15-441: Computer Networks Spring 2010
Homework #2

Due: Feb 23^{rd} 2010, in class
Lead TA: Rui Meireles (`firstname@cmu.edu`)

Ethernet

1. Five prisoners are locked up in adjacent cells in a prison. They would like to communicate with each other but the walls and doors are too thick. One day, one of the prisoners discovers that if he hits the water pipe in his cell with a metal spoon, the sound travels as far as two cells in each direction. I.e., the sound from cell i can be heard in cells $i-2$, $i-1$, $i+1$, and $i+2$, assuming these cells exist. After some experiments, they discover this is true for all cells.

   Over lunch, they decide to define a protocol that will allow efficient communication using say, Morse code, over the water pipes. One of the prisoners has taken 15-441 and argues that this is very much like an Ethernet so they decide to use the Ethernet protocol over their Water Pipe Network. Unfortunately, there are some problems. Can you help them?

   (a) (9 points) Ethernet uses CSMA/CD as its medium access mechanism. Can you explain how the three concepts that are used in CSMA/CD (CS, MA, and CD) map onto specific aspects of this network? We are looking for one or two line answers.

      1. Carrier Sense (CS):

      2. Multiple Access (MA):

      3. Collision Detection (CD):

(b) (7 points) The prisoners started planning a jail break using their new network. During this time, they were all talking to each other frequently. Unfortunately, they found that using CSMA/CD over the Water Pipe Network resulted in a significant packet loss rate. Can you identify the problem responsible for the packet losses with an example? Remember that in the Water Pipe Network, not all cells can hear each other.

IP addressing

2. (7 points) Having a different IP address for every network interface on a computer seems like an awful waste of addresses. What fundamental characteristic of IP addresses prevents us from using a single address per host? Think of what would break if we had only a single address.

3. Imagine you have three new startup companies coming to you in need of IP addresses. Dunder Mifflin has 256 machines, Bluth Company has 1000 and Veridian Dynamics is the largest with 5000 machines in their premises.

   (a) (6 points) If traditional classful IP addressing with classes A, B and C is used, what could be a valid address assignment to fulfill these organizations needs and how many addresses would be wasted?

   (b) (6 points) Due to your careless assignment strategy you are suddenly confronted with a shortage of addresses and you decide to finally adopt Classless Inter-Domain Routing (CIDR). What CIDR blocks could you assign to the organizations in order to minimize the number of unused addresses? Because we are focusing on the size of the network, you can omit the prefix and answer something like `/<number>` . How many unused addresses are there now with you new assignment?

Routing loops

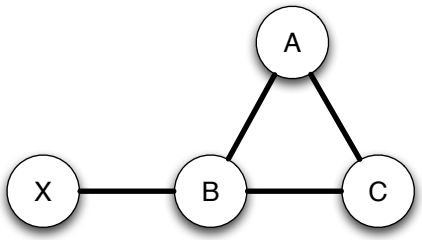
4. As you saw in class, a routing loop might easily occur in a mesh network using the Routing Information Protocol (RIP), preventing proper routing due to the circulation of incorrect routing information. The symptom of such a routing loop is counting to infinity: while routing updates on an unreachable network are incorrectly replaced by the older routing information, the metric gradually increases as the information repeatedly gets passed from router to router.

   Two of the techniques that can be used to prevent loops from occurring are:

   Split horizon - Where a node never sends information about a route back in the direction from the information came in the first place.

   Poison reverse - Where a node sends route information back to its source but setting the cost to positive infinity.

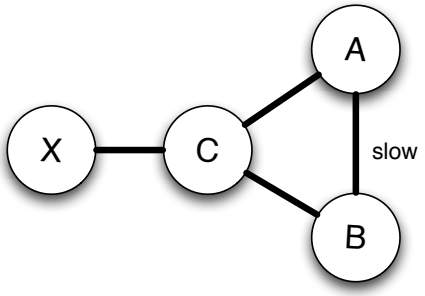
   (a) (7 points) Consider the following network with unit-cost links:



   Imagine node X fails. Assuming A, B and C are using split horizon, could a routing loop be formed (e.g. if B's infinity packet to A gets lost)? Would it be different if they were also running poison reverse? Justify your answer by writing the states.

   (b) (7 points) Suppose split horizon routers A and B somehow reach a state in which they forward traffic for a given destination X through each other. Describe how this situation would evolve with and without the use of poison reverse.

(c) (7 points) Consider the network in the following figure, where links have unit cost and the link between A and B is very slow:



Give a sequence of events that lead A and B to a looped state where they route through each other as in part b), even with poison reverse enabled.

Border Gateway Protocol (BGP)

5. Suppose a hacker obtains control of all the BGP-speaking routers in several different Autonomous Systems (ASes). Our hacker has each AS "hijack" several IP blocks. That is, each AS under his or her control announces via BGP that it owns IP blocks for which it does not. For example, our hacker has AS (CMU) announce a one-hop path to the IP block 18.0.0.0/8 (MIT).

   (a) (6 points) Assuming that the AS graph still converges to a stable state, can this attack cause routing loops to form? Explain why or why not.

(b) (6 points) Suppose the ASes under attack are identified. Can other ASes change their routing policies to ensure that their traffic still reaches the hijacked IP blocks? Explain.

(c) (7 points) In response to this attack, suppose all ASes agree to check a central registry for IP block ownership before a path is considered valid. That is, whenever an AS receives a route to a prefix P, it checks that the last AS in the route actually owns P. For example, upon receiving a path to 18.0.0.0/8 (MIT), an AS will check that the last AS in the route is 3 (MIT). Can a hacker still hijack IP address blocks belonging to ASes he or she does not control? (i.e., can he or she cause traffic destined to those IP blocks to be routed to the ASes he controls?) Explain.

Unix network utilities

Unix/Linux provides a series of useful utilities to configure, analyze and debug networks. This section is designed for you to gain an understanding of what these tools are and what you can use them for. You should execute commands from an Andrew Unix/Linux machine. If you have trouble finding a specific utility, try `/sbin/<utility-name>` or `whereis <utility-name>` to find it.

6. (3 points) `ifconfig` allows you to configure and analyze your network interfaces. Run `ifconfig -a`. What are your IP address, broadcast address, netmask and physical address for the first wired network interface (eth0)?

7. (3 points) `netstat` gives you numerous network interface statistics and displays network connections and routing tables. Run `netstat -rn` to look at your routing table. What is the IP of your gateway to the internet and how did you identify it in the routing table?

8. (3 points) `ping` is a network utility that you can use to test whether a particular host is reachable across an IP network and to measure the round-trip time (RTT). Run `ping <your-gateway-address>` and `ping www.gentoo.org`. What are the respective RTTs? Is there a significant difference? Why?

9. (3 points) When you pinged your gateway, the Address Resolution Protocol (ARP) was used to get its physical address. For performance reasons, the operating system saved that physical address in an ARP cache. Run `arp -a` to list the cache contents. What is your gateway's the machine/host name and what is it's physical address?

10. The Unix utility `traceroute` can be used to find the path that a packet follows to reach a certain destination. There is also a utility `whois` that uses the protocol with the same name to query a database in order to determine the registrant or assignee of Internet resources, such as a domain name, an IP address block, or an Autonomous System Number (ASN).

    (a) (7 points) Read the man page or other `traceroute` documentation to understand how it works. Now use `traceroute` to find a path to: i) your gateway and ii) `www.gentoo.org`. Write down an ordered list of servers traversed to reach each address. Use `whois -h whois.cymru.com " -v <ip-address>"` to annotate the servers with their ASNs and their owner (i.e. CMU, Verizon, ...). Also try to classify the servers as local, regional or backbone. You can Google an ASN and/or owner to find out about their operations.

    (b) (6 points) What will happen if `traceroute` is used to find the path to an unassigned address? Does it matter if the network portion or only the host portion is unassigned?