NETWORKING BASICS LAB1: NETWORK INTRODUCTION

Objectives

At the end of this laboratory exercise, student should be able to:

use the basic Windows command-line networking tools to check connectivity

Command-Line Networking Tools

There are a number of Command-Line (or Window's Console) programs included with the Windows operating systems.

The following programs used in this module's laboratory exercises are located on the C drive.

Program	Description
`IPCONFIG.EXE`	IPCONFIG.EXE is used to view current network configuration.
`NET.EXE`	NET.EXE used to view Microsoft network shared resources.
`PING.EXE`	PING.EXE is a basic connectivity test between two systems running TCP/IP.
`ARP.EXE`	ARP.EXE uses ARP (Address Resolution Protocol) to provide dynamic mapping from an IP address to the corresponding hardware (MAC) address.
`TRACERT.EXE`	TRACERT.EXE traces the route that IP datagrams follow from one host to another
`NETSTAT.EXE`	NETSTAT displays protocol statistics and current TCP/IP network connections.

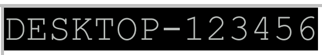
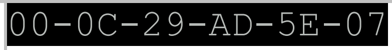
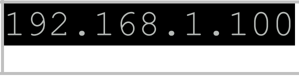
EXERCISE 1 – CHECK COMPUTER NETWORK CONFIGURATION

Check configuration of the network interface card (NIC)

Open the Command Prompt window by clicking into the Search Box at the lower left of the computer screen and type **cmd**, which will cause a command prompt window to appear (Windows users).

IPCONFIG

Enter the `ipconfig /all` command and note the following:

Host Name	 DESKTOP-123456
Physical (MAC) addresses	 00-0C-29-AD-5E-07
IP Address	 192.168.1.100

DHCP server	192.168.1.1
DNS server	192.168.1.1
Default Gateway	192.168.1.1

Note:
MAC Address: (Physical Address): Hardware address that uniquely identifies each node on a network. Each Network Card is given a unique MAC address when it is manufactured, e.g., `00:03:6D:40:00:A2`
IP Address: Every user on a TCP/IP system has to be assigned a unique identifier called an IP address. A unique number that identifies a computer so that it may communicate via Internet protocols. It consists of four numbers separated by periods e.g. 147.252.238.100
DHCP: (Dynamic Host Configuration Protocol) – This is a protocol that automatically assign an IP Addresses to a computer. To connect to the internet an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer.
DNS: (Domain Name Service) A Domain Name System (or Service) translates alphabetic domain names into numeric IP addresses. For example, the domain www.itb.ie might translate into an IP address of 193.1.36.24
Default Gateway: The default gate way is another name for a router. It is where data that does not have a local address is sent. It is the way in and out of the local network.
Windows Networking Tools
There are a number of Command-Line (or Window's Console) programs included with all versions of Windows operating systems. Some are listed below.

1) Ping

PING is a basic Internet program that lets you verify that a particular Internet address exists and can accept requests. To “ping” is the act of using the ping utility or command. Pinging is diagnostically used to ensure that a host computer, which you are trying to reach, actually operates.

a) First try to ping your own machine by entering:

```
ping localhost
```

What IP address is used when pinging your own machine? 127.0.0.1

b) You can also ping a PC on a different Network:

```
ping 104.18.143.17
```

What is the average time? 12 milliseconds

What is the TTL? 59

You can also ping using a domain name: type

```
ping www.rte.ie
```

What is the average time? 12 milliseconds

What is the TTL? 59

Other Options

-n number of times a packet is sent

-l (note that this command uses the letter l as in Lima) size of packet sent

Try: `ping -n 10 -l 5000 <some public ip address that will allow this ping - most web sites will not respond to this ping for security reasons!>`

This will send 5000 bytes of data to a public ip address 10 times.

You could try: ping -n 10 -l 5000 104.18.143.17

Try to ping Google:

```
ping www.google.com
```

Was it successful? No

Note: Both ***ping*** and ***tracert*** (see later) use the ICMP protocol. The college firewall blocks all incoming and outgoing ICMP data for security reasons. For example, you could continuously ping a web server with a large amount of data. This would slow down the web site and under certain conditions you could “crash” the web server. This is known as a *denial of service* attack. So if we type, on campus, ***ping www.google.com***, it will not work as the college firewall will block it.

2) Tracert

Tracert traces the route from your PC to a destination PC. It lets us know how many ***routers*** the message passes through before it gets to its destination.

Command	Number of Hops	Number of Routers
`tracert www.rte.ie□`	16	15

`tracert  www.hea.net□` 14 13

Web-based Trace Route

As stated earlier ***ping*** and ***tracert*** use the ICMP protocol. The college firewall blocks all incoming and outgoing ICMP data for security reasons.
Try, next time you are in a networking lab in college:

```
tracert  www.google.com
```

What would you expect will happen?: Nothing

There are several ***web-based*** trace route utilities that allow us to get some idea as to the path that data takes between source and destination.
Log on to HYPERLINK "http://www.traceroute.org" www.traceroute.org.

Here you will find a list of web sites that you can trace a route **back to, for instance, to** RTE, from them. From the router names you ***may*** be able see where they are geographically

Select the Princeton University site in the USA. Do a trace route:
How many routers does the message pass through to get to home: 17
Can you identify any **cities** or countries it passed through:
Dublin, Ireland; London, United Kingdom; New York City, United States; Princeton, United States

Select any Australian site (e.g., **Telstra**). Do a trace route:
How many routers does the message pass through to get to home: 20
Can you identify any cities or countries it passed through:
Dublin, Ireland; London, United Kingdom; Sydney, Australia