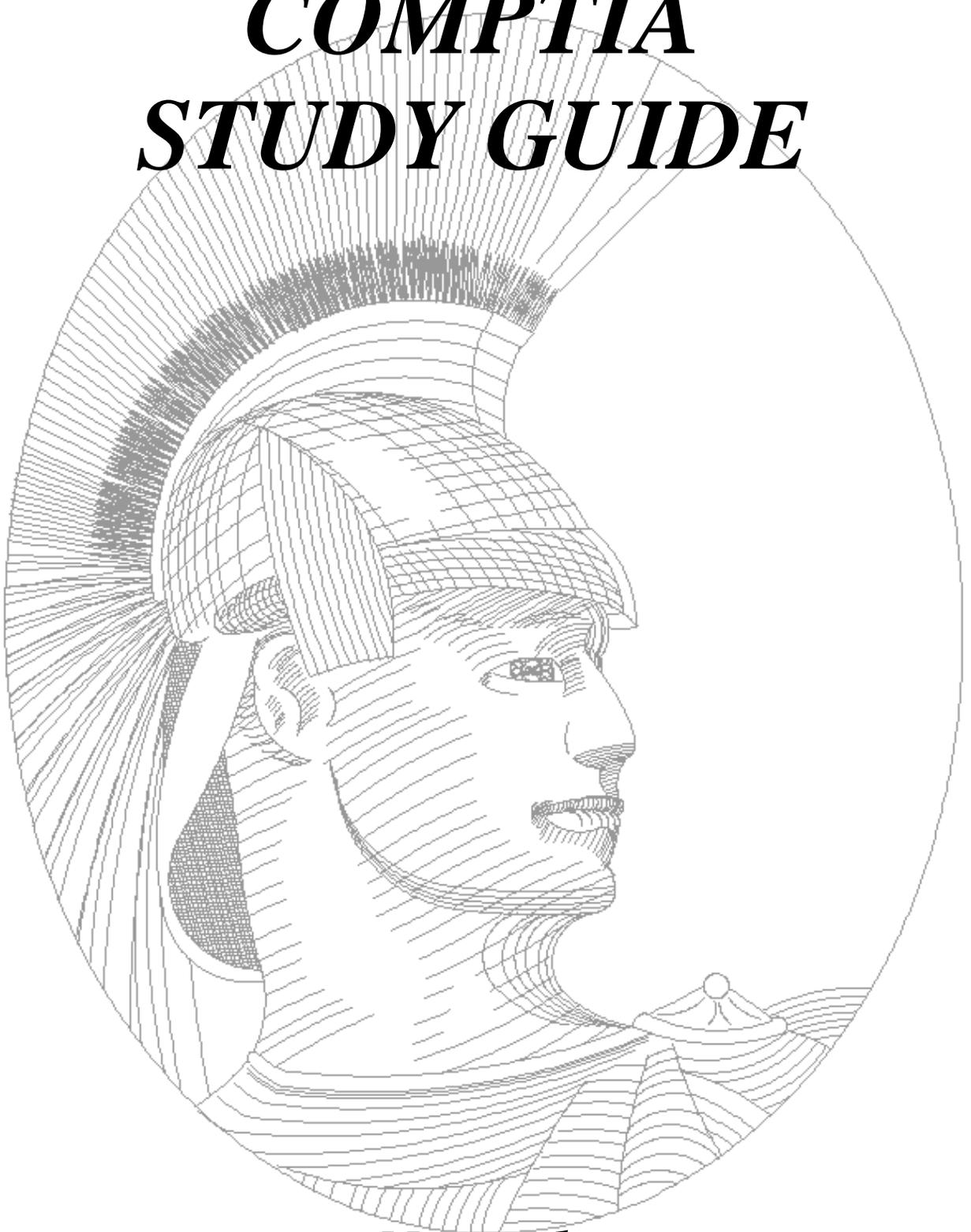


AND WITH YOU FOR
THE BEST OF
THE

COMPTIA STUDY GUIDE



Network+

Edition 3

Congratulations!!

You have purchased a *Troy Technologies USA* Study Guide.

This study guide is a selection of questions and answers similar to the ones you will find on the official CompTIA Network+ exam. Study and memorize the following concepts, questions and answers for approximately 10 to 12 hours and you will be prepared to take the exams. We guarantee it!

Remember, average study time is 10 to 12 hours and then you are ready!!!

GOOD LUCK!

Guarantee

If you use this study guide correctly and still fail the exam, send your official score notice and mailing address to:

Troy Technologies USA
8200 Pat Booker Rd. #368
San Antonio, TX 78233

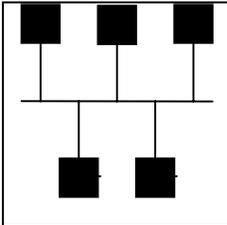
We will gladly refund the cost of this study guide. However, you will not need this guarantee if you follow the above instructions.

This material is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

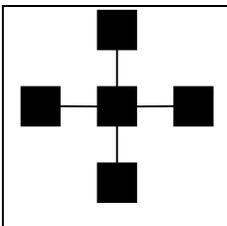
© Copyright 1998, 1999 and 2000 Troy Technologies USA. All Rights Reserved.

Networking Concepts

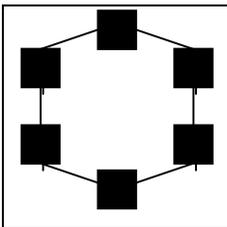
Standard Topologies



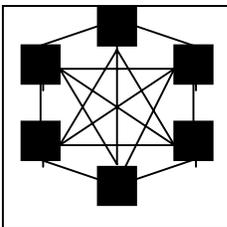
Bus - all computers are connected via a single cable that runs to all PCs.



Star - All computers connect to a centralized hub via cable segments. Star is the most popular network configuration in use today.



Ring - All computers are connected via a single cable. However, the ends are not terminated and the cable forms a full loop connecting the last computer to the first computer.



Mesh - All computers on the network are directly connected to every other computer on the network.

Network Characteristics

Segment - A length of cabling connecting a device to a concentration device or routing device. It can also be a logical group of devices which communicate within a given subnet that is separated by a bridge, router, brouter, or hub.

Backbone - The foundation of the LAN/WAN where the servers are linked together on a common series of concentration devices. This gives the servers the most bandwidth to serve other devices including other servers.

Network Operating Systems

Windows NT

A networking operating system designed using a Directory to manage certain resources. NT's primary file system is NTFS. Provides an inherently GUI console at the server.

Clients - Windows NT Workstation best serves Windows NT Server because of the common NTFS file system and they are optimized to work best with each other. However, Windows95/98, Windows for Workgroups, DOS, UNIX, Macintosh, and even NetWare clients can be connected to a Windows NT environment.

Novell NetWare

A networking operating system designed using a bindery or Directory Service to manage most resources. NetWare's primary file system is a combination of FAT (File Allocation Table) and DET (Directory Entry Table). Provides an inherently text based and command prompt console at the server.

Clients - Novell NetWare works well with most popular clients such as DOS, Windows 3.11, Windows 9x, Windows NT Workstation.

UNIX

UNIX is a command line operating system written in the C programming language. GUI interface can be achieved by installing special software such as X-Windows. Used mainly in a multi-user environment on minicomputers. Several different version available and allows a great deal of flexibility when performing network operations. Many UNIX protocols are the standard for today's Internet.

Clients - Unix specific clients such as Sun Sparc stations work best with their manufacturer's Network Operating System (NOS).

Network Protocols

IPX - Internetwork Packet Exchange. It's the Novell NetWare designed protocol, which is the default for all NetWare networks. Offers speed, works well with routers, and takes up very little RAM. Resides in Network Layer of the OSI model.

IP - Internet Protocol. Default protocol for the Windows NT and UNIX networks. Lacks speed and takes up a large amount of memory. However, it is robust and universally supported, and is the protocol upon which the Internet is based. IP functions at the Network layer of the OSI model.

NetBEUI - NetBIOS Enhanced User Interface. Microsoft designed protocol for speedy packet delivery in a small network without much configuration. It's not routable. It operates at the Network and Transport layers of the OSI model.

The OSI Model

The Open System Interconnection (OSI) Model is a seven layer model that helps designers of network operating systems and software to create relatively standardized software. This is useful when trying to get different operating systems to talk to each other. Although the model is only a blueprint, it is almost universally followed.

Layer	Name	Protocols	Devices	Function
7	Application	SMB, NCP, FTP, TFTP, NFS, SNMP, Telnet, SMTP	Gateways	Program-to-program communication.
6	Presentation	NCP, Telnet, FTP, TFTP, NFS, SNMP, SMTP	Gateways	Manages data presentation conversions. For example, the Presentation Layer would be responsible for converting from EBCDIC to ASCII.
5	Session	Telnet, FTP, TFTP, NFS, SNMP, SMTP	Gateways	Responsible for establishing and maintaining communications channels. In practice, this layer is often combined with the Transport Layer.
4	Transport	SPX, TCP, UDP, NetBEUI	Gateways	Responsible for end-to-end integrity of data transmission.
3	Network	IPX, IP, ICMP, RIP, OSPF, EGP, IGMP, NetBEUI, DLC, DECNet	Routers & Brouters	Routes data from one node to another.
2	Data Link	HDLC, ARP, RARP, NDIS, ODI, LLC, SAP	Switches, Brouters & Bridges	Responsible for physically passing data from one node to another.
1	Physical	CSMA/CD & Token Passing	Repeaters	Manages putting data onto the network media and taking the data off.

Networking Devices

Internetworking devices offer communication between local area network (LAN) segments. There are five primary types of internetworking devices: repeaters, bridges, routers, brouters, and gateways. The OSI layer at which they establish the LAN-to-LAN connection can differentiate these devices very generally. Each device offers the functionality found at its layer(s) of connection and uses the functionality of all lower layers.

Device	OSI Layer	Description
Repeater	Physical	<p>A network device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission loss. Analog repeaters frequently can only amplify the signal while digital repeaters can reconstruct a signal to near its original quality.</p> <p>In a data network, a repeater can relay messages between subnetworks that use different protocols or cable types. Hubs can operate as repeaters by relaying messages to all connected computers. A repeater cannot do the intelligent routing performed by bridges and routers.</p>
Bridge	Data Link	<p>A device that connects two local-area networks (LANs), or two segments of the same LAN. The two LANs being connected can be alike or dissimilar. For example, a bridge can connect an Ethernet with a Token-Ring network.</p> <p>Unlike routers, bridges are protocol independent. They simply forward packets without analyzing and re-routing messages. Consequently, they're faster than routers, but also less versatile.</p>
Router	Network	<p>A device that connects two LANs. Routers are similar to bridges, but provide additional functionality, such as the ability to filter messages and forward them to different places based on various criteria.</p> <p>The Internet uses routers extensively to forward packets from one host to another.</p>
Brouter	Data Link/Network	<p>Short for bridge router, a device that functions as both a router and a bridge. A brouter understands how to route specific types of packets, such as TCP/IP packets. Any other packets it receives are simply forwarded to other network(s) connected to the device (this is the bridge function).</p>
Gateway	Top 4 layers	<p>In networking, a combination of hardware and software that links two different types of networks. Gateways between e-mail systems, for example, allow users on different e-mail systems to exchange messages.</p>

Network Cabling

Type	10base2 Thinnet	10base5 Thicknet	10baseT Twisted Pair	100baseTX Fast Ethernet	Fiber Optic
Wire	Coaxial RG58-A/U	Coaxial	UTP Category 2,3,4,5	UTP Category 5	Fiber
Distance	185m	500m	100m	100m	2000m
Connector	BNC	AUI/DIX	RJ-45	RJ-45	
Speed	10Mbps	100Mbps	4 - 100Mbps	100Mbps	Over 100Mbps

Networking Terms

Half-duplexing - A communication method, which can carry data in either direction but not both directions at once.

Full-duplexing - A term used to describe a communications channel down which data can travel in both directions at once.

LAN - Local Area Network. A data communications network, which is geographically, limited (typically to a 1 mile radius) allowing easy interconnection of terminals, microprocessors and computers within adjacent buildings. Ethernet, Token-ring, and FDDI are examples of standard LANs.

WAN - Wide Area Network. Usually constructed with serial lines, extending over distances greater than one mile.

Server - A computer, which provides some service for other computers, connected to it via a network. The most common example is a file server, which has a local disk and services requests from remote clients to read and write files on that disk.

Workstation - A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time. A device, which accesses available resources from servers typically found in a distributed processing environment

Host - A computer connected to a network. The term node includes devices such as routers and printers, which would not normally be called "hosts".

Peer-to-Peer Network - A network that does not rely on the use of a central file server to share files. Each workstation relies on another workstation to have it's resources made available. They are very difficult to maintain security, must be limited number of peers to

keep administration costs low, slow response time, but they are inexpensive, no central point of failure and no special training required.

Server-based network - Requires a central file server and a networking operating system that can handle the job. They require a separate machine and therefore expensive hardware, expensive NOS, and without the proper training it is difficult to install and maintain. On the other hand, data transfer speeds are greater, security is more robust, LAN expansion is simpler, and there are management tools available.

Cable - provides the pathway for network communications. It's a component of a topology determined by the NIC and standard being used. The most common types of LAN cabling are coaxial, unshielded twisted pair, shielded twist pair, and fiber optic.

NIC - An adapter circuit board installed in a computer to provide a physical connection to a network.

Hub - A wiring concentrator for a LAN or WAN that provides a central attachment point for network cabling. Coaxial cable doesn't use hubs. There are three types of hubs: passive (absorbs some signal; no electronics to process data signal), active (cleans signal; electronics to amplify signal), and intelligent (managed & switching hubs).

Switching hub - Intelligent hub, which contains circuitry that very quickly, routes signals between ports on the hub. A communications paradigm in which a dedicated communication path is established between the sender and receiver along which all packets travel. The telephone system is an example of a circuit switched network. Also called connection-oriented.

MAU - Media Access Unit. In a Token Ring network, a device to attach multiple network stations in a star topology, internally wired to connect the stations into a logical ring. The MAU contains relays to short out non-operating workstations. Multiple MAUs can be connected into a larger ring through their Ring In/Ring Out connectors.

Transceivers - Transmitter-receiver. The physical device, which connects a host interface (e.g. an Ethernet controller) to a local area network. Ethernet transceivers contain electronics that apply signals to the cable and sense other host's signals and collisions.

MAC address - Also known as the physical addresses, operates on the data link layer. Each address is a unique 12-digit hexadecimal ID number, which is hard coded to the network adapter by the factory, and is used by devices to direct packets to other devices.

Crossover cable - A cable used to daisy-chain two network hubs together. Can also be used to connect two PCs together and eliminate the need for a hub.

Routable protocol - permits its packets to be sent beyond a single LAN/WAN segment.

Nonroutable protocol - Packets all remain on the originating LAN segment.

Default Gateway - The exit and entry point of a subnet.

Subnetwork - A portion of a network, which may be a physically independent network segment, which shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to an Internet.

Connectionless Protocol - The data communication method in which communication occurs between hosts with no previous setup. Packets sent between two hosts may take different routes. UDP is a connectionless protocol. Also called packet switching. This is on contrast to circuit switching, which is connection-oriented.

Connection-oriented Protocol - A type of transport layer data communication service that allows a host to send data in a continuous stream to another host. The transport service will guarantee that all data will be delivered to the other end in the same order as sent and without duplication. Communication proceeds through three well-defined phases: connection establishment, data transfer, and connection release. The most common example is Transmission Control Protocol (TCP).

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.

Baseband - Uses digital signaling over a single frequency. Transmits bi-directionally.

Broadband - Uses analog signaling over a range of frequencies. Transmits uni-directionally. Uses amplifiers for signal regeneration.

IEEE 802 Definitions

802.2	LOGICAL LINK CONTROL
802.3	CSMA/CD (ETHERNET)
802.4	TOKEN BUS
802.5	TOKEN RING
802.6	METROPOLITAN AREA NETWORK (MAN)
802.7	BROADBAND COMMUNICATION
802.8	FIBER OPTIC COMMUNICATION
802.10	NETWORK SECURITY
802.11	WIRELESS NETWORKS
802.12	DEMAND PRIORITY ACCESS METHOD FOR 100 MB OPERATION

TCP/IP Suite

TCP - Transmission Control Protocol, the most common transport layer protocol used on Ethernet and the Internet. It was developed by DARPA. TCP is built on top of the Internet Protocol (IP) and is nearly always seen in the combination TCP/IP (TCP over IP). It adds reliable communication, flow-control, multiplexing and connection-oriented communication. It provides full-duplex, process-to-process connections.

UDP - User Datagram Protocol. Internet standard network layer, transport layer and session layer protocols which provide simple but unreliable datagram services. It adds a checksum and additional process-to-process addressing information. UDP is a connectionless protocol, which, like TCP, is layered on top of IP. UDP neither guarantees delivery nor does it require a connection. As a result it is lightweight and efficient, but all error processing and retransmission must be taken care of by the application program.

POP3 - Post Office Protocol version 3. POP3 allows a client computer to retrieve electronic mail from a POP3 server via a TCP/IP or other connection. It does not provide for sending mail, which is assumed to be performed via SMTP or some other method. POP is useful for computers without a permanent network connection and which require a "post office" (the POP server) to hold their mail until they can retrieve it.

SMTP - Simple Mail Transfer Protocol, a protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages. The SMTP dialog usually happens in the background under the control of the message transport system, but it is possible to interact with an SMTP server using telnet to connect to the normal SMTP port, 25.

SNMP - Simple Network Management Protocol, the Internet standard protocol developed to manage nodes on an IP network. SNMP is not limited to TCP/IP and can be used to manage and monitor all sorts of equipment including computers, routers, wiring hubs, etc.

FTP - File Transfer Protocol, a client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also the client program the user executes to transfer files.

HTTP - HyperText Transfer Protocol, the client-server TCP/IP protocol used on the World-Wide Web for the exchange of HTML documents. It conventionally uses port 80.

IP - Internet Protocol, the network layer for the TCP/IP protocol suite widely used on Ethernet networks. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.

PPP - Point-to Point Protocol, the Internet standard for transmitting network layer datagrams (e.g. IP packets) over serial point-to-point links. PPP has a number of

advantages over SLIP; it is designed to operate both over asynchronous connections and bit-oriented synchronous systems and it can configure connections to a remote network dynamically, and test that the link is usable. PPP can be configured to encapsulate different network layer protocols (such as IP, IPX, or AppleTalk) by using the appropriate Network Control Protocol (NCP).

SLIP - Serial Line Internet Protocol, software that allows the Internet Protocol (IP), normally used on Ethernet, to be used over a serial line, e.g. an RS-232 serial port connected to a modem. SLIP modifies a standard Internet datagram by appending a special SLIP END character to it, which allows datagrams to be distinguished separately. SLIP does not provide error detection, being reliant on other high-layer protocols for this.

PPTP- Point to Point Tunneling Protocol, a protocol for connecting Windows NT clients and servers over Remote Access Services (RAS). PPTP can be used to create a Virtual Private Network between computers running NT. It is an extension of PPP sponsored by Microsoft. Microsoft Point to Point Encryption may be used with PPTP to provide an encrypted connection, but PPTP itself does not use encryption.

Telnet - The Internet standard protocol for remote login. Runs on top of TCP/IP. Unix BSD networking software includes a program, telnet, which uses the protocol and acts as a terminal emulator for the remote login session.

IP Routing

Internet Protocol (IP) Routing is the process of delivering an IP packet to a host on a separate/remote PC.

Dynamic Routing

Routing tables are built dynamically and routers share information with other routers using one of the two common types of protocols:

Routing Information Protocol (RIP): A distance vectoring protocol, determines the number of hops needed to deliver a packet. Stores that information in its routing table.

Open Shortest Path First (OSPF): Creates less broadcast traffic because it only updates information when a change occurs.

Static Routing

Requires routing tables to be built manually. Static routers are secretive, do not share routes or any other information.

Name Resolution

Name resolution is the method of resolving a computer name to its IP address. The computer can have two names: a NetBIOS name and a Host name. NetBIOS name - Microsoft's naming system implemented with LAN Manager, Windows and Windows NT. Host name - an older naming system primarily used with UNIX systems.

There are several files that are used to perform name resolution. These files are searched in different orders depending on which type of name resolution is in use.

NetBIOS & Host Name Resolution

Resolution Sources

- Local NetBIOS name Cache
- WINS Server
- B-node Broadcast
- LMHOSTS file
- HOSTS file
- DNS Server

Redefining what type of resolution node a system will use can change the search order.

Local NetBIOS name cache

The NetBIOS name cache contains every NetBIOS name that was recently associated with an IP address. This local cache helps reduce network traffic by eliminating the need for broadcasting or WINS queries.

NetBIOS name resolution nodes

H-node	Hybrid node. The computer will first query the WINS Server for the mapping, then if not successful, will use (up to) 3 b-node broadcasts. By inserting the IP address of the WINS Server in the computer's network properties, it defaults to H-node.
M-node	Mixed node. The computer will first use (up to) 3 b-node broadcasts, then if not successful, will query the WINS Server.
P-node	Point-to-point (aka Peer-to-peer). The computer will only query the WINS Server.
B-node	Broadcast. The computer will send out a broadcast to all computers on its local network to have the computer with the requested name send back a confirmation with its IP address. B-node is the default node method for non-WINS clients.

Alter which node a system uses by making the necessary changes in the DHCP Server.

LMHOSTS File

The LMHOSTS file contains a list of NetBIOS name to IP address mappings. It is a regular text file.

Example:

```
192.141.101.1          Server1          #PRE #DOM:CENTRAL
192.141.120.23        Computer1
192.141.120.12        Computer2
```

The tags (#) associated with the LMHOSTS file are as follows:

#PRE	Will cause the entry to be preloaded into the NetBIOS name cache.
#DOM:domain name	Specifies the domain master browser in another domain. Must be preceded by the #PRE tag.
#INCLUDE: \\server\share\lmhosts	Specifies the LMHOSTS file on another computer, and will parse it as if it were local.
#BEGIN_ALTERNATE	Precedes multiple #INCLUDE statements.
#END_ALTERNATE	Succeeds multiple #INCLUDE statements.

Host Name Resolution

UNIX machines use Host names instead of NetBIOS names. A host name is an assigned identifier used to designate a specific TCP/IP machine. It can have many host names that are the same or different than its NetBIOS name.

Resolution Sources

Local host name
HOSTS files
DNS Server
WINS Server
B-node Broadcast
LMHOSTS

HOSTS file

The HOSTS file, originally used with UNIX systems, contains a list of host name to IP address mappings. It is a regular text file named HOSTS. The HOSTS file is case sensitive.

Example:

```
102.54.94.97          rhino.acme.com   # source server
38.25.63.10           x.acme.com       # x client host
```

Address Resolution Protocol (ARP)

ARP resolves IP addresses to hardware addresses. Each network adapter has a unique hardware address (commonly referred to as a MAC address), which it uses for identification on the network.

TCP/IP communication begins with ARP. ARP resolves IP addresses to the machines network adapter (MAC) addresses for outgoing packets. Checks its cache for a correct entry. If no entry is found in the cache, broadcasts a request to the local subnet. ARP will resolve the MAC address to the gateway router address if the packet is not local.

ARP Cache

Already resolved addresses are stored in a part of the computers memory known as the ARP Cache. Entries can be static (manually entered) or dynamic. Static entries remain in memory until power is turned off. Dynamic entries remain for two minutes if not accessed and for ten minutes if accessed.

Example:

204.91.242.35	20-53-52-43-00-00	dynamic
206.172.119.90	20-53-52-43-00-00	dynamic
209.1.224.17	10-37-39-17-00-00	dynamic
140.140.102.37	13-55-50-40-00-00	static

WINS - Windows Internet Naming Services

WINS is a dynamic database located on a Windows NT Server, which stores NetBIOS names to IP address mappings.

WINS replication

WINS operates with a push/pull replication method. WINS databases can be configured as one or the other, or both.

Push - The server will send its database changes once the number of changes has met a predetermined value in the push settings. This could cause traffic at the wrong time of day, and is not recommended over WAN links.

Pull - The server will pull database changes from another server at a predetermined time of day, or at regular timely intervals, as determined in the pull settings. Is recommended for WAN links, as it can be setup to pull changes after hours or at times of day which traffic is not as heavy.

WINS Proxy

A WINS Proxy is an NT computer, which is not already a WINS Server, which listens for b-node broadcasts from non-WINS computers. Once a b-node broadcast is detected, it intercepts the broadcast, and checks its local NetBIOS cache for the requested computer name. If the computer name is not found in the proxy's cache, it forwards the request to a WINS Server. The WINS Server then returns the mapping for the name, and the WINS Proxy forwards its findings to the requesting non-WINS computer.

Non-WINS computers can have their NetBIOS name mappings stored in the WINS Servers database by being manually added. If the network was using LMHOSTS files before adding the WINS Server, it is possible to import it into the database in the Add Static Mappings option.

DNS - Domain Name Services

Domain Name Services is a hierarchical server database, which contains host name to static IP address mappings. DNS can be used to resolve NetBIOS names, but only when the box is checked to enable DNS for NetBIOS name resolution in TCP/IP properties of the Network configuration window.

DNS Server Types

Primary: A DNS Server can be setup to be a zone transfer server. Zone transfer will allow the DNS Server to query other DNS Servers if it is unable to resolve the request.

Secondary: A Secondary DNS server uses Zone Transfers to collect the DNS database from it's Primary DNS Server.

Caching DNS Server: A Caching DNS Server does not maintain any static DNS records. All of it's records are created by resolving DNS queries to a Primary or Secondary DNS server. Caching DNS servers thus add redundancy to the DNS namespace.

DHCP - Dynamic Host Configuration Protocol

DHCP is a server-based administration utility used to automatically assign IP addresses to clients. DHCP clients communicate with DHCP Servers via BOOTP broadcast messages, which can only cross routers if the router is a RFC1542-compliant router, and has BOOTP forwarding enabled. When a DHCP server receives a request for an IP address, it selects from a pool of available addresses and offers a lease to the client. If no address exists in the pool, the client cannot initialize TCP/IP.

Configuration information supplied to DHCP clients by a DHCP server include:

- IP address
- Subnet Mask
- Default gateway address
- Domain Name Server (DNS) address
- NetBIOS Name Server address

DHCP clients automatically attempt to renew their IP address lease after 50% of the lease has expired. It will broadcast to the DHCP Server for a renewal. If the DHCP Server is not available to renew the IP address, the client will wait until 87.5% (7/8) of the lease has expired, and send a broadcast to all DHCP Servers for a renewal.

Client Reservations need to be made for DHCP clients that require having a static IP address reserved, so that no DHCP clients attempt to take that address, such as Domain controllers, member servers, web servers, etc.

DHCP Relay Agent

BOOTP (DHCP) relies on broadcast. If a broadcast cannot pass a router, then routers must act as a BOOTP (DHCP) relay agent. On NT Server, this is enabled as a service through control panel, network. If routers do not support BOOTP relay, a DHCP Server is necessary on each subnet.

DNS vs. WINS vs. DHCP

DNS and WINS are really for doing two different things. But, each has been co-opted to assist the other in some cases and as a last resort. Domain Naming System (DNS) servers, resolve Domain Naming System names (host names) to IP addresses.

Windows Internet Naming Services (WINS) servers resolve NetBIOS names to IP addresses. The NetBIOS protocols require that NetBIOS nodes 'defend' their name from other machines attempting to use the same name.

Likewise, a "HOSTS" file resolves DNS names to IP addresses while an "LMHOSTS" file resolves NetBIOS names to IP addresses. As shown, the DNS server maps to the HOSTS file, and the WINS server maps to the LMHOSTS file.

The order of use of these name resolutions is dependent on various host options, check boxes, and the assigned node types. But in general, if a DNS name cannot be resolved to an IP address, then the WINS method will be used as a back-up resolution method. Conversely, the DNS Server can be selected, or on some OS versions defaults, to backing up the WINS/LMHOSTS resolution for NetBIOS names. The exact order of each separate method is dependent on which NetBIOS node types are being used as well.

The most important advantage of using WINS name resolutions is that WINS is integrated with DHCP. DHCP 'leases' IP addresses to stations when they are initializing their TCP/IP software. This leasing means that stations do not have to know or configure their own IP addresses locally; these addresses can be centrally administered on the DHCP server, and the software will correctly configure the address and other parameters at boot time.

DHCP communicates dynamic assignments to the WINS server, thus making these dynamically assigned addresses resolvable. DNS is largely a fixed, static database. Now with the integration of WINS and DNS, even the DNS clients can participate in this name resolution scheme. DHCP will offer addresses to WINS, which is supporting the DNS server, which means that addresses can be dynamically allocated and resolved with both methods.

SNMP - Simple Network Management Protocol

SNMP is a management tool used to monitor and control remote network devices. It can be used to poll specific information from the agent.

An SNMP *community* is a functional group of SNMP agents and managers. Agents receive requests and report information to the SNMP managers for the communities the agents belongs to. An SNMP *trap* is an alert, that under predefined conditions or thresholds, the SNMP agent sends to the SNMP manager.

It is *important* to understand that the SNMP Manager controls what information is provided by the SNMP Agent through a series of "GET" commands. The only message initiated by the SNMP Agent is the "TRAP".

SNMP Security

SNMP Agents allow configuration of parameters that are very helpful in managing you system security.

Send Authentication Trap - sends a message to the trap destinations if it receives a request with an incorrect community name.

Only Accept SNMP packets from these hosts - allows agent to accept only packets from defined hosts. Defined hosts are known by either their IP or IPX addresses or by their host name.

IP Addressing Fundamentals

A host is a computer or device on a TCP/IP network. Every TCP/IP host is uniquely identified by its IP address. An IP address consists of a network ID and a host ID. If two different hosts belong to the same network, they have the same network ID. The two

hosts will have different host ID's and can communicate with each other locally without going through a router. If two hosts have different network ID's, they belong to different segments on the network. They must communicate with each other remotely through a router or default gateway.

An IP address consists of 32 binary bits, where each bit is either a 0 or 1. We first write the 32 bits into four 8-bit numbers (octets) separated by a periods.

For Example: 11000001 . 00001010 . 00011110 . 00000010 (IP address in binary form)

To convert the IP address from binary to decimal form, we convert each of the four 8-bit numbers according to the following table:

Decimal Value	128	64	32	16	8	4	2	1
Octet Value	x	x	x	x	x	x	x	X

So the first octet in the above binary number would be translated as:

Decimal Value	128	64	32	16	8	4	2	1
Octet Value	1	1	0	0	0	0	0	1

Everywhere a 1 appears in table, the decimal value in that column is added to determine the decimal value of the entire octet.

or $128 + 64 + 1 = 193$

Using the same table to translate the other three octets would give us the following result.

$00001010 = 8 + 2 = 10$

$00011110 = 16 + 8 + 4 + 2 = 30$

$00000010 = 2$

So in decimal form, the above IP address is: 193 . 10 . 30 . 2

An IP address consists of two parts, one identifying the network and one identifying the host. The Class of the address determines which part is the network address and which part is the host address.

Address Classes

There are 5 different address classes. Classes can be distinguished by decimal notation of the very first octet. The following Address Class table illustrates how to determine to which class and address belongs.

CLASS	FIRST OCTET	NETWORK ID	DEFAULT SUBNET MASK	AVAILABILITY
A	1-126	First Octet	255.0.0.0	AVAILABLE
B	128-191	First 2 Octets	255.255.0.0	AVAILABLE
C	192-223	First 3 Octets	255.255.255.0	AVAILABLE
D	224-239	N/A	N/A	RESERVED FOR MULTICASTING
E	240-255	N/A	N/A	RESERVED

Note: 127 is reserved for loopback (127.0.0.1) and is used for internal testing on a local machine.

Using this table we can see the IP address in our above example is a Class C address. We can also see which part of that IP address is the Network ID and which is the Host ID.

Network ID: (First 3 Octets) = 193.10.30

Host ID: (However many Octets are left) = 2

Whenever referring to the entire network with an IP address, the host section is set to all 0's (binary=00000000) = 0. For example 193.10.30.0 specifies the network ID for the above address. When the host section is set to all 1's (binary=11111111) = 255, it specifies a broadcast that is sent to all hosts on a network. 193.10.30.255 specifies the broadcast address for our example subnet.

TCP/IP Commands & Utilities

Know what all of these commands and utilities are used for.

NBTSTAT - Displays protocol statistics and current TCP/IP connections using NetBIOS. It is also used to display NetBIOS name cache.

NETSTAT - Displays protocol statistics and current TCP/IP network connections. Netstat shows statistics since the server was booted.

ARP - Used to display and edit the ARP cache. It is used to resolve IP addresses to hardware addresses.

TRACERT - Is used to determine what route a packet takes to get from the source to the destination.

ROUTE - Used to display and edit static routing tables.

IPCONFIG - Quickly displays Windows IP configuration settings.

LPQ - Displays status of a remote LPD print queue.

LPR - Sends a print job to a remote print queue.

Ping- will send ICMP echo packets to verify connections to a remote host (or local if using the loopback address)

Fault Tolerance

In order to secure a system against loss of valuable data, establish some sort of fault tolerance program. This program will allow recovery of data should there be a disk failure. RAID (Redundant Array of Inexpensive Disks) is a method of disk configuration that will assist in this goal.

RAID Levels

Level	Name	Function
Level 0	Disk Striping	Divides data into 64k blocks and spreads it equally among all disks in the array. It is not fault tolerant.
Level 1	Disk Mirroring	Duplicates a partition on another physical disk.
Level 1	Disk Duplexing	Duplicates a partition on another physical disk that is connected to another Hard Drive Controller.
Level 2	Disk Striping w/ ECC	Data blocks are broken up and distributed across all drives in array with error checking.
Level 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.
Level 4	Disk Striping with large blocks	Complete blocks of data are distributed across all drives in the array.
Level 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.

Tape Backup

Another essential method of providing some fault tolerance is to use a tape backup system and strategy.

Type	Description
Full (Normal) Backup	<p>Copies all selected files and marks each file as having been backed up. Normal backups give the ability to restore files quickly because files on the last tape are the most current.</p> <p>Advantages of performing normal backup include the fact that files are easy to find because they are always on a current backup of a system or on one tape or tape set. In addition, recovery requires only one tape or tape set.</p> <p>Disadvantages of a normal backup are that it is the most time-consuming. If files do not change frequently, backups are redundant. Normal backups also require a large amount of tape space.</p>
Incremental Backup	<p>Only backs up files that were created or changed since the last normal or incremental backup. It marks files as having been backed up. If using a combination of normal and incremental backups, restoring requires starting with the last normal backup and then working through all the incremental tapes.</p> <p>The incremental method requires the least amount of data storage space and is the least time-consuming. However, files can be difficult to find because they are spread across several tapes; therefore, recovery takes longer than if files were on a single tape.</p>
Differential Backup	<p>Copies files that were created or changed since the last normal (or incremental) backup. It does not mark files as having been backed up. If performing normal and differential backups, restoring requires only the last normal and last differential backup tape.</p> <p>Differential backups are less time-consuming than normal backups, and recovery only requires the last normal backup tape and last differential tape.</p> <p>If large amounts of data change daily, differential backups can be more time consuming than incremental.</p>

Environmental Factors

Room conditions - It's important to setup the room with normal humidity to prevent electrostatic discharge (ESD). Air conditioning should be used to prevent the CPU from overheating. Be sure to put the equipment in a secured room to prevent someone from tampering with unsupervised equipment during off hours.

Building contents and personal effects - Consider the effects of heat on electrical signals, electromagnetic interference (EMI) from power lines or unshielded power cables as well as TV and radio interference. A common source of EMI is fluorescent lights, elevator motors, large generators, and refrigerator magnets.

Computer equipment- Computer equipment can affect the unshielded data cables with electromagnetic interference (EMI), such as monitor radiation or CPU power supplies. If the computer equipment is faulty then the network components may appear to have problems.

QUESTIONS NETWORK + EXAM

1. **The unique number that is hard coded on every Ethernet card is call what?**
A: MAC Address
2. **Two Unix servers need to transfer e-mail from one to the other, what protocol can be used to do this?**
A: SMTP
3. **What protocol is used to *pull* e-mail from the server to the client computer?**
A: POP3
4. **All workstations in one room work fine during the day, but at night, when the lights are on, users have trouble accessing the network. What is the problem?**
A: Faulty network cabling.
5. **How could you test your workstation to see if TCP/IP is working?**
*A: Ping loopback address (127.0.0.1).
Ping the local host IP address.*
6. **Who created the NDIS standard?**
*A: Microsoft
3COM*
7. **What is the IEEE 802 standard for a Token Ring LAN?**
A: 802.5
8. **What is the advantage of ISDN over the Public Telephone Network?**
A: ISDN is faster.
9. **All PCs in one certain room are spontaneously rebooting. Everything checks out, but the room is cold and there are a lot of space heaters. What is the problem?**
A: Voltage drop at outlet.
10. **What layer of the OSI model does the Bridge operate under?**
A: Data Link
11. **Troy Technologies has 500 users connected with UTP Cat 3 cabling on a 10BaseT network.**

- Required:** Add 50 more workstations to the network.
Change to a 100 Mbps network.
- Optional:** Increase the speed of the application server.
Allow clients to more quickly connect to the Server.
- Solution:** Replace the existing NIC with 100mbps NICs.
Place 100 Mbps NICs in the new machines.
Add more RAM to the Server.
Reconfigure Protocol bindings on the NICs to use most common protocol first.

A: Does not meet required results (Need 100Mbps hub and Cat 5 UTP).

12. Which OSI layer is responsible for reliable, sequenced and error free packet delivery?

A: Transport

13. What resolution does the following solution provide?

- Required:** Provide for retrieval of data in the event of disk failure.
- Optional:** Provide for safety of data in the event of natural disaster.
Provide against theft and vandalism.
- Proposed:** Use a tape backup system and manual verification.
Store tapes on-site in a locked room in a controlled access locker.

A: Provides for required and only one optional.

14. What is the maximum distance a Thicknet coax network cable can run?

A: 500 meters

15. You have a 10BaseT cable 90 meters long, a three meter patch cord at one end, and a ten meter cable at the wiring closet. Why doesn't the workstation?

A: Total cable length is to long -103 meters- Move the workstation closer.

16. Servers are continually rebooting. The room they are in has 40% humidity and temperature of 95 degrees. You have UPS and it appears to be working. What do you need to do?

A: Lower the temperature

17. Which routing method requires the most administrative overhead?

A: Static

18. What is a sudden flood of messages that clogs up your network called?

A: Broadcast Storm

19. You successfully enter into a FTP session, what transport layer protocol can you deduct is working properly?

A: TCP

20. How would you protect you network against viruses from the Internet?

A: Network Virus Protection Suite

21. Weatherman Industries wants to install Windows NT Workstation on 900 new computers when they arrive next week.

Required Results: Install the operating system over the pre-installed Windows 98 on each machine.

Configure every machine to use TCP/IP and have a unique IP address.

Optional Results: Use the most efficient file system that will still allow for communication with the NetWare servers.

Configure the 6.4 GB hard drives as one partition.

Solution: Create an unattended installation file to place Windows NT Workstation in the C:\WINDOWS directory.

Specify each workstation is to get its configuration data from a DHCP server on next boot and set the lease to lifetime.

During the install, have the unattended script change the file system on the existing partition from FAT32 to NTFS.

A: The solution meets the required results but not the optional results.

22. Which TCP/IP utility can you use to view a routing table?

A: Route

23. What are the OSI layers above and below the Session layer:

A: Transport and Presentation

24. You perform a full backup on your server every Friday. Each other day you perform an incremental backup. If your server crashed on Thursday night after the nightly backup, which set of backups would you need to restore?

A: The last full backup and all 6 incremental backups

25. Printing services will not load on one of your servers after a recent reboot. Where should you look to determine the source of the problem?

A: Server log files

26. Which UART chip provides modem connection speeds of 115,200 bps or higher?

A: 165xx

27. What do routable protocols include?

A: IP and IPX/SPX

28. How many clients can you have on one segment of 10Base2 cabling?

A: 30

29. What must the cabling be at least, to migrate from a 10BaseT network to 100BaseT?

A: CAT 5

30. Which type of hub has to boost signal strength?

A: Active

31. In Windows95, what can be used to restrict user desktop settings?

A: System policies

32. What resolution does the following solution provide?

Required: Connect two locations for file sharing over Internet.

Optional: Provide a secure connection.
Provide a permanent connection.

Proposed: Enable PPTP on the web server at headquarters.
Use an ISP from the field office to connect to the Internet.
Use PPTP to connect to headquarters.

A: Provides for required and only one optional.

33. What is a benefit of RAID 5?

A: Can lose one drive and continue operation.

34. The Data Link layer of the OSI model is actually divided up into what two sublayers?

A: LLC
MAC

35. What are the two devices shown in the exhibit? The exhibit shows two boxes that have in and out ports and many machines hanging off them in a star topology. The boxes are connected to each other with the “out” of one to the “in of the other and vice versa. This is typical of a Token Ring network.

A: MAU's.

36. Which IEEE 802.x specification specifies an architecture that is very similar to Ethernet?

A: 802.3

37. What file can be edited on a UNIX machine to resolve the name www.myserver.com?

A: HOSTS

38. Which of the following are connectionless? (Select 2)

A: TFTP, HTTP

39. What is a hardware device that can divide a signal into two or more channels called?

A: *Multiplexer*

40. Which TCP/IP protocol assigns a logical address to a host?

A: *IP*

41. What is the token in a Token Ring network generated by?

A: *The active monitor*

42. The IEEE standard that describes integrated voice and data networks is called?

A: *802.9*

43. How many wires are in a RJ-45 connector?

A: *8*

44. Which router on your segment is sent all packets destined for a remote network?

A: *Default Gateway*

45. What could be used to make your whole network visible through only one IP address to the Internet?

A: *Proxy Server*

46. A 10base2 network can have up to 5 separate segments. How many of those segments can actually have clients on them?

A: *3*

47. What WAN technology uses a 53 byte fixed length packet?

A: *ATM*

48. Breaking up and routing parts of a message to the destination independently is known as what?

A: *Packet switching*

49. Choose two protocols that are connection-oriented?

A: *FTP*
NetBEUI

50. You have a 10BaseT network connection that is 10 meters between the NIC and the wall socket and 90 meters from the socket to the wiring cabinet. It is then an additional 3 meters to the hub. Your computer cannot connect.

Required: **Decrease network downtime.**
 Improve network connectivity.

Solution: **Install a Fiber optic NIC.**

A: Does not meet requirements.

51. You are attempting to back up your data to a DLT tape drive. You receive an error message that the tape drive is not available. This occurs even if you try a new cartridge. What do you do?

A: Put a tape cleaner into the drive

52. You have 20 NT servers, 5 UNIX servers and 1 Novell 5 server. You also have several Windows 95 workstations. What protocol should you use to connect the computers on the network?

A: IP

53. The distance from patch panel to wall panel is 90 meters. The distance from wall panel to the computer is 10 meters. The distance from patch panel to hub is three meters. The computer has no connectivity.

Required: Connect to network.

**Optional: Provide a faster connection.
Provide better security.**

Proposed: Replace 10 meter cable with a 5 meter cable.

A: Provides for required result only.

54. What is the maximum distance a Thinnet coax network cable can run?

A: 185 meters

55. Which protocol is used for network management?

A: SNMP

56. Which utility is used to check TCP/IP configuration parameters on a Windows NT Workstation?

A: IPCONFIG

57. You want to send a message to a friend at Gary@network.au. Your address is Jefferson@usa.com. What is the order that your domain names are resolved?

A: usa.com, com, au, network.au

58. What OSI layer falls immediately below the Presentation Layer?

A: Sessions

59. What protocol would you use to copy a file from a UNIX server?

A: ftp

60. What is the maximum length of a NetBIOS name?

A: 15 characters

61. What functionality does Windows share level security provide?

A: Allows read only, or full access permissions along with password protection.

62. What data access method does Ethernet use?

A: CSMA/CD

63. A Windows NT domain can have how many primary domain controllers?

A: One

64. What is the functionality of the OSI model Data Link layer?

*A: Includes the MAC and LLC sublayers
Includes bridges and switches
Packages bits from the Physical layer into frames for the Network layer.*

65. Which two backup methods clear the archive bit?

A: Full and Incremental

66. At which layer of the OSI model does a repeater operate?

A: Physical

67. What common protocol is used by routers for discovery and *dynamic* routing?

A: RIP

68. What OSI layer falls directly beneath the Sessions Layer?

A: Transport

69. What two methods can you use to resolve UNIX host names to IP addresses?

A: HOSTS file and DNS

70. What utility can you use to follow the route of a TCP/IP packet to its destination?

A: Tracert

71. What occurs to packets descending through a protocol stack?

A: They have information added to them

72. How does a server on the Internet know where to send data packets?

A: Port Number

73. What is a function that web proxy server can perform?

A: Manages web ports

74. What serial line protocol can only be use by TCP/IP?

A: SLIP

75. What IP address is in the B class?

A: 191.023.21.54

76. Which two frame types do NetWare networks use?

*A: 802.2
802.3*

77. What is the highest level of security available on a network that does not use a Server?

A: Share Level

78. What is type of backup that copies all files that have been added or changes since the last full (normal) backup and does not clear the archive bit?

A: Differential

79. What system uses NDS?

A: Novell

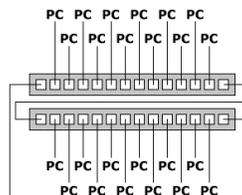
80. What are virus definition updates also called?

A: Signatures

81. Which IP parameters can you configure on a workstation? (Choose 4)

A: DNS, IP, WINS, and Default Gateway

82. What is this diagram?



A: MAU

83. What is the degradation of a signal as it travels further away from its point of origin?

A: Attenuation

84. While manning the help desk, you receive two calls at the same time. The first is from a user who cannot print a Word file, and the second is from a user who cannot restore payroll records. How should you handle the two calls?

A: Handle the payroll user first.

85. What connector is used with 10Base5 cabling?

A: AUI/DIX

86. Which protocol is used to send Email packets to an Email Server on the Internet?

A: SMTP

87. What OSI layer is responsible for data encryption?

A: Presentation

88. A user complains that it is slow to access a server. What utility can you use to find the bottleneck?

A: Tracert

89. Which IEEE standard describes Ethernet (CSMA/CD)?

A: 802.3

90. Which OSI layer is responsible for placing the signal on the cable?

A: Physical

91. Which signal transmission method uses analog signaling over a range of frequencies and transmits uni-directionally?

A: Broadband

92. Which of the following uses the hardware address in a frame in deciding whether to forward the frame?

A: A Bridge

93. At which two layers of the OSI model does a Router operate?

*A: Network
Data Link*

94. What is the connection type for UDP?

A: Connectionless

95. What type of network topology would allow you to provide multiple links to your router for redundancy?

A: Mesh

96. What command would result in the following output?

Internet Address	Physical Address	Type
195.93.150.14	00-00-27-66-44-7e	Dynamic

A: ARP

97. What is the easiest way to reduce collisions in an Ethernet LAN?

A: Install a switch

98. What type of network cable is most resistant to EMI?

A: Fiber Optic

99. What is the maximum amount of users you can have on one segment of 10BaseT cable?

A: 1024

100. Which network device has multiple ports that connect multiple segments and can guarantee full network bandwidth on each port?

A: Switch

101. What network component provides services to users?

A: Server

102. What type of device strips off the old protocol and repackages it in a new one before sending on to the next network?

A: Gateway

103. What is the NetWare 4.11 directory service or naming system called?

A: NDS

104. What protocols are not routable?

A: DLC
NetBEUI

105. What is the outer conductor in a coax cable?

A: The ground

106. What is the default port for http?

A: 80

107. Sound cards most commonly use which IRQ?

A: 5

108. What is the loopback address for a TCP/IP machine?

A: 127.0.0.1

109. What is a network generally confined to a specific geographical area?

A: LAN

110. You try to connect to a web server via HTTP. However, the connection is very slow. What command could you use to figure out where the problem is?

A: Tracert

111. What are the advantages of PSTN (Choose 3)

A: cheaper, easy to configure, and 64 KB speed

112. You are having a problem with a workstation. You notice that the link light on the NIC does not illuminate. You replace the workstation patch cable. What should you do next?

A: Attempt to log in to the server

113. Which type of server can automatically configure IP parameters for a client?

A: DHCP

114. What is it called when you configure several modems to combine into a single transmission bandwidth that is equal to the sum of their individual data transmission speeds?

A: Multi-link

115. Which cross platform name resolution method do all operating systems have support for in their TCP-IP stacks?

A: DNS

116. Which type of network cable would be most susceptible to electronic interference?

A: UTP

117. What is the fastest transmission speed possible with a 10BaseT cable?

A: 100Mbps

118. What device can you use to protect against a power failure?

A: UPS

119. What type UTP cable must be used for a 100Mbps network?

A: Cat 5

120. What is the NetWare protocol that equates to UDP?

A: IPX

121. Which RAID level encompasses both Disk Mirroring and Disk Duplexing?

A: RAID 1

122. Common TCP/IP problems are caused by invalid what?

A: subnet masks and default gateways

123. Which of the following is a class C address?

A: 205.254.97.13

124. What is the format for a UNC path name?

A: \\servername\sharename\filename

125. Where are you most likely to find patches to hardware and software products? (Choose 2)

*A: Manufacturer's Web Site
Support CD-ROM*

126. You have several users who all access the same basic sites on the World Wide Web. What could you install to improve performance?

A: HTTP Proxy

127. What can all TCP/IP devices connected to your network can be referred to?

A: Hosts

128. What is the main difference between user level and share level security?

A: User level security has centralized management

129. Which 100 Mbps Ethernet standard uses two pair of wires on a Cat 5 cable?

A: 100BaseTX

130. What are valid IP addresses for a client computer? (Choose all that apply)

*A: 198.200.200.1
2.1.1.254*

131. You get a call from Thelma who works in the accounting department. She states that she cannot print to the network printer. She is in a group that has the correct permissions to print. All other users of the same group can print to the printer. What can be the problem?

A: Her user access permissions are wrong.

132. Under what layer of the OSI model does the Router operate?

A: Network

133. What is one security function of a firewall?

A: Restricts unauthorized users from accessing sensitive data

134. You setup a network with FTP and use a SLIP protocol. You cannot transfer files with FTP and have problems connecting to the Internet, what is a possible alternative?

A: Change to PPP

135. You install new a virus suite in your network of 120 computers. You configure RAID in one system. You are experiencing sporadic system crashes throughout your network, what do you do?

A: Check the virus vendor for system patches or service packs

136. What connectors are used on SCSI cables? (Select 3)

*A: DB 25, female
50 Pin Centronics
68 Pin*

137. You place a new NIC card in a workstation. You cannot connect to the network. There are no resource conflicts. Everything is configured and installed correctly yet you still can't connect. What do you do?

A: Use a hardware loopback connector

138. You place a new NIC card in a workstation. You cannot connect to the network. There are no resource conflicts. Everything is configured and installed correctly yet you still can't connect. What do you do?

A: Check it with diagnostic troubleshooting software

139. You place a new NIC card in a workstation. You cannot connect to the network. There are no resource conflicts. Everything is configured and installed correctly yet you still can't connect. You check the NIC card with the manufacturer's internal diagnostic software. What do you do?

A: Check it with external hardware loopback

140. What utility do you use to check your IP configuration on a Windows 95/98 workstation?

A: WINIPCFG

141. Which security scenario is more restrictive?

A: User level access

142. Your entire network of 100 computers is bogged down. Everything is connected properly and there are no conflicts that you are aware of. What can you use to help you narrow down the problem?

A: Network Monitor

143. What does a patch cable connect to in a Token Ring Network?

A: Connects two MAU's together

144. What utility can you use to troubleshoot a http server?

A: Telnet

145. What is the default port for the FTP protocol?

A: 21

146. A user complains that he can't log onto a server. What troubleshooting steps should you take to resolve the problem? (Select 3)

*A: Ask a user on the same segment to try to connect
Ask a user on a remote segment to try to connect
Try to ping the server*

147. What three things do you need to specify on a workstation for DNS resolution?

*A: Domain name
Host name
IP address of the DNS server*

148. To send a formatted file to a Novell network printer from DOS you would use the command:

A: NPRINT

149. You cannot connect to a network server. The light in the back of the NIC card is not flashing. You change the patch cable and it is still not flashing. You go into the wiring closet and switch the connector from one connection on the hub to another. You check the NIC light and it is blinking. What should you do next?

A: Log in and try to transfer a file

150. What cable can you use to connect to a server 1 KM away without having to use a repeater?

A: Fiber Optic or 10BaseFX

151. To connect a transceiver to the cable in a Thicknet network you could use:

A: A vampire tap

152. You have a workstation over 103 meters from the server. There is no repeater and you are using 10BaseT wiring. You cannot connect to the network.

Required objectives: Connect to the server.

Optional Objectives: Provide a faster connection.
Provide easier access for users.

Proposed solution: Replace the NIC with a 100baseFX NIC

Which results are accomplished?

A: This does not meet the required or optional objectives.

153. Peer-to-peer networks should usually be limited to how many computers?

A: 10 or less

154. You are installing a NetWare based server system. You have 10 Win95 workstations and 4 UNIX computers. What do you install on the Win 95 systems that will allow you to connect to the NetWare server? (Choose 2)

*A: NetWare Client for Windows
Microsoft Client for NetWare*

155. What is a secure password policy?

A: Change passwords regularly

156. Collisions in an Ethernet network indicate a problem and corrective action should be taken.

A: False

157. What is the easiest way to fault protect the disk on a small NT Server?

A: Disk Mirroring

158. What is the maximum length of one 100BaseTX segment?

A: 100 meters

159. What starts a comment line in a HOSTS file?

A: #

160. One of your workstations is not able to connect to the Intranet web server. What do you do to make sure that the workstation is not the problem?

A: Try connecting to the Intranet through a different computer.

161. What is the most effective password for user one?

A: User\$one

162. What is the default subnet mask for the IP class C?

A: 255.255.255.0

163. Email and FTP works at which layer of the OSI model?

A: Application

164. Which use FDM (Frequency Division Multiplexing)?

A: Broadband.

165. You are a network administrator for a big company. One of the company managers calls you and complains that he can't connect to the Internet. You tried to connect from his workstation and were able to connect using his account and password. But the employee complains that he still can't connect to the Internet. What is the problem?

A: The employee is trying to connect incorrectly

166. Your organization has two offices; one in London and another one in Boston. You want to use the Internet to establish a secure and encrypted communication between two locations, also known as Virtual Private Network. What connection protocol should you use?

A: PPTP

167. What network topology is the most fault tolerant and has the most redundancy?

A: Mesh

168. You have been asked to design a network for a manufacturing company. The company runs mission critical applications and each computer on the network must have guaranteed access to the network. What network access method will be the most appropriate in this situation?

A: Token Ring

169. You are troubleshooting a Token Ring Network. Each node on the network is connected to the MAU by a dedicated cable segment. What physical topology is used on your network?

A: Star

170. Disk mirroring requires a minimum of how many hard drives and hard disk controllers?

A: 2 hard drives 1 hard disk controller

171. Disk duplexing requires a minimum of how many hard drives and hard disk controllers?

A: 2 controllers and 2 hard disks

172. You configure your TCP/IP to connect WINS. What configuration on your PC is required?

*A: Primary WINS
Enable WINS Resolution*

173. What is the disadvantage of more than 100 clients on bus topology?

A: - Prone to cable errors

174. What utility do you use to view how many hops to destination?

A: TRACERT

175. What type of transport layer connection is used for a safe connection?

A: Connection oriented TCP

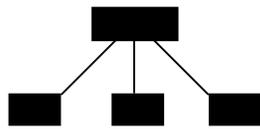
176. What is a MAC-address?

A: Be able to identify the address

177. What does the output from the utility TRACERT look like?

A: Be able to identify the output.

178. What topography does this identify?



A: Star

179. What is the default TCP port for SMTP transfer?

A: 25