15-441 Computer Networks
Homework #3
Out: Oct 27th Due: Nov 10th, 2005, Noon Wean Hall 7112

Purpose: This assignment gives you experience with what actually happens on actual network wires. In order to achieve this we will use a packet sniffing and network analysis tool called "*ethereal*" and its terminal mode counterpart "*tethereal*". "Ethereal" will allow you to monitor and analyze network packets on the LAN in the CS 441 lab. By capturing data and examining packets you will become more familiar with TCP/IP, and how layered protocols are represented within packets.

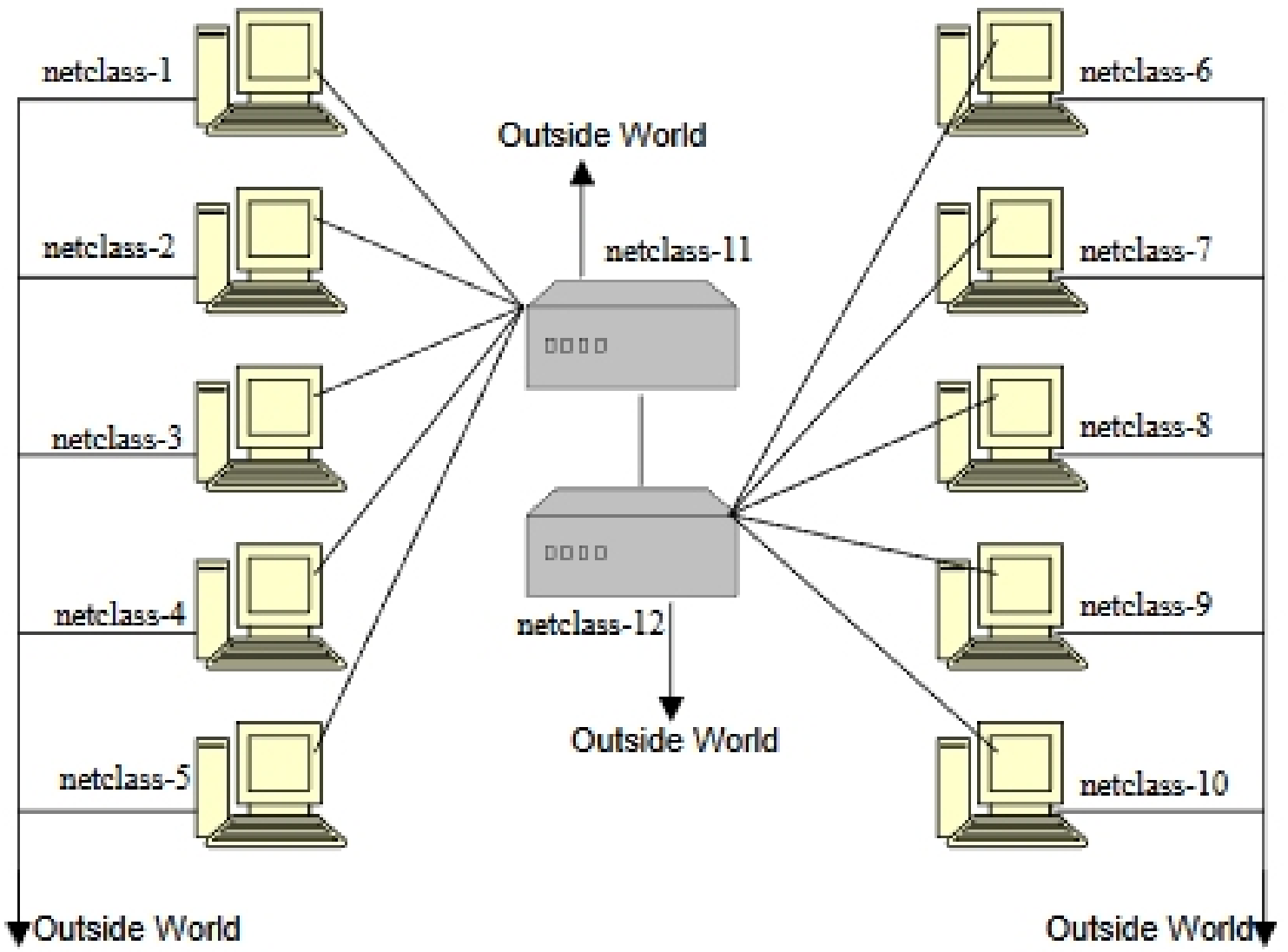
Please do this lab on your own. DO NOT WORK IN GROUPS!! You can ask the TAs or other students for help, but you should do the work yourself.

I. Preparing for the lab: Follow the instructions below to set-up your account on the netclass machines (machines in the CS441 lab). You won't be able to log in if you don't follow everything completely:

- Create a directory in your Andrew home directory called 15-441.
- Now you need to give access to *campusnet* so type the following:
  a. **>fs sa /afs/andrew.cmu.edu/usr/<your_username> system:campusnet l**
  b. **>fs sa /afs/andrew.cmu.edu/usr/<your_username>/15-441 system:campusnet rl**
- Create a file called *.klogin* inside the 15-441 folder which contains: *your_username@ANDREW.CMU.EDU*
- You can not use unsecure telnet to connect to netclass machines. Therefore, either use Nifty Telnet or use *ssh*. **The username you will use will be your_username@andrew.cmu.edu** not just your Andrew-id. Therefore, if you use *ssh* don't forget to use the "– l" flag with the correct username as otherwise, ssh will try to use just your Andrew-id and therefore you won't be able to login.
- If you have any problems with logging in, send email to Sachin Kulkarni – skulkarn@andrew.cmu.edu

II. Setup for this Lab

The topology of the CS441 lab is shown below: (all end with .intro.cs.cmu.edu)



The lab consists of 12 PCs as shown with 2 of them (11 and 12) configured as routers and the rest configured as endpoints. As can be seen the PCs are connected to form a LAN as well as being connected to the outside world (that's how you can telnet in). This is achieved by the use of 2 interfaces on each PC – one connected to local LAN and one to the outside world. The traffic going on in the LAN is considered private traffic – it is isolated from the outside world. In order to login to these machines use your **andrew-id** and **password** and don't log on to 11 and 12.

III. Determining important hardware addresses

The hardware addresses on our LAN are 6 byte Ethernet addresses. You will want to know two hardware addresses on the LAN: the address of the PC on which you are running the Analyzer ("ethereal") and a target machine (Netclass-11 or Netclass-12) which are emitting packets to the other PCs on the LAN and from which you will be sniffing the network traffic.

Note: If you get a "command not found" message when attempting to use the "ping", "arp" and "traceroute" commands or any other command, then they are not in your command search path. You can get around this by using the full pathnames ("/usr/sbin/ping or /sbin/arp or /usr/sbin/traceroute or /sbin/route") on the command line. For finding help about a certain command use "man <command name>".

EXERCISES:

a) Telnet to a pc in the LAN (other than 11 or 12) using your username and password. Use the ping command to contact Netclass-12. Ping will cause your local host to create an entry in the arp cache for each of these hosts. Find the IP and Hardware addresses of "netclass-12" (hint: lookup the *arp* command)

b) Now we want to get the Ethernet hardware address and the IP (inet) address for the Ethernet interfaces on Netclass-8. (hint: look up *ifconfig*)

c) Determine which ethernet card is used for the default route (use the man pages as a guide to find the command to use)

IV. Capturing and Viewing packets

Open up a terminal window. Since you don't have write access to the directories other than the local temp go to "/tmp". Create a subfolder with your username. You will create your dumpfile (the file which will contain the captured packets) in that subfolder. We will capture the packets using "tethereal" which is in "/usr/bin". First run tethereal –help to see the command line options. We want to capture 500 packets from the external traffic (hint: there are 2 Ethernet cards on each PC (eth0 and eth1). You need to determine which one is dealing with the LAN traffic and which one is connected outside (which would mean you will see telnet packets when you look at the dump) Save the packets you sniff in a file (so that we can look at them with a graphical interface). Now start up "/usr/bin/ethereal" (make sure your X-Server is running). "Ethereal" will ask for the root password – just choose "Run unprivileged". When "ethereal" is started up it will have three empty panes. Go to File -> Open and open up the capture file.

EXERCISES:

Select the "+" sign in front of each of the protocol layers to get more detail about each protocol header.

a) View the captured broadcast packet data. Select the "Source" column to sort the packets by the source address. What is the most common source address?

b) What protocols (ncp, sap, tcp, icmp, arp, udp, etc...) do you see? (HINT: select the "Protocol" column to sort by protocol)

c) Which protocol is most common in your captured packets?

d) Select a packet in the top frame that is labeled as a TCP packet. Determine the following values for this packet

Ethernet destination address
IP source address
IP TTL
TCP source port

e) Select the "header length" field of the IP header. This should cause a byte in the raw data pane to be highlighted. What does this byte have and what does it mean?
