

MCSE NETWORK ESSENTIALS CRAM SESSION

2nd Edition

Prepared by

Osama Salah Ghazy

sgr@frcu.eun.eg

No claim is made that the information provided is correct.

If you find errors, any topic that has not been covered or did not get the attention it deserves then please contact me for additon/correction.

Please be critical and report any errors to: sgr@frcu.eun.eg

You may freely distribute this document as long as it is kept in its original form.

New versions of this document, when released, will be hosted by the MCSE Guide Team at:

www.members.tripod/~MCSEGUIDE

Interrupt Requests

Memorize this table. You will get questions where you need to know which IRQs are still available to be used by a NIC so it won't conflict with another device using the same interrupt.

Each device must use a unique Interrupt and a unique I/O setting.

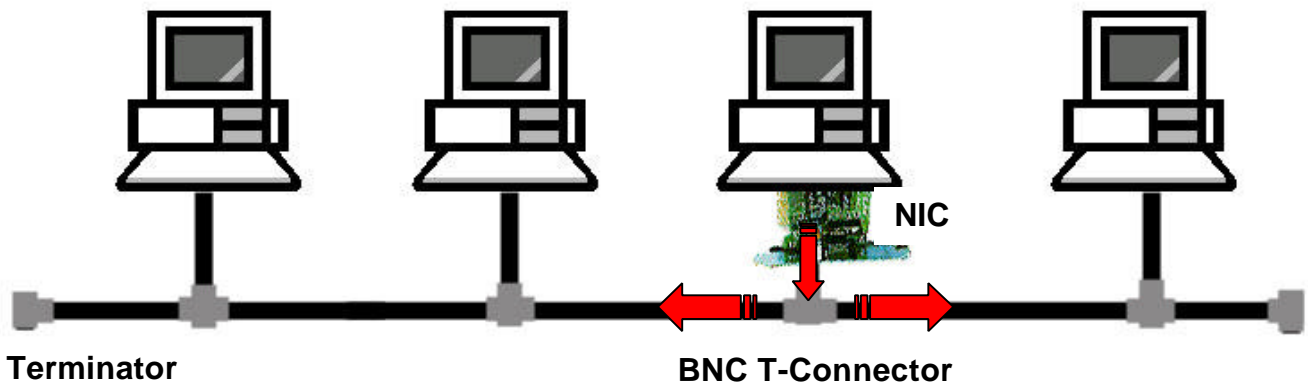
You can have several network cards in one PC but all with their own unique Interrupt and I/O.

IRQ 1	Keyboard
IRQ 2	Video Card
IRQ 3	Com2, Com4
IRQ 4	Com1, Com3
IRQ 5	LPT2
IRQ 6	Floppy Disk Controller
IRQ 7	Parallel Port (LPT1)
IRQ 8	Real-time clock
IRQ 9	Redirected IRQ2
IRQ 10	Available
IRQ 11	Available
IRQ 12	PS/2 Mouse
IRQ 13	Math Coprocessor
IRQ 14	Hard Disk Controller
IRQ 15	Available

LAN Topologies

Bus: A bus topology consists of nodes linked together in series with each node connected to a long cable or bus (trunk).

A break anywhere in the cable will usually cause the entire segment to be inoperable until the break is repaired (examples: 10BASE2 and 10BASE5).

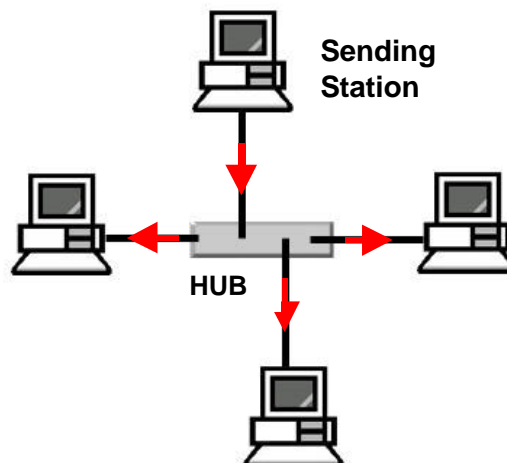


Packet travels in both directions from the sending station.

Packet is “swallowed” at the terminator and does not “bounce” back.

Star: Computers are connected to a centralized hub via cable segments. The primary advantage of this type of network is reliability, for if one of these “point-to-point” segments has a break, it will only affect the two nodes on that link. Other computer users on the network continue to operate as if that segment was nonexistent. However if the hub fails then all users are disconnected (complete hub failure, if only a port fails then only the segment on that port is disconnected.)

If the hub would fail all stations connected to it or some ports might not be functional. It needs significantly more cabling than a bus topology.



Ring: Connects all computers on a single cable. Ends are not terminated, but form a full loop connecting the last computer to the first computer. The computers are centrally connected to a concentrator building up a logical ring, physically from the outside it still looks like a star. The signal, or token, passes around the ring through each computer in a clockwise direction. The station that holds the token is allowed to transmit a message on the network.

On a Token Ring network, computers must wait for a free token in order to transfer data. When a computer that has data to send receives a free token, it modifies the token, and sends the data around the ring. When the data is received by the destination computer, an acknowledgment is generated and sent back to the source computer. After verifying the acknowledgment, the source computer creates a new token and passes it on to the network.

The ring topology provides equal access for all computers on the network.

Star-Bus: A combination of the linear bus and star topologies. 10BaseT and 100BaseX are normally configured in a star pattern but internally use a bus signaling system like other Ethernet configurations

Mesh: A mesh is a topology commonly used in WANs. A mesh network connects remote sites over multiple telecommunication links. It relies on routers to search among different active paths and determine the best path. Mesh's are often used in fault tolerant networks.

Access Methods

CSMA/CD- Carrier Sense Multiple Access with Collision Detection
Listens to cable prior to sending data. **(Ethernet)**

CSMA/CA- Carrier Sense Multiple Access with Collision Avoidance
Announces intention to send data. **(AppleTalk)**

Token-Passing- Token revolves around ring, computer which has the token is permitted to send the data. This mechanism prevents data collisions like on Ethernet. **(Token-Ring)**

Subnet Mask: Each IP address has two parts: the network ID and the host ID. A subnet mask is used to mask a portion of the IP address so that TCP/IP can distinguish the network ID from the host ID. TCP/IP hosts use the subnet mask to determine whether the destination is located on a local or remote network.

Frames:

A frame is a package of information transmitted as a signal unit.

Ethernet Frames: Ethernet frames are not uniform in length, they can be between 64 to 1518 bytes long. They only have preambles that mark the start of the frame. The CRC field on an Ethernet frame stores error checking and control information, not the source and destination addresses

Token Ring Frames: Have beginning and ending delimiters.

Network Types

peer-to-peer network: It provides each user the ability to manage his own shared resources. A peer-to-peer network does not require a powerful central server or a network administrator to provide centralized resource administration. Each user is responsible for the administration of his own resources. A peer-to-peer network will only be appropriate if there are fewer than 10 users and security is not an issue. A peer-to-peer network is a special type of client/server network, any computer is both a client and a server.


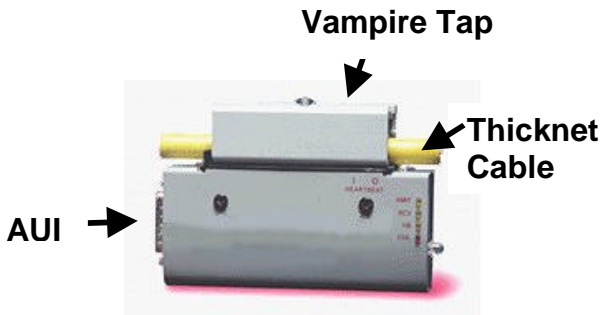
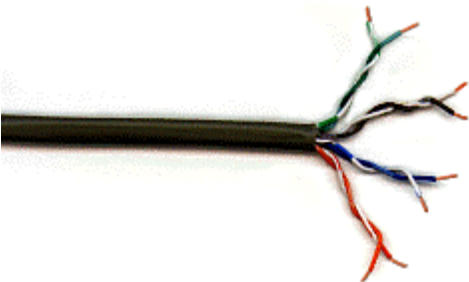
server-based network: A server-based network is the best network for sharing resources and data and it provides extensive resources and user security

Client/Server: The client/server approach is the most efficient way to provide database management and centralized file storage. In a client/server environment, all tasks are divided between a back end (the server), which stores and distributes data, and a front end (the client) which requests specific data from the server. The most common client/server application is a database management system using SQL. In a client/server environment, the database query is sent from the client but processed on the server. Only the results are sent across the network back to the client.

client/server network with each computer acting as both a client and a server:

is actually a peer-to-peer network.

Cables

Description	Thickness	Max. Length
<p>Thinnet Coaxial (RG-58 Family)</p>  <p>RG-58 /U Solid Copper Core RG-58 A/U Stranded Wire Core RG-58 C/U Military Specification of RG-58 A/U RG-59 Broadband transmission (TV Cable) RG-62 ArcNet Network Cable</p>	0.25 inches	185m
<p>Thicknet Coaxial</p>  <p>Uses a transceiver (Vampire Tap) to make connection with thicknet core.</p>	0.5	500
<p>Unshielded Twisted Pair (UTP)</p>  <p>Is susceptible to crosstalk. It is the cheapest.</p>	Twisted pair wiring	100
<p>Shielded Twisted Pair</p> <p>Has foil or braided jacket around wiring to help reduce crosstalk and to prevent electromagnetic interference.</p>	Twisted pair wiring	100

Suitable
for
10BaseT



UTP/STP Category	Speeds
Cat 2	4 MBps
Cat 3	10 MBps
Cat 4	16 MBps
Cat 5	100 MBps

Fiber Optic 100MBps-200,000Mbps	Glass Core	
---	------------	--

Term Definitions:

Attenuation	The degrading of a signal as it travels farther from its origination.
Crosstalk	Signal overflow from one wire to another adjacent wire.
Jitter	Instability in a signal wave. Caused by signal interference or an unbalanced FDDI ring or Token Ring.

Subnet Mask: Each IP address has two parts: the network ID and the host ID. A subnet mask is used to mask a portion of the IP address so that TCP/IP can distinguish the network ID from the host ID. TCP/IP hosts use the subnet mask to determine whether the destination is located on a local or remote network.

Redirector: A redirector forwards file and data requests. The redirector is a section of code in the network operating system that intercepts requests from the computer. It determines whether a file request is intended for the local machine or for a remote computer. For NetWare networks, a redirector needs to be individually installed at each client computer.

Frames: A frame is a package of information transmitted as a signal unit.

Ethernet Frames: Ethernet frames are not uniform in length, they can be between 64 to 1518 bytes long. They only have preambles that mark the start of the frame. The CRC field on an Ethernet frame stores error checking and control information, not the source and destination addresses

Token Ring Frames: Have beginning and ending delimiters.

Broadcast: Every computer on the network must process each broadcast message. This can potentially cause broadcast storms. A broadcast storm occurs if the number of broadcast messages on the network approaches or surpasses the capacity of the network bandwidth so that the network can no longer carry

messages from any other computer. Such a broadcast storm can shut down a network. Routers do not pass broadcasts, and they can be used to prevent broadcast storms.

Broadcast messages are processed by every computer on the network.


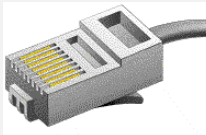
UNC names consist of a server or a computer name followed by a share name (a directory path or printer name). For example, in the UNC string "\\CAIRO\USERS\" CAIRO is the computer name and USERS is the share name.

Ethernet Repeater Rule (5-4-3 Rule)

An Ethernet network must fulfill the following rules:

- Total number of **segments** is less than or equal to **5**.
- Total number of **repeaters** is less than or equal to **4**.
- Not more than **3 segments have devices** other than the repeaters we already counted.

Ethernet Topology

Type	Cable types	Connector
10Base2	RG-58 thinnet coaxial cable	AUI
10Base5	Thicknet coaxial cable	BNC 
10BaseT	Category 3, 4, or 5 UTP cable	RJ-45 
100BaseT	Category 5 UTP cable	RJ-45

Signal Transmissions

<u>Baseband</u>	<p>Uses digital signaling over a single carrier frequency. Transmits bi-directional.</p> <p>Uses repeaters for signal regeneration.</p> <p>Ethernet, Token Ring and Arcnet LANs use baseband transmission.</p>
<u>Broadband</u>	<p>Uses analog signaling over a range of frequencies.</p> <p>Transmits unidirectional. Uses amplifiers for signal regeneration ("B-ISDN")</p>

OSI Model

Remember: **ALL PEOPLE SEEM TO NEED DATA PROCESSING**

7	Application Layer	Serves as a window for applications to access net services (file transfer, virtual terminal, electronic mail, file servers...). Handles general network access, flow control and error recovery.	FTP , TFTP, SMTP, MIME, SMB , HTTP , TELNET, DHCP, BOOTP, DNS, SNMP , NFS
6	Presentation Layer	Layer is the network's translator. The redirector operates here. Determines data format. Responsible for protocol conversion, and data translation, encryption and compression.	ASCII, EBCDIC, SMB
5	Session Layer	Allows applications on two PC's to connect and establish a session. Provides synchronization between communicating computers.	Printing, File Sharing, RPC , NetBios
4	Transport Layer	Defines how data should be presented to the next receiving layer and packages data accordingly. Responsible for packet handling. Ensures error-free delivery. Repackage messages, divides messages into smaller packets, and handles error handling. Issues such as how reliable transport over an Internetwork are the concern of the transport layer. In providing reliable service, the transport layer provides mechanisms for the establishment, maintenance, and orderly termination of virtual circuits, transport fault detection and recovery, and information flow control (to prevent one system from overrunning another with data).	TCP , SPX , UDP, NWLink , NetBeui
3	Network Layer	The network layer is a complex layer that provides connectivity and path selection between two end systems that may be located on geographically diverse <i>subnetworks</i> . A subnetwork, in this instance, is essentially a single network cable (sometimes called a <i>segment</i>). Because a substantial geographic distance and many subnetworks can separate two end systems desiring communication, the network layer is the domain of routing. subnetworks. Translates logical addresses to physical addresses. Traffic Management: Packet switching, routing, congestion control.	NetBeui , IP , IPX , RIP , ICMP, IGMP, SLIP , CSLIP , PPP

2	Data Link Layer	Sends data frames from network layer to physical layer. Packages bits to frames and insures their error free transmission. <u>LLC</u> - Manages link control and defines SAP's (Service Access Points). <u>MAC</u> - Communicates with adapter card. (physical addressing)	DLC , IEEE 802.2 (LLC), 802.3, 802.5, ATM, ISDN, Frame Relay, HDLC, LAPB
1	Physical Layer	Transmits binary data over a physical communications medium. Defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems. Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other, similar, attributes are defined by physical layer specifications.	10BaseT, 100BaseT, 10Base2, FDDI, Modem, T1, E1, BRI, PRI, RS0232, V.35, Sonet

You do not have to know in which layer all the mentioned services are found. Just remember the most important ones that you keep hearing during your study preparation like, TCP/IP, NetBeui, etc.

IEEE 802 Specifications

802.1	Internetworking
802.2	LLC (Logical Link Control)
802.3	CSMA/CD - Ethernet
802.4	Token Bus LAN
802.5	Token Ring LAN
802.6	MAN (Metropolitan Area Network)
802.7	Broadband Technical Advisory Group
802.8	Fiber-Optic Technical Advisory Group
802.9	Integrated Voice/Data Networks
802.10	Network Security
802.11	Wireless Networks
802.12	Demand Priority Access LAN, 100 Base VG - AnyLAN

LAN Components

Device	Function
Repeater	<p>Works at the physical layer.</p> <p>Regenerates signals for retransmission to overcome attenuation or cable length limits. Can move packets from one media to another (Coax ↔ UTP), but <u>cannot</u> translate from one protocol to another.</p> <p>Passes broadcast storms.</p>
Bridge	<p>Works at the MAC sublayer of the Data Link Layer.</p> <p>Bridges are used to segment networks (split overloaded networks). They forward packets based on address of destination node (MAC address). Uses RAM to build a routing table based on <u>source addresses as they become available</u>. Forwards a packet only if the destination MAC address is physically located on a segment other than the segment from which the packet was received.</p> <p>Since all information contained in the higher levels of the OSI model is unavailable to them, bridges cannot filter protocols like routers or translate protocols like gateways. However, since bridges do not distinguish between one protocol and another, they can be used with nonroutable protocols such as NetBEUI.</p> <p>Bridges will thus connect dissimilar network topologies (connecting a Token Ring segment with an Ethernet segment, but no filtering like possible with routers). Forwards all protocols. Regenerates the signal at the packet level. Passes all broadcasts.</p>
Remote Bridge	<p>Same as bridge, but used for telephone communications. Uses STA (Spanning Tree Algorithm).</p>
Router	<p>Works at the Network Layer.</p> <p>Is used to switch and route packets across multiple networks. Uses RAM to build a routing table based on <u>network addresses</u>.</p> <p>They filter by specific protocol. Routers were born out of the necessity for dividing networks logically instead of physically. An IP router can divide a network into various subnets so that only traffic destined for particular IP addresses can pass between segments.</p> <p>They share status and routing information to other routers to provide better traffic management and bypass slow connections. Routers are slower than bridges due to complex functions.</p>

<p style="text-align: center;">Router</p>	<p>When packets are passed from router to router, the routers strip off and recreate Data Link layer source addresses and destination addresses. This enables a router to send a packet across different network architectures such as from a TCP/IP Ethernet network to a Token Ring network.</p> <p>Routers can accommodate multiple active paths between LAN segments.</p> <p>Routers can choose between multiple paths while bridges cannot choose between multiple paths.</p> <p>Will not pass broadcast storms.</p> <p>Routed protocols are protocols that are routed over an internetwork (<i>IP, DECnet, AppleTalk, NetWare, OSI, Banyan VINES, and Xerox Network System (XNS)</i>).</p> <p>Routing protocols are protocols that implement routing algorithms. Put simply, they route routed protocols through an internetwork.</p> <p>Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Exterior Gateway Protocol (EGP), Border Gateway Protocol (BGP), OSI Routing, Advanced Peer-to-Peer Networking, Intermediate System to Intermediate System (IS-IS), and</p> <p><u>Routing Information Protocol (RIP):</u></p> <p>Routing Information Protocol (RIP) can use distance-vector algorithms to determine routes. With RIP, routers share information among other routers to update their internal routing tables and determine the best routes. Both TCP/IP and IPX/SPX support RIP</p>
<p style="text-align: center;">Brouter</p>	<p>Routes selected routable protocols.[DECnet, IP, IPX, OSI, XNS, AppleTalk] Bridges nonroutable protocols. [LAT, NetBEUI, DLC]</p>
<p style="text-align: center;">Gateway</p>	<p>Resides in the Transport, Session, Presentation and Application Layers of the OSI model. A gateway is a connectivity device that acts as a translator between two systems that do not use the same Communication protocols, data formatting structures, languages or architectures.</p> <p>Used for communications between different network types (i.e. Windows NT and IBM SNA, Ethernet and TokenRing, NT and NetWare). Takes the packet, strips off the old protocol and repackages it for the receiving network.</p> <p>Note: Some Gateways can use all seven layers!</p>
<p style="text-align: center;">Multiplexer</p>	<p>A device that allows several users to share a single circuit.</p> <p>It allows the transmission of multiple signals (voice and data) simultaneously on a single channel. It funnels different data streams into a single stream. At the other end of the communications link, another multiplexer reverses the process by splitting the data stream back into the original streams.</p>

<p style="text-align: center;">Switches</p>	<p>Principally the same as a hub but sends the packets only to the port where the receiving node is attached.</p> <p>Cut-through switches only examine the destination address before forwarding it on to its destination segment.</p> <p>A store-and-forward switch, on the other hand, accepts and analyzes the entire packet before forwarding it to its destination. It takes more time to examine the entire packet, but it allows the switch to catch certain packet errors and keep them from propagating through the network.</p> <p>There are a large number of hybrid switches available that mix both cut-through and store-and-forward architectures.</p> <p>Switches separate a network into collision domains, allowing network design rules to be extended. Each of the segments attached to an Ethernet switch has the full bandwidth shared by fewer users which results in better performance (as opposed to hubs).</p> <p>Switches are a good choice to improve network performance.</p>
<p style="text-align: center;">Hub</p>	<p>Hubs are used to connect together two or more Ethernet segments of any media type. They only allow users to share Ethernet. A network of hubs/repeaters is termed a "shared Ethernet", meaning that all members of the network are contending for transmission of data onto a single network (collision domain). This means that individual members of a shared network will all only get a percentage of the available network bandwidth.</p>
<p style="text-align: center;">Transceiver</p>	<p>A transceiver is a transmitter/receiver device that connects a computer to the network. A transceiver can switch the parallel data stream used on the computer's bus into a serial data stream used in the cables connecting the computers. Most network adapter cards have built-in transceivers.</p> <p>Transceivers are used to connect nodes to the various Ethernet media. Most computers and network interface cards contain a built-in 10BASE-T or 10BASE2 transceiver, allowing them to be connected directly to Ethernet without requiring an external transceiver. Many Ethernet compatible devices provide an AUI connector to allow the user to connect to any media type via an external transceiver. The AUI connector consists of a 15 pin D-shell type connector, female on the computer side, male on the transceiver side. Thickwire (10BASE5) cables also use transceivers to allow connections.</p> <p>When using cards with multiple transceivers (Combo Cards) you must make sure that the card is set to the correct transceiver. Most cards offer a "Autodetect" mode.</p>

OSI Layer / Networking Device Summary

	OSI Layer	Short Description	Device
7	Application Layer	Applications	Gateway Some support also <u>all seven</u> layers!
6	Presentation Layer	Data Interpretation data compression and translating the data format	
5	Session Layer	Session Control Synchronization between user tasks by placing checkpoints in the data stream	
4	Transport Layer	Transmission Control flow control and ensures messages are delivered error free	
3	Network Layer	Flow Control, Routing	Router
2	Data Link Layer	Maintain Data packages raw data bits into data frames	Bridge (MAC Sublayer)
1	Physical Layer	Physical Definition	Repeater

Spanning Tree Algorithm - was developed for bridges to determine the most efficient network in path when there are multiple paths to choose from.

Multiplexing - Several signals from different sources are collected into the component and are fed into one cable for transmission.

Protocols

<u>Routable</u>	IP, IPX, OSI, AppleTalk, DECnet, XNS.
<u>Non routable</u>	NetBEUI, LAT, DLC ← just remember those three
<u>NetBEUI</u>	Microsoft protocol designed for small LANs. NetBEUI is a small, efficient and fast Transport layer protocol. It does not require a lot of memory, and it offers good error protection. However, it is not routable, and its performance across WANs is poor.
<u>IPX/SPX</u>	Fast protocol for small and large Novell networks; is routable. Also known in NT as NWLink.
<u>TCP/IP</u>	Internet Protocol; is routable.
<u>DECnet</u>	Defines communications over FDDI MANs; is routable.
Appletalk	Apple protocol designed for small LAN file and print sharing.
<u>XNS</u>	Designed by Xerox as an Ethernet protocol. Was replaced by TCP/IP
DLC	The Data Link Control protocol (DLC) is a non-routable protocol. It is often used by HP -series network interface print devices to connect directly to the network. It can also be used to enable a computer to communicate with other computers running the DLC protocol stack, such as IBM mainframes .

Connectionless: Message oriented communication that provides fast dataflow but lacks reliable delivery mechanisms.

Connection oriented: A type of communication that provides assurance of packet delivery.

Packet Switching Networks

Packet Switching - Packets are relayed across network along the best route available.

Type	Function
X.25	Designed to connect remote terminals to mainframe host systems. Is very slow due to constant error-checking → reliable data transmission.
Frame Relay	Point-to-point system which uses digital leased lines. It does not have unnecessary accounting and error checking functions, and therefore is much faster than X.25. Requires frame relay capable bridge or router for transmission. Frame relay uses a private virtual circuit (PVC) to transmit variable length frames at the OSI Data Link layer. Thus it transmits variable-length frames at the Data Link layer through the most cost-effective path. It can provide bandwidth as needed.
ATM	Advanced implementation of packet switching. Transmits at speeds of 155Mbps to 622Mbps with capabilities of higher speeds. Transmits data in 53 byte (48 application, 5 header) cells. Uses switches as multiplexers to permit several computers to simultaneously transmit data on a network.
ISDN	Transmits at 128k/sec. Has three data channels - 2 B channels @ 64k/sec & 1 D channel @ 16k/sec. The B channels carry data while the D channel performs link management and signaling. ISDN is intended to replace analog phone lines.
FDDI	100 Mbps token-passing ring network which uses fiber-optic media. Uses a dual-ring topology for redundancy and in case of ring failure. Each ring is capable of connecting 500 computers over 100 kilometers (62 miles). Can be used as a network backbone. Uses beaconing for ring troubleshooting.

Beaconing - Computers are used to detect network faults, then transmit the fault signal to the server.

SMB: Server message blocks (SMBs) are standard formatted packets that contain instructions required by the Windows NT Server service. SMBs are passed to a transport layer like NetBEUI or NetBIOS over TCP/IP for transmission across a network link.

Security levels

Share-level security - Used in Windows 95 to share resources. A password is needed to access the resource. Passwords are assigned to each shared resource on a network.

User-level security - Used in Windows NT (Server and WS) to share resources. When you attempt to access a shared resource, the server will make sure your user account has been authorized to access the resource. More secure than share-level security since every user has his own password instead resource having only one password know to several users. It is also easier to administer (centralized administration).

Network Diagnostic Tools

Tool	Function
Digital Volt Meters (DVM)	Measures voltage passing through a resistance. Primarily used for network cable troubleshooting.
Time-Domain Reflector (TDR)	Sends sonar-like pulses to look for breaks, shorts or or crimps in cables. Can locate a break within a few feet of actual fault.
Oscilloscope	Measures amount of signal voltage per unit of time. Displays crimps, shorts, opens, etc.
Network Monitor	Examines packet types, errors and traffic to and from each computer on a network.
Protocol Analyzer	Looks inside the packet to determine cause of problem. Contains built in Time-Domain Reflector. Gives insights to many problems including connection errors, bottlenecks, traffic problems, protocol problems, etc.

Multiple Disk Sets

Fault Tolerant Systems protect data by duplicating data or by placing data in different physical sources.

Level	Description	Function
0	Disk Striping	Divides data into 64k blocks and spreads it equally among all disks in the array. Requires at least two disks.
1	Disk Mirroring	Duplicates a partition on another physical disk.
1	Disk Duplexing	Duplicates a partition on another physical disk which is connected to another Hard Drive Controller.
2	Disk Striping w/ ECC	Data blocks are broken up and distributed across all drives in array with error checking.
3	Disk Striping w/ ECC stored as parity	Data blocks are broken up and distributed across all drives in array with one drive dedicated to storing parity data.
4	Disk Striping with large blocks	Complete blocks of data are distributed across all drives in the array.
5	Disk Striping with parity	Distributes data and parity information across all disks in the array. The data and the parity information are arranged so they are always on separate disks. A parity stripe block exists for each row across the disk. The parity stripe is used for disk reconstruction in case of a failed disk. Supports a minimum of three disks and a maximum of thirty-two disks. The smallest common amount of free space on the disks is used for the stripe set. If you have n=number of disks, s=smallest common free space of disk then: Stripe set size = $n \times s$ (<i>includes parity</i>) Actual data size = $(n-1) \times s$ (<i>raw data, no parity</i>)

Windows NT supports RAID Levels 0, 1, and 5, but only 1 and 5 offer Fault Tolerance.

Sector Sparring - Automatically adds sector-recovery capabilities to the files system while the computer is running. If bad sectors are found during disk input/output operations, the system will attempt to move the data to a good sector and map out the bad sector. Available when using RAID methods. Only available with SCSI drives. Supported by NT.

NDIS

Network Device Internet Specification [developed by Microsoft and 3COM].

Windows device driver interface that enables a single network interface card to support multiple network protocols. It overcomes the need for proprietary network interface drivers for each network operating system and protocol.

For example, with NDIS a single NIC can support simultaneously both TCP/IP and IPX connections. Also, if a computer contains multiple NICs because it is connected to more than one network, NDIS can route traffic to the correct card.

ODI

Open Data-link Interface [developed by Novell and Apple].

Same functionality as NDIS but for NetWare.

RAS – Remote Access Service

RAS can use TCP/IP, NWLink, or NetBEUI protocols for dial-in and dial-out connections.

TCP/IP and NWLink are routable, NetBeui is not.

RAS Supports: RAS, PPP and SLIP.

SLIP: little overhead, no error checking, manual IP configuration

PPP: error checking, flow control, dynamic IP configuration

Backup Methods

Normal backup: All data is backed up and marked as such.

Incremental backup: The incremental method only backs up files that were created or changed since the last normal or incremental backup. **It marks files as having been backed up.**

Differential backup: A differential backup copies files that were created or changed since the last normal or incremental backup. **It does not mark files as having been backed up.** Differential Backups are usually bigger than incremental Backups and thus take more time.

Connectivity

DNS: Domain Name Service, resolves Host names to IP Addresses.

HOSTS file: Provides mappings of remote host names to IP Addresses.

WINS: Resolves NetBIOS names to IP Addresses.

LMHOSTS file: Provides mapping of NetBIOS names to IP Addresses.

DHCP: **Dynamic Host Configuration Protocol**
Responsible for dynamically assigning and maintaining IP addresses for DHCP clients located on a local subnet.

ARP: The Windows NT TCP/IP protocol stack assembles network packets based on IP addresses. Each computer (or routing device) on the network has a network interface card (NIC) with its own unique address (sometimes called a MAC or hardware address). Each network interface card also has an ARP (address resolution protocol) cache that is used to map IP addresses into NIC addresses.

NetWare Connectivity

In order for NetWare clients to access resources on a Windows NT server, the Windows NT server must have both the **NWLink** protocol and **File and Print Services for NetWare** installed.

In order for Windows NT workstation to connect to a NetWare server, the Windows NT workstation must have **Client Service for NetWare** installed.

Gateway Service for NetWare is used to allow NT workstations access to NetWare resources through a Gateway. This solution does not require any changes on the NT workstations.
