Last updated June, 2000. Click here for updates.

Click here to see additional documents related to this study guide. Click here to receive free practice questions for Network + Certification.

Contents

Cramsession™ for Network + Certification

Abstract:

This Cramsession will help you to prepare for the CompTia Network + Exam. Exam topics include Knowledge of Networking Technologies, Layers, TCP/IP, Knowledge of Networking Practices, Installing, Supporting and Troubleshooting Networks.

Notice: While every precaution has been taken in the preparation of this material, neither the author nor BrainBuzz.com assumes any liability in the event of loss or damage directly or indirectly caused by any inaccuracies or incompleteness of the material contained in this document. The information in this document is provided and distributed "as-is", without any expressed or implied warranty. Your use of the information in this document is solely at your own risk, and Brainbuzz.com cannot be held liable for any damages incurred through the use of this material. The use of product names in this work is for information purposes only, and does not constitute an endorsement by, or affiliation with BrainBuzz.com. Product names used in this work may be registered trademarks of their manufacturers. This document is protected under US and international copyright laws and is intended for individual, personal use only. For more details, visit our legal page.

Network + Certification

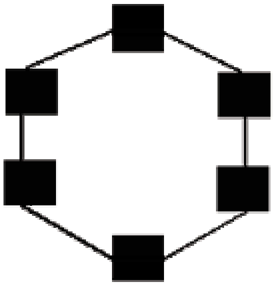
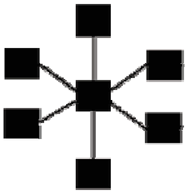
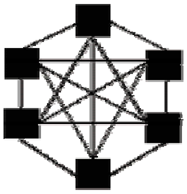
I. Knowledge of Networking Technology 67%

I.1 Basic Knowledge 16%

I.1.1 Demonstrate understanding of basic network structure, including

- The characteristics of star, bus, mesh, and ring topologies, their advantages and disadvantages
  - **Star** - A star physical topology means that the nodes/devices are all connected to a centralized hub or switch and is commonly used for 10BASE5, 10BASE-T or 100BASE-TX
    - **Pros:** cabling is inexpensive, easy to wire, more reliable and easier to manage because of the use of hubs which allow defective cable segments to be routed around; locating and repairing bad cables is easier because of the concentrators; network growth is easier
    - **Cons:** All nodes receive the same signal therefore dividing bandwidth; max computers is 1,024 on a LAN; max UTP length is 100 meters (approx 330 ft); distance between computers is 2.5 meters.
  - **Bus** - a bus physical topology means that all of the devices are connected to a common backbone; signal is sent in both directions, but some buses are unidirectional; can be used for 10BASE5, 10BASE2 or 10BROAD36
    - **Pros:** Good for small networks
    - **Cons:** Difficult to troubleshoot and locate where the break in the cable is or which machine is causing the fault; when one device fails the rest of the LAN fails.
  - **Mesh** - A mesh physical topology is when every device on the network is connected to every device on the network; most commonly used in WAN configurations
    - **Pros:** helps find the quickest route on the network; provides redundancy
    - **Cons:** very expensive and not easy to set up
- **Ring** - A ring physical topology is when the devices are wired in a circle, but almost always implemented in a logical ring topology on a star physical topology. Each device has a transceiver which behaves like a repeater which moves the signal around the ring; ideal for token-passing access methods
  - **Pros:** Signal degeneration is low; only the device that holds the token can transmit which reduces collisions.

- **Cons:** Difficult to locate a problem cable segment; expensive hardware

Bus	Ring	Star	Mesh
			

- The characteristics of segments and backbones
  - Segments - Typically a trunk of cabling connecting a device to a concentration device or routing device, also a logical group of devices which communicate within a given subnet that is separated by a bridge, router, brouter, switching hub, or multiplexer.
  - Backbones - The foundation of the LAN/WAN where the servers are linked together on a common series of concentration devices or that are just a few hops away. This gives the servers the most bandwidth to serve other devices including other servers.

I.1.2 Identify the following:

- The major network operating systems, including Microsoft Windows NT, Novell NetWare, and Unix.
  - MS Windows NT - A networking operating system designed using a Directory to manage certain resources. NT's primary file system is NTFS (New Technology File System). Provides an inherently GUI console at the server.
  - 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.

Unix

- The clients that best serve specific network operating systems and their resources.
  - 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. Best file transfer throughput would be NT Workstation.

- Novell NetWare works well with most popular clients OS's such as DOS, Windows 3.11, Windows 9x, Windows NT Workstation, but the clients that serves NetWare are DOS flavors, and DOS based OS's such as Windows 95/98 for file sharing. Macintosh and OS/2 work with NT and NetWare but work best with the NOS written for them.
- Unix specific clients such as Sun Sparc stations work best with their manufacturer's NOS.

- The directory services of the major network operating systems.
    - Windows NT uses a directory service database that contains information related to users, groups and computers. It can be replicated between Domain Controllers by a schedule or on demand. Windows 2000 uses Active Directory which is a hierarchical security model, similar to NDS.
    - NetWare 3.x uses bindery services, NW 4.x and 5 both use Novell Directory Services (NDS). Bindery is restricted to the machine it sits on, NDS uses a tree structure.
    - Unix uses ???

I.1.3 Associate IPX, IP, and NetBEUI with their functions.

- IPX - Internetwork Packet Exchange. It's the Novell NetWare designed protocol which is the default protocol during installation. Packet sizes for Ethernet are approx 1500 bytes, for Token Ring they are approx 4Kb. Performs addressing and routing functions. Resides in Network Layer. Requires some configuration.
- IP - Internet Protocol. DOD standard designed for ARPAnet. Based on two models, the DOD model (4 layers) and the OSI model (7 layers), which is the Windows NT and Unix default protocol during installation. Requires a lot of configuration. IP functions on the Internet layer of the DOD model and on the Network layer of the OSI model. A connectionless protocol responsible for addressing and routing packets between hosts.
- NetBEUI - NetBIOS (Network Basic Input Output System) Enhanced User Interface. Microsoft designed protocol for fast packet delivery in a small network without much configuration, its shortcoming is that it's not routable. It operates on the Network and Transport layers of the OSI model.

I.1.4 Define the following terms and explain how each relates to fault tolerance or high availability:

- Mirroring - RAID 1: Duplicates a partition on another physical disk with one data channel, 2 drives, 1 used for data, 1 for parity, advantages are fault tolerance; disadvantages are it's expensive and requires twice the disk space
- Duplexing - RAID 1: Duplicates a partition on another physical disk that is connected to another Hard Drive Controller using two data channels simultaneously, two data cables and two DASD, 1 used for data, 1 for parity,

advantages and disadvantages are the same as mirroring but duplexing provides much faster read speeds than mirroring.

- Striping (with and without parity) - data striping is when blocks or bits of data are written to each drive in the array in succession. It's used in most RAID levels and is great for improving read/write speeds because the I/O request are being distributed between all I/O data channels. Parity checking relies on an extra bit called a parity bit, which is used to compare the bit string to an odd or even count. If the odd or even count is not matched based on the setting of the parity bit, then the data string is sent again. Extra drive space is used for the parity bits. Not using parity will improve overall data transmission because of the omission of the parity bit calculation, but should be used when speed is of greater importance than fault tolerance. RAID 5 provides the best fault tolerance because it uses several drives with block interleaving, a distributed check sum for parity and has fast reads.
- Volumes - are active segments of a physical server hard drive which may be fully contained in a single hard drive, spanned over several disks or multiple volumes can occupy one hard drive.
- Tape backup - offline storage and is easily removable, slow read/write compared to hard disk, high capacity on magnetic tape, excellent choice for fault tolerance because it's cheap and the media can be sent elsewhere for protection.

I.1.5 Define the layers of the OSI model and identify the protocols, services, and functions that pertain to each layer.

- Application - (layer 7) Allows applications to use the network. Handles network access, flow control and error recovery. messages are sent between layers
    - Protocols - SMB, NCP
    - Services - Telnet, FTP use TCP, TFTP, NFS, SNMP, SMTP use TCP
    - Functions - User interface with applications & Gateways

- Presentation - (layer 6) Translates data into a form usable by the application layer. The redirector operates here. Responsible for protocol conversion, translating and encrypting data, and managing data compression. messages are sent between layers
    - Protocols - NCP
    - Services - Telnet, FTP use TCP, TFTP, NFS, SNMP, SMTP use TCP
    - Functions - Gateways

- Session - (layer 5) Allows applications on connecting systems to establish a session. Provides synchronization between communicating computers. messages are sent between layers
    - Protocols - N/A
    - Services - Telnet, FTP use TCP, TFTP, NFS, SNMP, SMTP use TCP

  - Functions - Gateways

- Transport - (layer 4) Responsible for packet handling. Ensures error-free delivery. Repackages messages, divides messages into smaller packets, and handles error handling. segments of message fragments are sent between layers
  - Protocols - SPX, TCP, UDP and NetBEUI function on this layer
  - Services - TCP/SPX - connection-oriented communication for applications to ensure error free delivery; UDP - connectionless communications and does not guarantee packet delivery between transfer points
  - Functions - Gateways function on this layer

- Network - (layer 3) Translates system names into addresses. Responsible for addressing, determining routes for sending, managing network traffic problems, packet switching, routing, data congestion, and reassembling data. Datagrams are sent between layers
  - Protocols - IPX, IP, ICMP, ARP, RARP, RIP, OSPF, EGP, IGMP, NetBEUI, DLC, and DecNET function on this layer
  - Services - software & hardware addresses and packet routing between hosts and networks (IP/IPX); software addresses to hardware addresses are resolved (ARP/RARP), sends messages and reports errors regarding packet delivery (ICMP), reports host group membership to local multicast routers (IGMP)
  - Functions - Routers and Brouters function up to this layer

- Data link - (layer 2) Sends data from network layer to physical layer. Manages physical layer communications between connecting systems. Data frames are sent between layers
  - Protocols - HDLC (High-level Data Link Control); Supports asynchronous and synchronous transmissions. Uses LLC flow control
  - Services - Ethernet, Token Ring, and other communications occur here via frames. LLC - (802.2) Manages link control and defines SAP's (Service Access Points). MAC - (802.3, 802.4, 802.5, 802.12) Communicates with adapter card.
  - Functions - Switches, brouters and bridges function on this layer using the MAC sublayer

- Physical - (layer 1) Transmits data over a physical medium. Defines cables, cards, and physical aspects. Data bits are sent.
  - Protocols - No protocols function on this layer
  - Services - Ethernet (CSMA/CD), Token Ring (token passing), and other communications occur

  - o Functions - Repeaters and multiplexers function on this layer; bits are sent across the wire

I.1.6 Recognize and describe the following characteristics of networking media and connectors:

- The advantages and disadvantages of coax, Cat 3, Cat 5, fiber optic, UTP, and STP, and the conditions under which they are appropriate
  - o Coax - commonly used for thick ethernet, thin ethernet, cable TV and ARCnet, coaxial cabling that uses BNC connectors; heavy shielding protects data, but expensive and hard to make connectors
  - o CAT 3 - UTP/STP can be used for voice or data, but can be used for data up to 10Mps. Good for cable segments to workstations or printers
  - o CAT 5 - UTP/STP can be used for voice and/or data, but data transmissions up to 100Mps. Good as a backbone, but also good for cable segments to workstations or printers since price is dropping.
  - o Fiber optic - (IEEE 802.8) Cable in which the center core, a glass cladding composed of varying layers of reflective glass, refracts light back into the core. Max length is 25 kilometers, speed is up to 2Gbps but very expensive. Best used for a backbone due to cost.
  - o UTP - Unshielded Twisted Pair; uses RJ-45, RJ-11, RS-232, and RS-449 connectors, max length is 100 meters, speed is up to 100Mps. Cheap, easy to install, length becomes a problem. Can be CAT 2,3,4 or 5 quality grades.
  - o STP - Shielded Twisted Pair; uses RJ-45, RJ-11, RS-232, and RS-449 connectors, max length is 100 meters, speed is up to 500Mps. Not as inexpensive as UTP, easy to install, length becomes a problem. Can be CAT 2,3,4 or 5 quality grades.

- The length and speed of 10Base2, 10BaseT, and 100BaseT
  - o 10Base2 - max length 185 meters, max speed 10Mps (Thin Ethernet)
  - o 10BaseT - max length 100 meters, max speed 10Mps
  - o 100BaseT - max length 100 meters, max speed 100Mps

- The length and speed of 10Base5, 100Base VGAnyLan, 100Base TX
  - o 10Base5 - max length 500 meters, max speed 10Mps (Thick Ethernet)
  - o 100Base5 - max length 500 meters, max speed 100Mps
  - o VGAnyLan - max length 250 meters, max speed 100Mps
  - o 100BaseTX - max length 100 meters, max speed 100Mps
- The visual appearance of RJ 24 and BNC and how they are crimped.

I.1.7 Identify the basic attributes, purpose, and function of the following network elements:

- Full- and half-duplexing
  - Half-duplexing - each device in the configuration can send and receive information, but only one at a time; while sending the device cannot receive, very much like walkie-talkies.
  - Full-duplexing - each device in the configuration can send and receive simultaneously. The best example of this is the telephone.

- WAN and LAN - A LAN is a local area network that is a small collection of workstations in a geographic area of less than 1 mile and is very fast for data transfer. A wide area network is a network of LANs. A WANs geographic location is considered to be global using advanced routers. WANs are much slower than LANs but are increasing in speed.
- Server, workstation, and host
  - Server - a device providing resources to other devices on the network typically found in a distributed processing environment
  - Workstation - a device which accesses available resources from servers typically found in a distributed processing environment
  - Host - an addressable computer system on a TCP/IP network such as workstations, servers, minicomputers, mainframes, and routers which typically offers resources to network nodes.

- Server-based networking and peer-to-peer networking
  - A peer-to-peer network does not rely on the use of a central file server to share file but 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.
  - A 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, an 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, NIC, and router
  - 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 - Network Interface Card is component added to a computer circuit board expansion slot and connects directly to network cabling. NOS software is installed on the workstation to allow communication between the workstation OS and the server NOS.

  - Router - means a connection between similar or dissimilar topologies using the same protocol operating at the OSI Network Layer.

- Broadband and baseband
  - **Baseband** transmissions use the entire medium's capacity for a single channel over digital signaling. Since only one signal at a time can occupy a channel, the use of a MUX will allow multiple devices to send multiple signals using a single transmission medium. Provide excellent throughput because the digital signal occupies the entire channel.
  - **Broadband** transmissions share the medium's bandwidth over multiple analog channels unidirectionally. This is performed using different frequencies and a process known as FDM (frequency division multiplexing). Since these transmission work very well over long distances, WAN communications take advantage of this technology.
- Gateway, as both a default IP router and as a method to connect dissimilar systems or protocols
  - A default gateway is an IP address used to forward packets from one subnet to another subnet.
  - A gateway that connects dissimilar systems or protocols allows different platforms to inter-operate, which adds expansion and functionality to a LAN. A gateway basically grants a workstation a direct connection to the host computer and acts as a messenger between the two systems. Gateways operate between the OSI Transport layer through the Application Layer.

I.2 Physical Layer 6%

I.2.1 Given an installation, configuration, or troubleshooting scenario, select an appropriate course of action if a client workstation does not connect to the network after installing or replacing a network interface card. Explain why a given action is warranted. The following issues may be covered:

- Knowledge of how the network card is usually configured, including EPROM, jumpers, and plug-and-play software
- Use of network card diagnostics, including the loopback test and vendor-supplied diagnostics
- The ability to resolve hardware resource conflicts, including IRQ, DMA, and I/O Base Address.

I.2.2 Identify the use of the following network components and the differences between them:

- Hubs - a hub is 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).
- MAUs - (Multistation Access Unit) an access device used to connect the main cabling structure to devices in use on a Token Ring network. This device adds

fault tolerance to the network so that a single failure doesn't stop the whole network

- Switching hubs - are intelligent hubs which contain circuitry that very quickly route signals between ports on the hub. This method reduces bandwidth waste because only the device which needs to receive the packet does, rather than the entire network segment.
- Repeaters - devices that amplify and regenerate a signal to extend the distance of a LAN
- Transceivers - connect different Ethernet nodes together in an organized fashion across an individual Ethernet segment; allows multiple Ethernet segment nodes to connect to each other to create a segment.

I.3 Data Link Layer 5%

I.3.1 Describe the following data link layer concepts

- Bridges, what they are and why they are used
  - Bridges are used to segment networks. They forward packets based on address of destination node. Uses RAM to build a routing table based on hardware addresses. Some bridge types are capable of connecting dissimilar network topologies. Will forward all protocols. Regenerates the signal at the packet level
- The 802 specs, including the topics covered in 802.2, 802.3, and 802.5
  - 802.2 - LLC (Logical Link Control manages link control and defines SAPs); Adds header fields to identify upper-layer protocols. It provides reliable, intelligent information to otherwise dumb frames. Also, acts as a switch board to make sure MAC frames find their way to the right Network layer process.
  - 802.3 - (MAC communicates with adapter card) CSMA/CD - Ethernet; Provides physical layer options including different topologies, media types, data rates and signaling modes.
  - 802.5 - (MAC communicates with adapter card) Token Ring LAN; Uses token-passing media access protocol across a physical star, logical ring and differential Manchester encoding to provide data rates
- The function and characteristics of MAC addresses
  - MAC addresses, which are a.k.a physical addresses, operate on the data link layer. Each address is unique 12-digit hexadecimal ID number, which is hard coded to the network device by the factory, and is used by devices to direct their packets to other devices.

I.4 Network Layer 5%

I.4.1 Explain the following routing and network layer concepts, including

- The fact that routing occurs at the network layer
  - Routers help organize a large network into terms of logical network segments using logical network IDs

- The difference between a router and a brouter
  - A router functions on the network layer of the OSI model
  - A brouter functions as a bridge on the data link MAC sublayer and as a router on the network layer.
- The difference between routable and non-routable protocols
  - A routable protocol permits its packets to be sent beyond a single LAN/WAN segment whereas a non-routable protocol's packets will remain on the originating LAN segment
- The concept of default gateways and subnetworks
  - A default gateway is the exit and entry point of a subnet.
  - Subnetworks are a division of the entire internetwork which are created to provide security and/or reduced traffic over a WAN or congested networks
- The reason for employing unique network IDs
  - Unique network IDs prevent confusion between devices and help them to properly direct their packets/datagrams. When a router receives a packet which is destined for a network ID on the other side, the router will know how to behave.
- The difference between static and dynamic routing.
  - Static routing requires human interaction to fill the routing tables and to provide accurate IP addressing, subnet masking and the default gateway of the router
  - Dynamic routing uses information from neighboring routers to fill the routing tables, therefore, in a high volume environment the human error factor is greatly reduced when adding routes

I.5 Transport Layer 4%

I.5.1 Explain the following transport layer concepts**:**

- The distinction between connectionless and connection-based transport
  - Connectionless - internal nodes along the message path do not participate in error correction and flow control.
  - Connection-based - an acknowledgement (ACK) verifies that the host has received each segment of the message, which results in reliable delivery service. If the ACK is not received after a given time period, then the data is resent. If segments are not delivered to the destination device correctly, then the Transport layer can initiate retransmission or inform the upper layers. Uses segmentation, flow control, and error checking to insure packet delivery
- The purpose of name resolution, either to an IP/IPX address or a network protocol
  - Name resolution helps upper layer services communicate segment destinations with lower layer services.

I.6 TCP/IP Fundamentals 12%

I.6.1 Demonstrate knowledge of the following TCP/IP fundamentals:

- The concept of IP default gateways
    - A default gateway is the entry and exit point of datagrams between subnets
    - As a packet passes through a router, the TTL is decremented by at least 1 until the packet TTL reaches 0; this prevents a packet from traveling forever
    - If a packet is too large for the gateway then it is fragmented with the following information: 1) a flag which indicates that there are other packets, 2) a fragment ID to identify the fragment and 3) a fragment offset to indicate how to reassemble the packets
    - The default gateway MUST have the same subnet mask as the network it resides on
- The purpose and use of DHCP, DNS, WINS, and host files
    - DHCP - Dynamic Host Configuration Protocol;
        - Dynamic allocation of IP address, default gateway and subnet mask to a requesting IP client; reduces administrative overhead
        - DHCP uses the BOOTP protocol to communicate with clients and uses BOOTP to cross routers if the router is RFC 1542 compliant and has BOOTP forwarding enabled
        - When setting up a scope, the scope's range is limited to a particular subnet
        - Add a scope to provide services for additional subnets.
        - 4 step process: client request, server offer, client select, server acknowledges
        - Clients attempt to renew after 50% of their lease life has expired by sending a DCHPREQUEST packet
        - Clients will attempt to renew again at 87.5% expiration of lease life if DHCPREQUEST from before was not responded to
        - To confirm IP assignment use utilities such as IPCONFIG, WINIPCFG
        - Clients retain IP assignment until lease expires or until a DHCPRELEASE command is sent from client
        - DHCP Relay Agent will forward DHCP messages between clients and servers
    - DNS - Domain Name Services
        - Helps clients resolve host names to IP addresses internally and externally
        - Uses static mapping in a hierarchical database (root-level/top-level/second-level/host name)

    - Can be used to resolve NetBIOS names with NT if you check the box to "Enable DNS for Windows Resolution" in the TCP/IP properties configuration dialog box in the WINS Address tab
    - A CNAME is a method of DNS aliasing for something such as a www or ftp server
    - You can setup zone transfers between Primary and Secondary DNS servers for fault tolerance
  - WINS - Windows Internet Naming Service
    - Eliminates the need for clients to send broadcasts for computer name resolution
    - Uses dynamic mapping
    - Eliminated the need for LMHOSTS files
    - Process includes 1) WINS client registers its NetBIOS name and IP Address at startup with WINS server, 2) WINS client sends a name query request to the WINS server to talk to another host, and 3) if IP and host name are found in database then the WINS server will send to requesting WINS client
    - Upon proper shutdown, the WINS client will send a name release to the WINS server
    - WINS requests are routable datagrams
    - WINS Proxy Agent is used for non-WINS clients (UNIX) to resolve NetBIOS names of MS clients; one proxy agent per subnet but no more than two agents per subnet
    - MS Clients can resolve the host names of UNIX computers as long as the host names are 15 char or less, no special chars and the UNIQUE UNIX computer names + IP are entered into WINS statically
    - No WINS Macintosh support
  - HOSTS & LMHOSTS files
    - HOSTS is for DNS and UNIX, therefore they are case sensitive for UNIX hosts
    - Syntax is IP address TAB host name. Multiple hosts can be on one line BUT where the first instance of the IP address is found will be the IP assigned to that host name.
    - EX. 123.45.6.78 www.bubba.com www.bubbaco.com
    - HOSTS is a static map of IP addresses to host names of machines, typed into a text file
    - On NT can be up to 256 char long
    - Must have one file on each computer that is not using DNS
    - Names are read in order one at a time, so the most commonly used names should be at the beginning of the file
    - LMHOSTS is for WINS and is not case sensitive

        - Static map of IP address to NetBIOS name
        - Required for non-WINS clients that use NetBIOS broadcasts for NetBIOS name resolution
        - Maps NetBIOS name to IP address using a static text file
        - Syntax example on a PDC 123.45.6.78 sales #pre #dom:bubbaco
        - On each BDC put an entry for the PDC in the LMHOSTS file
        - # means comment unless in front of a special command such as #pre, #dom, #include, #begin_alternate, #end_alternate

- The identity of the main protocols that make up the TCP/IP suite, including TCP, UDP, POP3, SMTP, SNMP, FTP, HTTP, and IP
    - TCP - Transmission Control Protocol: a reliable, connection-based protocol; good for large amounts of data with a lot of ACK overhead
    - UDP - User Datagram Protocol: an unreliable, connectionless protocol for sending small amounts of data without the overhead of ACKs
    - POP3 - Post Office Protocol version 3: a method of transferring mail files from a mail server to a mail client from it's source
    - SMTP - Simple Mail Transfer Protocol: a method of transferring mail files from a mail client to mail server prior to the destination
    - SNMP - Simple Network Management Protocol: a management tool used to monitor and control remote network devices which can poll specific information from the agent
    - FTP - File Transfer Protocol: a fast and error-free method to transfer files from host to host
    - HTTP - HyperText Transfer Protocol: the common protocol used on the World Wide Web to transfer files from a server to a web browser
    - IP - Internet Protocol: a connectionless protocol responsible for addressing and routing packets between hosts
- The idea that TCP/IP is supported by every operating system and millions of hosts worldwide
- The purpose and function of Internet domain name server hierarchies (how email arrives in another country).

I.6.2 Demonstrate knowledge of the fundamental concepts of TCP/IP addressing, including

- The A, B, and C classes of IP addresses and their default subnet mask numbers
    - Class A - network ID start bit is 0 and default subnet mask is 255.0.0.0; decimal range 1-126
    - Class B - network ID start bit is 10 and default subnet mask is 255. 255.0.0.0; decimal range 128-191

    - Class C - network ID start bit is 110 and default subnet mask is 255. 255. 255.0; decimal range 192-223

- The use of port numbers (HTTP, FTP, SMTP) and port numbers commonly assigned to a given service.
    - Ports are assigned by RFC 1060 to create a socket connection
    - HTTP - port number 80/tcp
    - FTP - port number 21/tcp
    - SMTP - port number 25/tcp

I.6.3 Demonstrate knowledge of TCP/IP configuration concepts, including

- The definition of IP proxy and why it is used
- The identity of the normal configuration parameters for a workstation, including IP address, DNS, default gateway, IP proxy configuration, WINS, DHCP, host name, and Internet domain name.

I.7 TCP/IP Suite: Utilities 8%

I.7.1 Explain how and when to use the following TCP/IP utilities to test, validate, and troubleshoot IP connectivity:

- ARP - used to gather hardware addresses of local hosts and the default gateway, you can view the ARP cache and check for invalid or duplicate entries
    - Command syntax
        - arp -a [inet_addr] [-N [if_addr]]
        - arp -d inet_addr [if_addr]
        - arp -s inet_addr ether_addr [if_addr]
    - Command switches
        - -a or -g - displays the current contents of the arp cache
        - -d - deletes the entry specified by inet_addr
        - -s - adds a static entry to the cache, mapping an IP address to a physical address
        - -N - displays the arp entries for the specified physical address
        - inet_addr - IP address, written in dotted decimal format
        - if_addr - IP address of the NIC whose cache should be modified, if no IP address, the first NIC is used
        - ether_addr - the physical address in hex separated by hyphens

- Telnet - this is a terminal emulation program that will allow you to run interactive commands on the telnet server. Until a connection is established, no data will pass and if the connection should break telnet will inform you. Good for testing login configuration parameters to a remote host.

- Command syntax
  - Telnet

- NBTSTAT - reports statistics and connections for NetBIOS over TCP/IP. Use for DNS and WINS name resolution, local cache lookup, and referral to LMHOSTS and HOSTS files. Troubleshoot name-to-address mappings with NBTSTAT
  - Command syntax
    - Nbtstat [-a remotename] [-A IPaddress] [-c] [-n] [-R] [-r] [-S] [-s] [interval]
  - Command switches
    - -a remotename - lists the remote computer's name table by the remote computer's name
    - -A IP address - lists the remote computer's name table by the remote computer's IP address
    - -c - lists the contents of the name cache, mapping each IP address to a name
    - -n - lists local NetBIOS names
    - -R - if LMHOSTS lookup is enabled, then it will purge the name cache and reload it from the LMHOSTS file
    - -r - lists name-resolution statistics for Windows networking
    - -S - displays workstation and server sessions, listing hosts by IP address
    - -s - displays workstation and server sessions, attempting to list hosts by name
    - interval - the number of seconds between refreshes of statistics
- Tracert - used to determine the route a packet took to reach its destination
  - Command syntax
    - Tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name
  - Command switches
    - -d - specifies that IP addresses should not be resolved to host name
    - -h maximum_hops - can only search up to the specified number of hops
    - -j host-list - specifies the loose source route
    - -w timeout - waits the number of milliseconds specified by timeout for each reply
- NETSTAT - this command displays protocol statistics and gets information about TCP/IP connections

  - Command syntax
    - Netstat [-a] [-e] [-n] [-s] [-p protocol] [-r] [interval]
  - Command switches
    - -a - displays connections and listening ports and their current state, but not the server sessions
    - -e - displays Ethernet stats
    - -n - displays active connections, listed by IP address
    - -s - displays per-protocol statistics for IP, ICMP, TCP, and UDP
    - -p protocol - displays active connection statistics for the chosen protocol (TCP or UDP), can use with the -s switch for more information
    - -r - displays the contents of the routing table

- ipconfig/winipcfg - these utilities display IP-addressing information for the local network adapter(s) or a specified NIC.
  - Command syntax
    - ipconfig [/all | /renew [adapter] | /release [adapter]]
  - Command switches
    - /all - all information about adapter(s)
    - /renew - renew DHCP lease information for all local adapters if none is named
    - /release - release DHCP lease information thereby disabling TCP/IP on this adapter

- FTP - this utility is used to transfer files between server and client. This is a reliable method of data transfer because it uses TCP. There is a long list of session commands for file management
  - Command syntax
    - ftp [-v] [-n] [-i] [-d] [-g] [-s: filename] [hostname]
  - Command switches
    - -v - suppresses any display server responses (@echo off in DOS)
    - -n - prevents automatic login when connection has been established
    - -I - turns off interactive prompting during file transfer
    - -d - displays all ftp commands exchanged between client and server, for debugging
    - -g - disables the globbing capability
    - -s: filename - specifies a text file containing ftp commands and then runs the commands within the file, similar to a batch file
    - hostname - the host to connect to and MUST be the LAST parameter specified

- ping - will send ICMP echo packets to verify connections to a remote host (or local if using the loopback address)
  - Command syntax
    - ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] destination-list
  - Command switches
    - -t - ping until interrupted
    - -a - ping address and resolves host name
    - -n count - send number of echo packets
    - -l length - send echo packets of a specified size
    - -f - sends a DO NOT FRAGMENT command to gateways
    - -i ttl - sets the TTL field
    - -r count - records the route of the outgoing and returning packets
    - destination-list - specifies the remote hosts to ping, by domain name or by IP address

I.8 Remote Connectivity 5%

I.8.1 Explain the following remote connectivity concepts:

- The distinction between PPP and SLIP
  - PPP - Point-to Point Protocol - routes IP packets via a dial-up connection and supports compression and IP address negotiation
  - SLIP - Serial Line Internet Protocol - routes IP packets via a dial-up connection and does NOT support compression and IP address negotiation by itself
- The purpose and function of PPTP and the conditions under which it is useful
  - PPTP makes possible a secure connection across the Internet. Users can connect to any ISP, use the ISP's network as a gateway and then connect to the office network. The PPTP packets are encapsulated into es and procedures
  - The need to employ data encryption to protect network data
  - The use of a firewall.

II. Knowledge of Networking Practices 33%

II.1 Implementing the Installation of the Network 6%

II.1.1 Demonstrate awareness that administrative and test accounts, passwords, IP addresses, IP configurations, relevant SOPs, etc., must be obtained prior to network implementation.

II.1.2 Explain the impact of environmental factors on computer networks. Given a network installation scenario, identify unexpected or atypical conditions that could either cause problems for the network or signify that a problem condition already exists, including

- Room conditions (e.g., humidity, heat, etc.)
    - It is important to setup the room with normal humidity to prevent electrostatic discharge (ESD), air conditioning to prevent CPU overheating and system shutdown
    - Put the equipment in a secured cabinet in a secured room to prevent someone from tampering with unsupervised equipment during off hours
- The placement of building contents and personal effects (e.g., space heaters, TVs, radios, etc.)
    - 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. Common sources of EMI are fluorescent lights, elevator motors, large generators, and refrigerator magnets.
    - Casements are often the best places to store computer equipment because the ground can absorb most air waves
- Computer equipment
    - Other computer equipment can effect the unshielded data cables because of EMI, such as monitor radiation or CPU power supplies
    - If the computer equipment is faulty then the network components may appear to have problems
    - Sometimes diagnostic software may point out faulty computer parts without wasting time guessing at the problem
- Error messages
    - These are clues to help boil down the problem to the least common denominator. Once isolated, the proper remedy can be applied without too much guess work.
    - Some error messages are misleading and additional diagnostic software may be required to make a more educated guess.

II.1.3 Recognize visually, or by description, common peripheral ports, external SCSI (especially DB-25 connectors), and common network componentry, including

- Print servers
- Peripherals
- Hubs
- Routers
- Brouters

II.1.4 Given an installation scenario, demonstrate awareness of the following compatibility and cabling issues:

- The consequences of trying to install an analog modem in a digital jack
    - When an analog modem is installed into a digital jack, such as a PBX, you take the risk of burning out your modem
- That the uses of RJ-45 connectors may differ greatly depending on the cabling
    - If you are cabling for 10BASE-T then the use of 2 pairs of CAT 3 wires is sufficient, but if you plan to upgrade to 100BASE-TX in the future then you will need CAT 5 and 2 pairs of wires.
- That patch cables contribute to the overall length of the cabling segment.

II.2 Administering the Change Control System 4%

II.2.1 Demonstrate awareness of the need to document the current status and configuration of the workstation (i.e., providing a baseline) prior to making any changes.

II.2.2 Given a configuration scenario, select a course of action that would allow the return of a system to its original state.

Do a full restore from the previous day tape backup. Wipe out the partition information and rebuild the operating system and server services from scratch.

II.2.3 Given a scenario involving workstation backups, select the appropriate backup technique from among the following

- Tape backup
- Folder replication to a network drive
- Removable media,
- Multi-generation.

II.2.4 Demonstrate awareness of the need to remove outdated or unused drivers, properties, etc. when an upgrade is successfully completed.

II.2.5 Identify the possible adverse effects on the network caused by local changes (e.g., version conflicts, overwritten DLLs, etc.).

II.2.6 Explain the purpose of drive mapping, and (given a scenario) identify the mapping that will produce the desired results using Universal Naming Convention (UNC) or an equivalent feature. Explain the purpose of printer port capturing and identify properly formed capture commands, given a scenario.

II.2.7 Given a scenario where equipment is being moved or changed, decide when and how to verify the functionality of the network and critical applications.

II.2.8 Given a scenario where equipment is being moved or changed, decide when and how to verify the functionality of that equipment.

II.2.9 Demonstrate awareness of the need to obtain relevant permissions before adding, deleting, or modifying users.

II.2.10 Identify the purpose and function of the following networking elements

- Profiles
- Rghts
- Procedures/policies,
- Administrative utilities,
- Login accounts, groups, and passwords.

II.3 Maintaining and Supporting the Network 6%

II.3.1 Identify the kinds of test documentation that are usually available regarding a vendor's patches, fixes, upgrades, etc.

II.3.2 Given a network maintenance scenario, demonstrate awareness of the following issues:

- Standard backup procedures and backup media storage practices
- The need for periodic application of software patches and other fixes to the network
- The need to install anti-virus software on the server and workstations
- The need to frequently update virus signatures.

II.4 Identifying, Assessing, and Responding to Problems 6%

II.4.1 Given an apparent network problem, determine the nature of the action required (i.e., information transfer vs. handholding vs. technical service).

II.4.2 Given a scenario involving several network problems, prioritize them based on their seriousness.

II.5 Troubleshooting the Network 11%

II.5.1 Recognize the following steps as a systematic approach to identifying the extent of a network problem and, given a problem scenario, select the appropriate next step based on this approach:

- Determine whether the problem exists across the network,
- Determine whether the problem is workstation, workgroup, LAN or WAN,
- Determine whether the problem is consistent and replicable, and
- Use standard troubleshooting methods.

II.5.2 Identify the following steps as a systematic approach for troubleshooting network problems and, given a problem scenario, select the appropriate next step based on this approach:

- Identify the exact issue,
- Recreate the problem,
- Isolate the cause,
- Formulate a correction,
- Implement the correction,
- Test,
- Document the problem and the solution, and
- Give feedback.

II.5.3 Identify the following steps as a systematic approach to determining whether a problem is attributable to the operator or the system and, given a problem scenario, select the appropriate next step based on this approach:

- Have a second operator perform the same task on an equivalent workstation,
- Have a second operator perform the same task on the original operator's workstation,
- See whether operators are following standard operating procedure.

II.5.4 Given a network troubleshooting scenario, demonstrate awareness of the need to check for physical and logical indicators of trouble, including

- Link lights
- Power lights
- Error displays
- Error logs and displays
- Performance monitors.

II.5.5 Identify common network troubleshooting resources, including

- Knowledge bases on the World Wide Web
- Telephone technical support
- Vendor CDs.

II.5.6 Given a network problem scenario, including symptoms, determine the most likely cause or causes of the problem based on the available information. Select the most appropriate course of action based on this inference. Issues that may be covered include

- Recognizing abnormal physical conditions
- Isolating and correcting problems in cases where there is a fault in the physical media (patch cable)
- Checking the status of servers
- Checking for configuration problems with DNS, WINS, HOST file
- Checking for viruses
- Checking the validity of the account name and password
- Rechecking operator logon procedures
- Selecting and running appropriate diagnostics.

II.5.7 Specify the tools that are commonly used to resolve network equipment problems. Identify the purpose and function of common network tools, including

- Crossover cable
- Hardware loopback
- Tone generator
- Tone locator (fox and hound).

II.5.8 Given a network problem scenario, select appropriate tools to help resolve the problem.

If you have any questions, please click below:
Network+ Questions

Special Thanks to David Schwartzberg - CNE, MCP for writing the original Cramsession for this exam!