Homework 2

Scott Ouellette

Scott_Ouellette@hms.harvard.edu

1a.)

Explain in detail what is meant by a collision domain and a broadcast domain in an 802.3 network. Explain how collision domains and broadcast domains are implemented by ethernet hubs, ethernet switches and routers. Note the differences and similarities between how each device implements them.

802.3 was an early implementation of the Ethernet protocol. These two domains specify physical areas of the network that are very important in controlling the performance of the overall network.

With an ethernet hub, the broadcast and collision domains are the same. They encapsulate the entire network, due to the broadcasting nature of a hub.

With a switch, the broadcast domain remains the same, but the collsion domains change quite a bit. For a given Node/Client the physical link and the switch port it is connected to are both collision domains. Basically, the Host cannot send anything "out on the wire" if there is something incoming from the switch port "down the wire".

A router terminates broadcast and collision domains because a router doesn't propgate broadcast traffic to the outside world (its a layer 3 device).It also incorporates a smrter sense of where to send traffic (routing table) avoiding these types of collisions.

1b.)

Your small business has 15 computers, 10 of which are used as desktop machines and the remaining 5 are file servers or mail servers. All of the computers have both wireless and wired Ethernet cards. Your local ISP has provided you with a wireless router (witha built-in Ethernet switch) that has 8 physical ports as well as a wireless antenna. Assuming no difficulties in wiring, how would you allocate the eight wired Ethernet ports to the fifteen computers in you office? Explain you rationale.

Personally I would hardwire the 5 file/mail servers for a more robust upstream connection as they will likely have > 1 users utlizing them at a given time. For the remaining 10 desktops I think that proximity to the wireless router/switch as well as what the end user of a given machine would be doing with it that would aid in determining which would be hard wired vs. wireless.

1c.)

How do the network characteristics of a "server" differ from a “desktop” machine? Be specific, and provide some examples from the literature or your own experience.

In general a server has more users accessing it than a desktop machine. Servers are usually configured to be accessible from a larger portion of the network than a desktop, and are usually configured to be accessible to the WAN. Servers will usuablly be allocated more performant network hardware to aid with performance.

2.)

In a sentence or two, explain what the traceroute command does. Then, in a few paragraphs explain how the traceroute command works. Include details on the types of packets that are used, and the important protocol fields.

The `traceroute` command follows along and report on the hops taken over the network from the source machine to a specific destination supplied by the user.

Over the course of this probe the (IP) packet will be touched and retransmitted by a variety of different routers along the routing path. Traceroute cleverly exploits a field in the IP packet header called the TTL. Whenever a "hop" is taken between routers, the TTL field's value is decremented. When a given packet's TTL is 0, the router making the final decrement sends a message back to the source saying: "Hey I dropped your packet". So knowing this, traceroute sends packets in an iterative fashion to determine each routers identity along the way to the destination. A TTL of 1 is set at first, and the first router decrements it to 0, in doing so sends back its ICMP response to the sender. This process is continued until the destination is reached. Sometimes traceroute fails when a network/router doesn't support ICMP.

3.)

Every ethernet NIC that has been manufactured has a unique Ethernet address (also called a MAC or hardware address) and this means that each machine that has a NIC, has a unique address. Given this, why is it necessary for machines to also have an IP address? Explain in detail.

A MAC/Ethernet address is really only important when you get to a link local/private portion of a network. When communicating over ethernet in a LAN, it is much easier to exploit the broadcast functionality to figure out destinations. It's not until a packet that isn't destined for the local network is found that IP is really needed. A host needs both of these addressing schemes to be identifiable on both sides of a router.

4.)

Consider a network consisting of four hosts: A, B, C and D. Each host is connected to a different port on a switch. Specifically, A is connected to Port 1, B to Port 2, C to Port 3, and D to Port 4. Assume that the switch forwarding table is completely empty when the following three events occur:(1) Host A sends a frame to host C(2) Host D sends out a broadcast frame(3) Host C sends a frame back to host A. Describe the operation of the switch as these events occur. Your answer should include details on how the frames are distributed by the switch, and describe the information that is contained in the switch forwarding table after each event.

In this scenario a frame arrives at port one from host A. This frame includes source and destination MAC adresses, among other information. This switch maps host A's MAC address to port 1 in its forwarding table, and then proceeds to forward the frame to the destination MAC address. Since there isn't already an entry for the destination MAc addresses port, all remaining ports except the sending port, are flooded with the frame. Only then, when the destined host responds, will the forwarding table be updated appropriately. When D sends out a braodcast frame, all accessible ports besides the sending one are given the frame and the forwarding table is updated to include port and MAC information from the responding hosts. When C finally sends a frame destined for A, it simply happens since the forwading table is already populated with an entry for A.

5.)

We discussed the "star of stars" Ethernet switch layout in class. A savvy network administrator has pointed out that this type of network configurationhas several "single points of failure."For example, the failure of a switch port that is used to connect to another switch could take down many machines in the office. The network admin proposes connecting the stars (i.e., the switches) together with additional ethernet cables. Without using technologies or protocols not discussed in class (such as the spanning-tree protocol), would this work? Why or why not? What would happen if these additional cables were installed between two switches?

At first glance this looks like a bad idea to me. It seems to me that even though this type of approach may work in providing more redundancy for network failures, it also creates an even larger collision domain disrupting nework performance. I think a VLAN-based approach would alleviate this issue as well since that bumps up to routers on layer 3.

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.

As far as topology goes a LAN has two flavors: Infrastructure networks & Ad-Hoc networks Multiple devices can access the outside world through an upstream connection, or multiple devices can "talk amongst themselves" and be cut off from the commercial internet, respectively.

6b.)

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

I think this question ties in tightly with the lecture 5's talk on VLANS. When looking at a typical network diagram, it is fairly easy to imagine the physical nework that it represents. There are different classes of devices interconnected by physical mediums. This same physical network can be configured in such a way by adminitstrators, such that the diagram alone, will not properly represent the functionality of the network. An example of this logical distinction of the network functionality can happen within a VLAN. A VLAN can be configured to provide hosts access to portions of a network that the physical mediums alone wouldn't allow for.

7.)

The literature and the industry talk about different protocol reference models including the four-layer model, the five-layer model,and the seven-layer model. Compare and contrast these three different reference models. Next, choose one of them as the “best” model and explain your choice. Note that it is more important to us that you describe in a coherent and thoughtful way why you picked one model versus the others, than which particular model you chose. Important note: we will use the five-layer protocol reference model as our reference model for this course.

The 4-layer models is a simplified version of the OSI model listed as follows:

- Application Layer
- Transport Layer
- Network Layer
- Link layer

The 5-layer model is a simplified version of the OSI model listed as follows:

- Application Layer
- Transport Layer
- Network Layer
- Link layer
- Physical layer

The 7-layer model (OSI model) is as follows:

- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Link layer
- Physical layer

For myself, a novice in the networking world, I can appreciate the granularity provide with the 7-layer model as opposed to the other two. Although, I also see why newer, more simplistic models are being adopted. I'm not sure if I'm entirely correct in saying this, but: It seems like the Session layer is implicitly defined within the protocol that the layered model is to represent. There are probably scenarios that a more generic model like this affords for, but I don't know enough currently to make any claims. It also seems to me that having a layered model that is too generic could hinder the implementation/design of future protocols if they have one-off attributes/procedures that don't exactly fit the larger modelling. Personally, I think the "best" model, at least for myself, currently is the 4 layer model. There is less information to remember upfront, and the removal of the Physical layer made sense because that seems to be the layer that would be the least changed over time. When learning a new concept, its always easier to add complexity as needed than to learn said complexity, and then retract from it.