Homework 2: Forwarding and Routing

Due: Monday, October 30 @ 11:59 pm EDT

Overview and instructions

This homework has 3 problems. Most problems involve writing a short response, or filling out some tables with your answers. You can write your responses in your own document or add annotations to this one.

Note on collaboration

You are welcome (and encouraged!) to collaborate with your peers, but the solutions you write down must be **your own work** (ie, written by you). You are responsible for independently understanding all work that you submit—after discussing a problem as a group, you should ensure that you are able to produce your own answers independently to ensure that you understand the problem. For more information, please see the course Collaboration Policy.

In your submission, we ask that you include a brief *collaboration statement* describing how you collaborated with others on each problem—see the next section for details.

How to submit

You will submit your work in PDF form on Gradesope. Your PDF should conform to the following requirements:

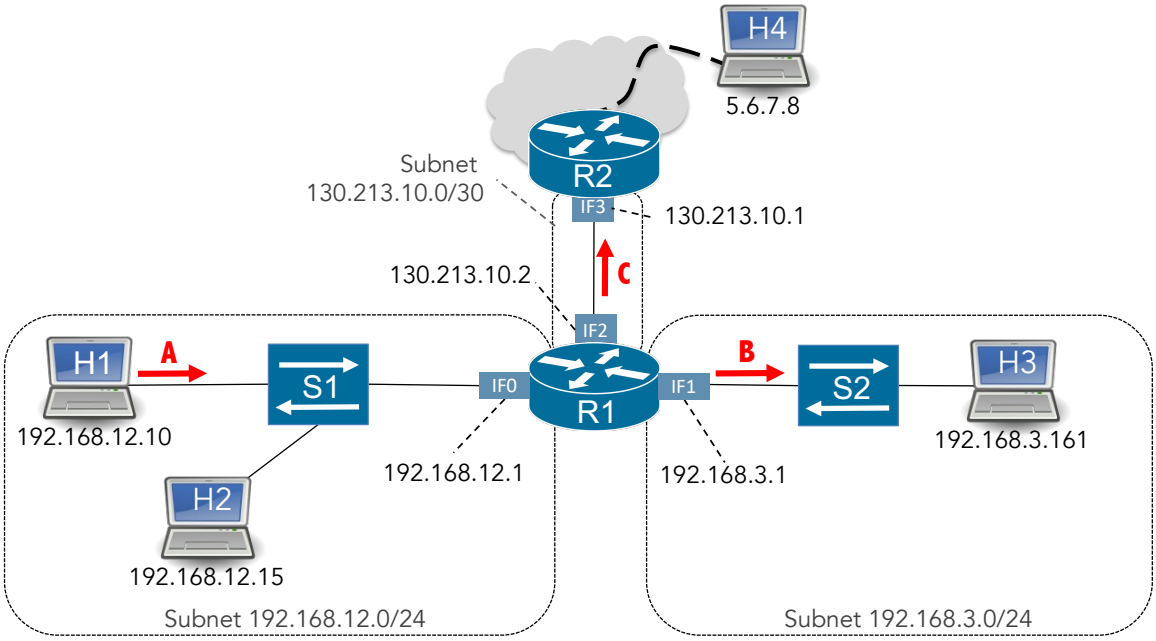
- Please **do not** include any identifying information (name, CS username, Banner ID, etc.) in your PDF, since all homeworks are graded anonymously
- Each problem (where "problem" is one of the Problems 1–4) should start on a separate page. When you submit on Gradescope, you will be asked to mark which pages correspond to which problem
- At the start of each problem, write a brief *collaboration statement* that lists the names and CS usernames of anyone you collaborated with and what ideas you discussed together
- If you consulted any outside resources while answering any question, you should cite them with your answer

1 Almost Local Networks

(Relevant lectures: Lectures 7–8)

Consider the network pictured below, which has two private subnets connected to router R1 via Ethernet switches S1 and S2. R1 also connects both subnets to the Internet using Network Address Translation (NAT), as the 192.168.0.0/16 prefix is not routable on the Internet.

Assume that all hosts are configured correctly with an IP address, network mask, and default gateway to match the figure. Additionally, assume that the router's forwarding table is configured appropriately to access both private subnets and the Internet (using NAT).



a) First, H1 sends an IP packet to H3. (Assume that this sends an ARP request, which happens successfully.) For the IP packet, write the source and destination addresses in both the L2 (Ethernet) and L3 (IP) header when it is crossing the link labeled **A** in the figure. For MAC addresses, you can use names based on the name of the host or router interface, eg. `MAC_H1` for H1, `MAC_IF1` for R1's IF1, etc.

	Src Addr	Dest Addr
Ethernet	**`MAC_H1`**	**`MAC_IF0` (Interface on R1)**
IP	**192.168.12.10**	**192.168.3.161**

b) Router R1 is a cheap model and can only hold 4 entries in its forwarding table. Given that it has to route packets to both local subnets, and to the entire Internet (including H4), what are the entries in R1's forwarding table? (Assume a default route has already been provided, as shown.)

Destination Network	Out Port/Next Hop
192.168.12.0/24	**IF0**
192.168.3.0/24	**IF1**
130.213.10.0/30	**IF2**
0.0.0.0/0	130.213.10.1

c) Similar to part (a), write the source and destination addresses in both the L2 (Ethernet) and L3 (IP) header for the IP packet when it is crossing the link labeled **B** in the figure. (Again, assume any relevant ARP queries are made and handled successfully.)

	Src Addr	Dest Addr
Ethernet	**MAC_IF1 (R1)**	**MAC_H3**
IP	**192.168.12.10**	**192.168.3.161**

d) Now H1 wants to send a packet to H4, which is a server out on the Internet. Note that R1 uses NAT to send the outgoing packet, as the 192.168.0.0/16 addresses are not routable on the Internet. What are the source and destination L2 and L3 addresses for this packet when it is crossing link **C** in the figure?

	Src Addr	Dest Addr
Ethernet	**MAC_IF2 (R1)**	**MAC_IF3 (R2)**
IP	**130.213.10.2**	**5.6.7.8**

e) **True or False**: If H1 moved to the same subnet as H3, it would need to change its IP address before it could receive any packets. **Explain why or why not.** You answer should be at most 1–2 sentences.

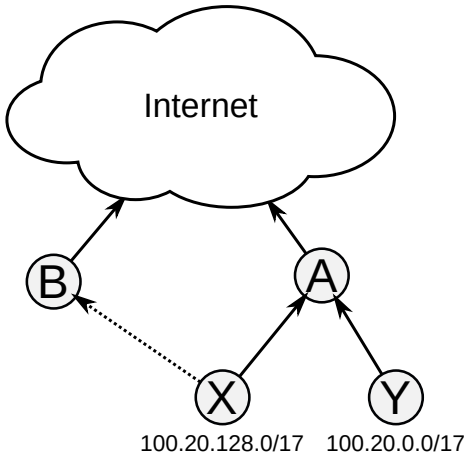
True. The IP address represents where the device is located on the network. If it kept the same address, it wouldn't be able to receive packets on the new network.

2 BGP Scenarios

(Relevant lectures: Lectures 10–11, start of lecture 12)

Looking at the figure below, where nodes are ASes, arrows represent customer-provider AS relationships. Assume that ASes follow the Gao-Rexford model we discussed in class, and that ASes A and B eventually learn all of the advertisements that the other one makes, through their respective providers.

Warning: The arrows in the figure do not constrain the direction of traffic, they only relate to BGP announcements!



Answer the following questions about different scenarios that could occur given these AS relationships. For each question, your answer should be no more than 1–2 sentences.

a) What is the largest prefix that A can advertise to its providers, given that it has the two customers X and Y with the prefixes in the figure?

A can aggregate the prefixes for X and Y and advertise 100.20.0/16.

b) If X decides to also become a customer of B (creating the dashed line), what new prefix will B advertise to its providers? B will advertise X's prefix, 100.20.128.0/17.

c) **True or False**: If B and A decide to become peers, B will start advertising Y's prefix. **Explain your reasoning.** False. As a peer, B will learn about X and Y from A, but it will not advertise routes to them. If B did this, it would end up receiving transit traffic for X and Y, which is not in B's best interest.

d) Normally, X receives BGP announcements about Y from A, which allows nodes in X to know how to reach nodes in Y. When X becomes a customer of B (ie, when the dashed line is created), **does B receive a route to reach Y via X? Why or why not?** No. X will not export routes to A or Y to B, since B is a provider for X. If B advertised these routes, it would end up receiving transit traffic for A and Y, which is not in X's best interest.

e) Say the administrators of X were considering becoming a customer of B, but then decided not to do so (ie, no dashed line). B's administrators get mad and advertise X's prefix anyway, even though they have no link to X. If they do this, **what could happen to traffic sent to or from X?**This would be prefix hijacking. Assuming that other routers listen to B's advertisements, some traffic for X would get routed to B.

3 Conversations

Note: We will have covered all of the material we need for this problem after Lecture 13 on Thursday, October 19.

(Relevant lectures: Lectures 12–13)

You are the administrator for a small ISP. You captured a sample of traffic from a router that connects your customers and the Internet, which is shown in the table below (last column is blank for you to fill in):

Pkt#	Source		Destination		TCP Flags	Connection #
	IP	Port	IP	Port		
P1	1.2.3.4	44444	5.6.7.8	80	SYN	**1**
P2	1.2.3.4	55555	5.6.7.8	80	SYN	**2**
P3	5.6.7.8	80	1.2.3.4	44444	SYN,ACK	**1**
P4	1.40.57.33	55555	5.6.7.8	80	SYN	**3**
P5	5.6.7.8	33333	1.2.3.4	22	SYN	**4**
P6				...		

Answer the following questions based on the captured traffic info:

a) **How many unique TCP connections are represented by these packets?** To show your work, label each packet with a "connection number" such that packets from the same connection have the same number. (You can fill in the last column in the table, or just write something like, "Connection N has P0, P1, ...")

Marked on table above.

b) Assuming that all of these packets are for valid connections (ie, the destination eventually responds, etc.) **which IPs have open listen ports, and what ports are open?**
(Write your answer as a list of IP:port.)

5.6.7.8:80, 1.2.3.4:22

c) Say the host with IP 1.2.3.4 is a customer on your network. You want them to be able to access the Internet, but don't want them to be able to run servers that listen for incoming connections (maybe this is a premium service and they haven't paid for it).
If you can configure your router to block certain traffic based on the packet fields in the table, how would you prevent 1.2.3.4 from receiving incoming connections? You can write your answer in a form like, "block traffic where source IP is X and ..."

Would want to block all traffic where `dest IP == 1.2.3.4 AND TCP flags == SYN`.

d) **What are two other kinds of traffic you could block just by looking at the 5 packet fields in the table?** In 1–2 sentences, *speculate* on at least two possible ideas—"kinds of traffic" can be anything you want, so long as you map it to (one or more of) the 5 packet fields. There are many possible answers here (and many ways around this kind of blocking)—we just want to see your initial reasoning about the possibilities.

Lots of possible ideas, including (but not limited to):

(a) Block traffic to/from specific IPs or ranges of IPs

(b) Block specific protocols by port number (HTTP, SSH, etc.)

(c) Time-based variants of the above (connection duration, rate limiting, etc.)