CO223 : LABORATORY SESSION 2

GAMAGE C.T.N.

E/13/107

GROUP 06

SEMESTER 3

26/02/2016

**PART 1 : Network Tools**

1. **Ping**

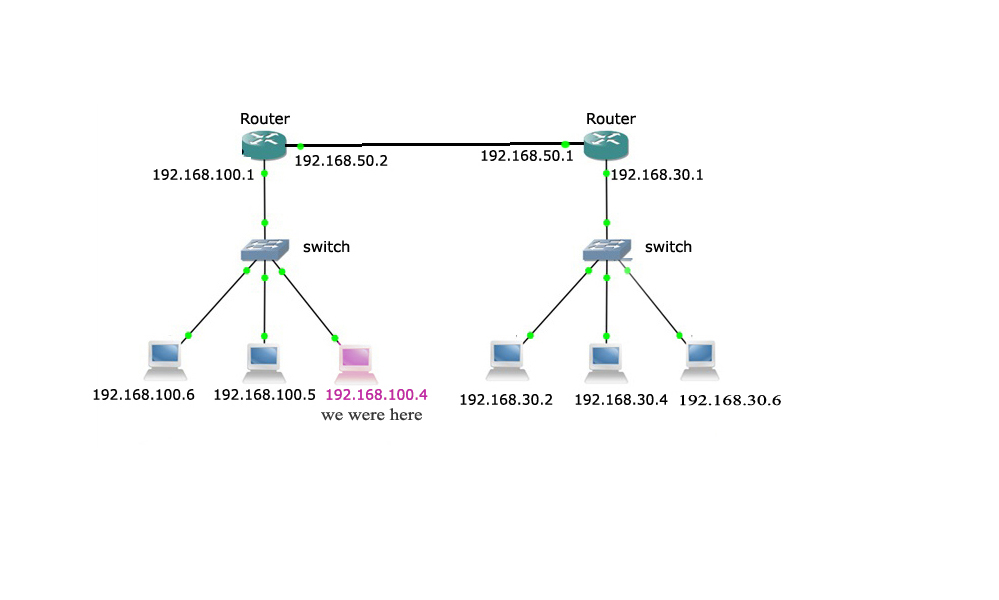
Ping is the name of a computer command to test the accessibility of another engine through a network IP. The command also measures the time taken to receive a response . It is the abbreviation of Packet InterNet Groper.

Using the ping we can check whether a network is working without errors so that data packets can be sent to an address without any interference. It is mainly used to determine that a specific ip address is accessible.

Ping also has the ability to return the time which is taken to complete an packet to go to the other IP and come back(approximate round trip). It also shows the number of packets sent, received and lost

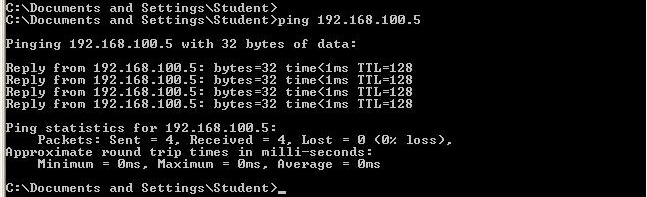
The ping captures this data by sending a special kind of packets called as ICMP (Internet Control Message Protocol) packets to the destination address and checking the returned packets.

The network available in the lab is shown below

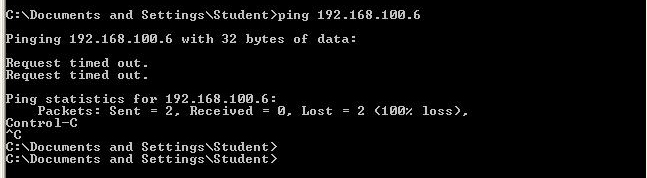


The below are the results we obtained by pinging the different IPs

First we checked an ip which belongs to the same router which out computer was connected.

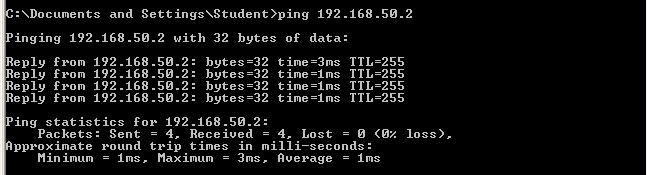


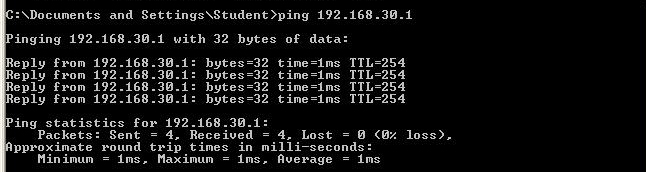
We can observe that the connection was successful. Then we tried to connect another computer connected to the same router.



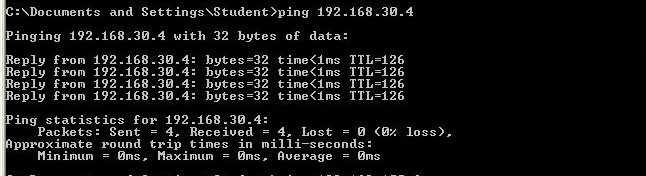
We can see that there comes a message as the “Request timed out”. Is says that the connection was unsuccessful (100% loss). This may be due to reasons like server being offline; the machines are configured not to respond to the command or errors in physical connection. Actually in this case we check the ping of the particular computer after manually removing the network cable.

Then we checked the ping for the 2 routers





We can observe that the connection was successful. Finally we verified the connection for a computer connected to the other router.



It was also successful.

In the aspect of delay when we analyze the above results we can see that the average delay of the network is either 1ms or 0ms which means that the delay is negotiable. This is because our network is not so widespread and the links are very short.

When observing those results we can see that there is a value as TTL for every packet sent. The TTL means “Time to leave”. It represents the maximum number of routers the specific packet can pass through before it is discarded. Here’s how it is calculated, whenever a packet passes through a router the TTL value is decremented by 1. Once the TTL becomes zero the packet is discarded. The default TTL value depends on the operating system. For windows it is 128 and for Linux it is 192. From the above results it is clear that the computer which is connected to same router of ours is with the TTL 128 and the computer which is connected to the other router has a TTL value of 126 since it has to go through 2 routers.

1. **Traceroute**

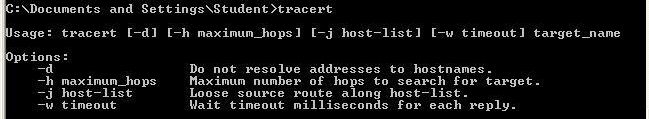
Traceroute is a command which is used for network diagnostic , it is found on most operating systems , to determine the path followed by a packet. The traceroute command allows to draw a map of the routers present between a source machine and a target machine. The traceroute command differs across operating systems.The command is used as traceroute in Linux and as tracert as in windows.

Here’s how it works, First the computer we used to check the traceroute will send a packet with 1 TTL value. When it reaches the 1st router, the TTL value will be reduced by one and becomes 0. That means the router will drop the packet and it will send a “Request time out” ICMP message back to the source. Then the router will send packets with TTL value of 2 and they will be drop by the 2nd router. In this way traceroute will calculate the number of routers that the packet will travels through until the destination, finally when it reached the target it will return a ICMP echo reply as in ping.

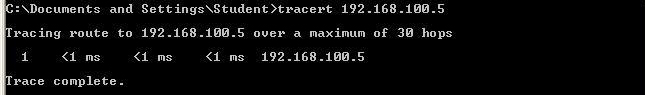
There are three columns because the traceroute sends three separate signal packets. This is to display consistency, or a lack thereof, in the route.

Here are the results that we gained by tracert command to check different IPs in the lab network.

Here is the manual for tracert command

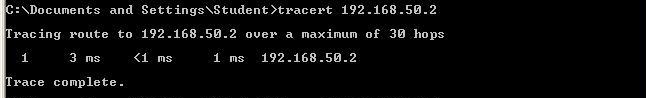


When we chek a IP of a computer connected to the same router, the result is.



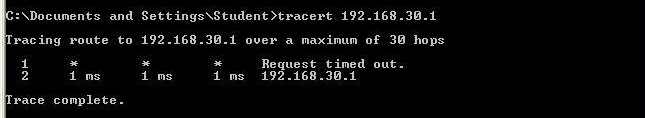
From this we can see that the the packet hasn’t pass through anr router.

Then let’s check the router which our computer is connected.



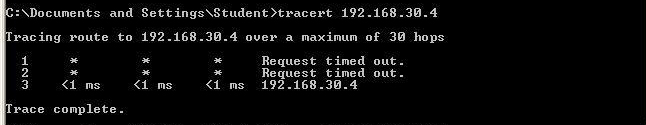
Since it has not passed through any router yet it sends only one packet.

Then let’s check the traceroute of the 2nd router



It gives the result that it has been passed through another router. Which is the 1st router (the one our computer is connected)

Then we checked the traceroute of an IP which is connected to the 2nd router.



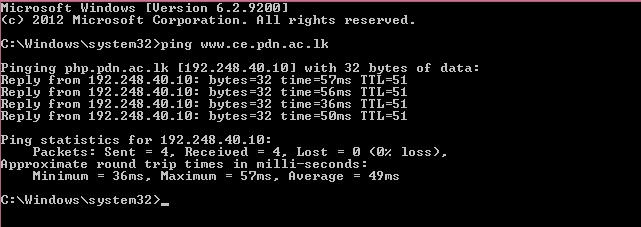
The results clarify the definition of traceroute.

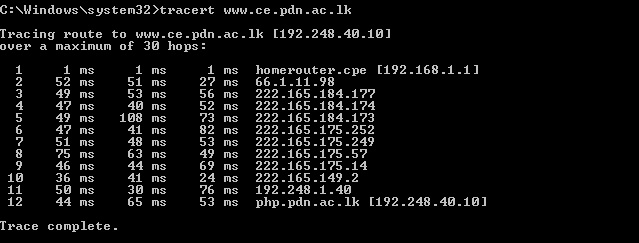
When we looked at the results from the aspect of delay, we can see that the delay is 1ms or less in each case, this is because our network is small and it spreads in a short range.

**c) Ping and traceout for domains**

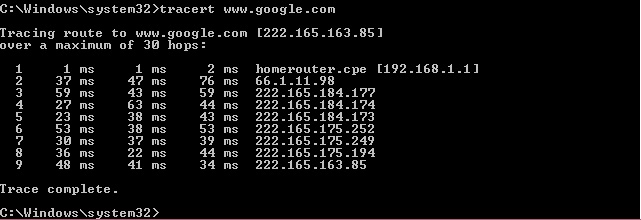
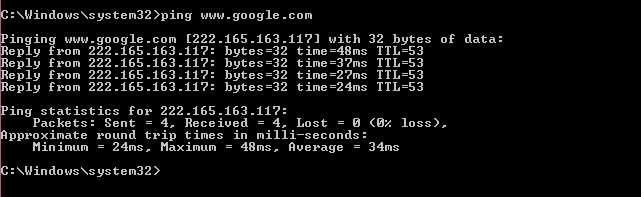
Let’s check ping and tracert for some domains. When we use this commands with a domain they gets the corresponding IP of the given domain and continue.

1. www.ce.pdn.ac.lk

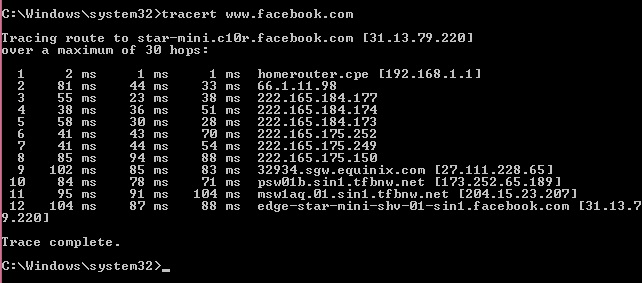


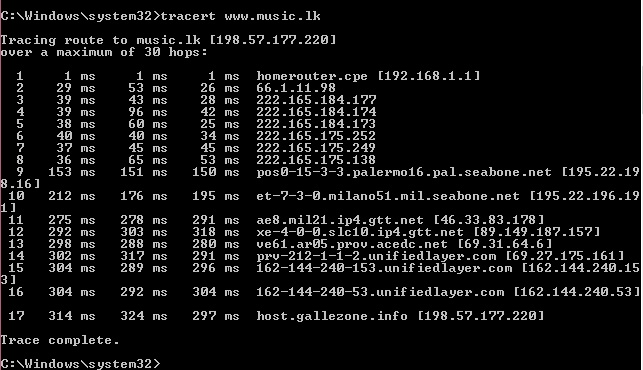
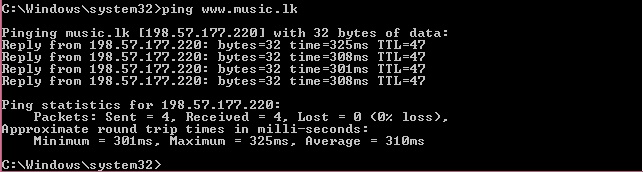


2) www.google.com

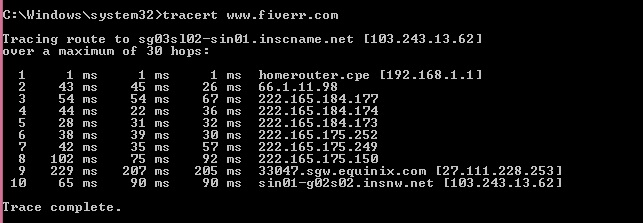


3) www.facebook.com



4) www.music.lk

5) www.fiverr.com



The above results show the delay,TTL, number of routers between us and IP and many more information.

When we compare the above 1 and 2 we can see that TTL values are 51 and 53 respectively and average approximate round trips are 49ms and 34ms. Hence it is clear that when connecting to the ce.pdn.ac.lk at goes through more number of routers than when connecting to the google’s IP. Since the TTL of ce’s is larger than that of goole’s.

The above statement is proven by the results obtained by the tracert. We can see that in CE it goes through 11 routers while in google it goes through 8 routers.

From the results for tracert we can see that the delay is not always increasing for each intermediate node. If abnormal increase in delay in the beginning hops it may be due to the issue in the local area network. If a high latency is shown in the middle not in the beginning or end it may be due to setting the signal into lower priority in the router at that specific hop. It doesn’t indicate an issue. If this delay time is high in middle and seems constant it also doesn’t indicate any issue. If it increases highly towards the target it would be a cause of packet loss.

1. **More network tools and commands**

**Ipconfig**

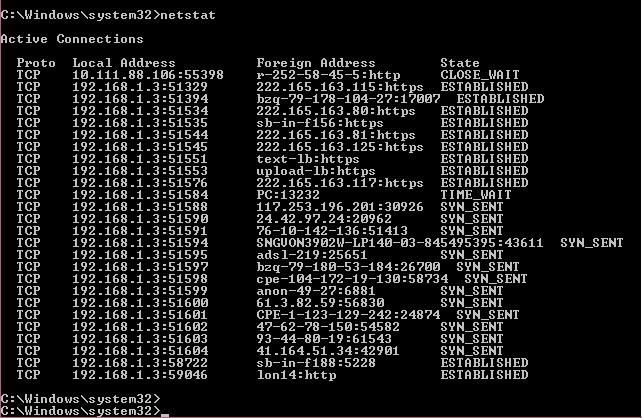
The ipconfig command (inconfig in linux) showa the ip address, subnet mask, default gateway and a route table. It is the abbreviation of Internet Protocol Configuration.

The results for ipconfig command in lab machine is shown below

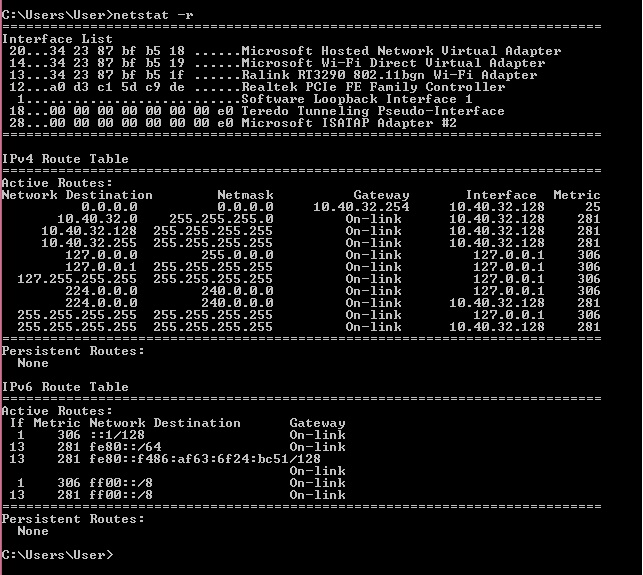


**Netstat**

Netstat is also a command line tool which is used to determine the traffic of the network and other errors in the network. Netstat refers to network statics. Basically it shows the connections for TCP routine tables and local address, foreign address and state of them. Below shows an output obtained by my pc while it is connected to the internet.



The netstat –r command will generate results separately for the IPv4 and IPv6.

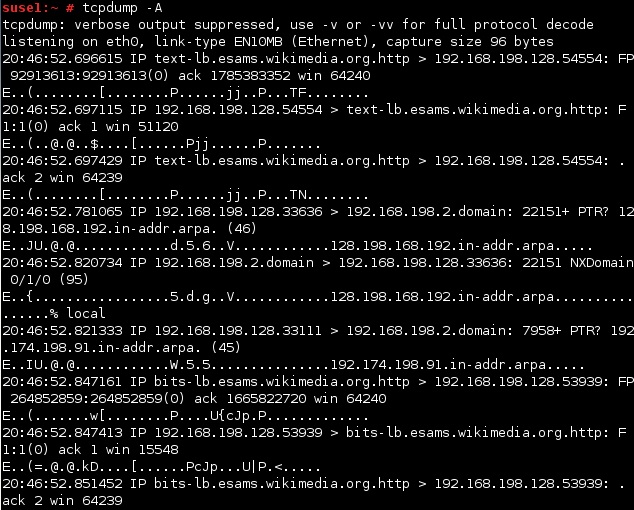


**Windump**

It is packet analyzers which are used to find to which computer do the packets which are being transmitted and received are attached. The Linux version of this command is tcpdump

An examle which has been run on a Linux machine is shown below.

(courtacy http://linux-bible.com/)

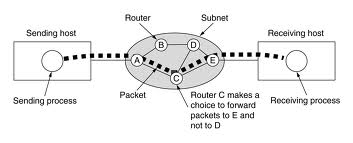


**PART 2 : Network Protocol Analyzer**

**Packets**

A packet is simply termed as a unit of data. A packet contains data, source, destination, network address, size and type etc. It is sent through internet or any other packet switched network.

The below illustration shows how packets are exchanged in a network.



1. **Network protocol analyzer**

A network protocol analyzer can be hardware or software or a combinational utility which can track the traffic passing through a network and keep the logs of them. They can also acts as protectors against malicious activity. They are also termed as packet sniffer, packet/network/protocol analyzer.

Listed below are some uses of a network protocol analyzer.

* Can obtain a statics of real time and recent past activities in the network.
* Can detect the problems in the network including unusual traffic levels, unusual packet characteristics,
* Can monitor network usage, bandwidth utilization, security status
* Can detect the network misuse by users.
* Debug client/server communications, and implementations.
* Can test anti-malware programs.

**Wireshark**

Wireshark is a reputed packet analyzer which has the ability to analyze and troubleshoot the network.

We ran the Wireshark at PCs in the network and captured packets and observed any network traffic in the ‘quiet network’ with no network applications or tools running.

The saved file is (double click to open):



Then we ran the ping and traceroute tools and capture packets to see the increased network activity.

The saved files are:



When we compare the result files from the Wireshark we can see that in the quiet state the output doesn’t show any variation. When we give the ping command the result shows that there are 4 request activities and 4 reply activities. This indicates the incoming and outgoing signals between the 2 IPs . It records the results of the packet exchange between the source and destination.

Same as in ping command result the Wireshark records the results of the tracert command with respect to source destination and time. The results sheet shows that there are 3 request and replies. The 3 requests are sent by the source and and the replies are from the 2 intermediate routers and the destination IP.