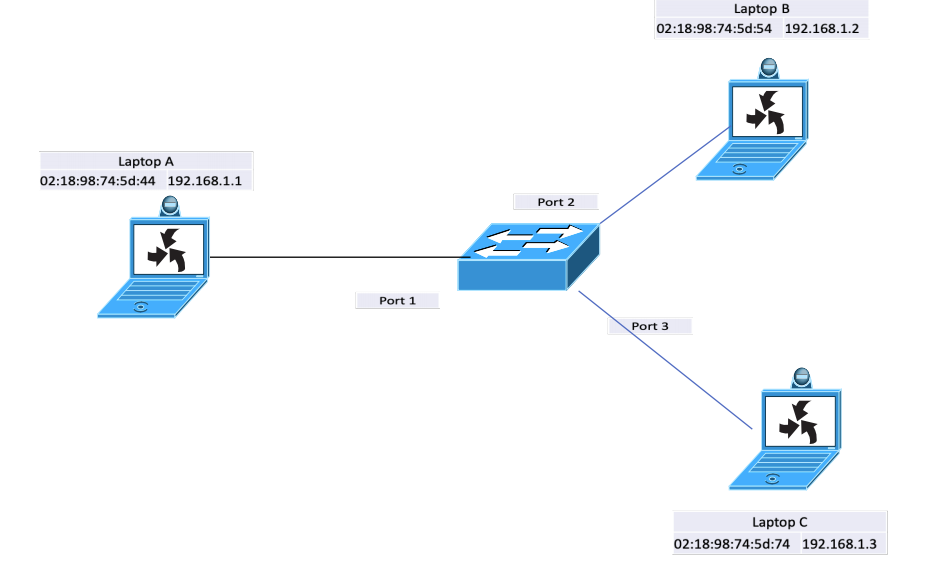
CS-GY 6843 Spring 2021 Midterm

Last Name: Vo First Name: Brandon \_Net ID:\_bdv9527

1. Refer to the following diagram with 4 elements:



1. (5 pts) Identify the broadcast domain(s) by listing the networking elements that make up the broadcast domain

These three laptops appear to share the same subnet. The three laptops share the same ethernet network, so they all share one broadcast domain.

1. (5 pts) Identify the collision domain(s) by listing the networking elements that belong to each collision domain.

There are three collision domains where each collision domain of A, B, and C are all separated by the switch in the middle.

This is because the switch separates collision domains into different ports. A, B, and C have their own different ports to separate the collision domains.

1. (10 pts) If laptop A issues an ARP Request for 192.168.1.2 what do each of the elements learn, if anything? Identify the protocol steps (layer2 & layer3) and addresses. What is stored in the ARP tables of each host and the CAM table of the switch?

Laptop A issues a layer 2 ARP request to laptop B. This ARP request will ask for the mac address associated with the IP address of 192.168.1.2 as well as give out the details of Laptop A’s MAC address and IP address. This ARP request is broadcasted to the ethernet’s entire broadcast domain. When the switch receives A’s message, it will flood it to the entire broadcast domain, meaning laptops B and C will receive A’s ARP request. The CAM table associates port 1 with Laptop A’s MAC address.

Laptop C will read A’s ARP request and record Laptop A’s MAC address on Laptop C’s ARP table, but it will also drop A’s request because the requested IP address does not match C’s IP address.

Laptop B will receive A’s ARP request. Laptop B will record A’s MAC address onto its ARP table and check if the requested IP address matches B’s IP address. Once it confirms the match, B will create an ARP reply message containing B’s IP address and MAC address. B sends this message via layer 2 as a unicast message.

The Switch’s CAM table

|  |  |
| --- | --- |
| Port 1 | 02:18:98:74:5d:44 |
|  |  |
|  |  |

The CAM table record’s A’s MAC address before flooding all ports.

A’s ARP table is empty as this stage as Laptop B hasn’t replied yet.

B’s ARP table:

|  |  |
| --- | --- |
| 02:18:98:74:5d:44 | 192.168.1.1 (Laptop A) |

B receives A’s ARP request and writes A’s IP address and MAC address.

C’s ARP table:

|  |  |
| --- | --- |
| 02:18:98:74:5d:44 | 192.158.1.1 (Laptop A) |

C receives A’s ARP request because the message was broadcasted into the entire domain, so C records A’s MAC address and IP address.

1. (10 pts) If laptop B sends an ARP Reply to laptop A what do each of the elements learn, if anything? Identify the protocol steps (layer2 & layer3) and addresses. What is stored in the ARP tables of each host and the CAM table of the switch?

The switch receives B’s ARP reply and associates B’s MAC address to Port 2. B is aware of Laptop A’s port in its CAM table, so it will forward the message directly to A. Nothing is sent to port 3. Laptop A receives B’s ARP reply and IP address. Laptop A records B’s IP address and MAC address into its ARP table.

CAM Table of the switch

|  |  |
| --- | --- |
| Port 1 | 02:18:98:74:5d:44 (Laptop A) |
| Port 2 | 02:18:98:74:5d:54 (Laptop B) |
|  |  |

The CAM table doesn’t hold anything for port 3 or laptop C because it never got a message from C.

A’s ARP Table

|  |  |
| --- | --- |
| 02:18:98:74:5d:54 | 192.168.1.2 (Laptop B) |

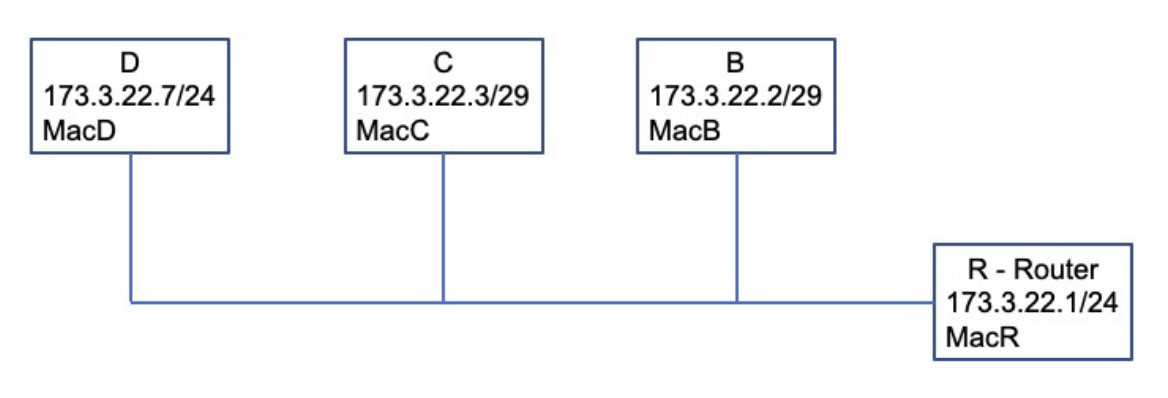
B’s ARP table

|  |  |
| --- | --- |
| 02:18:98:74:5d:44 | 192.168.1.1 (Laptop A) |

C’s ARP table

|  |  |
| --- | --- |
| 02:18:98:74:5d:44 | 192.168.1.1 (Laptop A) |

1. (10 pts) In the following network diagram, all computers are on the same shared Ethernet segment. If B sends an ICMP Request to 173.3.22.7 what does each of the hosts learn and how do they respond?



D’s /24 subnet is includes the IP address range of 0-255 for the subnet mask. When B and C share the same subnet mask, that means D’s subnet is overlapping with C and B.

When B attempts an ICMP request to D, it will first check to see if B has a MAC address associated with the IP address. If B doesn’t see one, it will send an ARP broadcast through the subnet. This ARP Request will reach C where C will record B’s MAC Address and IP address. Router R will receive B’s ARP request and send it out on all ports. This allows D to receive B’s ARP request. D will record and associate B’s MAC address and IP address received from the ARP request. D will then send a unicast ARP reply to B, but because B is within D’s subnet range, D can send its ARP reply directly to B.

B will then receive D’s MAC address and record D to its ARP table. B will then have to send the ICMP request itself and checks D’s subnet mask and notice that it doesn’t match. This is because while B is inside D’s subnet, D is outside of B’s subnet.

B will need the assistance of the router R. B will check Router R’s subnet mask and see that it matches with B. B can check if R is in B’s subnet range which it is, so B encapsulates the ICMP request within an Ethernet frame and send it to Router R.

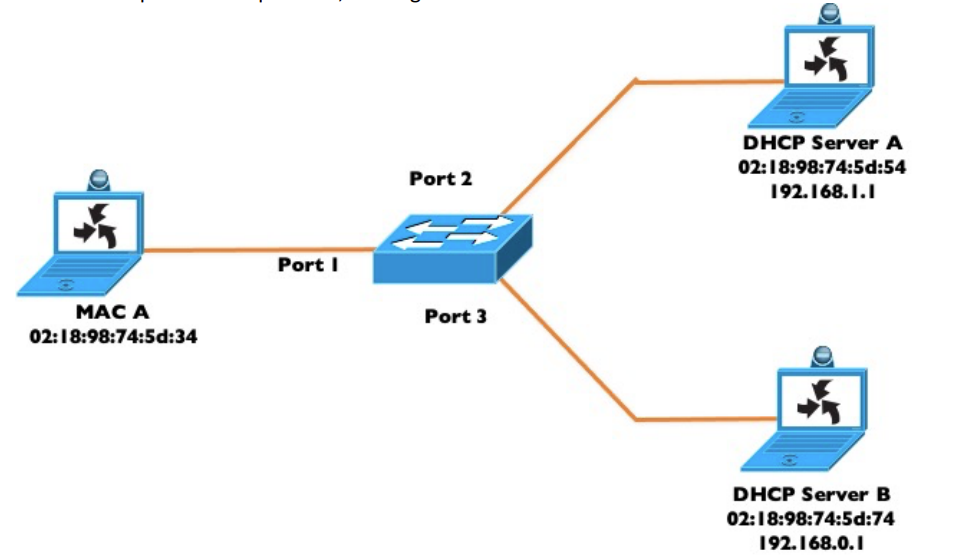
Router R will receive the message and check for the location of D. It will check the subnet mask and find that D is within R’s ethernet line. R will check the IP address to see that D is indeed within range and send B’s ICMP message to D.

Once D receives B’s message, it will unravel the message and read B’s ICMP request. It will create its own ICMP reply message, encapsulate it within an Ethernet frame and check the ARP table for B’s MAC address and IP address.

Because D already recorded B’s MAC address, it will send the ethernet frame directly to B instead.

C learns about B’s MAC Address from the ARP request but drops the message. B learns about D’s MAC address from its ARP reply and D learns about B’s MAC address from the ARP request.

1. (20 pts) Describe the DHCP operations that occur when MAC A wants to obtain an IP address. Be specific as to protocol, messages and addresses.



Mac A starts with no IP address, so it needs to receive one from a DHCP server. It doesn’t know what is on the network, so it has to broadcast a DHCP Request to the ethernet network. The DHCP request message will contain the source IP address of 0.0.0.0 sent to broadcast address of 255.255.255.255 along with A’s MAC address. The 0.0.0.0 IP address is because MAC A has no IP address, so it has to use an agreed upon address designated as the localhost. The port will receive this message and flood all ports with this message. It will also associate port 1 with the MAC address of A.

DHCP Server A and DHCP Server B will receive A’s DHCP request message. They will respond by sending their own DHCP offer message. This message contains an IP Address within their possible range along with a lease timer. The IP Address being leased out along with other settings are granted by what configurations the DHCP servers had set up prior to providing IP Address leases.

Guessing from DHCP Server A’s IP address and range, it will offer to lease an IP address of 192.168.1.2 or higher while DHCP B will send an offer for an IP address of 192.168.0.2 or higher. Once DHCP A and DHCP B send their offer message, a timer begins where if there is no response by the time the clock finishes, the lease is automatically rescinded.

These DHCP offer message are received by the switch which forwards it to port 1 back to Mac A. Mac A receive the DHCP Offer and chooses which one to accept. Usually, the first DHCP offer received is the one chosen. Mac A responds by echoing back the DHCP offer message. Mac A writes a DHCP Reply which contains the IP Address configurations of the offer that Mac A received. Mac A broadcasts the DHCP reply message to all ports to ensure that any offer offers are dropped.

This gets sent to the switch which sends it out to all ports again due to the broadcast. DHCP A and DHCP B gets this reply and check to see if the configurations match the offer they sent out. If one does not see a match, then they rescind their original offer and reclaim the IP address they offered. The server that does see a match will respond with a DHCP Acknowledgement message back to Mac A to confirm that Mac A can use the address.

The switch picks up the DHCP ACK message and forwards it to port 1 to Mac A. Mac A receives the DHCP Ack message and now beings using the IP Address given to it.

1. (10 pts) traceroute is a program that shows all the routers (IP address) an IP packet goes through to reach its destination address. Knowing the IP packet data structure and the IP protocol explain how traceroute works.

Traceroute is a program that takes advantage of ICMP’s TTL function. It sends an IP packet with the intended destination IP address, but it starts by sending a packet with a TTL of 1. In ICMP, the TTL is decreased every time the packet reaches a router. When the TTL reaches 0, the router that sees the 0 TTL will drop the packet and return an ICMP Time Exceeded error message to the source IP address.

This error message is sent to the source IP address, but it will also include the IP Address of the router that dropped the packet. When the source of the traceroute receives this message, it will learn the IP address of the router that the packet stopped at.

The goal of traceroute is to identify every router used to reach its destination. So during the traceroute program, the source will send a packet with a TTL of 1, receive info the first router that receives the packet. It sends a packet with a TTL of 2 and sees the second router that receives the packet. It will keep sending packets with one more TTL until it reaches its destination. Every router that receives a packet with TTL of 0 will return an error message and provide its own IP address.

This provides the source IP address with a list of all routers that every traceroute message jumps to on its way to the destination, effectively providing a path of every router it crosses on the way to the destination IP address.

1. (30 pts) Explain how TCP works; sequence numbers, ack numbers, receive window, sliding window, etc. You may use one or more diagrams to help with your explanation.

When a client needs to send a message to a server, they both need open sockets for open ports. Both sides open a send a