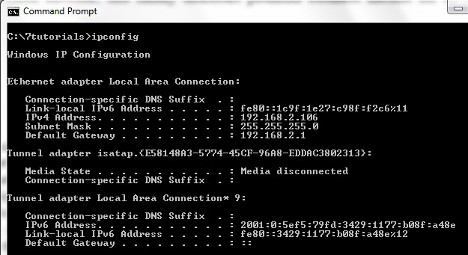
##### PRACTICAL: 03

##### AIM: - To study of various networking commands.

**Retrieving Information about Your Network Connection**

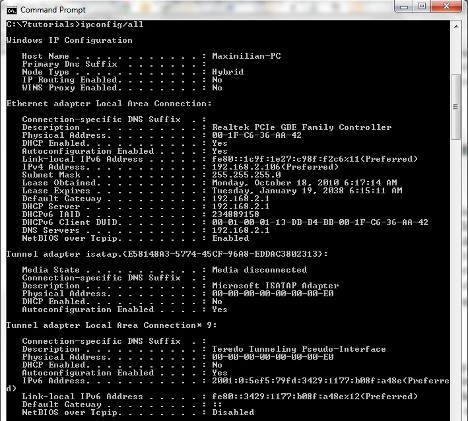
## ipconfig : To obtain detailed information about your network connection, use the *ipconfig* command. Type *ipconfig* in *Command Prompt* and press *Enter*. As you can see below, a list with the network devices existing on your system and their IP addresses is displayed. You get also details such the default gateway, subnet mask or the state of the network adapter.



## ipconfig /release: by this command host machine can release ip address and set to 0.0.0.0 or none.

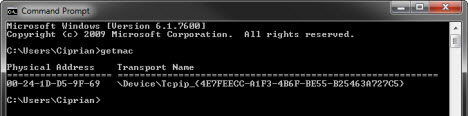
## ipconfig /renew: by this command host machine can make request for the renewing ip address. New ip may be same or not, it is depends on configuration of DHCP.

**ipconfig /all:** With the */all* switch you will get a whole new level of detail: DNS information, the [MAC (Media Access Control)](http://en.wikipedia.org/wiki/MAC_address) (in the *Physical Address* field) and other information about each network component. Check out the picture below to see a sample of the combination of *ipconfig* command with the */all* parameter.



**Finding Your Computer's MAC Address**

* **getmac:** Another way to obtain the *MAC* address is to use the *getmac* command. Just type *getmac* and press *Enter*, as shown below.

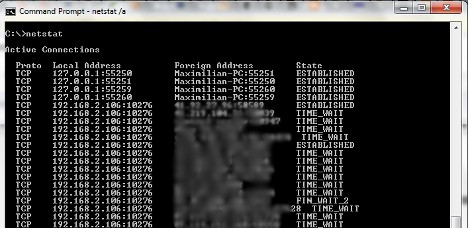


**Check Network Connections and Display Port Information**

**netstate:** With the *netstat* command you will be able to see active network connections between your system and any other systems on your network or the Internet.Netstat is basically a network utility tool that displays network connections (TCP, UDP), routing tables, number of network interface and network protocol statistics. The command is often used to find problems in the network, or determine the amount of traffic over the network as a performance measurement.

## netstate*/a* parameter shows all connections and listening ports.

* Foreign address is displayed on the third column. It is the IP address and port number of the remote computer to which the socket is connected. Local address is the IP address of your device, while foreign address is the address of the device you are connected to it.



## ping: To test your connection to a certain website or another network or Internet location, you can use the *ping* network command followed by a web-address or IP address.

* Ping operates by sending ICMP Echo Request packets to the target device and waiting for an ICMP Echo Reply. The program reports errors, packet loss, and a statistical summary of the results. (The **Internet Control Message Protocol** (ICMP) is a protocol that devices within a network use to communicate problems with data transmission.)

## 

## Types of Ping:

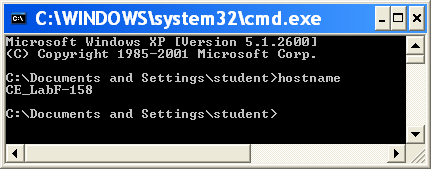
## Successful Ping

* Target Device not responding
* A Longer Test

Example: ping –n 500 192.168.1.1

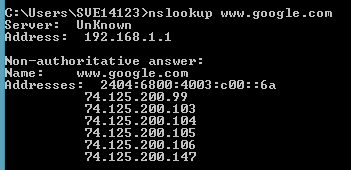
## hostname: display the hostname of winxp currently logged into.

* Windows version of the hostname command has no parameters. However, the Unix/Linux versions of hostname let you set the computer's host name as well as display it. You do that by specifying the new host name as an argument.



## pathping: use to find network latency and network loss. (E.g. pathping google.com)

* The advantages of PathPing over Ping and Traceroute are that each node is pinged as the result of a single command, and that the behaviour of nodes is studied over an extended time period, rather than the default ping sample of four messages, or default traceroute single route trace. The disadvantage is that it takes a total of 25 seconds per hop to show the PathPing statistics.
* **nslookup:** nslookup (from name server lookup) is a network administration command-line tool for querying the Domain Name System (DNS) to obtain the mapping between domain name and IP address, or other DNS records. Displays information that you can use to diagnose Domain Name System (DNS) infrastructure.
* It is used to find out phishing and cache poisoning attacks.
* A DNS cache poisoning attack is an attempt to trick a caching DNS server into caching a forged response. If **bank.example.com is at 192.0.** **2.193, and evil.example.com is at 198.18.** **8.17**, an attacker may try to poison a DNS server's cache by sending the forged response of “bank.example.com is at 198.18.



The DNS server I am using on client

## tracert: Traceroute is a computer network diagnostic tool for displaying the route (path), and measuring transit delays, of packets across an Internet Protocol (IP) network. Show the path a packet of information taken from your computer to the specified host.



You can see each step the data takes when it travels to the destination server of 192.168.1.1 These are called hops, and represent a system or router the data passes though.

As you can see, hop 3 in this example has not responded, but hop 4 has, meaning that hop 3 is not responding to the request but is handling the packets properly and forwarding traffic to the next hop.

**Lab Exercise**

1. **Why we are using *ping* command?**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **Explain *arp* command**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

***Sign of Faculty.***