

1. What is a Networking?

A *network* is a group of computers (often called *nodes* or *hosts*) that can share information through their interconnections. A network is made up of the following components:

- Computer systems (nodes or hosts)
- Transmission media--a path for electrical signals between devices
- Network interfaces--devices that send and receive electrical signals
- Protocols--rules or standards that describe how hosts communicate and exchange data

Despite the costs of implementation and maintenance, networks actually save organizations money by allowing them to:

- Consolidate (centralize) data storage
- Share peripheral devices like printers
- Increase internal and external communications
- Increase productivity and collaboration

There are several ways to classify networks. The following table lists several ways to describe a network.

Network Type	Description
Host Role	
Peer-to-Peer	In a peer to peer network, the hosts provide and consume network services, and each host has the same operating system. Advantages of peer to peer networks include: <ul style="list-style-type: none">• Easy implementation• Inexpensive
	Disadvantages of peer to peer networks include: <ul style="list-style-type: none">• Difficult to expand (not scalable)• Difficult to support• Lack centralized control

	<ul style="list-style-type: none"> No centralized storage
Client/Server	<p>In a client/server network, hosts have specific roles. For example, some hosts are assigned server roles, which allows them to provide network resources to other hosts. Other hosts are assigned client roles, which allows them to consume network resources. Unlike peer to peer networks, hosts in a client/server network have different operating systems. Advantages of client/server networks include:</p> <ul style="list-style-type: none"> Easily expanded (scalable) Easy support Centralized services Easy to backup <p>Disadvantages of client/server networks include:</p> <ul style="list-style-type: none"> Server operating systems are expensive Requires extensive advanced planning
Geography and Size	
Local Area Network (LAN)	LANs reside in a small geographic area, like in an office. A series of connected LANs, or a LAN connected across several buildings or offices, is called an <i>internetwork</i> .
Wide Area Network (WAN)	A WAN is a group of LANs that are geographically isolated but connected to form a large internetwork. When implementing a WAN, remember to provide local access to user resources to prevent a high rate of WAN traffic.
Participation	
Private	A LAN or WAN for private individual or group use which may or may not be secure. Examples include home and organization (small business, corporate, institute, government) networks. <i>Intranets</i> and <i>extranets</i> , although related to the Internet, are private networks. Both an extranet and intranet are tightly controlled, and made available only to select organizations. An



	extranet is made available to the public and an intranet is made available internally.
Public	A large collection of unrelated computers, with each node on the network having a unique address. The Internet, for example, is a public network. Because computers are unrelated and many companies and individuals share the same communication media, the public network is by nature insecure.



2. Topology

Topology is the term used to describe how devices are connected and how messages flow from device to device. There are two types of network topologies:

- The physical topology describes the physical way the network is wired.
- The logical topology describes the way in which messages are sent.

The following table describes several common physical topologies.

Topology	Description
 Bus	<p>A physical bus topology consists of a trunk cable with nodes either inserted directly into the trunk, or nodes tapping into the trunk using offshoot cables called drop cables.</p> <ul style="list-style-type: none">• Signals travel from one node to all other nodes on the bus.• A device called a <i>terminator</i> is placed at both ends of the trunk cable.• Terminators absorb signals and prevent them from reflecting repeatedly back and forth on the cable. <p>The physical bus:</p> <ul style="list-style-type: none">• Requires less cable than the star• Can be difficult to isolate cabling problems
 Ring	<p>A ring topology connects neighboring nodes until they form a ring. Signals travel in one direction around the ring. In ring topologies, each device on the network acts as a repeater to send the signal to the next device. With a ring:</p> <ul style="list-style-type: none">• Installation requires careful planning to create a continuous ring.• Isolating problems can require going to several physical locations along the ring.

	<ul style="list-style-type: none"> • A malfunctioning node or cable break can prevent signals from reaching nodes further along on the ring.
 <p>Star</p>	<p>A star topology uses a hub (or switch) to concentrate all network connections to a single physical location. Today it is the most popular type of topology for a LAN. With the star:</p> <ul style="list-style-type: none"> • All network connections are located in a single place, which makes it easy to troubleshoot and reconfigure. • Nodes can be added to or removed from the network easily. • Cabling problems usually affect only one node. • Requires more cable than any other topology. Every node has its own cable.
 <p>Mesh</p>	<p>A mesh topology exists when there are multiple paths between any two nodes on a network. Mesh topologies are created using point-to-point connections. This increases the network's fault tolerance because alternate paths can be used when one path fails. Two variations of mesh topologies exist:</p> <ul style="list-style-type: none"> • Partial Mesh--Some redundant paths exist. • Full Mesh--Every node has a point-to-point connection with every other node. <p>Full mesh topologies are usually impractical because the number of connections increases dramatically with every new node added to the network. However, a full mesh topology becomes more practical through the implementation of an ad-hoc wireless network. With this topology, every wireless network card can communicate directly with any other wireless network card on the network. A separate and dedicated network interface and cable for each host on the network is not required.</p>

You should be able to identify the physical topology by looking at the way in which devices are connected. However, it is not as easy to identify the logical topology. As the following table describes, there is often more than one way for messages to travel for a given physical topology.

Logical Topology	Physical Topology	Description
Bus	Bus	Messages are sent to all devices connected to the bus.
	Star	
Ring	Ring	Messages are sent from device-to-device in a predetermined order until they reach the destination device.
	Star	
Star	Star	Messages are sent directly to (and only to) the destination device.

© Sergey Gorokhod

MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®

E-mail: sergey@infosec.co.il

Mob: (+972) 526848757

3. Twisted Pair (RJ-45)

Twisted pair cables support a wide variety of fast, modern network standards.

Twisted pair cabling is composed of the following components:



- Two wires that carry the data signals (one conductor carries a positive signal; one carries a negative signal). They are made of 22 or 24-gauge copper wiring.
- PVC plastic insulation surrounds each wire.
- Two wires are twisted to reduce the effects of *electromagnetic interference (EMI)* and *crosstalk*. Because the wires are twisted, EMI should affect both wires equally and can be cancelled out.
- Multiple wire pairs are bundled together in an outer sheath. Twisted pair cable can be classified according to the makeup of the outer sheath:
 - Shielded Twisted Pair (STP) has a grounded outer copper shield around the bundle of twisted pairs or around each pair. This provides added protection against EMI.
 - Unshielded Twisted Pair (UTP) does not have a grounded outer copper shield. UTP cables are easier to work with and are less expensive than shielded cables.

The table below describes the different unshielded twisted pair (UTP) cable types (categories).

Type	Connector	Description
Phone cable	RJ-11	Used to connect a PC to a phone jack in a wall outlet to establish a dial-up Internet connection. Has two pairs of twisted cable (a total of 4 wires).
Cat 3	RJ-45	Designed for use with 10 megabit Ethernet or 16 megabit token ring.
Cat 5	RJ-45	Supports 100 megabit and 1 gigabit Ethernet and ATM networking.
Cat 5e	RJ-45	Similar to Cat 5 but provides better EMI protection. Supports 1 and 10 gigabit Ethernet (gigabit connections require the use of all four twisted pairs).

Cat 6	RJ-45	Supports high-bandwidth, broadband communications.
--------------	--------------	--

The table below describes the two types of connectors used with twisted pair cables.

Connector	Description
RJ-11 	<ul style="list-style-type: none"> • Has 4 connectors • Supports up to 2 pairs of wires • Uses a locking tab to keep connector secure in outlet • Used primarily for telephone wiring
RJ-45 	<ul style="list-style-type: none"> • Has 8 connectors • Supports up to 4 pairs of wires • Uses a locking tab to keep connector secure in outlet • Used for Ethernet and some token ring connections

Each type of UTP cable can be substituted for any category below it, but never for a category above. For example, Cat 6 can be substituted for a task requiring Cat 5e; however, neither Cat 5 nor Cat 3 should be used for this particular task.

© **Sergey Gorokhod**

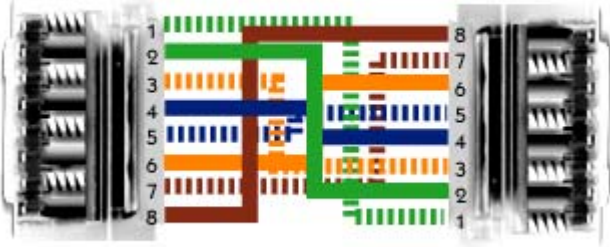
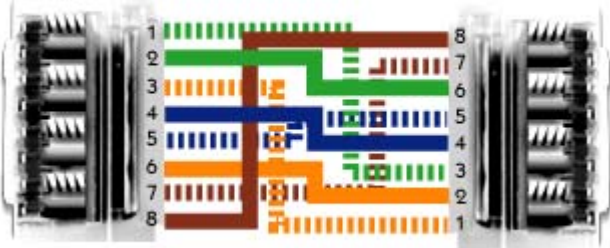
MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®

E-mail: sergey@infosec.co.il

Mob: (+972) 526848757

4. Cables

Twisted pair cables remain one of the primary ways that computers connect to a network. Computers connect to the network through a hub or switch with a straight-through cable. Computers can connect directly to one another using a crossover cable. The table below illustrates both straight-through and crossover cable configurations.

Cable	Description
	<p>There are two standards for creating straight-through cables:</p> <ul style="list-style-type: none">• T568A--To use this standard, arrange the wires from pins 1 to 8 in each connector in the following order: GW, G, OW, B, BW, O, BrW, Br.• T568B--To use this standard, arrange the wires from pins 1 to 8 in each connector in the following order: OW, O, GW, B, BW, G, BrW, Br. <p>It doesn't matter which standard you use, but once you choose a standard, you should do all your cables that way to avoid confusion during troubleshooting.</p>
	<p>The easiest way to create a crossover cable is to arrange the wires in the first connector using the T568A standard and arrange the wires in the second connector using the T568B standard.</p>

Ethernet specifications use the following pins (Tx - transmitting and RX - receiving):

- Pin 1: Tx+
- Pin 2: Tx-
- Pin 3: Rx+
- Pin 4: Unused
- Pin 5: Unused
- Pin 6: Rx-
- Pin 7: Unused
- Pin 8: Unused

© Sergey Gorokhod

MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®

E-mail: sergey@infosec.co.il

Mob: (+972) 526848757

5. Older Technology- Coaxial Cable

Coaxial cable is an older technology that is usually implemented with a bus topology. It is not suitable for ring or star topologies because the ends of the cable must be terminated. It is composed of two conductors, which share a common axis, within a single cable.

Coaxial cable is built with the following components:

- Two concentric metallic conductors:
 - The inner conductor, which carries data signals. It is made of copper or copper coated with tin.
 - The mesh conductor is a second physical channel that also grounds the cable. It is made of aluminum or copper coated tin.
- The insulator, which surrounds the inner conductor. It keeps the signal separated from the mesh conductor. It is made of PVC plastic.
- The mesh conductor, which surrounds the insulator and grounds the cable. It is made of aluminum or copper coated tin.
- The PVC sheath, which is the cable encasement. It surrounds and protects the wire. It is made of PVC plastic.



Coaxial cable has the following advantages and disadvantages:

Advantages	<ul style="list-style-type: none">• Highly resistant to EMI (electromagnetic interference)• Highly resistant to physical damage
Disadvantages	<ul style="list-style-type: none">• Expensive• Inflexible construction (difficult to install)• Unsupported by newer networking standards

The table below describes the different coaxial cable grades.

Grade	Uses	Conductor	Resistance Rating
RG-58	Ethernet networking	Tin-coated copper	50 ohms
RG-59	Cable TV and cable networking	Copper-plated steel	75 ohms
RG-6	Satellite TV	Solid copper	75 ohms

The table below describes the two types of connectors used with coaxial cable.

Connector	Description
<p>F-Type</p> 	<ul style="list-style-type: none">• Twisted onto the cable• Used to create cable and satellite TV connections• Used to hook a cable modem to a broadband cable connection
<p>BNC</p> 	<ul style="list-style-type: none">• Molded onto the cable• Used to create Ethernet network connections

© **Sergey Gorokhod**

MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®

E-mail: sergey@infosec.co.il

Mob: (+972) 526848757

6. Fiber Optic

To connect computers using fiber optic cables, you need two fiber strands. One strand transmits signals, and the other strand receives signals. Fiber optic cabling is composed of the following components:

- The core carries the signal. It is made of plastic or glass.
- The cladding maintains the signal in the center of the core as the cable bends.
- The sheathing protects the cladding and the core.

Fiber optic cabling offers the following advantages and disadvantages:



Advantages	<ul style="list-style-type: none">• Totally immune to EMI (electromagnetic interference)• Highly resistant to eavesdropping• Supports extremely high data transmission rates• Allows greater cable distances without a repeater
Disadvantages	<ul style="list-style-type: none">• Very expensive• Difficult to work with• Special training required to attach connectors to cables

Multi-mode and single mode fiber cables are distinct from each other and not interchangeable. The table below describes multi-mode and single mode fiber cables.

Type	Description
Single Mode	<ul style="list-style-type: none">• Transfers data through the core using a single light ray (the ray is also called a <i>mode</i>)• The core diameter is around 10 microns• Supports a large amount of data• Cable lengths can extend a great distance
Multi-mode	<ul style="list-style-type: none">• Transfers data through the core using multiple light rays• The core diameter is around 50 to 100 microns

- Cable lengths are limited in distance

Fiber optic cabling uses the following connector types:

Type	Description
<p>ST Connector</p> 	<ul style="list-style-type: none"> • Used with single and multi-mode cabling • Keyed, bayonet-type connector • Also called a push in and twist connector • Each wire has a separate connector • Nickel plated with a ceramic ferrule to insure proper core alignment and prevent light ray deflection • As part of the assembly process, it is necessary to polish the exposed fiber tip to ensure that light is passed on from one cable to the next with no dispersion
<p>SC Connector</p> 	<ul style="list-style-type: none"> • Used with single- and multi-mode cabling • Push on, pull off connector type that uses a locking tab to maintain connection • Each wire has a separate connector • Uses a ceramic ferrule to insure proper core alignment and prevent light ray deflection




	<ul style="list-style-type: none"> As part of the assembly process, it is necessary to polish the exposed fiber tip
<p>LC Connector</p> 	<ul style="list-style-type: none"> Used with single- and multi-mode cabling Composed of a plastic connector with a locking tab, similar to a RJ-45 connector A single connector with two ends keeps the two cables in place Uses a ceramic ferrule to insure proper core alignment and prevent light ray deflection Half the size of other fiber-optic connectors
<p>MT-RJ Connector</p> 	<ul style="list-style-type: none"> Used with single and multi-mode cabling Composed of a plastic connector with a locking tab Uses metal guide pins to ensure it is properly aligned A single connector with one end holds both cables Uses a ceramic ferrule to insure proper core alignment and prevent light ray deflection

7. USB and FireWire



You can create a network connection between two PCs by plugging a USB cable into their USB ports. You can also use software that allows you to connect multiple PCs through a USB hub. USB is a serial communication specification. There are two USB versions:

- USB 1.0 runs at 12 megabits per second.
- USB 2.0 runs at 480 megabits per second.

The table below describes the three types of USB connectors.

Connector	Description
A Connector 	<ul style="list-style-type: none">• Generally, plugs directly into the computer or a hub• To connect two computers together directly, select a USB cable with two A connectors
B Connector 	<ul style="list-style-type: none">• Generally, plugs into a hub, printer, or other peripheral device to connect the device to the computer• Most USB cables have an A connector on one end (to connect to the cable) and a B connector on the other end (to connect to the device)
Mini Connector 	<ul style="list-style-type: none">• Designed to plug in to devices with mini plugs such as a digital camera• Most USB cables with a mini connector have an A connector on the other end to connect to the computer

You can also create a network connection between two PCs using their FireWire (IEEE 1394) ports. The table below describes Firewire and its connectors.

Connector	Description
6-pin Connector 	<ul style="list-style-type: none"> • Supports data transfer speeds at upwards of 400 Mbps • 6-pin connector is used when making connections between PCs • 4-pin connector is used to connect to peripheral devices
4-pin Connector 	

© **Sergey Gorokhod**

MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®

E-mail: sergey@infosec.co.il

Mob: (+972) 526848757

8. Network Adapter and MAC Address

A network adapter connects a host to the network medium. Some computers, like laptops, come with built-in network adapters. Other computers use NICs (network interface cards) that plug in to the system's expansion slots or which are external to the computer and connect through an existing computer port.

A common network interface card is one used on an Ethernet network. The table below describes the components of an Ethernet NIC.

Component	Description
Media connectors	These connect the network interface and host to the network media.
Link indicator	This visually indicates the network connection status. Green generally indicates a good connection, and red or an unlit diode indicates a bad connection.
Transceiver	A NIC's transceiver is responsible for transmitting and receiving network communications. To send signals to the network, it converts digital data from a PC to digital signals. The type of signal the transceiver sends depends on the type of network. A fiber optic NIC sends light signals; an Ethernet NIC sends electronic signals. To receive signals, the transceiver converts digital signals from the network to digital data for the PC.
MAC Address	<p>The MAC address is a unique hexadecimal identifier burned into the ROM (physically assigned address) of every network interface.</p> <ul style="list-style-type: none">• The MAC address is a 12-digit hexadecimal number (each number ranges from 0-9 or A-F).• The address is often written as 00-B0-D0-06-BC-AC or 00B0.D006.BCAC, although dashes, periods, and colons can be used to divide the MAC address parts.• The MAC address is guaranteed unique through design. The first half (first 6 digits) of the MAC address is assigned to each manufacturer. The manufacturer determines the rest of the address, assigning a unique value which identifies the

	<p>host address. A manufacturer that uses all the addresses in the original assignment can apply for a new MAC address assignment.</p>
--	--

Note: *Some network cards allow you to change (logically assigned address) the MAC address through jumpers, switches, or software. However, there is little practical reason for doing so.*

A NIC communicates across the network using the following method:

1. The NIC receives data from the PC.
2. The NIC breaks the data into frames, which include the following information:
 - The receiving NIC's MAC address
 - The sending NIC's MAC address
 - The data it is transmitting
 - The CRC (cyclic redundancy checking) which is used to verify correct transmission and reception of the data
3. The NIC encodes the frames as electrical or light impulses and transmits them across the network.
4. The receiving NIC verifies the NIC addresses and CRC.
5. The receiving NIC tracks the frames and reassembles the data.
6. The receiving NIC sends the data to the PC.

The type of network interface card you choose depends on the type of network to which you are connecting.

- Use an Ethernet NIC (as described above) to connect to an Ethernet network.
- Use a token ring NIC to connect to a token ring network.
- Use a modem to use the phone line to communicate with remote computers (such as to connect to an ISP). Modems communicate through the telephone system by converting binary data to analog waves (*modulation*) on the sending end, and then converting the analog waves back to binary data (*demodulation*) on the receiving end.
- Use an ISDN NIC to connect through an ISDN network. ISDN is a dialup technology for host-to-host connections. However, unlike a modem, ISDN NICs send digital signals over a digital network.

9. Network Connection Device

The following table lists several common connection devices used *within* a LAN.

Device	Description
Hub	<p>A <i>hub</i> is the central connecting point of a physical star, logical bus topology. Hubs manage communication among hosts using the following method:</p> <ul style="list-style-type: none">• A host sends a frame to another host through the hub.• The hub duplicates the frame and sends it to <i>every</i> host connected to the hub.• The host to which the frame is addressed accepts the frame. Every other host ignores the frame.
Switch	<p>Switches provide functionality similar to hubs, but typically on a larger scale and with higher performance (A switch offers guaranteed bandwidth to each port). Unlike a hub, a switch forwards frames only to the intended host, not every host connected to the switch.</p> <p>A switch builds a database based on MAC addresses to make forwarding decisions.</p> <ul style="list-style-type: none">• The process begins by examining the <i>source</i> address of an incoming packet. If the source address is not in the forwarding database, an entry for the address is made in the database. The port it came in on is also recorded.• The <i>destination</i> address is then examined.<ul style="list-style-type: none">◦ If the destination address is not in the database, the packet is sent out all ports except for the one on which it was received.◦ If the destination address is in the database, the packet is forwarded to the appropriate port if the port is different than the one on which it was received.

	<ul style="list-style-type: none"> ○ Broadcast packets are forwarded to all ports except the one on which they were received. <p>Eventually, a switch learns the location of all devices on the network. Incoming frames are then sent directly to the switch port to which a specific host is connected.</p>
Bridge	<p>Bridges connect separate media segments (networks) that use the same protocol. Like a switch, bridges use MAC addresses to determine a frame's destination and to build a table of device addresses and their corresponding segments. This also allows a bridge to prevent messages within a media segment from crossing over to another segment. This keeps the network from wasting bandwidth by eliminating unnecessary traffic between segments.</p> <p>Bridges and switches are similar in functionality. However, switches typically have more ports and are cheaper and more common than bridges.</p>
Wireless Access Point (WAP)	<p>A wireless access point (WAP) is a hub for a wireless network. A WAP works like a hub except that hosts connect using radio waves instead of wires.</p> <p>Note: A WAP can have ports that interface with a wired portion of a segment, allowing you to connect the WAP to the wired network. Some WAPs even have built-in wired hubs or switches.</p>

10. Internetwork Device

In a broad sense, the term *network* can describe any collection of devices connected together to share information and resources. For example, the Internet is a worldwide network linking computers so they can share resources. The telephone company is another type of network, connecting phones and providing services. *Network*, as used in this context, simply indicates that devices can communicate with each other.

When speaking of network configuration and administration, however, the term *network* can mean:

- A collection of computers that are under one scope of management. For example, two companies could connect their internal networks to share data. In this case, you could call it one network. In reality, however, it is two networks, because each network is managed by a different company.
- A set of computers connected to the same transmission media segment that share a common network address. This type of network is often called a *subnet*.

Likewise, the term *internetwork* might mean connecting two separately managed networks together, or it might mean connecting two network segments together.

Devices such as hubs, switches, and bridges connect multiple devices to the same network segment. Internetwork devices connect multiple networks or subnets together, and enable communication between hosts on different types of networks. The following table lists several common internetworking devices.

Device	Description
Gateway	<p>A <i>gateway</i> is a generic term used to describe any device that connects one administratively managed network with another. For example, a gateway connects a business network to the Internet. The gateway device controls the flow of data between the two networks.</p> <p>In addition, the term <i>gateway</i> is often used to describe a specialized device that translates data sent between two networks using different protocols.</p>

Router	<p>A <i>router</i> is a device that connects two or more network segments or subnets.</p> <ul style="list-style-type: none"> • Each subnet has a unique, logical network address. • Routers can be used to connect networks within a single LAN, or they can be used as gateways to connect multiple LANs together. • Routers can be used to connect networks with different architectures (such as connect an Ethernet network to a token ring network). <p>In addition to simply linking multiple subnets together, routers keep track of other subnets on the internetwork and decide the direction data should travel to reach the destination.</p>
Firewall	<p>A <i>firewall</i> is a router with additional security features. Firewalls can be programmed with security rules to restrict the flow of traffic between networks.</p> <ul style="list-style-type: none"> • A firewall can control the type of traffic allowed in to a network and the type of traffic allowed out of a network. • Rules set up on the firewall determine the types of permitted and prohibited traffic. • A firewall can be either hardware devices or software installed onto operating systems.

Note: There are also some switches (called Layer 3 switches) that have built-in router functionality. These switches examine the logical network address (instead of the MAC address) to switch packets between networks.

11. IP Address and Subnet Mask

IP addresses allow hosts to participate on IP based networks. An IP address:

- Is a 32-bit binary number represented as four octets (four 8-bit numbers). Each octet is separated by a period.
- IP addresses can be represented in one of two ways:
 - Decimal (for example 131.107.2.200). In decimal notation, each octet must be between 0 and 255.
 - Binary (for example 10000011.01101011.00000010.11001000). In binary notation, each octet is an 8-digit number.
- The IP address includes both the network and the host address.
- Each IP address has an implied address class that can be used to infer the network portion of the address.
- The subnet mask is a 32-bit number that is associated with each IP address that identifies the network portion of the address. In binary form, the subnet mask is always a series of 1's followed by a series of 0's (1's and 0's are never mixed in sequence in the mask). A simple mask might be 255.255.255.0.

The following table describes each of the default IP address classes.

Class	Characteristics
Class A	<ul style="list-style-type: none">• The first octet is a number between 1 and 126.• The default subnet mask is 255.0.0.0. Therefore, the first octet is the network address (the last three octets are used for host addresses).• There are 126 Class A network IDs.• Each Class A network can have up to 16.7 million host addresses.• Most of these addresses are already assigned.
Class B	<ul style="list-style-type: none">• The first octet is between 128 and 191.

	<ul style="list-style-type: none"> • The default subnet mask is 255.255.0.0. Therefore, the first two octets are the network address (the last two octets are used for host addresses). • There are 16,384 Class B network IDs. • Each Class B network can have up to 65,534 host addresses. • Most of these addresses are assigned.
Class C	<ul style="list-style-type: none"> • The first octet is between 192 and 223. • The default subnet mask is 255.255.255.0. Therefore, the first three octets are the network address (the last octet is used for host addresses). • There are 2,097,152 Class C network IDs. • Each Class C network can have only 254 host ID addresses. • This class is the most likely to have an available ID address for assignment.
Class D	<ul style="list-style-type: none"> • These addresses range from 224.0.0.0 to 239.255.255.255. • These addresses represent multicast groups rather than network and host IDs.
Class E	<ul style="list-style-type: none"> • These addresses range from 240.0.0.0 to 255.255.255.254. • These addresses are reserved for experimental use.

As you are assigning IP addresses to hosts, be aware of the following special considerations:

Address	Consideration
Network	<p>The first address in an address range is used to identify the network itself. For the network address, the host portion of the address contains all 0's. For example:</p> <ul style="list-style-type: none"> • Class A network address: 115.0.0.0 • Class B network address: 154.90.0.0 • Class C network address: 221.65.244.0

Broadcast	<p>The last address in the range is used as the broadcast address and is used to send messages to all hosts on the network. In binary form, the broadcast address has all 1's in the host portion of the address. For example, assuming the default subnet masks are used:</p> <ul style="list-style-type: none"> • 115.255.255.255 is the broadcast address for network 115.0.0.0 • 154.90.255.255 is the broadcast address for network 154.90.0.0 • 221.65.244.255 is the broadcast address for network 221.65.244.0 <p>Note: The broadcast address might also be designated by setting each of the network address bits to 0. For example, 0.0.255.255 is the broadcast address of a Class B address. This designation means "the broadcast address for this network."</p>
Host Addresses	<p>When you are assigning IP addresses to hosts, be aware of the following:</p> <ul style="list-style-type: none"> • Each host must have a unique IP address. • Each host on the same network must have an IP address with a common network portion of the address. This means that you must use the same subnet mask when configuring addresses for hosts on the same network. <p>The range of IP addresses available to be assigned to network hosts is identified by the subnet mask and/or the address class. When assigning IP addresses to hosts, be aware that you cannot use the first or last addresses in the range (these are reserved for the network and broadcast addresses respectively). For example:</p> <ul style="list-style-type: none"> • For the class A network address 115.0.0.0, the host range is 115.0.0.1 to 115.255.255.254. • For the class B network address 154.90.0.0, the host range is 154.90.0.1 to 154.90.255.254. • For the class C network address 221.65.244.0, the host range is 221.65.244.1 to 221.65.244.254.

	Note: <i>A special way to identify a host on a network is by setting the network portion of the address to all 0's. For example, the address 0.0.64.128 means "host 64.128 on this network."</i>
Local Host	Addresses in the 127.0.0.0 range are reserved to refer to the local host (in other words "this" host or the host you are currently working at). The most commonly-used address is 127.0.0.1 which is the loopback address.

© Sergey Gorokhod

MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®

E-mail: sergey@infosec.co.il

Mob: (+972) 526848757

12. IP Mathematics

The following table shows the decimal value for various binary values with a single 1 bit.

Binary Value	1000 0000	0100 0000	0010 0000	0001 0000	0000 1000	0000 0100	0000 0010	0000 0001
Decimal Value	128	64	32	16	8	4	2	1

To find the decimal value of a number with multiple 1 bits, simply add the decimal value of the bits together. You can do this using a grid. For example, the decimal value of the binary number 10010101 is:

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

Total = $128 + 16 + 4 + 1 = 149$

You also need to know how to convert hexadecimal numbers to binary. The easiest way to do so is to memorize the binary values for each hexadecimal number using the following table.

Hexadecimal Value	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Binary Value	00 00	00 01	00 10	00 11	01 00	01 01	01 10	01 11	10 00	10 01	10 10	10 11	11 00	11 01	11 10	11 11
Decimal Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

13. Subnetting

Subnetting is the process of dividing a large network into smaller networks. When you subnet a network, each network segment (called a *subnet*) has a different network address (also called a *subnet address*). In practice, the terms *network* and *subnet* are used interchangeably to describe a physical network segment with a unique network address.

From a physical standpoint, subnetting is necessary because all network architectures have a limit on the number of hosts allowed on a single network segment. As your network grows, you will need to create subnets (physical networks) to:

- Increase the number of devices that can be added to the LAN (to overcome the architecture limits)
- Reduce the number of devices on a single subnet to reduce congestion and collisions
- Reduce the processing load placed on computers and routers
- Combine networks with different media types within the same internetwork (subnets cannot be used to combine networks of different media type on to the same subnet)

Subnetting is also used to efficiently use the available IP addresses. For example, an organization with a class A network ID is allocated enough addresses for 16,777,214 hosts. If the organization actually uses only 10,000,000 host IDs, over 6 million IP addresses are not being used. Subnetting provides a way to break the single class A network ID into multiple network IDs.

- Subnetting uses *custom* rather than the default subnet masks. For example, instead of using 255.0.0.0 with a Class A address, you might use 255.255.0.0 instead.
- Using custom subnet masks is often called *classless* addressing because the subnet mask cannot be inferred simply from the class of a given IP address. The address class is ignored and the mask is always supplied to identify the network and host portions of the address.

- When you subnet a network by using a custom mask, you can divide the IP addresses between several subnets. However, you also reduce the number of hosts available on each network.

The following table shows how a Class B address can be subnetted to provide additional subnet addresses. Notice how by using a custom subnet mask the Class B address looks like a Class C address.

	Default Example	Custom Example
Network Address	188.50.0.0	188.50.0.0
Subnet Mask	255.255.0.0	255.255.255.0
# of Subnet Addresses	One	254
# of Hosts per Subnet	65,534	254 per subnet
Subnet Address(es)	188.50.0.0 (only one)	188.50.1.0 188.50.2.0 188.50.3.0 (and so on)
Host Address Range(s)	188.50.0.1 to 188.50.255.254	188.50.1.1 to 188.50.1.254 188.50.2.1 to 188.50.2.254 188.50.3.1 to 188.50.3.254 (and so on)

Note: It is possible to use subnet masks that do not use an entire octet. For example, the mask 255.255.252.0 uses three extra binary bits in the third octet. However, for the Network+ exam, you do not need to know how to work with such custom masks.

© Sergey Gorokhod

MCT/MCSE/MCITP/MCTS/MCSA/CCSE/CCSA/CCNA/A+®

E-mail: sergey@infosec.co.il

Mob: (+972) 526848757

14. What is a VLSM?

Using classful addressing means that subnet boundaries exist only along default class boundaries, and the number of hosts for each subnet remains fixed.

However, for smaller or larger subnets, using classful addresses means that larger subnets are not possible, while smaller subnets result in a waste of possible IP addresses. The use of custom subnet masks with classless addressing allows you to customize the number of subnets and the number of hosts allowed on each subnet.

When you use a **variable length subnet mask** (VLSM), you vary the number of bits in the subnet mask to do the following:

- *Subnet* a single network address into multiple smaller subnets. For example, subnetting allows a single Class C network address to be divided to identify multiple smaller subnets. When you subnet a network address, you increase the number of masked bits in the subnet mask. This creates additional subnets, but reduces the number of hosts on each subnet.
- Create a *supernet* which combines multiple network addresses into a single larger subnet. For example, this allows multiple Class C addresses to be combined into a single network. When you create a supernet, you decrease the number of masked bits in the subnet mask. This reduces the number of available subnets, but increases the number of hosts on each subnet.

As you create subnets, you modify the number of bits in the subnet mask to create smaller subnets with fewer hosts per subnet. The following table lists several operations you need to be able to perform, along with a possible method for completing the task.

Scenario	Solution
Given a classful network address and a custom subnet mask, how many subnets do you get?	<p>Use the following process to identify the number of additional subnets you gain by using a custom subnet mask:</p> <ol style="list-style-type: none">1. If the subnet mask is in decimal format, convert the mask to binary. For example, a mask of 255.255.248.0 converts to: 11111111.11111111.11110000.00000000

	<ol style="list-style-type: none"> Count the number of 1 bits that are extra beyond the default subnet mask. In this example, if the address was a class B address, the mask would include 5 additional bits. Use the formula 2^n to calculate the number of subnets, where n is the number of extra masked bits. In this example: $2^n = 2^5 = 32$ subnets
<p>Given a classful network address and a custom subnet mask, what are the possible subnet addresses?</p>	<p>Use the following process to identify the possible subnet addresses when using a custom subnet mask:</p> <ol style="list-style-type: none"> If the subnet mask is in decimal format, convert the mask to binary. For example, a mask of 255.255.224.0 converts to: 11111111.11111111.11100000.00000000 Identify the octet that includes both 1's and 0's. Write out each possible combination of values, modifying only the 1 bits. In this example, possible values for the third octet are: <div style="margin-left: 40px;"> 00000000 10000000 00100000 10100000 01000000 11000000 01100000 11100000 </div> For each value, convert the decimal number to binary. In this example, you would have possible third octet values of 0, 32, 64, 96, 128, 160, 192, and 224. From the original classful network, complete the remaining octets. <ul style="list-style-type: none"> For an octet where the mask is 255, use the original decimal value from the network address. For the octet where the additional bits were used, use the values obtained in step 3.

	<ul style="list-style-type: none"> ○ For all remaining octets where the mask was 0, use 0 for the subnet address. <p>For example, if you were subnetting a class B address 166.12.0.0, you would have the following possible subnet addresses:</p> <p>166.12.0.0 166.12.128.0 166.12.32.0 166.12.160.0 166.12.64.0 166.12.192.0 166.12.96.0 166.12.224.0</p> <p>Tip: Instead of writing out every possible combination and converting each value in steps 2 and 3, you can take a shortcut by identifying an increment value (sometimes referred to as a magic number):</p> <ol style="list-style-type: none"> 1. Identify the last 1 bit in the subnet mask. Convert all other bits in that octet to 0. A mask of 255.255.224.0 gives you an octet value of 00100000. 2. Convert this binary value to decimal to get the increment value. (00100000 = 32) 3. Start with 0 as the first subnet address value. For each subsequent subnet, add the increment value to the previous value. In this example, this gives you the possible values of 0, 32, 64, 96, 128, 160, 192, and 224.
<p>Given a subnet address and the subnet mask, how many hosts can you have on the subnet?</p>	<p>To identify the number of hosts that are allowed on a subnet, use the following process:</p> <ol style="list-style-type: none"> 1. If the subnet mask is in decimal format, convert the mask to binary. For example, a mask of 255.255.248.0 converts to: 11111111.11111111.11110000.00000000 2. Count the number of unmasked bits. These are the bits that identify the host addresses. 3. Use the formula $2^n - 2$ to calculate the number of hosts, where n is the number of unmasked bits. In this

example:

$$2^n - 2 = 2^{11} - 2 = 2048 - 2 = 2046 \text{ host addresses}$$

Remember, the first address in a range on the subnet is the subnet address, and the last address in a range on the subnet is the broadcast address. These addresses cannot be assigned to hosts.

15. Subnetting Tables

As you work with subnetting operations, use the following tables to quickly find the information you need. By memorizing these tables, you will be able to quickly reproduce the values necessary for identifying the binary and decimal values you use most.

The following table lists the exponent values for powers of 2.

Exponent	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^{10}	2^{16}
Exponent value	2	4	8	16	32	64	128	256	1024	65,536

Tip: Memorize the shaded values. To find smaller or larger values, divide or multiply the exponent value by 2. For example, to get the decimal value of 2^{11} , multiply 2^{10} by 2 (giving you 2048). To find the value of 2^{12} , use $2^{10} \times 2 \times 2 = 4096$.

The following table lists the common binary and decimal values used in subnet masks:

Subnet mask value	Decimal equivalent
00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

Use the table as a shortcut guide to subnetting. **Tip:** Look for patterns in the table so you can easily reproduce the table at any time.

Masked Bits	Mask Value	Number of Subnets*	Number of Hosts per Subnet	
			Approximate	Actual ($2^n - 2$)**
/20	255.255.240.0	16	4000	4094
/21	255.255.248.0	32	2000	2046
/22	255.255.252.0	64	1000	1022
/23	255.255.254.0	128	500	510
/24	255.255.255.0	1 or 256	256 or 250	254
/25	255.255.255.128	2	128 or 125	126
/26	255.255.255.192	4	64 or 60	62
/27	255.255.255.224	8	32 or 30	30
/28	255.255.255.240	16	16 or 15	14
/29	255.255.255.248	32	8	6
/30	255.255.255.252	64	4	2

* The number of subnets is the number of subnets you get by subnetting a default network address (either class B or class C in this table). For example, if you subnet a class B network using a /24 mask, you would have 256 subnets.

** To identify the actual number of hosts per subnet, use the formula $2^n - 2$, where n is the number of unmasked bits in the subnet mask. Remember to subtract 2 for the addresses that are not assigned to hosts: - *The first address in the range is the subnet address and cannot be assigned to hosts;* - *The last address in the range is the broadcast address and cannot be assigned to hosts.*

16. What is a Port? Common Ports

Network ports are logical connections, provided by the TCP or UDP protocols at the Transport layer, for use by protocols in the upper layers of the OSI model. The TCP/IP protocol stack uses port numbers to determine what protocol incoming traffic should be directed to. Some characteristics of ports are listed below:

- Ports allow a single host with a single IP address to run network services. Each port number identifies a distinct service.
- Each host can have over 65,000 ports per IP address.
- Port use is regulated by the Internet Corporation for Assigning Names and Numbers (ICANN).

ICANN specifies three categories for ports.

Categories	Characteristics
Well Known	<ul style="list-style-type: none">• Assigned for specific protocols and services• Port numbers range from 0 to 1023
Registered	<ul style="list-style-type: none">• ICANN can assign a specific port for a newly created network service• Port numbers range from 1024 to 49151
Dynamic (Private or High)	<ul style="list-style-type: none">• Assigned when a network service establishes contact and released when the session ends• Allows applications to 'listen' to the assigned port for other incoming requests (traffic for a protocol can be received through a port other than the port that protocol is assigned, as long as the destination application or service is 'listening' for that type of traffic on that port)• Port numbers range from 49,152 to 65,535

The following table lists the well-known ports that correspond to common Internet services.

Port(s)	Service
20, 21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
50, 51	IPSec
53	Domain Name Server (DNS)
67, 68	Dynamic Host Configuration Protocol (DHCP)
69	Trivial File Transfer Protocol (TFTP)
80	Hyper Text Transfer Protocol (HTTP)
110	Post Office Protocol (POP3)
119	Network News Transport Protocol (NNTP)
123	NTP
135-139	NetBIOS
143	Internet Message Access Protocol (IMAP4)
161	Simple Network Management Protocol (SNMP)
389	Lightweight Directory Access Protocol
443	HTTP with Secure Sockets Layer (SSL)

Note: To protect a server, ensure that only the necessary ports are opened. For example, if the server is only being used for e-mail, then shut down ports that correspond to FTP, DNS, and HTTP (among others).

17. Common TCP/IP Protocols

The following table lists several protocols in the TCP/IP protocol suite.

Category	Protocol	Description
MAC Address Resolution	Address Resolution Protocol (ARP)	ARP provides IP address-to-MAC address name address resolution. Using ARP, a host that knows the IP address of a host can discover the corresponding MAC address.
	Bootstrap Protocol (BootP)	Both BootP and RARP are used to discover the IP address of a device with a known MAC address. BootP is an enhancement to RARP, and is more commonly implemented than RARP. As its name implies, BootP is used by computers as they boot to receive an IP address from a BootP server. The BootP address request packet sent by the host is answered by the server.
	Reverse Address Resolution Protocol (RARP)	
Network Layer Protocol	Internet Protocol (IP)	IP is the main TCP/IP protocol. It is a connectionless protocol that makes routing path decisions, based on the information it receives from ARP. It also handles logical addressing issues through the use of IP addresses.
Transport Layer Protocols	Transmission Control Protocol (TCP)	TCP operates at the Transport layer. It provides connection-oriented services and performs segment sequencing and service addressing. It also performs important error-checking functions, uses flow control, and is considered a host-to-host protocol.
	User Datagram Protocol (UDP)	UDP is considered a host-to-host protocol like TCP. It also performs functions at the Transport layer. However, it is not connection-oriented like TCP. Because of less overhead, it transfers data faster, but is not as

		reliable. It is a good protocol to use for small amounts of data and applications that use a simple query/response model.
Web Browsing	HyperText Transfer Protocol (HTTP)	Web browsers and Web servers to exchange files (such as Web pages) through the World Wide Web and intranets use HTTP. HTTP can be described as an information requesting and responding protocol. It is typically used to request and send Web documents, but is also used as the protocol for communication between agents using different TCP/IP protocols.
	HyperText Transfer Protocol over Secure Socket Layer or HTTP over SSL (HTTPS)	HTTPS is a secure form of HTTP that uses SSL as a sublayer for security.
Security Protocols	Secure Sockets Layer (SSL)	SSL secures messages being transmitted on the Internet. It uses RSA for authentication and encryption. Web browsers use SSL (Secure Sockets Layer) to ensure safe Web transactions. URLs that begin with <i>https://</i> trigger your Web browser to use SSL.
	Transport Layer Security (TLS)	<p>TLS ensures that messages being transmitted on the Internet are private and tamper proof. TLS is implemented through two protocols:</p> <ul style="list-style-type: none"> • TLS Record--Can provide connection security with encryption (with DES for example). • TLS Handshake--Provides mutual authentication and choice of encryption method. <p>TLS and SSL are similar but not interoperable.</p>

File Transfer	File Transfer Protocol (FTP)	FTP provides a generic method of transferring files. It can include file security through usernames and passwords, and it allows file transfer between dissimilar computer systems. FTP can transfer both binary and text files, including HTML, to another host. FTP URLs are preceded by <i>ftp://</i> followed by the DNS name of the FTP server. To log in to an FTP server, use: <i>ftp://username@servername</i> .
	Trivial File Transfer Protocol (TFTP)	TFTP is similar to FTP. It lets you transfer files between a host and an FTP server. However, it provides no user authentication and uses UDP instead of TCP as the transport protocol.
	Secure File Transfer Protocol (SFTP)	SFTP is a file transfer protocol that uses Secure Shell (SSH) to secure data transfers. SSH ensures that SFTP transmissions use encrypted commands and data which prevent data from being transmitted over the network in clear text.
	Secure Copy (SCP)	SCP is associated with Unix/Linux networks and used to transfer files between systems. Like SFTP, SCP relies on SSH to ensure that data and passwords are not transmitted over the network in clear text.
	Remote Copy Protocol (RCP)	RCP is used to transfer files between computers however, it is an insecure protocol and transmits data over the network in clear text.
E-mail	Simple Mail Transfer Protocol (SMTP)	SMTP is used to route electronic mail through the internetwork. E-mail applications provide the interface to communicate with SMTP or mail servers.
	Internet Message Access Protocol (IMAP)	IMAP is an e-mail retrieval protocol designed to enable users to access their e-mail from various locations without the need to transfer

		messages or files back and forth between computers. Messages remain on the remote mail server and are not automatically downloaded to a client system.
	Post Office Protocol 3 (POP3)	POP3 is part of the TCP/IP protocol suite and used to retrieve e-mail from a remote server to a local client over a TCP/IP connection. With POP3, e-mail messages are downloaded to the client.
Network Management	Simple Network Management Protocol (SNMP)	SNMP is a protocol designed for managing complex networks. SNMP lets network hosts exchange configuration and status information. This information can be gathered by management software and used to monitor and manage the network.
	Remote Terminal Emulation (Telnet)	Telnet allows an attached computer to act as a dumb terminal, with data processing taking place on the TCP/IP host computer. It is still widely used to provide connectivity between dissimilar systems. Telnet can also be used to test a service by the use of HTTP commands.
	Secure Shell (SSH)	SSH allows for secure interactive control of remote systems. SSH uses RSA public key cryptography for both connection and authentication. SSH uses the IDEA algorithm for encryption by default, but is able to use Blowfish and DES. SSH is a secure and acceptable alternative to Telnet.
File and Print Services	Network File System (NFS)	Sun Microsystems initially developed NFS. It consists of several protocols that enable users on various platforms to seamlessly access files from remote file systems.
	Line Printer Daemon/Line	LPD/LPR is the most widely used cross platform print protocol. LPD/LPR establishes connection between printing devices and

	Print Remote (LPD/LPR)	workstations. LPD is usually loaded on the printing device. LPR is usually loaded onto the client workstation.
Additional Protocols	Internet Control Message Protocol (ICMP)	ICMP works closely with IP in providing error and control information, by allowing hosts to exchange packet status information, which helps move the packets through the internetwork. Two common management utilities, ping and tracert , use ICMP messages to check network connectivity. ICMP also works with IP to send notices when destinations are unreachable, when devices' buffers overflow, the route and hops packets take through the network, and whether devices can communicate across the network.
	Internet Group Membership Protocol (IGMP)	IGMP is a protocol for defining host groups. All group members can receive broadcast messages intended for the group (called multicasts). Multicast groups can be composed of devices within the same network or across networks (connected with a router).
Services	Domain Name System (DNS)	DNS is a system that is distributed throughout the internetwork to provide address/name resolution. For example, the name www.mydomain.com would be identified with a specific IP address.
	Network Time Protocol (NTP)	NTP is used to communicate time synchronization information between systems on a network.
	Network News Transport Protocol (NNTP)	NNTP is the most widely used protocol that manages notes posted on Usenet Newsgroups.

	Lightweight Directory Access Protocol (LDAP)	LDAP is used to allow searching and updating of a directory service. The LDAP directory service follows a client/server model. One or more LDAP servers contain the directory data, the LDAP client connects to an LDAP Server to make a directory service request.
--	---	---

The TCP/IP protocol suite was developed to work independently of the Physical layer implementation. You can use a wide variety of architectures with the TCP/IP protocol suite.

18. What is a DNS?

The Domain Name System (DNS) is a hierarchical, distributed database that maps logical host names to IP addresses. The DNS hierarchy is made up of the following components:

- . (dot) domain (also called the *root* domain)
- Top Level Domains (TLDs) such as .com, .edu, .gov
- Additional domains such as yahoo.com, microsoft.com, etc.
- Hosts

DNS is a distributed database because no one server holds all of the DNS information. Instead, multiple servers hold portions of the data.

- Each division of the database is held in a *zone* database file.
- Zones typically contain one or more domains, although additional servers might hold information for child domains.
- DNS servers hold zone files and process name resolution requests from client systems.

When you use the host name of a computer (for example if you type a URL such as `www.mydomain.com`), your computer uses the following process to find the IP address.

1. The host looks in its local cache to see if it has recently resolved the host name.
2. If the information is not in the cache, it checks the Hosts file. The Hosts file is a static text file that contains hostname-to-IP address mappings.
3. If the IP address is not found, the host contacts its preferred DNS server. If the preferred DNS server can't be contacted, it continues contacting additional DNS servers until one responds.
4. The host sends the name information to the DNS server. The DNS server then checks its cache and Hosts file. If the information is not found, the DNS server checks any zone files that it holds for the requested name.
5. If the DNS server can't find the name in its zones, it forwards the request to a root zone name server. This server returns the IP address of a DNS server that has information for the corresponding top-level domain (such as .com).

6. The first DNS server then requests the information from the top-level domain server. This server returns the address of a DNS server with the information for the next highest domain. This process continues until a DNS server is contacted that holds the necessary information.
7. The DNS server places the information in its cache and returns the IP address to the client host. The client host also places the information in its cache and uses the IP address to contact the desired destination device.

You should know the following facts about DNS:

- A *forward* lookup finds the IP address for a given host name. A *reverse* lookup finds the host name from a given IP address.
 - An *authoritative* server is a DNS server that has a full, complete copy of all the records for a particular domain.
 - Zone files hold records that identify hosts.
 - A records map host names to IP addresses.
 - PTR (pointer) records map IP addresses to host names.
 - *Recursion* is the process by which a DNS server or host uses root name servers and subsequent servers to perform name resolution. Most client computers do not perform recursion; rather they submit a DNS request to the DNS server and wait for a complete response. Many DNS servers will perform recursion.
 - Some DNS servers might forward the name resolution request to another DNS server and wait for the final response rather than performing recursion.
 - Root DNS servers hold information for the root zone (.). Root servers answer name resolution requests by supplying the address of the corresponding top-level DNS server (servers authoritative for .com, .edu, and such domains).
 - On very small networks, you could configure a HOSTS file with several entries to provide limited name resolution services. However, you would have to copy the HOSTS file to each client. The work involved in this solution is only suitable for temporary testing purposes or to override information that might be received from a DNS server.
-

19. Addressing Method

The following table lists several options for assigning IP addresses.

Method	Uses
Dynamic Host Configuration Protocol (DHCP)	<p>A DHCP server is a special server configured to pass out IP address and other IP configuration information to network clients.</p> <ul style="list-style-type: none">• When a client boots, it contacts the DHCP server for IP configuration information.• The DHCP server is configured with a range of IP addresses it can assign to hosts (Microsoft calls these ranges <i>scopes</i>).• The DHCP server can also be configured to pass out other IP configuration such as the default gateway and DNS server addresses.• The DHCP server ensures that each client has a unique IP address.• The DHCP server can be configured to not assign specific addresses in the range, or to assign a specific address to a specific host.• The DHCP server assigns the IP address and other information to the client. The assignment is called a <i>lease</i>, and includes a lease time that identifies how long the client can use the IP address.• Periodically and when the client reboots, it contacts the DHCP server to renew the lease on the IP address.• The DHCP lease process uses frame-level broadcasts. For this reason, DHCP requests typically do not pass through routers to other subnets. To enable DHCP across subnets:<ul style="list-style-type: none">◦ Enable BootP (DHCP broadcast) requests through the router.

	<ul style="list-style-type: none"> ○ Configure a computer for BootP forwarding to request IP information on behalf of other clients. • You can configure a DHCP server to deliver the same address to a specific host each time it requests an address. Microsoft calls this configuration a <i>reservation</i>. <p>Use DHCP for small, medium, or large networks. DHCP requires a DHCP server and minimal configuration.</p>
Automatic Private IP Addressing (APIPA)	<p>APIPA is a Microsoft implementation of automatic IP address assignment without a DHCP server. Using APIPA, hosts assign themselves an IP address on the 169.254.0.0 network (mask of 255.255.0.0). With APIPA:</p> <ul style="list-style-type: none"> • The host is configured to obtain IP information from a DHCP server (this is the default configuration). • If a DHCP server can't be contacted, the host uses APIPA to assign itself an IP address. • The host only configures the IP address and mask. It does not assign itself the default gateway and DNS server addresses. For this reason, APIPA can only be used on a single subnet. <p>Use APIPA:</p> <ul style="list-style-type: none"> • On small, single-subnet networks where you do not need to customize the IP address range. • As a fail safe for when a DHCP server is unavailable to provide limited communication capabilities. <p>Note: The IPv6 addressing standard also reserves all addresses beginning with a binary 1111 1110 10 (hexadecimal FE80::/64) for automatic assignment (this is called the link-local address range).</p>
Static (manual) assignment	<p>Using static addressing, IP configuration information must be manually configured on each host. Use static addressing:</p>

- | | |
|--|--|
| | <ul style="list-style-type: none">• On networks with a very small number of hosts.• On networks that do not change often or that will not grow.• To permanently assign IP addresses to hosts that must always have the same address (such as printers, servers, or routers).• For hosts that cannot accept an IP address from DHCP.• To reduce DHCP-related traffic. |
|--|--|

Note: *Static addressing is very susceptible to configuration errors and duplicate IP address configuration errors (two hosts that have been assigned the same IP address). Static addressing also disables both APIPA and DHCP capabilities on the host.*

20. What is a DHCP Server and “D.O.R.A.” Process

The table below describes the method clients use to obtain an address from a DHCP server.

Broadcast	Description
DHCP Discover (D)	The client begins by sending out a DHCP Discover frame to identify DHCP servers on the network.
DHCP Offer (O)	A DHCP server that receives a Discover advertisement from a client responds with a DHCP Offer. The offer contains the IP address. If more than one DHCP server sends an offer packet, the client responds to the first offer packet that it receives.
DHCP Request (R)	The client accepts the offered address by sending a DHCP Request.
DHCP ACK (A)	The DHCP responds to the request by sending a DHCP ACK (acknowledgement).

A DHCP server might need to be authorized before it will begin answering DHCP requests from clients:

- Authorization is required if you are using Active Directory; no authorization is required for a standalone server.
- When using Active Directory, DHCP servers must either be domain controllers or domain member servers before you can authorize them for DHCP.
- When you authorize a DHCP server, its IP address is added to a list of authorized DHCP servers maintained in Active Directory.
- To authorize a DHCP server, you must be a member of the Enterprise Admins group. In the DHCP console, right-click the DHCP node in the console and choose **Manage authorized servers...**
- When a DHCP server starts, its IP address is compared to the Active Directory list. If it is found, the server is allowed to issue IP addresses. If it is

not found, the server automatically shuts down before completing the start up process.

- A Windows DHCP server checks for authorization when it boots and reauthorizes every five minutes.
- Windows Server versions 2000/2003/2008 check for authorization. DHCP servers running other operating systems (e.g., UNIX, NetWare, or Windows NT) do not check for authorization before assigning addresses.
- You can authorize a server before or after DHCP is installed.
- In most cases, when you install DHCP on a domain controller, it will be authorized automatically.

To configure a DHCP server to deliver IP addresses, configure the following:

Configuration Object	Description
Scope	<p>A <i>scope</i> is the range of IP addresses for subnet hosts that receive IP addresses from DHCP. Be aware of the following when working with scopes:</p> <ul style="list-style-type: none">• A scope has a subnet mask that determines the subnet for a given IP address. To change the subnet mask used by a scope, you must delete and recreate the scope. You cannot selectively change the subnet mask in an existing DHCP scope.• The scope must be activated before the DHCP server will assign addresses to clients. After you activate a scope, do not change its range of IP addresses.• Lease duration values are part of the scope properties and determine the length of time a client can use the IP address leased through DHCP.
Exclusion	<p>Use <i>exclusions</i> to prevent the DHCP server from assigning certain IP addresses. For example, exclude any IP addresses for devices that are not DHCP clients.</p>
Reservation	<p>Use <i>reservations</i> to make sure a client gets the same IP address each time from the DHCP server. The reservation associates the MAC address with the IP address the client should receive. For</p>

	<p>example, use a reservation for servers and printers to keep their IP addresses consistent while still assigning the addresses dynamically.</p>
--	---

Note: *When using reservations, do not exclude the addresses you want to assign.*

21. DHCP Options

Through DHCP, you can deliver a wide range of TCP/IP configuration parameters (not just the IP address and mask). Additional parameters are delivered by configuring DHCP options. Common options include:

Option	Description
003 Router	The IP address of the default router (the default gateway).
006 DNS Servers	The IP address of DNS server or servers.
015 DNS Domain Name	The domain that the client belongs to. The client uses this domain name to update its DNS record.

DHCP options can be set at the following levels:

Level	Description
Server	Options set on the IPv4 node or the IPv6 node are delivered to all clients of that DHCP server on any scope.
Scope	Options set on the scope are delivered to all computers that obtain an IP address from within the scope.
Reservation	Options set on a reservation are delivered to the specific client.

Be aware of the following when working with DHCP options:

- Options are applied in the order listed above. If conflicting settings are delivered, the last parameters delivered take precedence over the previous settings.
- Any values configured manually on the client override options delivered through DHCP.
- DHCP options are configured separately for IPv4 or IPv6.
- You can use Group Policy to configure some DNS options. Group Policy settings override DHCP-delivered settings. Settings delivered through Group Policy cannot be manually altered, even if the user has administrator privileges.

22. Internet Connectivity Parameters

To connect a Windows workstation to the Internet, you need, at a minimum, to configure the IP address, subnet mask, default gateway, and DNS server parameters. Depending upon the network configuration, you may also need to configure the workstation with the IP address of the proxy server. The following table summarizes many of the configuration settings for a TCP/IP network.

Parameter	Purpose
IP address	Identifies both the logical host and logical network addresses. Two devices on the same network must have IP addresses with the same network portion of the address.
Subnet mask	Identifies which portion of the IP address is the network address. Two devices on the same network must be configured with the same network mask.
Default gateway	Identifies the router to which packets for remote networks are sent. The default gateway address is the IP address of the interface on the same subnet as the local host. Without a default gateway set, most clients will be unable to communicate with hosts outside of the local subnet.
Host name	Identifies the logical name of the local system.
DNS server	Identifies the DNS server that is used to resolve host names to IP addresses.
MAC address	Identifies the physical address. On an Ethernet network, this address is burned in to the network adapter hardware.

23. What is a ICS?

Internet Connection Sharing (ICS) is a service available on Windows systems that enables multiple computers on a single small network to access the Internet by sharing one computer's connection. With ICS, most configuration tasks are completed automatically. When using ICS:

- The ICS system is configured as a NAT router, a limited DHCP server, and a DNS proxy (name resolution requests from the private network are forwarded to DNS servers on the Internet).
- The IP address for the private interface is automatically changed to 192.168.0.1 with a mask of 255.255.255.0.
- The default gateway of the ICS system is set to point to the Internet connection.
- Hosts on the private network should use DHCP for address and DNS server information.
- The ICS system uses DHCP to deliver the following information to hosts on the private network:
 - IP address in the range of 192.168.0.0 with a mask of 255.255.255.0.
 - DNS server address of 192.168.0.1 (the private interface of the ICS system).
 - Default gateway address of 192.168.0.1.
- Do not use DHCP servers, DNS servers, or Active Directory on your private network.

24. NAT and Private Address Ranges

Network Address Translation (NAT) allows you to connect a private network to the Internet without obtaining registered addresses for every host. Private addresses are translated to the public address of the NAT router.

- Hosts on the private network share the IP address of the NAT router.
- The NAT router maps port numbers to private IP addresses. Responses to Internet requests include the port number appended by the NAT router. This allows the NAT router to forward responses back to the correct private host.
- NAT supports a limit of 5,000 concurrent connections.
- NAT provides some security for the private network because it translates or hides the private addresses.
- A NAT router can act as a limited-function DHCP server, assigning addresses to private hosts.
- A NAT router can forward DNS requests to the Internet.
- Dynamic NAT allows internal (private) hosts to contact external (public) hosts but not vice versa.
- Static NAT allows external hosts to contact internal hosts but prevents the use of dynamic NAT.
- Dynamic and Static NAT, in which two IP addresses are given to the public NAT interface (one for dynamic NAT and one for static NAT), allows traffic to flow in both directions.

When connecting a private network to the Internet through NAT, assign IP addresses in several predefined private address ranges. These address ranges are guaranteed to not be in use on the Internet and do not need to be registered.

Address Ranges
<ul style="list-style-type: none">• 10.0.0.1 to 10.255.255.254• 172.16.0.1 to 172.31.255.254• 192.168.0.1 to 192.168.255.254