Communication Protocols and Internet Architectures
Harvard University
CSCI S-40

Homework Assignment #2 Solutions
Total points: 24

Question 1) 5 points total

1a, 1b and 1c, Explain in detail what is meant by a collision domain and a broadcast domain in an 802.3 network…. **see the homework for the complete question.**

1a. Answer

For an ethernet network, a broadcast domain is a group of hosts connected together in such a way that when one host sends a broadcast frame (i.e., a frame whose destination address is the broadcast address of all 1s) onto the network, all the hosts in the group receive the frame. All of the hosts that receive the broadcast frame are considered members of the same broadcast domain. (These hosts can be connected together by both hubs and switches.)

A collision domain is a group of hosts connected together in such a way that where when one of the hosts sends out a frame, there is the potential that another host could also be sending a frame at the same time and hence, a collision could result. This group of hosts would typically be connected together by hubs, but not switches. (NOTE: Data is not always lost due to a collision, only that one transmission is lost. The senders detect the collision and retransmit at a later time.)

A hub (also known as a repeater) is a level 1 (physical) device. Every frame that is received on one port is transmitted out all the other ports. This is the case regardless of whether the frame is a unicast frame or a broadcast frame. This means that a hub implements a single collision domain and a single broadcast domain.

A switch is a level 2 (link layer) device. Once a switch has (passively) learned the location of all hosts relative to its input ports, it no longer floods frames that it receives out all of its ports. In the case where only a single host is located off of each switch port, this means that only the frames destined for the specific host are sent out that port. As such, it creates a separate collision domain on each port. At the same time, broadcast frames are flooded out to all ports (except the one the frame was received on) and hence it does not create multiple broadcast domains. (NOTE: Because a switch is a level 2 device, it handles Ethernet frames and looks at just the MAC addresses; it has no knowledge of IP datagrams or of IP addressing.)

A router is a level 3 (network layer) device. It forwards IP datagrams between networks based on the IP address. Frame level broadcasts are not forwarded from one router port to another. Therefore, a router creates separate broadcast domains as well as separate collision domains.

1b. Answer

One straightforward answer to this question is to use five of the switch ports for the five servers and use wireless connectivity for the remaining desktop machines. This

design did not completely fill all the switch ports in order to allow for future server expansion.

If future expansion is not a concern, three of the ten desktops could be added to the switch. They can be selected by making an educated guess as to which machines are the heaviest network users. A more sophisticated approach would be to actually analyze the traffic on the LAN and use wireless for the desktops with the least amount of traffic and the switch for the desktops with the most traffic.

1c. Answer

A server and a desktop machine may initially appear to be very similar. Both indeed have CPU, memory, network and storage resources. However, servers typically have more powerful operating systems and faster hardware in order to be able to provide different services to many different end-users and applications in the network. For example, a server may provide database or e-mail services to multiple end-users and applications, and, as such, will support a large network workload compared to desktop machines.

In contrast, desktop machines are typically intended for personal use and will usually support client applications for an individual end-user. As a result, desktop machines will have smaller network workloads when compared to a server and will run applications that support small numbers of users rather than many different users. The consequences of these different characteristics are:

- Servers must have more robust network hardware and other resources than desktop machines. Servers typically have multiple network interfaces and each interface can have multiple IP addresses.
- Servers will generate more network traffic than desktop machines.
- Outages and data loss on servers are more costly, since they will impact many end-users and applications rather than a single end-user.

Question 2) 2 points

In a sentence or two, explain what the traceroute command does….. .(Please see the homework for the complete question.)

The traceroute command displays a list of the routers between two hosts. That is, if you execute "traceroute b.nowhere.com" on host A, the program will display a list of the routes between A and B. Many implementations of traceroute also print estimates of the round-trip times between A and each router along the way.

The traceroute compiles this data by utilizing certain features of the UDP, IP, and ICMP protocols. Specifically, when a user on host A executes "traceroute b.nowhere.com," it transmits one or more UDP datagrams to B, with each datagram's destination-port field filled with a particularly high number not expected to be in use. (Many Linux implementations of traceroute, for instance, transmit these datagrams to UDP port 33,000 or higher.)

The UDP packet is encapsulated in an IP packet whose TTL field is set to 1. That packet is then sent to the nearest router, which decrements the TTL and, seeing it fall to 0, discards the datagram, returning an ICMP time-exceeded message (that is, an ICMP message whose TYPE field is 11 and whose CODE field is 0) back to A, along with the IP header and first 64 bits of the dropped datagram. Upon receiving that ICMP message, host A discovers the first hop between it and B.

This process continues with host A sending out additional UDP datagrams, encapsulated in IP packets, with incrementally larger TTLs. Therefore the datagram with TTL 2 will reveal to A the second hop between it and B, and so on.

When a datagram finally reaches B, it arrives on an unusually high UDP port, the result of which is that B will most likely reject the datagram with an ICMP Destination Unreachable message (TYPE 3, CODE 3). Upon receipt of that message, A terminates the traceroute program, having discovered every router on the way to B.

Question 3) 3 points

Every NIC that has been manufactured has a unique Ethernet address…...(Please see the homework for the complete question.)

A primary purpose of the Internet Protocol is to create a logical internetwork from many different physical networks. To accomplish this, an abstraction is required from a physical addressing scheme to a global addressing scheme, and the IP address provides this.

The main reason is that the structure of the IP addressing mechanism was carefully designed to make routing possible. As you know, the IP address is made up of two-component: the network identifier and the host identifier. Given this, routers forward IP packets from network to network based on the network number. This keeps routing tables to a manageable size.

In contrast to IP addresses, MAC addresses identify a particular host or NIC card, but this address contains no location specific or routing information. In other words, the MAC address does not identify where the device is located within the Internet. Without this information, routing becomes an impossible task since a routing table would have to contain some type of location information for every MAC address that is in use.

Having the IP address abstraction also means that hardware can change (i.e., a new network interface with a new MAC addresses can be installed) without changing the IP address information and without undue administrative overhead.

Finally, note that not all network devices even have a MAC address (Cell phones and an older protocols are examples) but even if all the physical networks in the world were 802 based, we would still need to use IP addresses for the reasons noted above.

Question 4) 4 points total

Consider a network consisting of four hosts: A, B, C and D. Each host is connected to…….Please see the homework for the complete question.

When a switch receives a frame, it will examine the frame's source MAC address and associate that address in its forwarding table as being located off the port from which it entered the switch.

It will then examine the destination MAC address of the frame. If the destination is a broadcast address, the switch will send the frame out all ports (except the port it arrived on.)

If the destination MAC address is not a broadcast address, the switch will look in the forwarding table for that destination MAC address. If it is not in the forwarding table, the switch will flood the frame out all the ports (except the port it arrived on). If the destination MAC address is found in the forwarding table, the switch will forward the frame out the port specified in the forwarding table.

Based on these operational rules, when the switch receives the frame sent from host A to host C, it will record host A as being located off of Port 1 in its forwarding table. It will then examine the destination MAC address and will not find it in its forwarding table. Therefore, it will flood the frame out all ports (except for Port 1). After recording host D as being located off of Port 4 in its forwarding table, the switch will forward the broadcast frame sent by D out all ports (except Port 4). This is because frames sent to the broadcast address are intended to be received by all nodes on the LAN. When host C sends a frame back to host A, the switch will record host C as being located off of Port 3 in its forwarding table. It will then examine the forwarding table for the destination MAC address and since it is in the table (from the earlier event), it will forward the frame only to Port 1.

Question 5) 3 points

We discussed the "star of stars" Ethernet switch layout in class. A savvy network administrator ….. please see the assignment for complete statement of the problem.

Connecting the switches together with additional ethernet cables would create a physical topology with multiple connections between the various switches. This would create what is referred to as a network loop. While such a configuration may appear to be appealing from a redundancy perspective, it would introduce several problems, the most serious of which are broadcast storms (from broadcast traffic), and corruption of the switch forwarding tables in each device.

When a switch receives a broadcast frame, such as an ARP broadcast, it will forward the frame out all ports (except the source port). Multiple connections between the various switches would result in such broadcast traffic being continuously forwarded throughout the network. These frames would not expire and would continue to loop around the network forever, saturating the network and preventing any useful traffic. This is called a broadcast storm.

The redundant paths would also result in corrupted forwarding tables. A frame sent by a computer on a switch that was multiply connected to two other switches, and given these two other switches were also interconnected, would result in the switches seeing the source MAC address of the sending computer quickly move from port to port. This could result in frames being discarded or being sent to the wrong port. Another issue is that destination nodes on the network can receive multiple copies of the same frame that arrives from different paths, and this wastes some bandwidth.

** Note that in this question we said you should not assume that a protocol called the Spanning Tree Protocol (STP) was running on the switches (since we have not studied it in class.) STP is a protocol that allows the implementation to include multiple paths between switches. It does this by noting the presence of loops and automatically putting one of the links in a non-active or standby mode. The reason that you would want multiple paths is that they improve overall reliability given that one of the individual links fail.

Question 6) 4 points total:

6a.) A topology describes the structure, configuration and connectivity of a network. Identify and describe in detail the different topologies that can be used in LANs.

6b.) What does it mean that network topologies can be considered either logical or physical in nature? Give an example of how the same network can differ in this way.

Answer to 6A

The most common LAN network topologies are: Point-to-Point, Star, Bus, Ring and Mesh topologies.

In a Point to Point topology, two nodes are connected to each other by a direct link, and data travels between the two nodes over this link. In a Star topology, all nodes in the network are connected to a central device. Data sent from a source node will travel through the central device before continuing on to its intended destination node. In a Bus topology, each node in the network is connected to a common shared communications cable, and this cable acts as a broadcast medium. Data sent from a source node is received by all the other nodes on the network. In a Ring topology, each node is directly connected to its two neighboring nodes to form a circular ring configuration. Data sent from a source node is typically forwarded by each station in the ring after it processes it so that all nodes on the ring receive the data that was sent by the source. Many variations of this model exist and some do not pass along the frame once it is received by the intended recipient. In a Mesh network topology, every node in the network is directly connected to one or more other nodes in the network, and therefore directly or indirectly connected to every other node in the network. Data sent from a source node in a mesh network can possibly take many different paths to reach its destination. This forwarding operation of course requires processing by intermediate nodes.

Answer to 6B

The physical topology of a network describes how the nodes in a network are physically connected to each other. That is, the actual layout of the physical cables and devices that are used to connect the nodes in a network together.

The logical topology describes how the network operates and the manner in which data flows in the network. For example, a simple ethernet network of a few nodes connected to a hub represents a physical star topology, since all of the nodes are connected to the central hub device. However, the same network operates logically as a bus topology. This is because the hub is used to connect a number of nodes together and simply forwards any data it receives to all the other devices connected to it. In this way, the hub logically functions as a shared communications cable, and it is a bus topology.

Question 7.). *(3 points)*

We have discussed the 4-layer, the 5-layer and the 7-layer protocol reference model in class….(Please see the homework for the complete question.)

In order to manage complexity, networks and protocols are defined and organized into layers. A protocol reference model defines the number of layers, and describes the specific functions that are performed at each of these layers. The goal is that each layer operate independently of the other layers so that changes made to one the layers, do not require that changes be made to other layers. Of course, as we have discussed in class, there are many interactions between the various layers in real world implementations.

Many different protocol reference models have been designed and discussed over the years. The various textbooks today typically describe the four-layer, the five-layer and the seven-layer models. These are summarized below.

4-LAYER MODEL	
LAYER	**IMPORTANT FUNCTIONS**
4 – Application	Provides services to the user: email, web, video, etc
3 – Transport	Manages reliable or unreliable end-to-end communications
2 –Internet	Defines global addressing and routing scheme, connectionless service
1 – Network Access	Formats bits into frame, defines how frames are sent on a link, and manages the transmission of raw bits (electrical, optical, etc.)

5-LAYER MODEL	
LAYER	**IMPORTANT FUNCTIONS**
5 - Application	Provides services to the user: email, web, video, etc
4 - Transport	Manages reliable or unreliable end-to-end communications
3 - Network	Defines global addressing and routing scheme, connectionless service
2 - Data Link	Formats bits into frames and defines how frames are sent on the link
1 – Physical	Manages the raw bits on a comm link, defines details of electrical, optical, RF, etc.

7-LAYER OSI MODEL	
LAYER	**IMPORTANT FUNCTIONS**
7 - Application	Provides services to the user: email, web, video, etc
6 - Presentation	Defines and manages the formatting of data for applications
5 – Session	Establishes and manages end-to-end comm channels with specific features
4 - Transport	Manages end-to-end communications, can be reliable or unreliable
3 - Network	Defines global addressing and routing scheme, can be CONS or connectionless
2 - Data Link	Formats bits into frames and defines how frames are sent on the link
1 - Physical	Manages the raw bits on a comm link, defines electrical, optical, RF, etc., details

Clearly the 7-layer OSI model does the most to separate functionality between the layers, but at the expense of complexity. It was widely discussed but rarely used in practice. The 5-layer model and 4-layer reference model take a more practical approach and combine OSI's application, presentation, and session layers into one layer called the Application Layer. The 7-layer OSI model and the 5-layer model distinguish between the Data Link Layer and Physical Layer, while the 4-layer reference model combines the data-link and physical layers into a single Network Access Layer.

Our main focus in the class is the 5-layer model because we feel it provides the best framework from which to learn about networking. We also believe that it is important to distinguish between the Data Link Layer and Physical Layer due to the complexity and technical issues at each of these layers: describing the format for a data frame is different than describing how the bits are put on the wire, or the photons are sent down the fiber.

[End of HW2]