The Network + Cram Sheet

This Cram Sheet contains the distilled, key facts about the CompTIA Network+ exam. Review this information as the last thing you do before you enter the testing center, paying special attention to those areas where you feel that you need the most review. You can transfer any of these facts from your head onto a blank sheet of paper immediately before you begin the exam.

MEDIA AND TOPOLOGIES

- Peer-to-peer networks are useful for only relatively small networks. They are often used in small offices or home environments.
- Client/server networks, also called server-centric networks, have clients and servers. Servers provide centralized administration, data storage, and security. The client system requests data from the server and displays the data to the end user.
- The bus network topology is also known as a linear bus because the computers in such a network are linked together using a single cable called a trunk, or backbone.
- If a terminator on a bus network is loose, data communications might be disrupted. Any other break in the cable will cause the entire network segment to fail.
- In a star configuration, all devices on the network connect to a central device, and this central device creates a single point of failure on the network.
- In the ring topology, the network layout forms a complete ring. Computers connect to the network cable directly or, more commonly, through a specialized network device.
- Breaking the loop of a ring network disrupts the entire network.
- The mesh topology requires each computer on the network to be individually connected to every other device. This configuration provides maximum reliability and redundancy for the network.
- Wireless networks use a centralized device known as a wireless access point (WAP).
- 802.2, the LLC sublayer, defines specifications for the Logical Link Control (LLC) sublayer in the 802 standard series.
- 802.3 defines the carrier-sense multiple-access with collision detection (CSMA/CD) media access method used in Ethernet networks. This is the most popular networking standard used today.
- 802.5 defines Token Ring networking.
- 802.11 defines standards for wireless LAN communication.
- Many factors cause EMI, including computer monitors and fluorescent lighting fixtures.
- Copper-based media are prone to EMI, whereas fiber-optic cable is resistant to it.
- Data signals may also be subjected to something commonly referred to as *crosstalk*, which occurs when signals from two cables, or from wires within a single cable, interfere with each other.
- The weakening of data signals as they traverse the media is referred to as *attenuation*.
- Half-duplex mode allows each device to both transmit and receive, but only one of these processes can occur at a time.
- Full-duplex mode allows devices to receive and transmit simultaneously. A 100Mbps network card in full-duplex mode can operate at 200Mbps.

CABLES AND CONNECTORS

- Thin coax is only .25 inches in diameter and has a maximum cable length of 185 meters (approximately 600 feet).
- Thick coax networks use a device called a tap to connect a smaller cable to the thick coax backbone. Thick coax has a 500-meter cable length.
- Attachment unit interface (AUI) ports are network interface ports that are often associated with thick coax (that is, 10Base5) networks. The AUI port is a 15-pin socket to which a transceiver is connected.
- SC and ST connectors are associated with fiber cabling. ST connectors offer a twist-type attachment and SC connectors are push-on connectors.
- RJ-45 connectors are used with UTP cable.

10BASEX, 100BASEX, AND 1000BASEX STANDARDS

- 10Base2, sometimes called Thinnet or Thin Ethernet, is the 802.3 specification for a network that uses thin coaxial cable (that is, RG-58 cable).
- 10Base2 specifies a maximum speed of 10Mbps and uses BNC barrel and BNC T connectors to connect the cable and computers. At the physical ends of each cable segment, a 50-ohm terminator absorbs the signal, thus preventing signal reflection.
- The 10Base2 standard specifies a limit of 185 meters per segment (approximately 600 feet).

NETWORK DEVICES

- Token Ring networks use special devices called multistation access units (MSAUs) to create the network.
- A straight-through cable is used to connect systems to the switch or hub using the MDI-X ports.
- In a crossover cable, Wires 1 and 3 and Wires 2 and 6 are crossed.
- Bridges are used to divide networks and thus reduce the amount of traffic on each network.
- Routing Information Protocol (RIP) is a distance-vector routing protocol for both Transmission Control Protocol (TCP) and Internetwork Packet Exchange (IPX).
- A MAC address is a 6-byte address that lets a NIC be uniquely identified on the network. The first three bytes (`00:D0:59`) identify the manufacturer of the card; the last three bytes (`09:07:51`) are the Universal LAN MAC address, which makes the interface unique.

OSI MODEL

- As data is passed up or down through the OSI model structure, headers are added (going down) or removed (going up) at each layer—a process called *encapsulation* (when added) or *decapsulation* (when removed).
- The Application Layer provides access to the network for applications and certain end-user functions. It displays incoming information and prepares outgoing information for network access.
- The Presentation Layer converts data from the Application Layer into a format that can be sent over the network. It converts data from the Session Layer into a format that can be understood by the Application Layer. It also handles encryption and decryption of data and provides compression and decompression functionalities.
- The Session Layer synchronizes the data exchange between applications on separate devices. It handles error detection and notification to the peer layer on the other device.
- The Transport Layer establishes, maintains, and breaks connections between two devices. It determines the ordering and priorities of data. It also performs error checking and verification and handles retransmissions, if necessary.
- The Network Layer provides mechanisms for the routing of data between devices across single or multiple network segments and handles the discovery of destination systems and addressing.
- The Data-link Layer has two distinct sublayers: LLC and MAC. It performs error detection and handling for the transmitted signals. It also defines the method by which the medium is accessed and defines hardware addressing through the MAC sublayer.
- The Physical Layer defines the physical structure of the network. It also defines voltage/signal rates and the physical connection methods, as well as the physical topology.
- Mapping network devices to the OSI model:

Hub	Physical (Layer 1)
Switch	Data-link (Layer 2)
Bridge	Data-link (Layer 2)
Router	Network (Layer 3)
NIC	Data-link (Layer 2)

PROTOCOLS

- A Class A TCP/IP address uses only the first octet to represent the network portion, a Class B address uses two octets, and a Class C address uses three octets.
- Class A addresses span from 1 to 126, with a default subnet mask of `255.0.0.0`.
- Class B addresses span from 128 to 191, with a default subnet mask of `255.255.0.0`.
- Class C addresses span from 192 to 223, with a default subnet mask of `255.255.255.0`.
- The 127 network ID is reserved for the local loopback.
- Application protocols map to the Application, Presentation, and Session layers of the OSI model. Application protocols include AFT, FTP, TFTP, NCP, and SNMP.
- Transport protocols map to the Transport layer of the OSI model and are responsible for transporting data across the network. Transport protocols include ATP, NetBEUI, SPX, TCP, and UDP.
- The NetBEUI protocol uses names as addresses.
- Network protocols are responsible for providing the addressing and routing information. Network protocols include IP, IPX, and DP.

- The TCP/IP protocol suite is used by all major operating systems and is a routable protocol.
- IPX/SPX protocol is associated with NetWare network and is routable.
- NetBEUI is used on Windows networks and is not routable.
- DHCP/BOOTP automatically assigns IP addressing information.
- DNS resolves hostnames to IP addresses.
- NAT/ICS translates private network addresses into public network addresses.
- WINS resolves NetBIOS names to IP addresses.
- SNMP provides network-management facilities on TCP/IP-based networks.
- In a network that does not use DHCP, you need to watch for duplicate IP addresses that prevent a user from logging onto the network.
- A Class A address uses only the first octet to represent the network portion, a Class B address uses two octets, and a Class C address uses three octets.
- Class A addresses span from 1 to 126, with a default subnet mask of `255.0.0.0`.
- Class B addresses span from 128 to 191, with a default subnet mask of `255.255.0.0`.
- Class C addresses span from 192 to 223, with a default subnet mask of `255.255.255.0`.
- The 127 network ID is reserved for the local loopback.

REMOTE ACCESS AND SECURITY PROTOCOLS

- The underlying technologies that enable the RAS process are dial-up protocols such as PPP and SLIP.
- SLIP also does not provide error checking or packet addressing, so it can be used only in serial communications.
- PPP provides several security enhancements compared to SLIP. The most important of these is the encryption of usernames and passwords during the authentication process.
- ICA protocol allows client systems to access and run applications on a server, using the resources of the server, with only the user interface, keystrokes, and mouse movement being transferred between the client and server computers.
- IPSec is designed to encrypt data during communication between two computers. IPSec operates at the Network layer of the OSI model and provides security for protocols that operate at higher layers.
- SSL is a security protocol used on the Internet. Secure Web site URLs begin with `https://` instead of `http://`. HTTPS connections require a browser to establish a secure connection. Secure SSL connections for Web pages are made through port 443 by default.
- The security tokens used in Kerberos are known as *tickets*.

RAID

- RAID 0 offers no fault tolerance and improves I/O performance. It requires a minimum of two disks.
- RAID 1, disk mirroring, provides fault tolerance and requires two hard disks. Separate disk controllers can be used, a strategy known as *disk duplexing*.
- RAID 5, disk striping with distributed parity, requires a minimum of three disks—the total size of a single disk being used for the parity calculation.

BACKUPS

- In a full backup, all data is backed up. Full backups do not use the archive bit, but do clear it.
- Incremental backups back up all data that has changed since the last full or incremental backup. Uses and clears the archive bit.
- Differential backups back up all data since the last differential backup. They use the archive bit but do not clear it.

VLANS AND NAS

- VLANs are used to segment networks. This is often done for organizational or security purposes.
- NAS is used to offload data storage from traditional file servers. NAS devices are connected directly to the network and use the SMB and NFS application protocols.

CLIENT CONNECTIVITY

- To log on to a NetWare server, you might need a username, password, tree, and context.
- Unix and Linux use the Network File System (NFS) protocol to provide file-sharing capabilities between computers.

SECURITY: PHYSICAL, LOGICAL, PASSWORDS, AND FIREWALLS

- A password that uses eight case-sensitive characters, with letters, numbers, and special characters, often makes a strong password.
- Windows 2000 permissions include Full Control, Modify, Read & Execute, List Folder Contents, Read, Write.
- When a user can't access files that other users can, verify that the correct permissions are set.
- A firewall is a system or group of systems that controls the flow of traffic between two networks. A firewall often provides such services as NAT, proxy services, and packet filtering.
- A proxy server allows Internet access to be controlled. Having a centralized point of access allows for a great deal of control over the use of the Internet.

NETWORK SUPPORT

- You can PING the IP address of the local loopback adapter by using the command ping `127.0.0.1`. If this command is successful, you know that the TCP/IP protocol suite is installed correctly on your system and functioning.
- `Tracert` reports the amount of time it takes to reach each router in the path. It's a useful tool for isolating bottlenecks in a network. ARP is the part of the TCP/IP suite whose function it is to resolve IP addresses to MAC addresses.
- ARP operates at the Network layer of the OSI model.
- `netstat` is used to view both inbound and outbound TCP/IP network connections.
- `nbtstat` is used to display protocol and statistical information for NetBIOS over TCP/IP connections.
- `ipconfig` shows the IP configuration information for all NICs installed within a system.
- `ipconfig /all` is used to display detailed TCP/IP configuration information.
- `ipconfig /renew` is used to refresh the system's DNS information.
- When looking for client connectivity problems using `ipconfig`, you should ensure that the gateway is correctly set.
- The `ifconfig` command is the Linux equivalent of the `ipconfig` command.
- winipcfg is the Windows 95, Windows 98, and Windows Me equivalent of the `ipconfig` command.
- The `nslookup` command is a TCP/IP diagnostic tool used to troubleshoot DNS problems.

MEDIA TOOLS AND LEDS

- A wire crimper is a tool that you use to attach media connectors to the ends of cables.
- Media testers, also called cable testers, are used to test whether a cable is working properly.
- An optical cable tester performs the same basic function as a wire media tester, but on optical media.
- The hardware loopback tests the outgoing signals of a device such as a network card.
- If the LED on a network card is constantly lit, you might have a chattering network card.