Networking

1. Contrast the terms "networking," "point-to-point," and "broadcast."

The term networking refers to the interconnection of computers and peripherals *via* network interface cards (NICs) and cabling or radio waves. NICs transform the parallel high-speed system bus signals into a slower sequential bit stream. Computer systems with directly coupled system buses are said to be tightly coupled, while computer systems interconnected via NICs are said to be loosely coupled. NICs come in many forms, but could be divided into two basic groups: serial or point-to-point and Ethernet or broadcast.

Point-to-point (PTP), or serial connections, are generally run long distances, send information slower than broadcast, and require two separate NICs to pass information onto another computer in the network. Broadcast (Ethernet), on the other hand, are generally run over short distances, are generally faster than PTP connections, and only require on NIC per host in the local area network.

2. Contrast coaxial, twisted pair, fiber optic, and wireless network media.

Coaxial cable has a center conductor that is wrapped in insulation that, in turn, is covered with a second conductor and wrapped again with a protective sheath. Coax offers high signal reliability in two ways. First, if the outer conductor is connected to earth ground, it shields the inner conductor from stray electromagnetic signals that may distort or cancel the desired signal. Second, coax is designed so that the ratio of the inner-conductor diameter to the second-conductor-inside diameter offers a fixed impedance at a given signal frequency. The fixed impedance allows the local area network to be designed with fixed distance and number of connections. Existing LAN coax cables can only handle up to 10 megabits per second or (assuming all zeros) a maximum Manchester encoded 20 MHz signal.

Twisted pair refers to the concentric twisting of two insulated conductors. The number of 360 degree twists per foot vary from "loose" (category one) to "tight" (category five). Twisted pairs are arranged so that an electrical signal and its return path share the twist. When bundled into larger cables, twisted pair conductors tend to induce excess electromagnetic impulses into the twist partner and not another twisted pair in the same cable. When an electromagnetic signal is imposed upon a twisted pair, the induced voltage is shared by the twist partners and thereby reduces signal distortion. The telephone company employs twisted pair wires throughout its network.

Fiber optic cable employs light as the signal and is therefore immune to the effects of frequency-related impedance and electromagnetic interference that plagues copper conductors. Fiber optic is faster, physically lighter and smaller than its copper counterparts and will eventually replace copper wire.

Since wire installation in some buildings may be too expensive and telephone companies control access to any wiring that crosses public space, wireless radio broadcast offers a medium speed (one to two megabits per second) alternative at a moderate cost.

3. **Explain how twisted pair (and fiber optic) cabling allow 100 Megabits (and 1 gigabit) broadcast Ethernet LANs and give the tradeoff.**

These broadcast LANs are an illusion! They are, in fact, a combination of PTP serial connections and an actively repeating hub. The "Ethernet" NIC appears to the software to send and receive broadcast network frames. Instead, the NIC sends and receives over two twisted pairs, and optionally employs two other twisted pairs, to simulate high speed broadcast. The illusion is completed with the hub actively moving packets from one incoming PTP line onto all outgoing PTP lines.

Fiber optic connections are essentially the same as twisted pair except that there is only one high speed optical cable between the NIC and hub.

Even though PTP emulation of broadcast incurs the cost of extra adapter and hub circuitry, it more than pays back this cost through continued use of a simplified network topology (no need for routes to non-adjacent computers) and through collision optimizations that improve network performance.

4. **Define and explain the role of a "collision domain."**

Generally, hubs buffer incoming frames before sending them onto the outgoing lines. Thus, it is possible for the hub to receive a "micro traffic burst" from several lines simultaneously, buffer each line and send out the frames in sequence upon completion of the micro traffic burst.

Network traffic between hubs is also usually buffered; therefore, it is said that two computers attached to two separate buffering hubs are in separate collision domains. Put another way, leaf node hosts exchanging information within one hub will not offer a traffic load to hosts attached to a second hub.

5. **Contrast the terms "repeater," "hub," "switching hub," "bridge," "router," "switching router," "gateway," and "firewall."**
    a. A **repeater** accepts a network frame, electrically or optically amplifies it, and sends the frame out over a second cable.
    b. Generally a **hub** is an Ethernet twisted pair repeater. A frame arriving on one line is repeated as an out going frame on the other lines. Depending on how the "hub" was constructed, a hub could also be a switching hub, a bridge, a router, or even a switching router.

c. A **switching hub** accepts a high speed frame, buffers the frame, and transmits the frame on a second cable at a lower speed (*e.g.*, a 10/100 Mbs hub or a 100/1000mbs hub).
d. A **bridge** is used to extend existing LANs and to isolate high-traffic segments within the same physical LAN. A bridge contains two or more NICs and manipulates "data link frames" that contain physical source and destination NIC addresses. Bridges extend LANs through the concatenation of multiple LAN segments. The bridge operates by transmitting a "new" incoming frame onto all outgoing NICs the first time it arrives. As time goes on, the bridge records the source station address associated with frame coming in from each NIC. In this way, the bridge can reduce overall LAN traffic by only transmitting an outgoing frame to a NIC associated with that destination station address. Broadcast frame, however, must still be propagated to all out going NICs.
e. A **router** interconnects networks. It generally connects smaller LANs and networks to larger networks. A router contains two or more NICs and manipulates "network addressed packets." The router also contains a "dispatch table" created by the network administrator and updated by special routing packets. Incoming packets are inspected and destination addresses extracted. The network address is compared to addresses held in the internal routing table. An address match directs the packet to the associated interface. One NIC is usually the "default" interface that accepts any address not destined for the other NICs and it, in turn, is connected to the larger network.
f. In addition to routing, a **switching router** records and shares its NIC network addresses with other switching routers. Thus, the switching routers may cooperate to form virtual LANs where two distant hosts appear to be on the same LAN. A switching router does in hardware what the **proxy ARP** protocol does in software.
g. A **gateway** is a general term referring to any active movement of information between two NICs done with high-level (application) software. For example, a computer that receives e-mail on one NIC and redistributes it on a second NIC is a mail gateway.
h. A **firewall** is a general term referring to any of the above active agents that restrict information flow between two NICs.

6. Describe Internet topology, the design tradeoff, and explain how competing ISPs can break the topology.

The Internet consists of levels of networks. At the first-level there are LANs that run throughout businesses, governments, schools, and even homes. These LANs are assigned Internet Protocol (IP) network addresses that were allocated by their Internet Service Providers (ISPs). These second-level ISPs form a city, metropolitan area, state-wide, or multi-state regional network. They receive their IP address from third-level ISPs that connect to national and world-wide routers. The third-level ISPs get their address from the Internet Assigned Numbers Authority.

Much like telephone networks, these levels allow high frequency exchange of data among local hosts without disturbing higher layers. Traffic at the highest layer is only used for inter-regional or international exchange of data.

Unfortunately, competing ISPs often break this hierarchical design. If two second-level competing ISPs service the same geographical area (say one services a university and the other services an associated city), and if they use separate third-level ISPs, then all local network traffic between students in their apartments and the local university computers must go through national routers. Furthermore, manually configured routing tables may make the problem worse. Let us assume that one third-level ISP directs its unknown destination packets to the east coast for national distribution, while the competing third-level ISP directs its unknown packets to the west coast for national distribution. Only after the packets reach either coast, are they recognized and sent back to the originating location. In this way, keystrokes from a student's virtual terminal session are sent to the west cost before returning to the local university computer. And as each typed character is echoed by the university computer, it is sent to the east coast before returning to the student's PC.

7. **Contrast the terms "station address," "network address," "port number," and "protocol."**

These terms represent the key concepts that allow two computers to communicate via a network.

a. **Station address** refers to the physical network address of the NIC. Generally, users are unaware of physical addresses or the separate protocol (ARP) that automatically translates logical network addresses into physical station addresses.
b. **Network address** is a logical address assigned to each host. In the Internet, this logical address is called an Internet Protocol (IP) address. All IP addresses are allocated by the Internet Assigned Numbers Authority, and paths to each IP address are manually placed in routers from the top level to the bottom level routers. So even though network addresses are logical, most IP address are geographically fixed.
c. **Port number** is a third level of addressing that selects one of many processes (programs) on one host that can communicate with one of many process on another host.
d. **Protocol** refers to the manner in which two programs choose to communicate. Two basic protocols are virtual circuits (modeled after the telephone) and datagrams (modeled after postal letters). A virtual circuit protocol requires the communicating programs to go through a series of steps similar to making a telephone call while a datagram is sent out much like dropping a letter into a mail box. Virtual circuits are said to be reliable while datagrams are considered unreliable.

8. **Describe the major components of an IP packet.**

An IP packet consists of a 20-byte header,optional status information, and data. Among other administrative information, the 20-byte header contains the

source and destination IP addresses of the two communicating hosts. The data consists of a virtual circuit (TCP) or datagram (UDP) message.

9. Describe the operation of a router and contrast static *versus* dynamic routing.

An IP router simply accepts a packet from one NIC and extracts the destination address which is compared to other addresses held in its internal routing table. An address match directs the packet to the associated interface. One NIC is usually the "default" interface that accepts any address not destined for the other NICs and it, in turn, is connected to the larger network.

The term "router" is a misnomer in that most routers simply dispatch IP packets to and from an Internet-connected NIC. The router only knows that if it cannot find a match in its table, it should send the packet out its default NIC to see if the next guy can figure out what to do with the packet.

In static routing, the table is set up by the network administrator. In dynamic routing, routers with two or Internet-connected NICs exchange table data indicating which neighbor can accept which addresses and at what speed.

10. Describe and give the design tradeoff of IP addresses.

Internet Protocol (IP) addresses are 32-bits, or four bytes in length. Addresses are written in a dotted decimal notation in which each byte is converted to a decimal number (0-255) with leading zeros not shown (unless the number is zero). Each byte is also separated by a "." (dot) character. Each host or router NIC has at least one IP address. If two or more IP addresses are associated with one NIC, it is assumed to be a "multi-homed" NIC that supports some form of virtual hosting.

IP addresses are grouped into "classes."

Network		Class Address Range	
Class	**Netmask**	**Start address**	**End address**
A	255.0.0.0	0.0.0.0	127.255.255.255
B	255.255.0.0	128.0.0.0	191.255.255.255
C	255.255.255.0	192.0.0.0	223.255.255.255
Multicast	240.0.0.0	224.0.0.0	239.255.255.255

Class A addresses occupy half of the total address space and are designed for use by third-level ISPs. Each class A address provides for the allocation of 16 million individual IP addresses. Class B addresses occupy one quarter of the address space and are designed for use by large organizations. Each class B address provides for the allocation of 65 thousand individual IP addresses.

Class C addresses occupy an eighth of the address space and are designed for use by small organizations. Each class C address provides for the allocation of 256 individual IP addresses. The remaining eighth of the IP address space is designed for group addressing and is generally unimplemented.

By examining the most significant (left hand side) of an IP address, you can determine its class and, therefore, where all of its allocated IP addresses are located. Thus, IP classes were used to limit the size of the high-level routing tables, but at the significant cost of over allocation of IP addresses. This over-allocation led to the development of IPV6 which has 128-bit (16-byte) network addresses.

Adaption of IPV6 will require rewriting the network protocol stack as well as any program that employs the network. To avoid the cost of switching to IPV6, ISPs have focused on efficient use of existing IPV4 addresses and faster computers have permitted large routing tables containing "classless" IP addresses.

11. Describe an IP network.

Internet Protocol (IP) networks are generally a sequence of IP addresses in which the most significant bits (left hand side) remain constant and the least significant (right hand side) bits change. The constant bits of the addresses make up the network address portion. The remaining bits make up the host address portion of the IP address. The number of bits shared by all addresses within a network is discovered through the use of the netmask. By convention, the IP addresses 0 and 255 have special meanings. The address 0 means "treat the most significant bits of this address as a network address", while the 255 address means "send a packet to all hosts contained in this network address." For example:

Host Address	192.168.1.3
Network mask	255.255.255.0
Network portion	192.168.1
Host portion	3
Network address	192.168.1.0
Broadcast address	192.168.1.255

Please note that some sites may be configured to use the network address as the broadcast address.