

## C N ASSIGNMENT 1

Name: Diksha Katake

Roll No. – 331023

G.R. No. – 21820112

Batch: A1

**Aim:** Study of basic TCP/IP network commands and utilities (e.g.: ping, ifconfig, tracert, arp, tcpdump, whois, host, netsat, nslookup, ftp, telnet etc...)

**Objective:** To understand how the basic commands work and to implement them on Packet tracer

**Theory:**

### **Ping:**

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.

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

### **Ifconfig:**

ifconfig in short “interface configuration” utility for system/network administration in Unix/Linux operating systems to configure, manage and query network interface parameters via command line interface or in a system configuration scripts.

The “ifconfig” command is used for displaying current network configuration information, setting up an ip address, netmask or broadcast address to a network interface, creating an alias for network interface, setting up hardware address and enable or disable network interfaces.

## Tracert:

The *tracert* command on a Cisco device can be used to identify the path used by a packet to reach its target. It identifies all the routers in the path from the source host to destination host and it can be useful when troubleshooting network problems. Using this command, you can figure out which router in the path to an unreachable target should be examined more closely as the probable cause of the network's failure.

```
Invalid Command.

C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  1  1 ms    0 ms    0 ms    10.0.0.1
  2  8 ms    0 ms    0 ms    192.168.1.2

Trace complete.

C:\>
```

## Arp:

ARP stands for Address Resolution Protocol. This protocol is used by network nodes to match IP addresses to MAC addresses.

The host checks its ARP cache to see if address mapping from IP to physical address is known:

- If mapping is known, physical address is placed in frame and sent
- If mapping is not known, broadcast message is sent and awaits a reply
- Target machine, recognizing IP address matches its own, returns answer

## The "arp" Command

**arp** displays and modifies entries in the Address Resolution Protocol (ARP) cache, which contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses.

```
Trace complete.

C:\>arp
Packet Tracer PC ARP
Display ARP entries: arp -a
Clear ARP table: arp -d

C:\>arp -a
Internet Address      Physical Address      Type
10.0.0.1              0002.1686.6b01       dynamic

C:\>
```

## Tcpdump:

tcpdump command is also called as packet analyzer.

tcpdump allows us to save the packets that are captured, so that we can use it for future analysis. The saved file can be viewed by the same tcpdump command.

When you execute tcpdump command without any option, it will capture all the packets flowing through all the interfaces. -i option with tcpdump command, allows you to filter on a particular ethernet interface.

Whois:

**WHOIS** (pronounced as the phrase "who is") is a query and response [protocol](#) that is widely used for querying [databases](#) that store the registered users or assignees of an [Internet](#) resource, such as a [domain name](#), an [IP address](#) block or an [autonomous system](#), but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format.<sup>[1]</sup> The current iteration of the WHOIS protocol was drafted by the [Internet Society](#), and is documented in [RFC 3912](#).

Hostname:

The **hostname command** is used to show or set a computer's **host name** and domain name. ... The -a option displays any aliases (i.e., substitute names) that are used for the **host name**. The -i option displays the IP address(es) of the host, which by default is 127.0.0.1.

Netstat:

Netstat — derived from the words *network* and *statistics* — is a program that's controlled via commands issued in the command line. It delivers basic statistics on all network activities and informs users on which **ports and addresses** the corresponding connections (TCP, UDP) are running and which ports are open for tasks.

[OPTION]	Command	Description
	Netstat	Standard listing of all active connections
-a	netstat -a	Displays all active ports
-b	netstat -b	Displays the executable file of a connection or listening port (requires administrator rights)

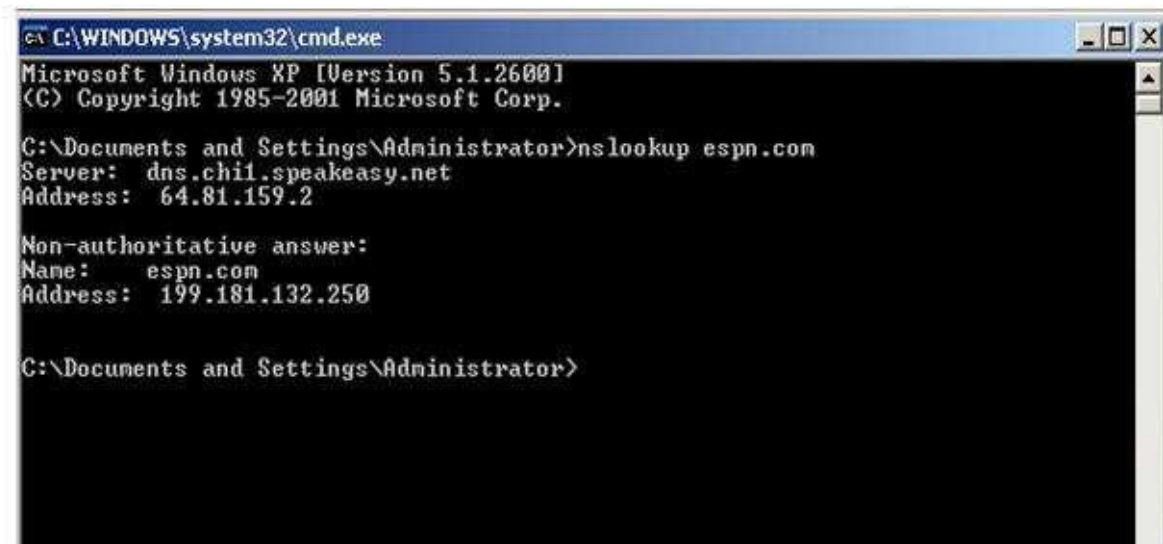
```
C:\Users\ayush>netstat
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	192.168.0.102:50941	52.139.250.253:https	ESTABLISHED

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.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>nslookup espn.com
Server: dns.chil.speakeasy.net
Address: 64.81.159.2

Non-authoritative answer:
Name:     espn.com
Address:  199.181.132.250

C:\Documents and Settings\Administrator>
```

Conclusion:

Hence we have successfully understood and tested network commands.