for automatic configuration and IP address allocation on both ethernet and wireless networks. See www.zeroconf.org

Standards Organizations

ICANN – register domain names and IP addresses

IETF – protocols

IEEE - Hardware

Backups

Full – backup everything

Differential – back up everything that has changed SINCE THE LAST FULL BACKUP

Incremental – back up everything that has changed since the last backup, regardless of what type of backup it was.

Authentication Protocols

Know how these work

CHAP – Challenge Handshake Authentication Protocol

EAP - Extensible Authentication Protocol

Kerberos

PAP -Password Authentication Protocol

General Items to Review

Netbios

WINS

Network Area Storage

Storage Area Networks

Active Active clusters

Active Passive Clusters

Fault Tolerant Clusters

Resources

<http://www.mcmcse.com/comptia/network/networkplus.shtml>

<http://www.studynotes.net/indnet.htm>

http://www.proprofs.com/mwiki/index.php?title=Network%2B_Cram_Notes