UTM

UNIVERSITI TEKNOLOGI MALAYSIA

Lab 2

Network Commands (Preliminary Works)

Basic knowledge for gathering information about a network using basic Command Line Interface (CLI)

Students will utilize basic *command-line* syntax to gather information about their network. This lab is intended to show that even basic CLI commands can yield valuable network information for a technician or to a potential hacker.

Recommended Resources for this Learning Activity

> *No external resources are needed for this lab. All commands and functions are built into the Windows operating system.*

The commands that will be used are:

IPCONFIG – IP addressing information (What IP address do I have?
Subnet-Mask? Default Gateway? Etc.)

Ping – connectivity check (Is the target host up?)

Netstat - TCP connections (What connections does this machine have?)

Tracert - Path taken to target machine (What is the map of the network?)

NSLookup - Identify DNS information

================== **IPCONFIG** ===================

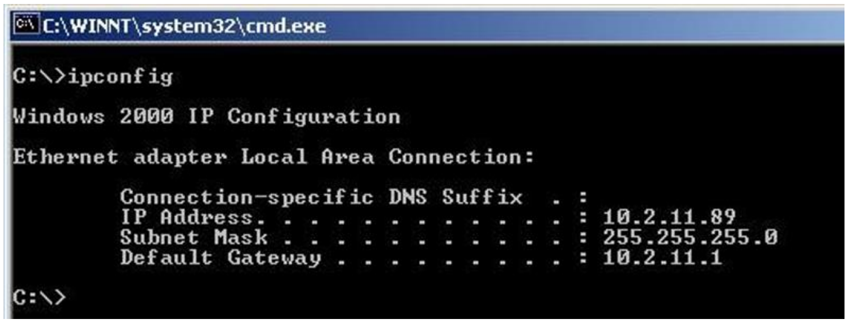
IPCONFIG show the IP configuration or modifies the IP configuration.

Syntax:

IPCONFIG /all	Display full IP configuration information.
IPCONFIG /release [adapter]	Release the IP address for the specified adapter.
IPCONFIG /renew [adapter]	Renew the IP address for the specified adapter.
IPCONFIG /flushdns	Purge the DNS Resolver cache.
IPCONFIG /registerdns	Refresh all DHCP leases and re-register DNS names.
IPCONFIG /displaydns	Display the contents of the DNS Resolver Cache.
IPCONFIG /showclassid adapter	Display all the DHCP class IDs allowed for adapter.
IPCONFIG /setclassid adapter [classid]	Modify the DHCP class id.

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

1) ipconfig

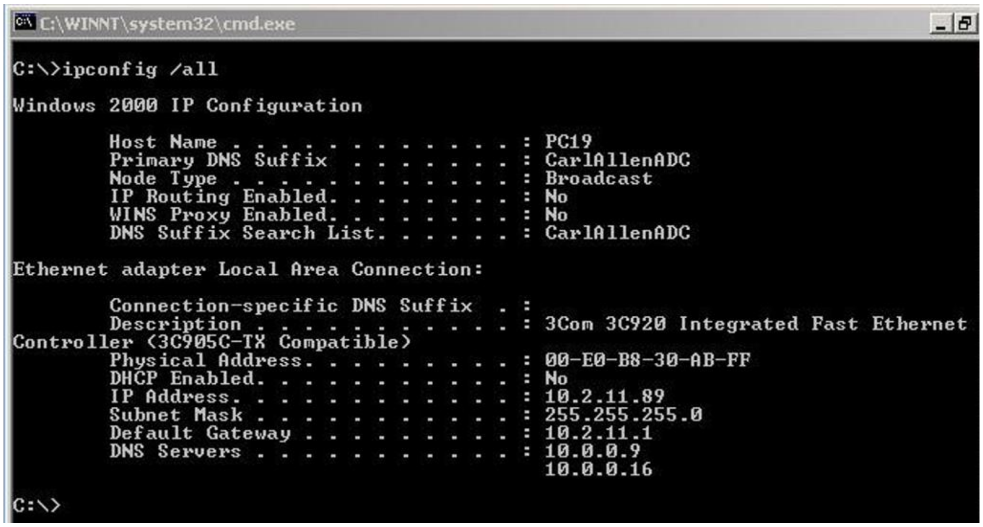


```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.2.11.89
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.2.11.1

C:\>
```

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

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

2) ipconfig /all [| more]



```
C:\>ipconfig /all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : PC19
        Primary DNS Suffix  . . . . . . . : CarlAllenADC
        Node Type . . . . . . . . . . . . : Broadcast
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : CarlAllenADC

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : 3Com 3C920 Integrated Fast Ethernet
Controller (3C905C-TX Compatible)
        Physical Address. . . . . . . . . : 00-E0-B8-30-AB-FF
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 10.2.11.89
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.2.11.1
        DNS Servers . . . . . . . . . . . : 10.0.0.9
                                            10.0.0.16

C:\>
```

ipconfig /all displays all available information that is known to the network card. To see all of the output, you may need to pipe "|" the output to *more*.

Examples:

ipconfig	... Show information.
ipconfig /all | more	... Show detailed information
ipconfig /release	... release DHCP configuration
ipconfig /renew EL*	... renew any connectionwith a name starting with EL
ipconfig /release *Con*	... release all matching connections, e.g. "Local Area Connection 1" or"Local Area Connection 2"
ipconfig /setclassid "Local Area Connection" TEST	... set the DHCP class-ID for the named adapter to TEST

=================== Ping ==================

Ping test a network connection - if successful, ping returns the IP address if using site name.

PING stands for **P**acket **I**nter**N**et **G**roper

Syntax: ping [options] {destination-IP address}

options

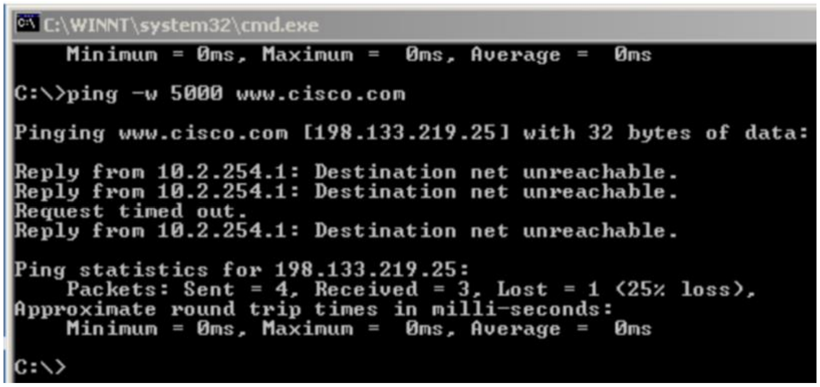
-w timeout	Timeout in milliseconds to wait for reply.
-i TTL	Time To Live.
-v TOS	Type Of Service.
-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-t	Ping the destination repeatedly.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet.
-r count	Record route for 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. destination_host The name of the
remote host

A response of "Request timed out" means there was no response to the ping attempt in the default time period of one second. Occasionally, administrators disable the ICMP feature in order to prevent ping scans of their network.

If the latency of the response is more than one second. use the -w option on the ping command to increase the time-out. For example, to allow responses within five seconds, use: ping -w 5000.

```
ping -w 5000 www.cisco.com
```

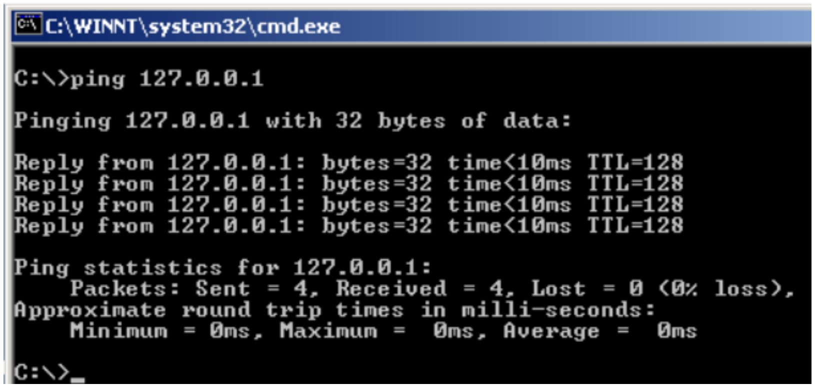


```
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping -w 5000 www.cisco.com

Pinging www.cisco.com [198.133.219.25] with 32 bytes of data:

Reply from 10.2.254.1: Destination net unreachable.
Reply from 10.2.254.1: Destination net unreachable.
Request timed out.
Reply from 10.2.254.1: Destination net unreachable.

Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

NOTE: ***The response of "Destination net unreachable" indicates that the gateway router was unable to receive a response from the target network. This is possibly due to firewall restrictions at the target network.***

1) Ping the *loopback address* to verify that TCP/IP is installed and configured correctly on the local computer. (i.e. 127.0.0.1)

```
PING 127.0.0.1
ping 127.0.0.1
```

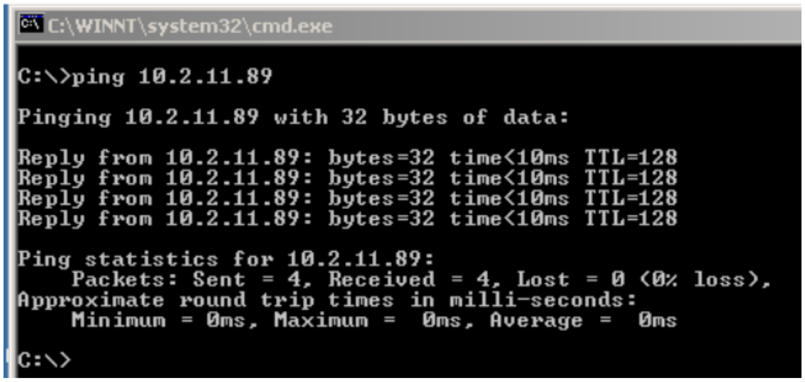


```
C:\>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>_
```

2) Ping the IP address of the local computer (host) to verify that it was added to the network correctly.

PING *local-host_IP-address*

```
ping 10.2.11.89
```



```
C:\>ping 10.2.11.89

Pinging 10.2.11.89 with 32 bytes of data:

Reply from 10.2.11.89: bytes=32 time<10ms TTL=128
Reply from 10.2.11.89: bytes=32 time<10ms TTL=128
Reply from 10.2.11.89: bytes=32 time<10ms TTL=128
Reply from 10.2.11.89: bytes=32 time<10ms TTL=128

Ping statistics for 10.2.11.89:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>
```

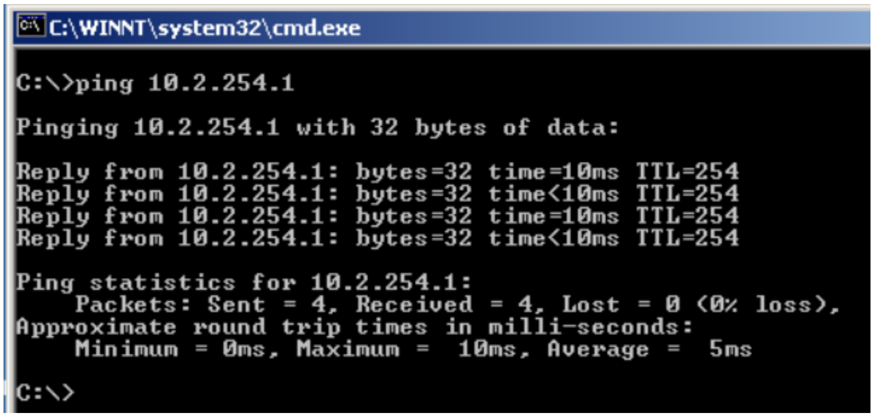
(Remember that the IP-address of your local host may be different than the one in the graphic. Use the command IPCONFIG to see your IP address.)

3) Ping the IP address of the default gateway to verify that the default gateway is functioning and that you can communicate with a local host on the local network.

```
PING default-gateway_ IP-address
```

(Use the command IPCONFIG to get your default gateway address –or– your instructor should have the gateway address)

```
ping 10.2.254.1
```



```
C:\>ping 10.2.254.1

Pinging 10.2.254.1 with 32 bytes of data:

Reply from 10.2.254.1: bytes=32 time=10ms TTL=254
Reply from 10.2.254.1: bytes=32 time<10ms TTL=254
Reply from 10.2.254.1: bytes=32 time=10ms TTL=254
Reply from 10.2.254.1: bytes=32 time<10ms TTL=254

Ping statistics for 10.2.254.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  10ms, Average =  5ms

C:\>
```

4) Ping the IP address of a remote host to verify that you can communicate through a router.

`PING remote-host_ IP-address`***(Choose any local host to ping.)***

If the network administrator has disabled ICMP on the router it may not give a valid reply.

Examples:

```
ping -n 1 -w 5000 workstation_name

ping -w 5000 host_addr|find "TTL=" && ECHO MyHost found

ping -w 5000 host_addr|find "TTL=" || ECHO MyHost not found

ping -n 5 -w 5000 www.microsoft.com

ping -n 5 -w 7500 microsoft.com
```

=====================NetStat =====================

NetStat reports active TCP connections, the ports the computer is listening to, the IP routing table and Ethernet statistics, IPv4 (for protocols IP, ICMP, TCP and UDP) and IPv6 (for protocols IPv6, ICMPv6, TCP on IPv6 and UDP on IPv6).

Syntax:

Netstat [-a] [-E] [-N] [-O] [-p *protocol*] [-S] [-r] [*interval*]

Parameters:

- a

Posts all active connections with the computer and lists them by TCP and UDP protocol.

- E

Posts Ethernet statistics, lists the number of bytes and packets sent and received. This parameter can be combined with - S.

- N

Posts active connections on TCP, but the number of the port and the addresses are in numerical format and no attempt is made to determine the names.

- O

Posts active connections TCP and includes the ID of process (PID) of each connection. You can determine the application on the basis of PID indicated.

/p protocol

Posts connections using the protocol indicated by protocol. The protocol can be TCP, UDP, tcpv6 or udpv6. If this parameter is utilized with - S to post statistics by protocol, the protocol can be TCP, UDP, ICMP, IP, tcpv6, udpv6, icmpv6 or ipv6.

- S

Posts statistics by protocol. By default, the statistics of TCP, UDP, ICMP and IP are posted. If the IPv6 is being used then the statistics will relate to TCP on IPv6, UDP on IPv6, and ICMP on IPv6. The parameter -p can be used to specify a whole list of protocols.

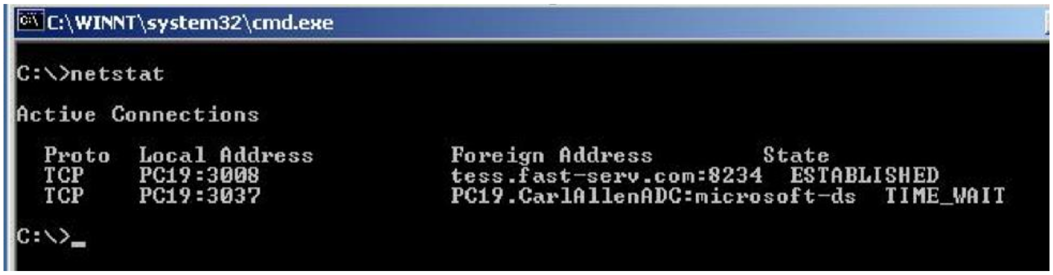
- r

Lists the contents of the IP routing table.

Using NetStat to gather network information.

1) netstat

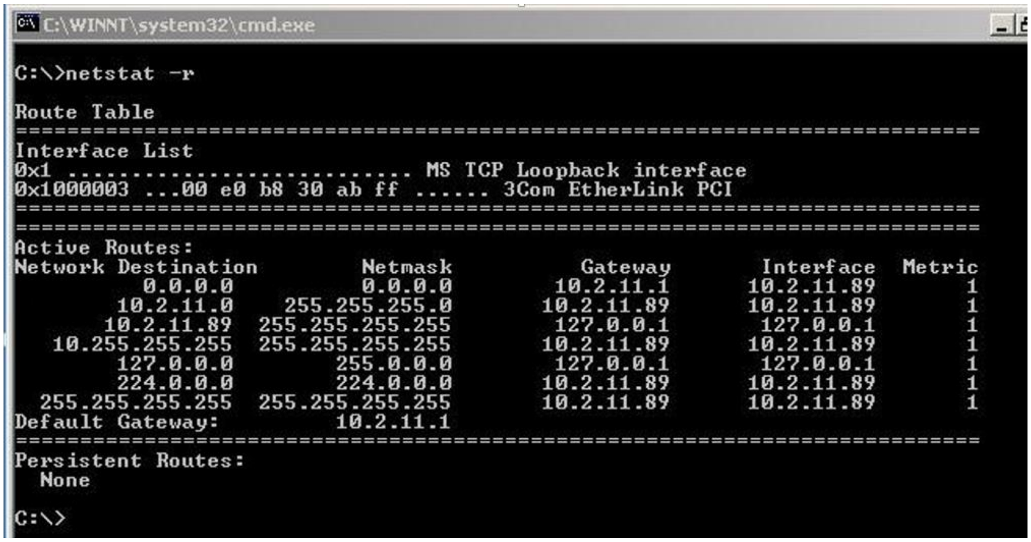
By simply entering netstat, the command will display the protocol, local host, foreign address/host that a connection is being made to, and the status of the connection.



```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    PC19:3008              tess.fast-serv.com:8234  ESTABLISHED
  TCP    PC19:3037              PC19.CarlAllenADC:microsoft-ds  TIME_WAIT

C:\>_
```

2) netstat –r

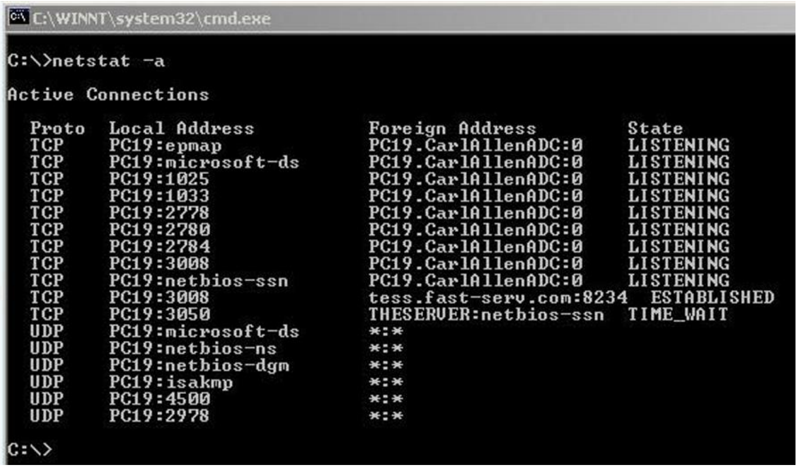
By entering the **–r** switch the netstat command will display the routing table information.



```
C:\>netstat -r

Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 e0 b8 30 ab ff ...... 3Com EtherLink PCI
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0        10.2.11.1     10.2.11.89       1
        10.2.11.0    255.255.255.0       10.2.11.89     10.2.11.89       1
       10.2.11.89  255.255.255.255        127.0.0.1      127.0.0.1       1
   10.255.255.255  255.255.255.255       10.2.11.89     10.2.11.89       1
        127.0.0.0        255.0.0.0        127.0.0.1      127.0.0.1       1
        224.0.0.0        224.0.0.0       10.2.11.89     10.2.11.89       1
  255.255.255.255  255.255.255.255       10.2.11.89     10.2.11.89       1
Default Gateway:         10.2.11.1
===========================================================================
Persistent Routes:
  None

C:\>
```

3) netstat –a

By using the **–a** switch it will display ALL connections, TCP or UDP, with your host. This can be used to identify other hosts on the network or to identify that a connection is made to your machine without your knowledge.



```
C:\>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    PC19:epmap             PC19.CarlAllenADC:0    LISTENING
  TCP    PC19:microsoft-ds      PC19.CarlAllenADC:0    LISTENING
  TCP    PC19:1025              PC19.CarlAllenADC:0    LISTENING
  TCP    PC19:1033              PC19.CarlAllenADC:0    LISTENING
  TCP    PC19:2778              PC19.CarlAllenADC:0    LISTENING
  TCP    PC19:2780              PC19.CarlAllenADC:0    LISTENING
  TCP    PC19:2784              PC19.CarlAllenADC:0    LISTENING
  TCP    PC19:3008              PC19.CarlAllenADC:0    LISTENING
  TCP    PC19:netbios-ssn       PC19.CarlAllenADC:0    LISTENING
  TCP    PC19:3008              tess.fast-serv.com:8234  ESTABLISHED
  TCP    PC19:3050              THESERVER:netbios-ssn  TIME_WAIT
  UDP    PC19:microsoft-ds      *:*
  UDP    PC19:netbios-ns        *:*
  UDP    PC19:netbios-dgm       *:*
  UDP    PC19:isakmp            *:*
  UDP    PC19:4500              *:*
  UDP    PC19:2978              *:*

C:\>
```

=================== Tracert ====================

Trace Route will find the IP address of any remote host. Tracert is useful for troubleshooting large or small networks where several paths can be taken to arrive at the same point. Tracert will potentially display routers and other key hardware components from your location to the destination. This command is great for mapping a network.

Syntax:
TRACERT [options] target_name
TRACERT [options] target_ip address
Key:

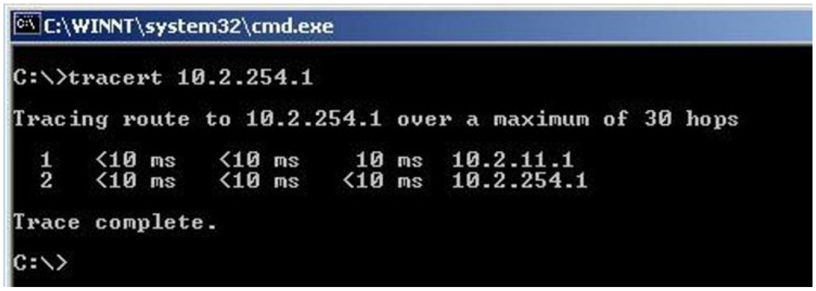
target_name	The HTTP or UNC name of the host.
target_ip address Options:	The 32 bit IP address of the target.

-d	Do not resolve addresses to hostnames. (avoids performing a DNS lookup)
-h max_hops	Maximum number of hops to search for target.
-j host-list	Trace route along given host-list.
-w timeout	Wait *timeout* milliseconds for each reply.

The functionality of TRACERT is the same under all versions of windows but the appearance of the output is improved under Windows XP.

Tracert uses the IP TTL field and ICMP error messages to determine the route from one host to another through a network. However, care must be taken when using this utility as it shows the optimal route, (best path selected, based on the metric for the routing protocol used on the network) not necessarily the actual route.

1) tracert 10.2.254.1



```
C:\>tracert 10.2.254.1

Tracing route to 10.2.254.1 over a maximum of 30 hops

  1    <10 ms    <10 ms     10 ms  10.2.11.1
  2    <10 ms    <10 ms    <10 ms  10.2.254.1

Trace complete.

C:\>
```

Examples:

TRACERT www.cisco.com

TRACERT 201.58.65.2

TRACERT gateway_IP_address

================== nslookup ===================

Google the internet looking for nslookup—it usage and command syntax