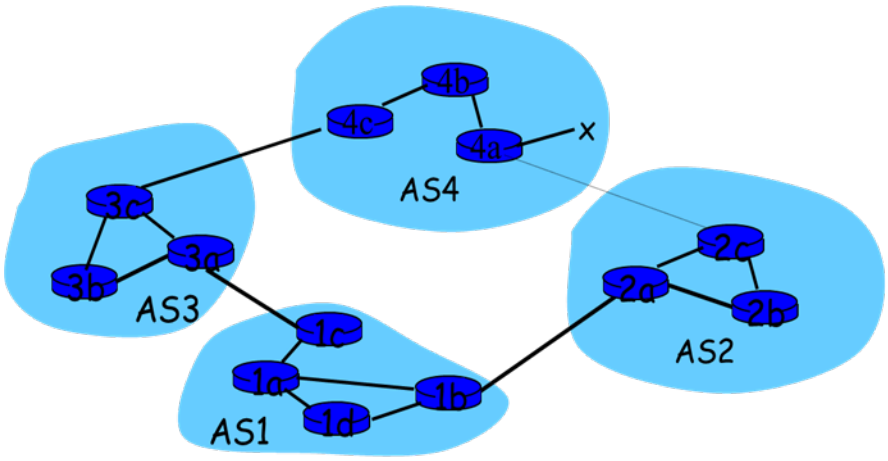
Homework 3

Network Architecture I, Spring 2016

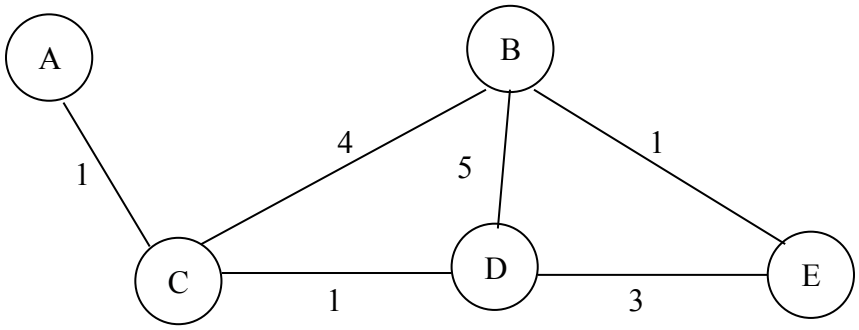
Due: paper submission, April 14 2:30 pm

(paper submission in class and electronic submission on Bb)

1. Consider the network shown below. Suppose AS2 and AS3 are running OSPF for their intra-AS routing protocol. Suppose AS1 and AS4 are running RIP for their intra-AS routing protocol. Suppose eBGP and iBGP are used for the inter-AS routing protocol. Initially suppose there is no physical link between AS2 and AS4.
   (a) Router 3c learns about prefix x from which routing protocol: OSPF, RIP, eBGP or iBGP?
   (b) Router 3a learns about prefix x from which routing protocol?
   (c) Router 1c learns about prefix x from which routing protocol?
   (d) Router 1d learns about prefix x from which routing protocol?



2. Consider the network shown below (the labels are the delay on the links).



(a) Show the operation of Dijkstra's (Link State) algorithm for computing the shortest path from C to all destinations.

(b) Show the distance table that would be computed by the distance vector algorithm in C. You don't have to show all the steps of the distance vector algorithm.

Laboratory Homework: Wireshark

In this part of the homework, you investigate the IP protocol, focusing on the IP datagram. You'll do so by analyzing a trace of IP datagrams sent and received by an execution of the traceroute (or pingplotter) program. You will inspect the various fields in the IP datagram, and study IP fragmentation in detail.

Download a packet trace file of this homework from the Blackboard, Assignment Section. Open the trace file[1] *on the Wireshark, and answer to the questions below.*

In your trace, you should be able to see the series of ICMP Echo Request (Windows machine) (the UDP segment in the case of Linux/Unix) sent by the user's computer and the ICMP Time Exceeded messages returned to the user's computer by the intermediate routers.

Whenever possible, when answering a question you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question.

Answer to the questions below.

IP Datagram

1. Select the first ICMP Echo Request message sent by the computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of the user's computer?
2. Within the IP packet header, what is the value in the upper layer protocol field?
3. How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

---

[1] *FYI, below are the steps taken for the packet capture in the given trace. You don't collect packets yourself due to University policy issues.*

- Start up the Wireshark, and start packet capture on Wireshark.
- Send series of ICMP messages (using pingplotter, or tracert in Windows or traceroute in Linux), initially with a length of 56 bytes, then with a length of 2000 bytes, and last with a length of 3500 bytes.
- Stop Wireshark tracing.

Next, sort the traced packets according to IP source address by clicking on the *Source* column header; a small downward pointing arrow should appear next to the word *Source*. If the arrow points up, click on the *Source* column header again. Select the first ICMP Echo Request message sent by the computer, and expand the Internet Protocol portion in the "details of selected packet header" window. In the "listing of captured packets" window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent other protocols running on the computer) below this first ICMP. Use the down arrow to move through the ICMP messages sent by the computer.

5. Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP messages sent by the computer?
6. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?
7. Describe the pattern you see in the values in the Identification field of the IP datagram Next (with the packets still sorted by source address) find the series of ICMP TTLexceeded replies sent to the computer by the nearest (first hop) router.
8. What is the value in the Identification field and the TTL field?
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to the computer by the nearest (first hop) router? Why?