PRACTICAL – 7

AIM: Run basic utilities and network commands: ipconfig, ping, tracert, netstat, pathping, route,hostname.

Network Command-line Utilities

These utilities must be run at the prompt of the Cmd.exe command interpreter. To open Command Prompt, click Start, click Run, type cmd, and then click OK. Some command-line toolsrequire the user to have administrator-level privileges on source and/or target computers.

- ipconfig
- ping
- tracert
- pathping
- netstat
- route
- hostname

ipconfig

This ipconfig command is used for finding the IP address and default gateway of your network. Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

```
C:\Users\Nemis Ruparel>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
       /showclassid     Displays all the dhcp class IDs allowed for adapter.
       /setclassid      Modifies the dhcp class id.
       /showclassid6    Displays all the IPv6 DHCP class IDs allowed for adapter.
       /setclassid6     Modifies the IPv6 DHCP class id.


The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is removed.

Examples:
    > ipconfig                      ... Show information
    > ipconfig /all                 ... Show detailed information
    > ipconfig /renew               ... renew all adapters
    > ipconfig /renew EL*           ... renew any connection that has its
                                        name starting with EL
    > ipconfig /release *Con*       ... release all matching connections,
                                        eg. "Wired Ethernet Connection 1" or
                                            "Wired Ethernet Connection 2"
    > ipconfig /allcompartments     ... Show information about all
                                        compartments
    > ipconfig /allcompartments /all ... Show detailed information about all
                                        compartments
```

This enables users to determine which TCP/IP configuration values have been configured by DHCP, Automatic Private IP Addressing (APIPA), or an alternate configuration.

Syntax of ipconfig

> ipconfig /all
> ipconfig /displaydns
> ipconfig /flushdns

Examples of ipconfig

> To display the basic TCP/IP configuration for all adapters, type: ipconfig
> To display the full TCP/IP configuration for all adapters, type: ipconfig /all
> To flush the DNS resolver cache when troubleshooting DNS name resolution problems, type: ipconfig /flushdns
>

Ping

The ping (packet Internet groper) command is usually used as a simple way to verify that a computer can communicate over the network with another computer or network device. The ping command operates by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination computer and waiting for a response. Used without parameters, ping displays help.

Ping command can be used to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name is not, you might have a name resolution problem. In this case, ensure that the computer name you are specifying can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.

Syntax of ping

> ping [-t] targetname(url) ping www.google.com
> [-a] targetname(url)

> [-n Count] targetname(url)

> [-l Size] targetname(url)

> [-i TTL] targetname(url)

> **Examples of ping**
> The following example shows ping command output:
> **C:\>ping example.microsoft.com**
> Pinging example.microsoft.com [192.168.239.132] with 32 bytes of data:
> Reply from 192.168.239.132: bytes=32 time=101ms TTL=124
> Reply from 192.168.239.132: bytes=32 time=100ms TTL=124
> Reply from 192.168.239.132: bytes=32 time=120ms TTL=124

> Reply from 192.168.239.132: bytes=32 time=120ms TTL=124

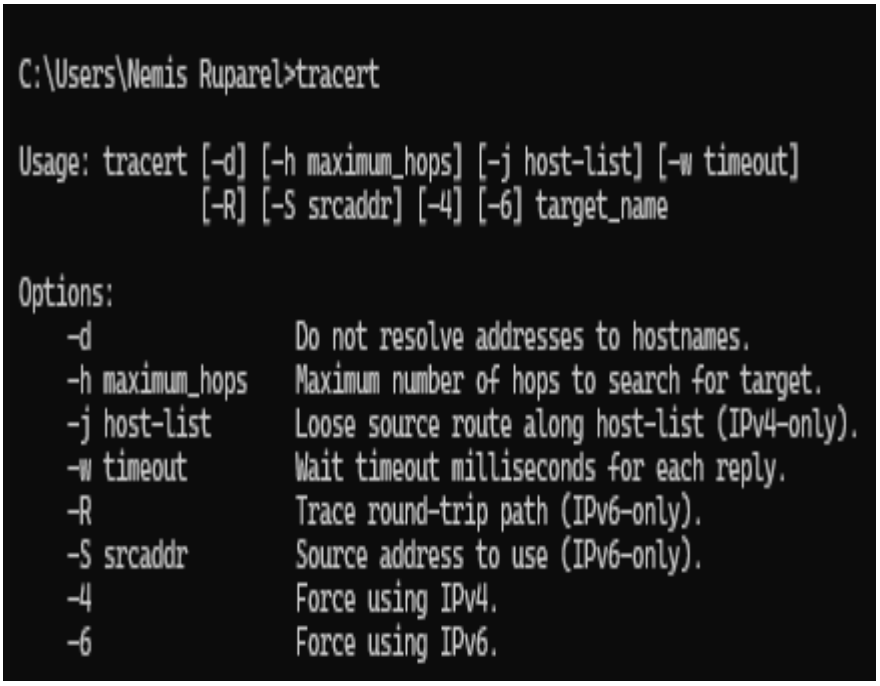
> **To ping the destination 142.250.207.206 and resolve 142.250.207.206 to its host name, type:**
ping -a 142.250.207.206

> **To ping the destination google.com with 10 Echo Request messages, each of which has a Data field of 1000 bytes,** type:

> ping -n 10 -l 1000 google.com

Tracert

The tracert command is a Command Prompt command that's used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded.Used without parameters, tracert displays help



This diagnostic tool determines the path taken to a destination by sending ICMP Echo Request messages with varying Time to Live (TTL) values to the destination. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it.

Effectively, the TTLis a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP Time Exceeded message to the source computer. Tracert determines the path by sendingthe first Echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequenttransmission until the target responds or the maximum number of hops is reached. The maximumnumber of hops is 30 by default and can be specified using the -h parameter.

The path is determinedby examining the ICMP Time Exceeded messages returned by intermediate routers and the Echo Reply message returned by the destination. However, some routers do not return Time Exceeded messages for packets with expired TTL values and are invisible to the tracert command. In this case,a row of asterisks (*) is displayed for that hop.

Syntax of tracert

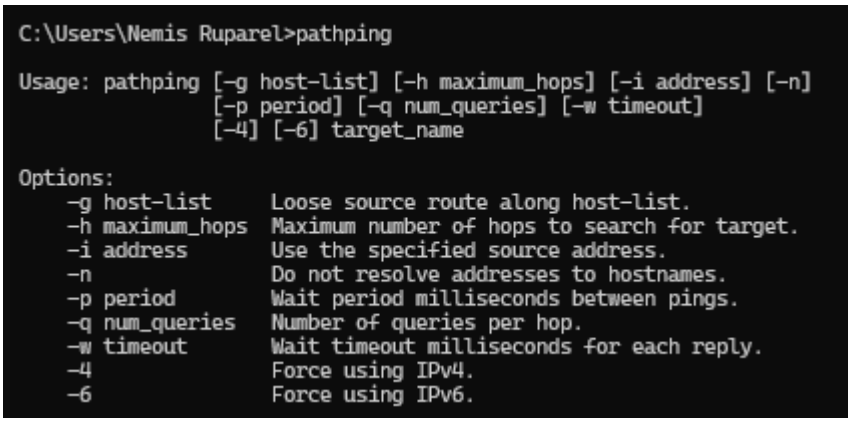
> tracert [-d]
> [-h MaximumHops]
> [-j HostList]
> [-w Timeout]
> [TargetName]

Examples of tracert

> To trace the path to the host named type: tracert google.com,
> To trace the path to the host named corp7.microsoft.com and prevent the resolution ofeach IP address to its name, type: tracert -d corp7.microsoft.com
> To trace the path type: tracert -w google.com
> To trace with number of hope,type: tracert -h 5 google.com

Pathping

Provides information about network latency and network loss at intermediate hops between a source and destination. Pathping sends multiple Echo Request messages to each router between a source and destination over a period of time and then computes results based on the packets returned from each router. Because pathping displays the degree of packet loss at any given router or link, you can determine which routers or subnets might be having network problems. Pathping performs the equivalent of the tracert command by identifying which routers are on the path. It then sends pings periodically to all of the routers over a specified time period and computes statistics based on the number returned from each. Used without parameters, pathping displays help.



Syntax of pathping

> pathping [-n]
> [-h MaximumHops]
> [-g HostList]
> [-p Period]
> [-q NumQueries]
> [-w Timeout]
> [-T]
> [-R]
> [TargetName]

Examples of pathping

> The following example shows pathping command output:
> pathping -n google.com
>
> When pathping is run, the first results list the path. This is the same path that is shown using the tracert command. Next, a busy message is displayed for approximately 90 seconds (the time variesby hop count). During this time, information is gathered from all routers previously listed

and fromthe links between them. At the end of this period, the test results are displayed.

> In the sample report above, the This Node/Link, Lost/Sent = Pct and Address columns show that the link between 172.16.87.218 and 192.168.52.1 is dropping 13 percent of the packets. The routers at hops 2 and 4 also are dropping packets addressed to them, but this loss does not affect their ability to forward traffic that is not addressed to them.

> The loss rates displayed for the links, identified as a vertical bar (|) in the Address column, indicatelink congestion that is causing the loss of packets that are being forwarded on the path. The loss rates displayed for routers (identified by their IP addresses) indicate that these routers might be overloaded.

Netstat

Netstat is a common command line TCP/IP networking utility available in most versions of Windows, Linux, UNIX and other operating systems. Netstat provides information and statistics about protocols in use and current TCP/IP network connections. Used without parameters, netstatdisplays active TCP connections.

```
C:\Users\Nemis Ruparel>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -c            Displays a list of processes sorted by the number of TCP or UDP
                ports currently consumed.
  -d            Displays DSCP value assocated with each connection.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -f            Displays Fully Qualified Domain Names (FQDN) for foreign
                addresses.
  -i            Displays the time spent by a TCP connection in its current state.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -q            Displays all connections, listening ports, and bound
                nonlistening TCP ports. Bound nonlistening ports may or may not
                be associated with an active connection.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -t            Displays the current connection offload state.
  -x            Displays NetworkDirect connections, listeners, and shared
                endpoints.
  -y            Displays the TCP connection template for all connections.
                Cannot be combined with the other options.
  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.
```

Syntax of netstat

> netstat [-a]
> [-e]
> [-n]
> [-o]
> [-p Protocol]
> [-r]
> [-s]
> [Interval]

Examples of netstat

> To display both the Ethernet statistics and the statistics for all protocols, type command:

> netstat -e -s

> To display the statistics for only the TCP and UDP protocols, type command:

netstat -s -p tcp udp

> To display active TCP connections and the process IDs every 5 seconds, type command:

> netstat -o 5

> To display active TCP connections and the process IDs using numerical form, type command:

> netstat -n -o

> **Route**

> Manipulates network routing tables.

```
C:\Users\Nemis Ruparel>route print
===========================================================================
Interface List
 21...6c 02 e0 57 66 7a ......Realtek PCIe GbE Family Controller
  5...0a 00 27 00 00 05 ......VirtualBox Host-Only Ethernet Adapter
 13...22 4e f6 88 18 3d ......Microsoft Wi-Fi Direct Virtual Adapter
 11...a2 4e f6 88 18 3d ......Microsoft Wi-Fi Direct Virtual Adapter #2
 12...20 4e f6 88 18 3d ......Realtek RTL8822CE 802.11ac PCIe Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   192.168.80.183    192.168.80.65     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
     192.168.80.0    255.255.255.0         On-link     192.168.80.65    311
    192.168.80.65  255.255.255.255         On-link     192.168.80.65    311
   192.168.80.255  255.255.255.255         On-link     192.168.80.65    311
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link     192.168.80.65    311
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link     192.168.80.65    311
===========================================================================
Persistent Routes:
  None

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 12     71 ::/0                     fe80::8c7a:19ff:fe91:a49e
  1    331 ::1/128                  On-link
 12     71 2409:40c1:200e:9285::/64 On-link
 12    311 2409:40c1:200e:9285:d4a5:16e0:b5f8:181d/128
                                    On-link
 12    311 2409:40c1:200e:9285:ec50:214:7500:d711/128
                                    On-link
  5    281 fe80::/64                On-link
 12    311 fe80::/64                On-link
 12    311 fe80::938d:a7fc:fa1d:3c75/128
                                    On-link
  5    281 fe80::c259:5a0e:41c4:c253/128
                                    On-link
  1    331 ff00::/8                 On-link
  5    281 ff00::/8                 On-link
 12    311 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

>

> **Syntax of route**

ROUTE [-f] [-p] [-4|-6] command [destination]
[MASK netmask] [gateway] [METRIC metric] [IF interface]

-f Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared prior to running the command.

-p When used with the ADD command, makes a route persistent across boots of the system. By default, routes are not preserved when the system is restarted. Ignored for all other commands,which always affect the appropriate persistent routes.

-4 Force using IPv4.

-6 Force using IPv6.

command One of these:

PRINT Prints a route

ADD Adds a route

DELETE Deletes a route

CHANGE Modifies an existing route

netmask Specifies a subnet mask value for this route entry.
If not specified, it defaults to 255.255.255.255.

gateway Specifies gateway.

> **Examples of route**

> route PRINT

> route PRINT -4

> route PRINT -6

> route PRINT 157* ..... Only prints those matching 157*

> route DELETE 157.0.0.0

*****