Question 1 (IP Addressing and Subnetting)

Assume you have two hosts, A and B, in a subnet 214.29.0.0/24. The subnet consists of an Ethernet. Assume you have a third host C that does not have an Ethernet (Ipad? ☺) and you want this host to be able to communicate with A and B. B and C have 802.11 (wifi) connectivity, so they can be configured to talk to each other (manually most likely).

a) Assuming that 214.29.0.0/24 are the only addresses available, if you configure the wifi between B and C as a subnet, what does that do to the number of addresses available for the Ethernet?

The number of addresses available for the Ethernet is now half, because you have to break 214.29.0.0/24 into two blocks of size /25. I.e. just trying to add one more host has cost you half of your IP addresses. There is however another alternative where you actually give a /31 to the WiFi, but then you have to give multiple subnet numbers (a /25, a /26, a /27, etc up to /31) to the Ethernet, but this is frowned upon, i.e., having multiple subnets per physical network can get confusing.

b) Instead of creating a new subnet, an alternative method for connecting C is to use proxy ARP and routing and to give C an address from 214.29.0.0/24. I.e., B agrees to route traffic to and from C and also answers ARP queries for C received over the Ethernet.

i. Give all packets sent, with physical addresses, as A uses ARP to locate and then send one IP message to C.

ARP REQ sent by A has the fields
- IP Source: IP Addr A
- Target IP: IP Addr C
- Physical Address of Source: Phys. Addr. of A
- Physical Address of Target: Emtpy

ARP REPLY sent by **B ← careful, it is B not C**
- IP Source: IP Addr A
- Target IP: IP Addr C
- Physical Address of Source: Phys. Addr. of A
- Physical Address of Target: Phys. Addr. of **B ← careful, it is B not C**

IP Message from A to C
- IP Source A
- IP Dest C

Ethernet header of the IP message from A to C
- Ethernet Source A
- Ethernet Destination B

ii. What peculiar change do we have to do to B's routing table to implement this?

Since the wifi is not a subnet per se, and we are making C appear to be on the Ethernet (even though it is not) we have to add an entry in B's routing table that matches the entire address of C, i.e. the IP address of C with a mask of /32. The entry of course points to the wifi as the next hop. Note that this works because of longest prefix match.

Question 2 (CIDR)

Consider CIDR. Assume that routing domains (i.e. ASms) advertise address blocks (i.e. network numbers in CIDR) even though a subset of the addresses contained in the address block is not contained within the routing domain.

Show me a scenario in which packets are routed to the wrong domain because of this.

Consider two service providers P and Q. Each has a block of addresses Pblock and Qblock. P has X as a client, so X has a block of addresses Xblock that are a subset of P's. X moves to Q (without renumbering), hence Q advertises its own block Qblock and that of X, Xblock, while P advertises only its original block, Pblock.

So far, we have the scenario that we discussed in class and all is well. Now, assume X has a subclient A, and Ablock is a subset of Xblock. Let A now move to P without renumbering. Note that Ablock is contained in Pblock, so P simply continues to advertise only Pblock (allowed by the rules of the question).

In this case, because Q advertises Xblock and P advertises Pblock, then anything for A will arrive to Q and not to P.

Question 3 (Internet Basics)

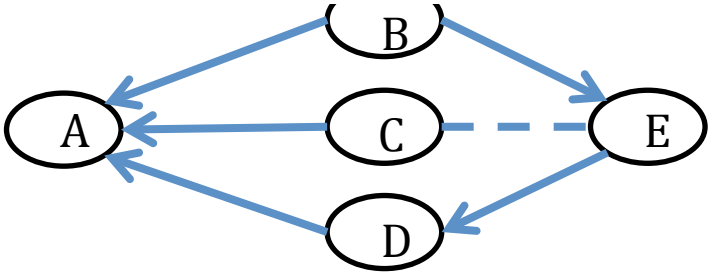
(a) Why do routers at the core of the Internet need to be aware of network numbers and not just autonomous system numbers?
Because AS numbers are not included in the IP header, and there is no relationship between IP network numbers and AS numbers.

(b) Why usually do all the routers within an AS at the core of the Internet speak BGP (i.e. all routers within a core AS must speak BGP)
Because they must be aware of all network prefixes in the world, and if only the border routers speak BGP then the network prefixes have to be injected into OSPF, and OSPF is unable to handle such a large number of networks.

(c) Give me two reasons why BGP advertise the entire AS-path to the destination (as opposed to simply advertising the number of AS-hops to the destination).
First: to avoid loops (don't follow a path if you are already contained in the path)

Second: implement flexible routing policies. By knowing the path you can decide if you like or not (not just if you like your neighbor from where you received it)

(d) In a LAN (such as Ethernet) why is it necessary for the LAN to be able to do a broadcast if we are considering including the LAN into the Internet (i.e. run IP on the machines in the LAN).
To do ARP, that would be the main reason.



Question 4: Routing Policies

Recall that in inter-domain routing, the main issue is to enforce financial relations between different ASes. Typically, an ISP (i.e., a network provider) tries to maximize its monetary gain by providing service and a customer network tries to minimize its expenses. Based on this general comment, consider the above network segment that shows five autonomous systems (ASes) having BGP neighboring relations. The specific relations among them are as follows:

i. B is a provider of both A and E
ii. C is a provider of A but is a peer of E
iii. D is a provider of A but is a customer of E

Consider a BGP route advertisement that originates from A and reaches E thru B, C, and D.

a. Considering the relations between E and its neighbors, which one of these updates E would be willing to accept/adapt and why?
b. How would you as a network administrator of E configure your BGP routers to enforce your decision above?

Consider the data traffic from senders in AS A for destinations in AS E.

c. What is the AS level path that E would prefer for this data traffic to reach itself, i.e., which of its neighbors E would prefer to receive this traffic from (B or C or D)?
d. Do an internet search on "AS Path Prepending". With this knowledge, what can E do to cause the traffic to propagate on that desired AS level path?
e. What are the conditions that need to hold so that E can achieve this outcome for A-to-E traffic to flow on E's desired AS level path?

a. It would adopt the one from D as D is its customer and E can charge D for the traffic that it will send thru D.
b. The network admin would use Local Preferences (LP) attribute and assign a high value of LP to the routes coming from D and second highest to the routes coming from C and the lowest to routes coming from B.
c. E would prefer D to forward that traffic to itself as E could charge D for carrying that traffic on the link.

d. E can try the trick of artificially extending the length of ASPATH attribute by including its AS number multiple times to make it look longer when it sends the BGP route advertisements on E-to-B and E-to-C links but not do so on the advertisement that it sends on E-to-D link. This way, when A receives the three routes, the ASPATH length on the one coming thru D would be the shortest. If A is choosing its routes based on shortest ASPATH length attribute,

then it could choose the one coming from D.

e. The requirement is that A is not using Local Preference attribute or this attribute values are the same for each route and then A falls back to using ASPATH length attribute for route selection.

Question 5 (Dispute Graphs)

a. Consider the system in slide 27 of the BGP divergence slides (the sytem with a single solution and node 5 ends with an empty path). Draw the dispute graph for this system (NOT the dispute wheel)

I will not draw the graph because I am typing this. Put all the following together and you have the graph.

Transmission edges:

30 ---> 130
10 ---> 210
20 ---> 420
210 ---> 5210

Conflict edges:

130 → 210
210 → 420

b. Add a path 3 1 0 at node 3 and make it higher ranked than 3 0. Show me the dispute graph of this new system.

We have the same edges as before, but we now have some additional edges:

Transmission edge 10 --- > 310

Conflict edges:

310 → 130
130 → 310
310 → 420

c. Two parts (justify your answers)
   i. Does the system have a stable state?

      Yes, the state in slide 27 is actually a stable state of this new system. Adding the path 310 does not change this.

ii. Does the system converge? (i.e. always reach a stable state?)

This one is a little trickier. Think of the three nodes 0 1 and 3 and a small "subsystem" of the whole system. The paths that they take have nothing to do with 2 and 5.

Thus, nodes 0 1 and 3, form basically a "disagree" type of graph (slide 28).Thus, it will stop either by 3 having path 3 0 and 1 having path 1 3 0, or it will stop with 1 having path 1 0 and 3 having path 3 1 0.

Consider now node 2. If node 1 stops at 1 3 0, then node 2 will stop at 2 0. If node 1 stops at 10, then 2 will stop at 2 1 0.

Consider now node 5. If node 2 stops at 2 1 0 then 5 stops at 5 2 1 0. If node 2 stops at 2 0 then node 5 stops with the empty path.

Question 7: Ethernet Multicast

a) Why is it necessary that membership reports be flooded throughout all network segments? Briefly explain.

It is necessary to flood membership reports to all network segments because the location of the receivers is not known initially, and furthermore, a source can appear in any LAN segment at any time. Hence, ALL bridges need to know in which direction are the receivers located.

BTW, recall that bridges are always organized in the form of a tree, so there is only one path between any two nodes in the extended LAN.

b) Assume that instead of the algorithm presented in class for Ethernet multicast, we do a flood-and-prune approach as in DVMRP. Would this be possible (it is not implemented like this of course, but could it be done? If not, explain why not, if yes, explain in general terms how this would work (the steps that would be necessary in this new protocol)

To do a flood and prune, when a source sends a message, each bridge forwards the message in all directions (a flood). The message does not go around in circles because extended LANS are always a tree.

Receivers could generate membership reports periodically. In this case, reports are NOT forwarded by the bridges (in the same way that IGMP messages are not forwarded by routers)

If a bridge does not need the multicast, it can send a non-membership report to the bridge from whom the multicast messages are arriving. You can come up with some format for the NMRs as long as it is not confused with a regular unicast message

The only thing left over is for a bridge X to know if it has received enough NMRs from an adjacent LAN to stop sending the multicast to that LAN. To do so, it needs to know how many other bridges are on that LAN. If it receives an NMR from all of them, it can stop sending multicast messages over than LAN and send an NMR to its own parent (the one that sends messages to X, i.e, the bridge along the path from the source S to X).

To know how many bridges are on the LAN segment, we could have each bridge periodically broadcast a "hello" message of some type on the LAN segment. The bridges would not forward this message anywhere. It would be simply used to count how many bridges are on the LAN segment.

Question 8: Reverse Path Flooding

a) Consider reverse path flooding (RPF) in a network with point-to-point links (what we covered in class). Assume that you also know that your unicast routing is based on distance vector routing (basic distance vector routing without split horizon/poisoned revers). Assume that each link has a positive (greater than 0) cost. Taking this into consideration, how can you improve the efficiency of RPF (i.e. reduce the number of messages it transmits?)

   You want to avoid sending broadcast messages to neighbors who will throw them away (who are not your children on the tree). Let node X have a neighbor Y, and the cost of the edge (X,Y) is c. If the distance vector from Y says that the cost of Y to the source S is not equal to the cost of X to S plus c, then Y is not a child of X. In this case, don't forward broadcast messages to Y.

b) Same as a) above, except that now your unicast routing protocol is link-state routing.

   If you use link-state routing, and assuming that all nodes break ties the same way (most likely true), then all nodes can compute the broadcast tree (shortest path from S to all other nodes) and hence they will not forward a broadcast message to a node if it is not a child. Basically, this is what MOSPF does, except we are talking broadcast not multicast.

Question 9: DVMRP

Consider the collection of subnets below (the blue boxes are routers, the subnet "name" is along side of it i.e. A, B, etc). You can break unicast next-hop ties in alphabetical order (i.e. LAN X wins as next hop over LAN Y if both are equidistant to the source), for determining the parent of the LAN, break ties in favor of lower router number.

i. In Reverse Path Broadcasting (RPB), identify for each LAN, which router is the parent router of the LAN with respect to source S.
ii. In Truncated Reverse Path Broadcast, indicate which LANs are leaf LANs, and which leaf LANs will be truncated.
iii. In Reverse Path Multicasting (basically the full-blown DVMRP), identify which routers send Non-Membership Reports, and to whom do they send them.
iv. After pruning, identify the LANS over which multicast messages from S are sent to group

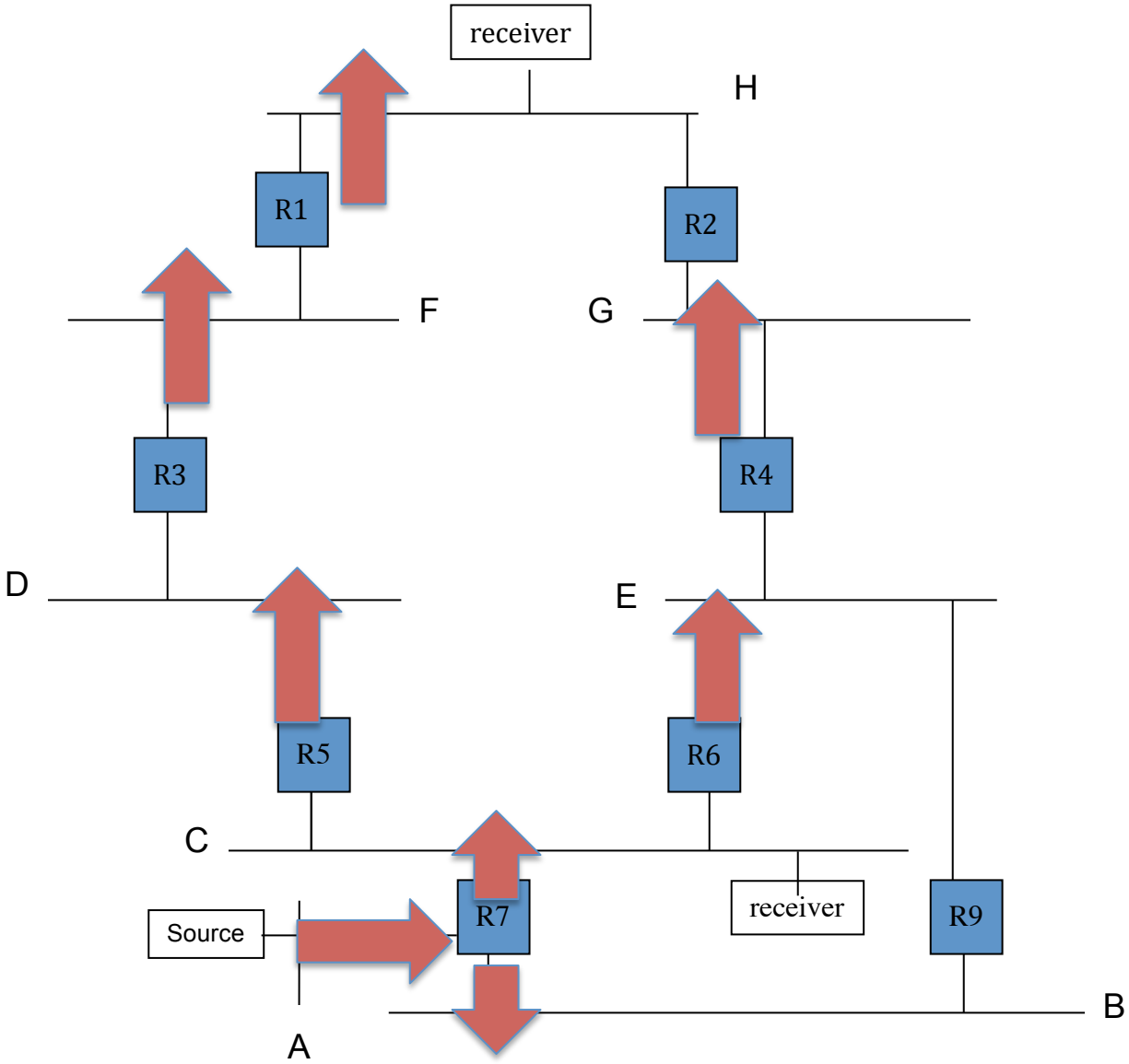
i. LAN A: Parent : Source
   LAN B: Parent: R7
   LAN C: Parent: R7
   LAN D: Parent: R5
   LAN E: Parent: R6
   LAN F: Parent: R3
   LAN G: Parent: R4
   LAN H: Parent: R1.

ii. Strangely enough, it appears that there are NO leaf links to be truncated. B is not a leaf link since R9 points to it as a next hop to source, and H is not a leaf since there is a receiver there)

iii. R9 sends NMR to R6
   R2 sends NMR to R4 (R2 has no child links)
   R4 sends NMR to R6 (because it received an NMR from R2)
   R6 sends NMR to R7 (got NMR from R4 and R9 is not using this link to get to source)
   R9 sends NMR to R7 (R9 has no child links)

iv. LANS: A, C, D, F, H

(SEE PICTURE ON NEXT PAGE …)


receiver
H
R1
R2
F
G
R3
R4
D
E
R5
R6
C
receiver
Source
R7
R9
B
A