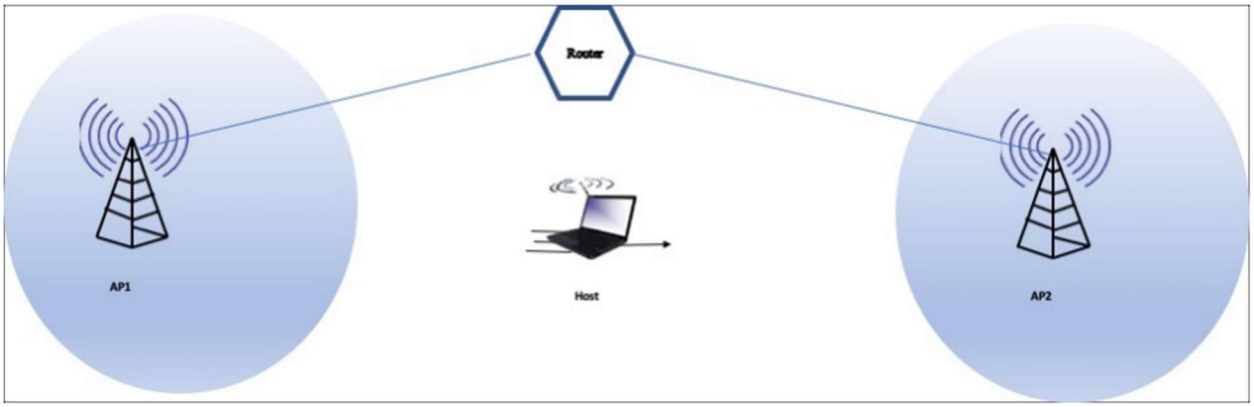
Vo, Brandon

CS 6843 Spring; 2021 Final Exam

Submit your exam in one file with your last name, first as the name of the file. Also put your lastname, firstname as the first line of your answer sheet. Type your answers so I can read them!

1) Wireless 802.11i



The Ethernet addresses of the AP1, AP2, Router and Host are respectively Mac1, Mac2, MacR and MacH. The IP address of the router is IPR

a) (5 pts) What values are in the ARP table of the host when it is associated with AP1?

Assuming the Host has spoken with the Router

IP Address	MAC Address
IPR	MacR

The host associates Access Points through their SSID and MAC address by listening to the AP beacon frames. While the host needs to know the MAC Address of AP1 to write an 802.11 frame, it can't record the AP's Mac Address into the ARP table because ARP is part of the 802.3 frame. The Wireless Access Points, however, do not have their own IP Address because APs are layer 3 devices that don't know what IP Addresses are or what ARP is. The purpose of an ARP table is to associate an IP Address with a MAC Address which cannot be done if there is no IP Address to associate with a MAC Address. Even though the host has to use the Access Point's MAC address in the 802.11 frame, the router isn't aware of the Access Point or that it's using a wireless line at all because the frame gets converted into an 802.3 frame. The host and the router will believe that they are directly connected using the Access Point as a bridge. The router will never see the AP MAC Address, and it will not care about the Access Point.

b) (5 pts) What values are in the ARP table of the host after it moves and is associated with AP2?

IP Address	MAC Address
IPR	MacR

In general, the host and router are not aware about their Access Points. When an AP transition occurs, it's usually done on the IP Layer, not the Ethernet layer. As far as the host and router are aware, the IP Address and the MAC Address of the host are still the same just on different interfaces, so it won't change anything. The host will still retain its original IP Address as well. The router will just see the message and assume that the host is on a different interface, and the host will not see a change with the router itself because both machines retain their IP Address and MAC Address. The router is self-learning, meaning that it will see a frame from the host in a different Access Point, but it will remember what port can be used to reach the host.

c) (5 pts) 802.3 can detect frame collisions while 802.11 is not. Why?

802.3 can detect frame collision because it's using the Ethernet as a medium which uses send lines and receive lines. In Ethernet, machines can listen into their channels before and while it is transmitting to detect if another machine is transmitting on the same line. In Ethernet, all hosts can see each other, and all hosts can listen into the Ethernet line before sending anything. Ethernet hosts can also detect a collision by measuring the time it takes for a message from the sender to reach the receiver and by listening into the Ethernet receive line before transmitting. It can identify a collision when a packet is being transmitted by time 2T.

802.11 cannot detect frame collisions, only avoid them. In wireless, not all machines in a network may be aware of each other, causing the hidden terminal problem. If not all machines are aware of each other, then there's a risk that the machines aren't even aware that they're causing an interference for another machine. In addition, wireless signals get weaker as it travels further away due to path loss. Collision detection requires the ability to send and receive transmissions at the same time which can't be done on radio waves. When the signal is weak, it's much more difficult or not possible at all to sense a collision.

802.11 can only prevent collisions using CSMA. One method is to have senders reserve available channels before sending any packets. All senders must listen into their channels to see if any other transmissions are being done before sending anything itself.

2) MPLS

a. (5 pts) In MPLS what is a circuit and how is it created? Be specific and refer to protocols.

A circuit is a network of links where the end-to-end systems reserve the necessary resources to sustain communications. To establish a circuit, the sender and the receiver must establish a connection to each other, both sides must maintain that state for the duration of the connection, and the channel they're using must maintain a constant transmission rate for the duration of the connection. MPLS uses end-to-end transmissions by creating virtual circuits in the network. Through virtual circuits, MPLS establishes a circuit by creating a series of paths that form a tunnel between the sender and the receiver.

In MPLS, a circuit is established when a sender wants to send a packet to a receiver. MPLS will use one of the two Signaling Protocols: Label Distribution Protocol (LDP) or Resource Reservation Protocol (RSVP).

Using LDP, it will behave similarly to ATM's One-Pass Method to establish a path. Before sending any messages, the source must find the destination and the path to reach the destination. The source will send a request to the Ingress node for a label to find the Egress node for the destination. The Ingress node will send a request to the next nearby node asking for a label to the Egress node. This repeats with every node sending a request until the Egress node is reached. The Egress node returns a label to inform the nearby

router what path to take. The next router applies a label to its path and informs the router before that one. The process repeats until the Ingress node is told what label to send to reach its destination, establishing a path from the sender to the receiver. The source will send a packet containing a label to inform the router where to forward the packet. That router will check its forwarding table to find the path and send it to each router. Each router will forward the packet until it reaches the Egress node which tears down the label before sending the packet to its destination.

Using RSVP with Traffic Engineering, the routers will determine the routing path based on a form of cost and bandwidth. RSVP checks for the best possible route that also has enough bandwidth to transmit the necessary information. For each router consulted to be used as a path, that router will return a label in an RESV message and reserve some bandwidth for the next and previous node to use. Because these routers are reserving bandwidth, it provides a guarantee that there is enough bandwidth to carry a message. RSVP-TE, similarly to circuits, provide a guarantee of service by reserving enough resources to carry a message from one end user to another end user. Labels are used to define the path needed to reach the other end, and this path forms a tunnel that allows both users to maintain a constant transmission rate using the reserved bandwidth pool. MPLS creates a virtual circuit which treats the sender and the receiver as though they're on a physical link and allow both sides to communicate through a wireless network. The sender will tear down its connection after finishing and the receiver receives the final message with the labels torn off, signaling the end of the MPLS connection.

Because MPLS also wants Fast Reroute, MPLS will precalculate a series of backup paths either one-to-one or many-to-one. For one-to-one, a backup path is established in case of a transmission failure while in many-to-one, multiple routes are shared as long as a backup has been prepared. This would create multiple different paths that will be consulted and used.

b. (5 pts) Why is label switching more efficient the routing?

In IP Routing, each hop has to find the next suitable router to hop to. This is done when the router receives a packet and has to extract the destination address. It will search the next available route by checking the longest matching prefix and the netmask of that packet to see if it's within range before choosing the next possible route to forward to.

For label switching, the route is established using a series of labels. When a path is established, each router stores a series of labels and what interface to forward to within a forwarding table. In routing, it is more efficient to use exact matches to identify a packet compared to IP Routing's prefix matching.

After establishing a route, all future routers will know where to forward a packet to if they see this address being used again, reducing the overhead of having to discover the next router. A label-switch router would only need to check the label in its forwarding table to know where to forward the packet compared to IP routing where the router would have to extract the destination IP address and perform a prefix match to discover where the next hop should be. This makes the label-switch forwarding table faster to consult because exact matching is more efficient and easier to implement compared to IP Lookups.

c. (5 pts) Why is routing more flexible than label switching? Or is it?

Label switching has the overhead of having to carry labels in a network. Label Switching hides any topologies that aren't the optimal path or a backup path. The source node also has to set up a connection and tear down the connection before and after sending a message to its destination through a set of predetermined set of routers which only change if a backup is needed.

Vo, Brandon

IP Routers work independently from one another. Each router makes its own decision on where to forward a packet, checking primarily to see if there is a neighboring router to forward to. This allows multiple paths to be viable if a router holding the packet chooses that particular path.

3) (5 pts) What netmask is used to specify an IP Multicast Group.

IP Multicast is not related to IP subnets, so Multicast group addresses themselves do not use subnet masks.

All Multicast IP Addresses also share the same first four bits of 1110 in order to utilize the Class D range, so all multicast IPs must start with 1110. This is to ensure that we can use the class D range of 224.0.0.0 up to 239.255.255.255 range.

4) (10 pts) for a multicast group consisting of one source and two listeners, all within the same IP subnet; for each IP packet sent out by the source how many IP multicast packets are generated for the listeners? How many Ethernet Multicast frames are generated? Explain.

The source sends out an IP multicast packet to all of its neighbors. When the listeners receive the packet, they will replicate the packet and send it to other interfaces except the interface where it received the packet. This means that the source will send its packets to both listeners. Then, the listeners will apply Reverse Path Forwarding and Flooding where the listeners will attempt to forward the packet to the other multicast group listeners. Once both listeners receive the packet from the source, they will duplicate the packet and forward it to its other interfaces, sending the packet to the other listener.

Under Reverse Path Forwarding and assuming that the listener and source are all connected, the source will generate an IP packet and broadcast it on all interfaces to the two listeners. These listeners will recognize the source as the shortest unicast path from the source node. The two listeners will attempt to send the packet to the other listener by duplicating the packet and sending it to all lines except for the line where it received the packet from.

The source node won't receive anything. The two listeners will send each other duplicates of the source node's packet, but they will drop the packets because they will recognize the duplicate packet to not be from the shortest unicast path.

- Reverse Path Forwarding:
- Host creates one IP multicast packet and floods it on all of its interfaces
    - Source sends out the packet only once.
- The two listeners receive the packet, duplicate it, then forward the duplicate packet to any other listeners
- The listeners both receive duplicate packets from the other listener and drop the packet because it did not come from the shortest unicast path to the sender.

When the source sends out an IP packet into an interface, the IP Packet will be embedded into a single Ethernet Multicast frame. That one frame will get carried out into the network similarly to a broadcast where everybody sees the frame, but only machines within the group will read the message.

5) (5 pts) Explain how the Administrative Address is set in OSPF

OSPF routers are identified using a Router ID which can be represented by an Administrative Address. If not manually specified, then the router will check its interfaces for the highest IP Address to serve as the Administrative Address and the router ID.

In the event that the Administrative Address is unavailable to use, then the router will have to check its remaining interfaces for the next largest IP Address that can be used. The next largest IP Address becomes the new Administrative Address. In addition, the Administrative Address can be manually set by the user and are used to serve as an IP Address which never goes down.

6) Explain what the IP address 0.0.0.0 means in the following and give examples

a. DHCP-

In DHCP, the host machine needs to acquire an IP Address but needs a way to label itself. The host machine uses a source IP Address of 0.0.0.0 to identify itself as a machine that is looking for an IP Address and broadcasts its DHCP Discovery and DHCP Request messages using this IP Address. The DHCP server which receives this message responds with its DHCP Offer which will direct itself back to the host machine. The host machine has to respond with a DHCP Request message but it still has to use the 0.0.0.0 source IP address because it still needs to confirm that the host machine wants to use the IP address provided by the DHCP server.

b. OSPF-

While machines in OSPF have their own addresses, the routes chosen by the machines in an area through priority. Priority is determined by the largest matching size of an IP address of the next router to send to. 0.0.0.0 is an address route that has the lowest priority to send to because it has the smallest address and is identified for all networks. This makes 0.0.0.0 the default route used by an OSPF router if there are no available routes to choose from.

When an OSPF network is being set up, a router can inject a default route into its area by advertising the address 0.0.0.0 into the OSPF domain. This will behave similarly to the command of **default-information** when advertising the default route to the OSPF area. Usually, when trying to forward packets to machines outside of the area, these packets will be sent to the default route. The default route usually leads to a router that can transmit a packet between areas, so border routers will typically advertise the default route of 0.0.0.0.

7) In DNS

a. (5 pts) What is an A record and how is it used?

An A record in DNS represents the host address. It translates domain names into IP Addresses.

R1 IN A 10.10.10.1

This identifies R1 as the name of the server holding the IP Address of 10.10.10.1 when searching within the domain of cn.

b. (5 pts) What is a NS record and how is it used?

An NS record identifies the domain name for a host that is running a name server. Hosts running as an NS will be responsible for resolving names and associating them with IP Addresses for a specified

domain. It identifies the authoritative DNS servers for a zone. NS-records will identify the names of a DNS server and delegates parts of the domain of that server to other DNS servers.

@ IN NS cn.

Above identifies the local machine as the NS record for the domain of cn. This informs other machines that this machine is the authoritative DNS server for that domain.

Because NS identifies the name of a DNS server, it still needs an A-Record to identify the server's IP Address. An A-Record is needed alongside the NS record.

c. (5 pts) What is a PTR record and how is it used?

PTR represents the pointer record. In reverse-DNS zones, pointer records do the opposite of A-Records where they map an IP address to the domain name. This allows for a reverse mapping by associating an IP address with a host name.

<IP Address> IN PTR R1.cn.

Reverse DNS Zones map IP Addresses to domain names unlike A-Records. Reverse zones help identify incoming machines and where they are coming from. A PTR can be used to identify a machine holding a particular IP Address and what name it has been given.

d. (5 pts) What is a MX record and how is it used?

MX is used to represent a Mail Exchange server. Similarly to NS, the host with this label is responsible for running a mail server which handles messages sent within that domain.

Example.com IN MX 60 mail.com mail.example.com

This indicates that emails sent under the example.com domain should be redirected to mail.example.com. After finding the MX server, DNS will check for an A-record that matches the IP address to the server using the mail-server name, so an A-record is needed alongside the MX record.

e. (10 pts) Describe Recursive vs Iterative DNS?

Iterative DNS is when the client and DNS servers will continue exchanging information which each other until the client receives the full name. The client will send a message asking for an IP Address associated with a name. If the server doesn't have the name, it will refer the client to check another DNS server that may have the answer. The process begins when the Root Name Server will strip off the section of the request that holds the subdomain that the Root Name server is aware of. The server will return the stripped message to the client and refer it to another name server within the Root Name server's subdomain. The client will ask the next DNS Name server using the stripped message. The Name Server will check the message and see if it has the requested domain. If it doesn't have the full name but it recognizes one of the subdomains, it will strip that part of the message and return the message back to the client, referring it to another DNS Name Server within that Name Server's subdomains. The process repeats until the final DNS Name Server matches up with the final parts of the stripped message. It will be a full match

Recursive DNS begins similarly with Iterative DNS where the client will send a message requesting the IP address associated with a requested name. However, the burden of discovering the match will be placed entirely on the DNS Server. When the Root Server receives the request, it will find the appropriate child name server in the subdomain. If there is an appropriate name server, it will strip the message of the

matching part and pass the message down to the appropriate name server. The next name server will see the stripped message, finding the matching part, strip that part of the message, and search for the appropriate name server within its subdomain and pass it down to the next name server. This process repeats until the final DNS server matches with the stripped message and returns the appropriate query. The resolution gets passed up to the previous name servers until it reaches the Root Name server. The Root Name server will return the full query back to the client. The server will look through its subdomains, collecting the names until it reaches the end or a full match where it will return the entire query back to the sender.

Recursive method puts the burden on the server. The server is responsible for gathering information for the entire name while iterative is focused on making several exchanges with different servers.

f. (5 pts) Describe a situation where one might be more favorable than the other.

Recursive Resolution would be better for long-distance work where there is a risk of high latency. This is because the Name servers are closely associated with each other and can quickly grab the necessary info to return to the client. In Iterative DNS, this would create more overhead because the client would have to constantly exchange messages with the other DNS servers over long distances before getting the entire name.

Iterative is better in terms of alleviating the burden on the DNS servers. Recursive puts the burden of finding the associated IP Address on the DNS servers while Iterative puts the burden on the client. It is up to the client to consult the DNS servers to find the appropriate address. In Recursive, the DNS server has to consult multiple other DNS servers to find the query, this requires overhead because each name server has to ask and wait for the next DNS server to return a reply. In Iterative, the DNS server would refer the client and move on to the next request. In terms of caching, this puts a higher demand on the DNS Servers to maintain their own caches of recently acquired query responses whereas in Iterative, the client would be able to retain its own cache of queries received from the DNS Name servers. Recursive DNS Name Resolution would be faster for this type of query but would put more performance cost on the DNS Servers than Iterative would.

g. (5 pts) In your DNS lab, was your DNS server authoritative for cn? Explain

A DNS Server is authoritative if it is responsible for storing and providing information about the name space within a zone. DNS servers that load a complete zone are authoritative for that zone. R1 is responsible for providing all the names to the machines in Area 0; R1 is the authoritative server for cn. In the same manner, R2 is the authoritative server for second.cn. because R2 is responsible for providing names to every router in area 2.