**Experiment No. 2**

**AIM:** To study basic TCP/IP utilities and commands. (eg: ping, ifconfig, tracert, arp, tcpdump, whois, host, netsat, nslookup, ftp, telnet etc…)

**OBJECTIVES:**

To learn the basic TCP/IP utilities and commands that are commonly employed to help set up, configure

and maintain TCP/IP internetworks. These utilities allows a network administrator to perform functions such as checking the identity of a host; verifying connectivity between two hosts; checking the path of routers between devices; examining the configuration of a computer; looking up a DNS domain name; and much more.

**THEORY:**

# Ping

PING Verifies connections to local or remote computers (Ping stands for Packet InterNet Groper, an excellent IP troubleshooting tool)

The PING utility tests connectivity between two hosts. PING uses a special protocol called the Internet Control Message Protocol (ICMP) to determine whether the remote machine (website, server, etc.) can receive the test packet and reply.

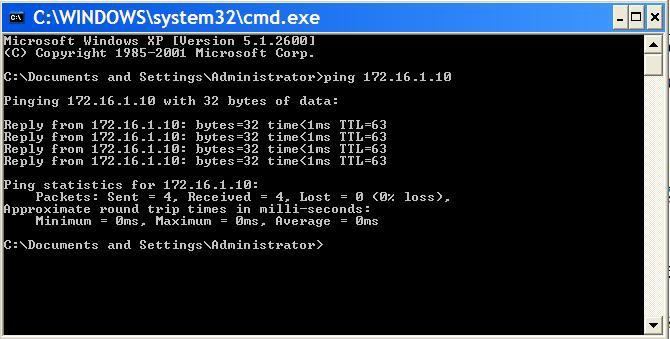
Also a great way to verify whether you have TCP/IP installed and your Network Card is working.

We‘ll start by Pinging the loopback address (127.0.0.1) to verify that TCP/IP is installed and configured correctly on the local computer.

**Ping 127.0.0.1**

This tells us that TCP/IP is working as well as Network Card.

To test out connectivity to a website all you have to do is **ping espn.com**



The results should tell us if the connection was successful or if we had any lost packets. Packet loss describes a condition in which data packets appear to be transmitted correctly at one end of a connection, but never arrive at the other. Why? Well, there are a few possibilities.

The network connection might be poor and packets get damaged in transit or the packet was dropped at a router because of internet congestion. Some Internet Web servers may be configured to disregard ping requests for security purposes.

Note the IP address of espn.com — 199.181.132.250. We can also ping this address and get the same result. However, Ping is not just used to test websites. It can also test connectivity to various servers: DNS, DHCP,

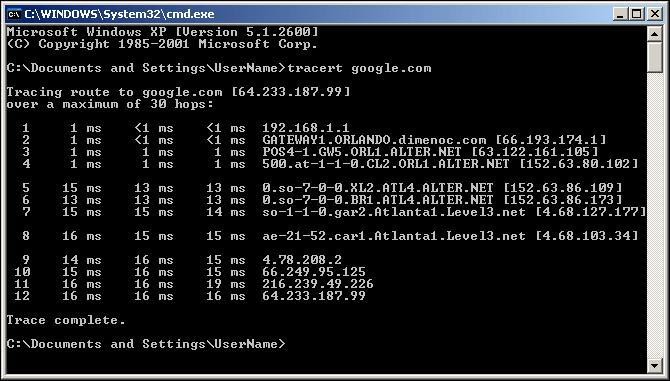
your Print server, etc

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS][-r count] [-s count] [[-j host-list] | [-k host-list]] [- w timeout] destination-list

|  |  |
| --- | --- |
| -t | Ping the specifed host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C. |
| -a | Resolve addresses to hostnames. |
| -n count | Count Number of echo requests to send. |
| -l size | Send buffer size. |
| -f | Don't Fragment flag in packet. |
| -i ttl | TTL Time To Live. |
| -v tos | TOS Type Of Service. |
| -r count | Record route for count hops. |
| -s count | Timestamp for count hops. |
| -j host-list | Loose source route along host-list. |
| -k host-list | Strict source route along host-list |
| -w timeout | Timeout in milliseconds to wait for each reply. |

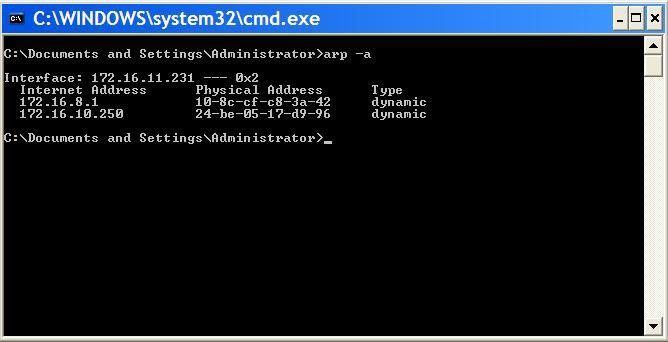
# Tracert

Tracert is very similar to Ping, except that Tracert identifies pathways taken along each hop, rather than the time it takes for each packet to return (ping). It is a nice little utility which can be used quite effectively for diagnosis of networks and routes. It can also be used to find IP addresses for items you only know by name. If I have trouble connecting to a remote host I will use Tracert to see where that connection fails. Any information sent from a source computer must travel through many computers / servers / routers (they‘re all the same thing, essentially) before it reaches a destination. It may not be your computer but something that is down along the way. It can also tell you if communication is slow because a link has gone down between you and the destination.



# ARP

The ARP utility helps diagnose problems associated with the Address Resolution Protocol (ARP). TCP/IP hosts use ARP to determine the physical (MAC) address that corresponds with a specific IP address. Type arp with the – a option to display IP addresses that have been resolved to MAC addresses recently.



ARP stands for Address Resolution Protocol. This provides IP to Ethernet addresses. Each hardware card has an address coded in. This allows deletion and addition to the ARP cache. The switches to be used can be obtained by just typing arp at a DOS command prompt.

ARP -s inet\_addr eth\_addr [if\_addr] ARP -d inet\_addr [if\_addr]

ARP -a [inet\_addr] [-N if\_addr]

|  |  |
| --- | --- |
| -a | Displays current ARP entries by interrogating the current protocol data. If inet\_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If  more than one network interface uses ARP, entries for each ARP table are displayed. |
| -g | same as -a |
| -N | if\_addr Displays the ARP entries for the network interface specified by if\_addr. |
| -d | Deletes the host specified by inet\_addr. |
| -s | Adds the host and associates the Internet address inet\_addr with the Physical address eth\_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent. |

# Netstat

Netstat (Network Statistics) displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It‘s a helpful tool in finding problems and determining the amount of traffic on the network as a performance measurement.

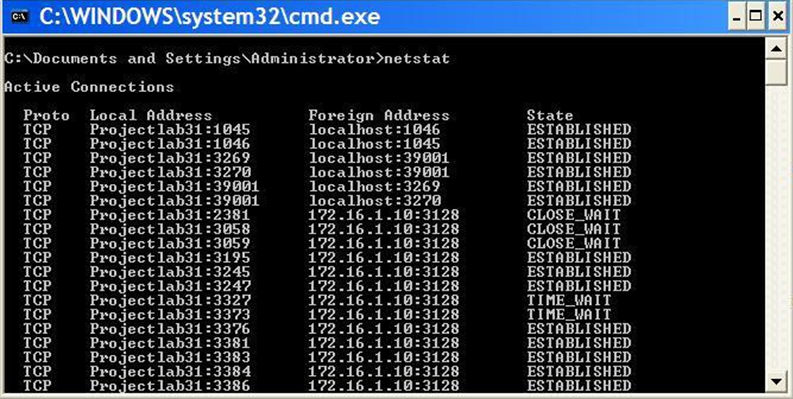
This utility provides the connection both the local and remote, ports and the state of the connection. It has several switches which maybe found by typing netstat /?

It provides the IP addresses and the ports of the remote computer(S) to which the socket is connected. If a port has not been established it is indicated by a \*. It shows the port numbers as well as IP address for the local computer.

It provides the type of protocol being used for the connection(s).It provides a status of the connection. Is it established?? Is it closed?? Or is it waiting?? And more

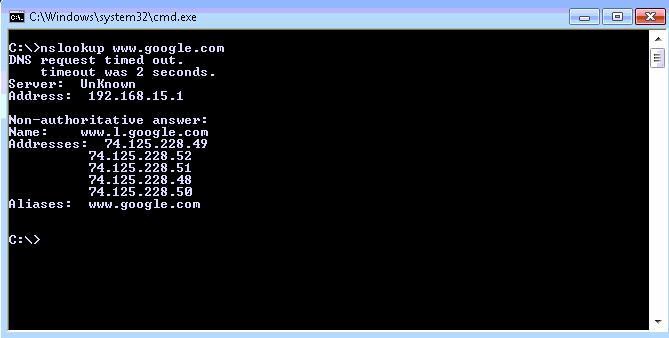
NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

|  |  |
| --- | --- |
| -a | Displays all connections and listening ports. |
| -e | Displays Ethernet statistics. This may be combined with the -s option. |
| -n | Displays addresses and port numbers in numerical form. |
| -p proto | Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the  -s option to display per-protocol statistics, proto may be TCP, UDP, or IP. |
| -r | Displays the routing table. |
| -s | Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default. |
| interval | Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once. |



# NSLookup

NSLookup provides a command-line utility for diagnosing DNS problems. In its most basic usage, NSLookup returns the IP address with the matching host name.

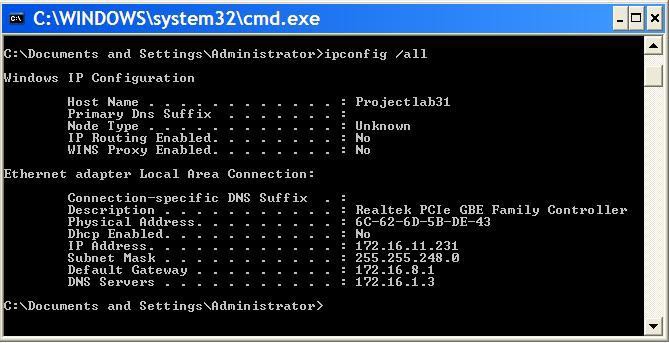


# IPConfig

Not part of the TCP/IP utilities but it is useful to show current TCP/IP settings.

The IPConfig command line utility will show detailed information about the network you are connected to. It also helps with reconfiguration of your IP address through release and renew.

Let‘s say you want to know what you‘re IP address is — **ipconfig** is what you type in the command prompt.



**ipconfig** will give a quick view of you IP address, your subnet mask and default gateway.

**ipconfig /all** will give you more detailed information.

Through **ipconfig /all** we can find DNS severs, if we have DHCP enabled, MAC Address, along with other helpful information. All good things to know if we have trouble getting connected to the internet.

SYNTAX

## ipconfig [/? | /all | /renew *adapter* | /release *adapter* | /flushdns | /displaydns | /registerdns | /showclassid adapter | /setclassid adapter *classid*

The adapter connection name can use wildcard characters (\* and ?).

OPTIONS

/? Displays this help message

/all Displays full configuration information

/release Releases the IP address for the specified adapter

/renew Renews the IP address for the specified adapter

/flushdns Purges the DNS Resolver cache

/registerdns Refreshes all DHCP leases and reregisters DNS names

/displaydns Displays the contents of the DNS Resolver Cache

/showclassid Displays all the DHCP ClassIds allowed for the specified adapter

/setclassid Modifies the DHCP ClassId

The default (with no parameters specified) is to display only the IP address, subnet mask, and default gateway for each adapter that is bound to TCP/IP.

For **/all**, Ipconfig displays all of the current TCP/IP configuration values, including the IP address, subnet mask, default gateway, and Windows Internet Naming Service (WINS) and DNS configuration.

For **/release** and **/renew**, if no adapter name is specified, the IP address leases for all adapters that are bound to TCP/IP are released or renewed.

For **/setclassid**, if no ClassId is specified, the ClassId is removed.

EXAMPLES

ipconfig Show information

ipconfig /all Show detailed information

ipconfig /renew Renew all adapters

ipconfig /renew EL\* Renew any connection whose name starts EL

ipconfig /release \*Con\* Release all matching connections, for example, "Local Area

Connection 1" or "Local Area Connection2"

# whois Command

To make it easier for administrators to find information about domains in this large distributed database, modern TCP/IP implementations generally come with an intelligent version of the whois utility. It is able to accept as input the name of a domain and automatically locate the appropriate registry in which that domain‘s information is located.

The utility is usually used as follows:

whois [-h <whois-host>] <domain>

In the above syntax, the term ―domain‖ represents the name about which registration information is requested. The administrator can use the ―-h‖ parameter to force the program to query a particular whois server, but again, this is usually not required.