My Dear Students:

There is NO Homework assignment this weekend. However there is a reading assignment

Read Chapter 1 in its entirety and when you do that do it with passion!!! And let me know if you have any questions.

Dear Students:

I would like you to try these utilities to gain a better understanding of the Delay concept, route concept, addressing, etc.... These utilities are mostly used for testing and troubleshooting (for example they may be used to determine where the Network is broken or where the packets are being discarded by a router etc… I hope you will try them and have some fun with them.

Go first to your command prompt:

In Windows, select Start > Programs > Accessories > Command Prompt

---

The first is called "**Ping**" which is used to test (troubleshoot) the network to discover whether a certain host is "reachable" and to record the characteristics of the route to this host. It sends at least three packets to a host and receives a report on the "RTT"

Go to your command prompt c:\ and enter (leave a space between Ping and the host name)

Ping www.usc.edu (or any other website you like). You will get to see whether the usc web server is on and how much (minimum and maximum) is the RTT (RTT is the round trip time (to be discussed this coming week)). Note that if you know the IP address of the site, you can enter it instead of entering the host name.

You can also use Ping to check the TCP/IP configuration in YOUR machine itself by using what is known as the "loop back address").

Enter

Ping 127.0.0.1

If the ping fails, there is a problem with the installation of the TCP/IP software in your machine. By the way, if the Ping is successful, you will notice that the RTT is very small since the command did NOT travel for long!!

Later (coming attractions!!!) you will ping the "default router/gateway" in your network and if the ping fails, you need to check the IP address of your router and make sure that is in the same "subnet" (coming attractions!!) as your own computer.

127.0.0.1 is the loopback IP address (sometimes called the "local host". This address is used to establish an IP connection to the same machine or computer being used by the end-user. The difference between connection to a host with an IP address and connecting to 127.0.0.1 is that the latter avoids using the local network interface hardware (note that if by accident a packet addressed to 127.0.0.1 reaches a router, the router will "drop it").

127.0.0.1 is used by application programmers or network managers to "test" the TCP/IP local stack, the operating system, etc… (Think about it as a trouble shooting procedure). When you ping 127.0.0.1, you will notice that the RTT (Round Trip Time) is almost zero (since the packet will not go outside the host. You will also get the number of Bytes (Packets) sent and you will also see the TTL: Time to Live. We shall discuss this in due time.

The second useful command is called "**Trace Route**" which is a command that traces the route a packet takes to a specific destination. It displays the series of routers (with their IP addresses) that are used to deliver the packet. If the packets are unable to reach the destination host, Trace route will display the "last router" that successfully forwarded the packet. Trace route sends out a packet (Three times) to each router (hop) along the way

Go to your command prompt c:\ and enter (leave a space between tracert and the host name)

tracert www.usc.edu (or any other website you like). You will get to see how many routers were involved in the delivery, The RTT to each of these routers (3 values since three packets are sent). Note that the first router that will be displayed is your default router (The ISP router of your ISP provider). Some routes may times-out and that will also get displayed. Again notice, you can enter the IP address of the destination of you know it instead of the host name.

Note that the "Trace Route" command in MAC OS X is different from that in Windows. That should be "**traceroute**" **in MAC OS X rather than** "**tracert**"

The next command I would like you to try is "IPCONFIG" which will display all current TCP/IP configurations in your machine including the host IP address, the default router IP address, the subnet mask (coming attraction), the IP address of the DNS server (The local one), the IP address of the DHCP server, etc… You would also get the MAC address (in the display it is referred to as the physical address) of your NIC card (and the type, for example Ethernet, wireless, etc…) if you also enter

C:\ipconfig/all

If your IP address is in the following ranges, it is a Private IP address. Private IP addresses are those address that are NON-routable, i.e. they are ONLY used in the private network and are not allowed to go to the public Internet. ICANN (Internet Corporation for assigned names and numbers) have allocated three blocks for IP addresses

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

the ipconfig utility differ a bit if you are **using MAC computer**

Just like you can open command prompt in Windows and hit "ipconfig" to get your local LAN/WLAN IP address, you have the same option on a Mac in OS X with the command "**ifconfig**".

Open terminal, eg. by pressing cmd+space and typing “terminal”. Type “ifconfig” and hit enter. Remember to include -a if you want to see the MAC (Hardware) address as well of your NIC card.

You could also see your IP address in MAC by clicking the Apple icon, then click on System preferences, then click on Networks, then click on your type of connection (WiFi or Ethernet)

The IP address format is x.x.x.x where each x is the decimal equivalent of an 8 bit binary (which means that the IP address is 32 bits long)

The MAC address is 48 bits long represented as

zz:zz;zz;zz;zz;zz

where each z is a "hexadecimal) representation for a 4 bit binary remember the hex is 0 ~ 9, A, B, C, D, E, F

example 5B:23:A7:D1:65:0E

Ethernet adapters and wireless LAN adapters allow your laptop to join the Ethernet/ wireless LAN respectively. The laptop normally needs only 1 Ethernet adapter and 1 wireless LAN adapter. When you run ipconfig/all, you will get a “cluttered” list of the so called “Tunneling Adapters” which are used with IPv.6. An example is the 6to4 tunnel adapters, the ISATAP tunnel adapters which allows to transmit IPV6 packets among dual-stacks nodes (implementing both IPv6 and IPv4) over IPv4 network. You may see Toredo tunnel adapters, which allows a computer behind NAT firewall with no IPV6 connectivity to access IPV6 resource over IPV4 network.

To remove all of these adapters (if you are not using IPv.6), follow the following:

Go to Control Panel
Left click to Device Manager
Left click to Network Adapter
Left click View
Left click on hidden devices

You will get a whole bunch of these adapters which you can disable). Keep only the

Wireless and the Ethernet Adapters. Then repeat ipconfig/all and hopefully you will see a clean screen (i.e. the information that we are interested in such as the MAC address, IP address, Subnet Mask, Local DNS, etc...

One more thing. If you want to find your IP address AFTER the NAT (i.e. the Public IP address (which is the address of your router on the public side. Open your router configuration page (Almost all routers can be accessed through a web interface where you can see and adjust settings. Open the web interface by entering the router's IP address (The private one that you got earlier using ipconfig command)) into a web browser. Note that the most common router addresses are:

- 192.168.1.1
- 192.168.0.1
- 192.168.2.1

Then click on Router Status. Under Internet Port in the Router Status, your IP address should be listed. This is the public IP address of your router. Any connections made out of your router will have this address. This IP address is assigned to you by your internet service provider. Most external IP addresses are dynamic, which means they change from time to time.

I apologize for this long e-mail (looks like a lecture) but I thought you would enjoy them.

I wish you all a happy and "safe" weekend. Please make it productive and read.
Will see you Tuesday.