BAY OF PLENTY POLYTECHNIC TAURANGA Te Kuratini o Poike	**COMP5003 IT Essentials and Networking**	**L01** **Tutorial 01**

LO1 Tutorial 01: Lab Exercise- Investigating the Networks in the Labs

AIM

- Students will investigate the setup of the networks that they will connect to during their COMP5003 course.
- Obtain basic familiarisation with the IP addressing used in the labs.
- Use some basic networking commands that will be useful in future for gathering information and for troubleshooting network problems.
- Become acquainted with some of the servers in the network.

The Networks

Corporate Network
The BoP Polytechnic maintains a "corporate" network for staff and the majority of students to use. The Windermere and Bongard campuses are linked by a high speed optical fibre link. The "corporate" servers are located at the Windermere campus and access to the Internet is via a "corporate" firewall.

IT students can use computers on this network but not all the specialised software required by IT students

The IT Student Networks – "Pandora" and "NetLab" (NL)
The computers on the corporate network are so locked down to prevent changes to the system that IT students cannot perform all the tasks they would be required to do during their course.

The IT teaching department maintains separate networks for IT students. These networks are separate from the main BoP Polytechnic corporate network and are for use by IT students enrolled the certificate and diploma courses. Students have more access/freedom (eg. local administration) on these computers.

The IT student networks comprise of two logical networks "Pandora" and "NetLab" (NL). These two logical networks are physically connected by switches/cables but because they use different IP addressing schemes, they behave as two separate networks.

Pandora and NetLab (NL) are "private" (or internal) networks but do have access to the public (external) Internet via gateway/firewall/proxy servers.

Although IPv6 is slowly transitioning on the Internet, IPv4 is still predominant. The Pandora and NetLab (NL) networks use IPv4 addressing and we will be using IPv4 for the COMP5003 course.

Rooms connected to the IT Student Networks

Bongard Level 3:
DT303, DT308 & DT312 teaching rooms

DT305 is the room containing the Pandora servers and they use Private IP addressing:
Network Address: 192.168.1.0/24
Subnet Mask: 255.255.255.0
Address Range: 192.168.1.0 to 192.168.1.255

Bongard Level 2:
DT219 teaching room
DT219 alcove is a space containing the NetLab (NL) servers and they use Private IP addressing:
Network address: 10.100.0.0/16)
Subnet Mask: 255.255.0.0
Address Range: 10.100.0.0 to 10.100.255.255

Rooms DT303, 308, 312 and DT219 all contain **"standard**" Pandora disks that are configured to connect to the Pandora servers.

Rooms DT303, 308 and DT219 also will have *separate* hard disk caddies (usually kept in a box at the back of the room) for students to install operating systems and to connect to the NetLab (NL) network and its servers.

The Pandora and NetLab networks each have a separate connection to the Internet.

>>>>> Refer to the network diagram on a following page. <<<<<

Pandora Host (ie. Computer) Names
Students in the COMP 5003 classes will typically only be using DT303 and DT308.

When using the **standard** Pandora hard disk caddy, the computers in DT303 and DT308 have a convention for their host (computer) names.

In DT303 the names will be:	PAN303-**nn** Where "nn" is the computer number eg. PAN303-06
In DT308 the names will be:	PAN308-**nn** Where "nn" is the computer number eg. PAN308-17

Note on Lab IP Addressing

You will learn more about IP addressing and TCP/IP settings later in the course. For now all you only need to know some basics to gain some familiarity with these concepts – the explanations will follow in later classes.

The Pandora and NetLab (NL) networks and servers use IP addresses that are known as "Private" IPv4 addresses. These private IP addresses are not allocated to hosts (ie. computers) on the public Internet. Internet computers use "public" IPv4 addresses.

Private IP Addresses
Private addresses have three ranges:

- 10.0.0.0 to 10.255.255.255 (known as Class A private addresses)*
- 172.16.0.0 to 172.31.255.255 (known as Class B private addresses)
- 192.168.0.0 to 192.168.255.255 (known as Class C private addresses)**

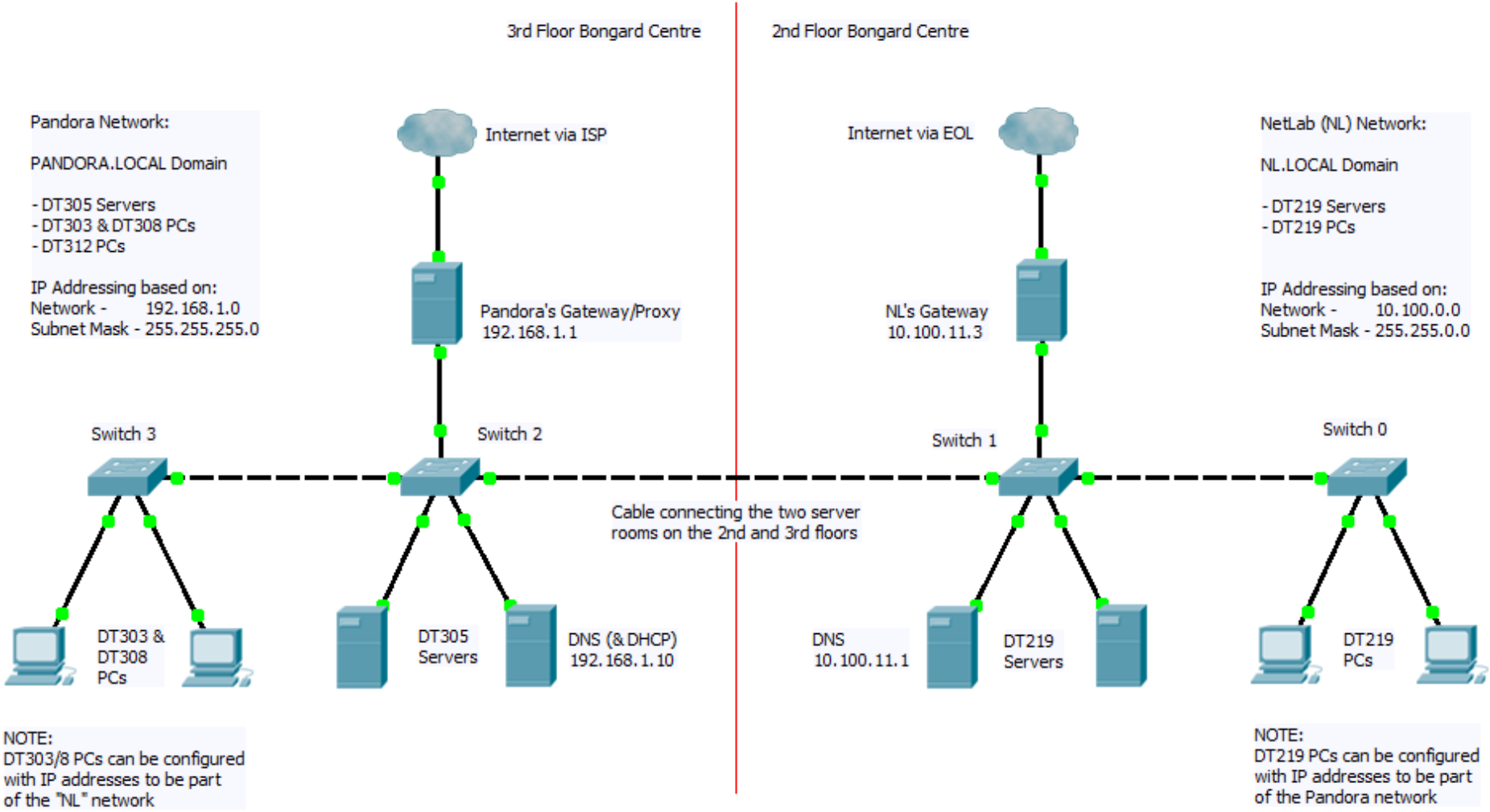
* NetLab (NL) uses a portion of (a subnet of) the private Class A network for its IP addressing.
** Pandora uses one of the private Class C networks for its IP addressing.

Private IP addresses do not exist on the Internet and are not routed to the Internet from private IP networks.

Public IP addresses (see https://www.iana.org)
The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the IP addressing, and other Internet protocol resources.

NAT
Private (internal) IP network addresses must be **translated** to a Public IP address provided by your Internet Service Provider (ISP). This translation of private to public addresses is done by a service called NAT (**Network Address Translation**). This NAT service runs on a "border" device that separates the internal private network from the public Internet. NAT typically resides on the private network's gateway/firewall/proxy device.

DAC COMP5003 & COMP5004: Network diagram depicting basic layout/connectivity (simplified version)



Classroom Computers - Hardware in DT303 and DT308

COMP5003 students will typically be using DT303 and DT308 for their tutorials and practical classes.

Note: There are two different models of HP PCs in each of DT303 and DT308.

Smaller Case PC:	**HP Compaq 8200 MT**
CPU:	Intel Core i5-2400 3.1GHz
Network Interface Card:	Intel 82579LM Gigabit
Graphics:	AMD Radeon HD 6450 video card
RAM:	8 GB
Motherboard:	**EFI** (Extensible Firmware Interface) compliant
Hard Disk:	in a removable caddy <<< NOTE

Larger Case PC:	**HP Compaq 8300 CMT**
CPU:	Intel Core i5-3470 3.2GHz
Network Interface Card:	Intel 82579LM Gigabit
Graphics:	Intel HD Graphics (integrated video card on the motherboard)
RAM:	8 GB
Motherboard:	**UEFI** (Unified Extensible Firmware Interface) compliant
Hard Disk:	in a removable caddy <<< NOTE

Hard Disk Drives – Use of Caddies

The PCs in DT303 and DT308 make use of a removable hard drive system (caddies) so that depending on what class students are in they can use the **standard** "Pandora" disk or take it out and put in a separate hard drive for installation of operating systems (eg. as will later be the case in the COMP5003 class).

The Standard PANDORA Hard Disk

In DT303 and DT308 the standard Pandora hard disk should be in the computer. If/when in the future you need to take it out, make sure it is replaced in position before you leave the classroom. The caddy requires a key to unlock it so it can be removed from the computer and the removal must take place with the computer's power OFF! This will be demonstrated to students by the class tutor.

If the caddy is not inserted and pushed in place properly or the key is not used to lock it (which also provides power to the hard disk) then the disk will not be detected by the computer and it will not boot.

The standard Pandora hard disk contains all the software and programming applications that students will need in other classes and this disk is shared by many students in many different classes (CIC, DAC L5 & L6). You will log onto it using your Pandora username and password.

>>>>>>> This exercise will only make use of the standard "Pandora" disk. <<<<<<<

PART A – PANDORA NETWORK

By default the standard Pandora disk's Windows operating system is setup to automatically connect to the Pandora network (IP address in the 192.168.1.0 network).

A DHCP (Dynamic Host Configuration Protocol) server on the network is set up to give DHCP clients a unique IP address and other settings to work on the Pandora network. The NIC (Network Interface Card) of your computer will get an address in the 192.168.1.0 network.

Your computer (i.e. your Windows operating system) is setup as a DHCP client, i.e. it will obtain its IP address and other settings automatically from the DHCP server on the network.

Task 1 – Logon and Access the Pandora Network

With the "standard' Pandora hard disk caddy inserted and locked into position, start the computer.

At the login screen provide your Pandora authentication credentials (ie. username/password).

Example:	Username: 9876543	- Your student id number.
	Password: *******	- Whatever you changed it to.

Note: You would have changed your password from its default at the student orientation session. If you have not changed it then it still should still be your surname (with a capital first letter), eg. "Smith".

Task 2 – Investigate Pandora's Shared Resources

When you logged on to Pandora, a logon script or policies would have given you access to network resources.

1. Open "Computer". Other than the local C:/D: drives you should also see H:, I: and X: drives. H, I and X drives are shared folders on a server in the server room DT305.

   - H: is your "Home" directory (ie. folder) is read/write by you only
   - I: is the "Info" directory is read only by you (tutors place info here for students to access)
   - X: a drop box for students to leave assignments for tutors.

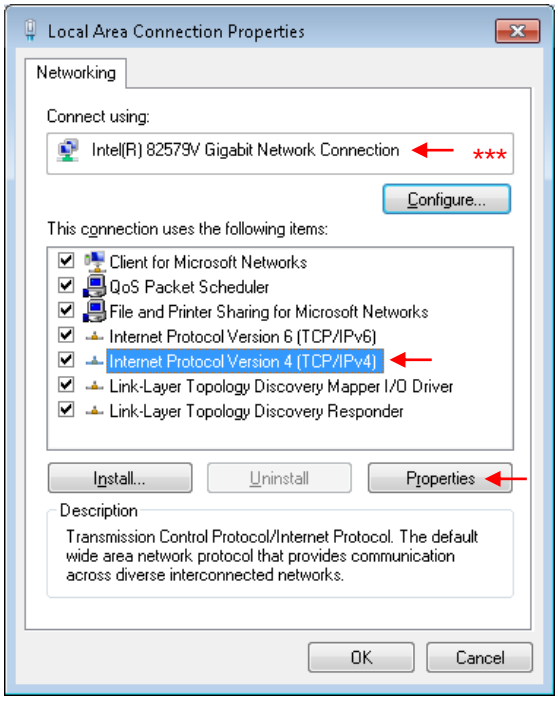
2. Open Control Panel > Devices and Printers.
   You should see a printer installed:
   - "rm303 HP Printer" in DT303
   - "rm308 HP Printer" in DT308.

   Devices and Printers should also be available directly in the Start menu.

Task 3 – Investigate Dynamic/Automatic IP Configuration

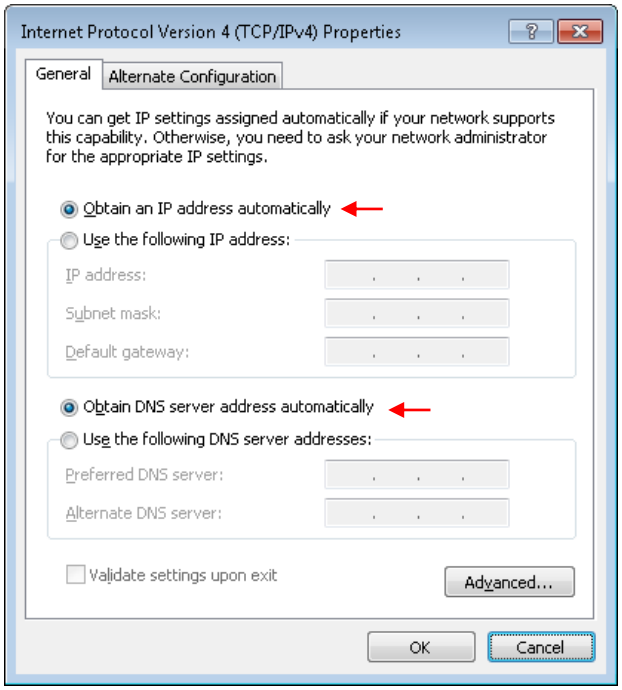
By default your NIC will be configured within Windows to have IP address settings obtained automatically (ie. your computer is a DHCP client).

1. See Network and Sharing Centre > Change Adapter Settings > Local Area Connection properties. Then Internet Protocol Version 4 (TCP/IPv4) properties. (Do not change anything). (See screen shots on the next page).



*** Your NIC's make/model may/will be different.

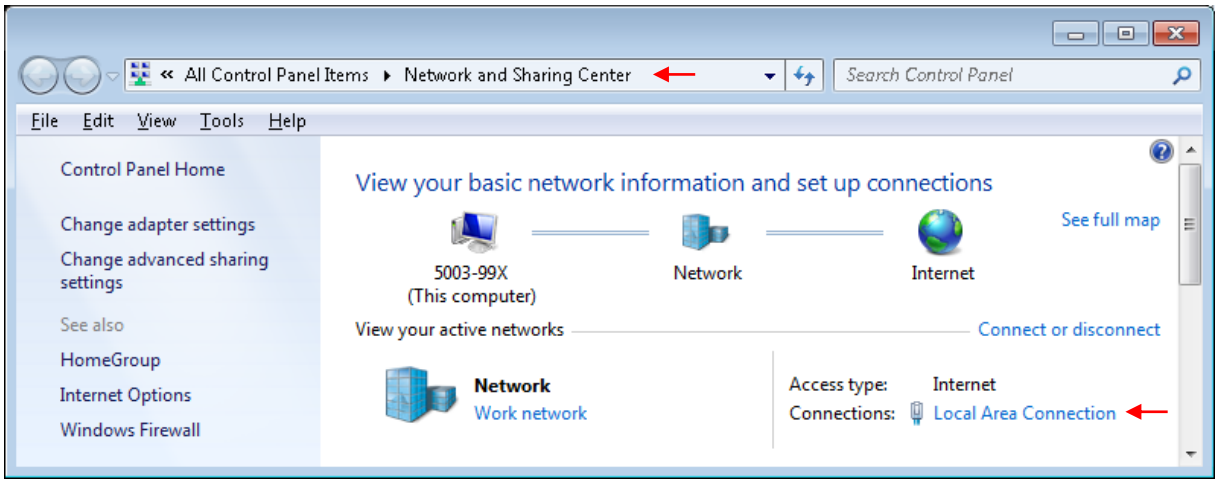
.



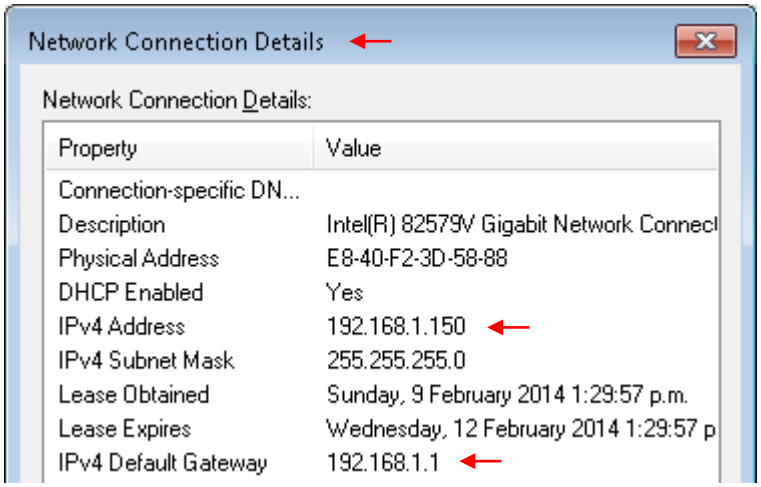
There is a **DHCP** (Dynamic Host Configuration Protocol) server on the "Pandora" network that provides DHCP clients (ie. your PC) with TCP/IP settings automatically.

Your PC's IP address will be 192.168.1.X, where "X" will be some number allocated by the DHCP server.

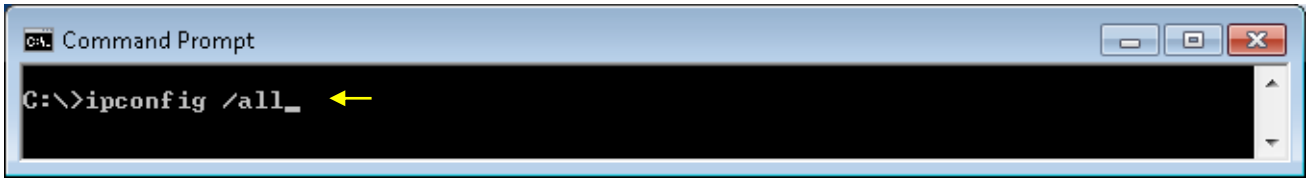
2. To view your automatically assigned TCP/IP settings, go to Network and Sharing Centre and then click on “Local Area Connection”.



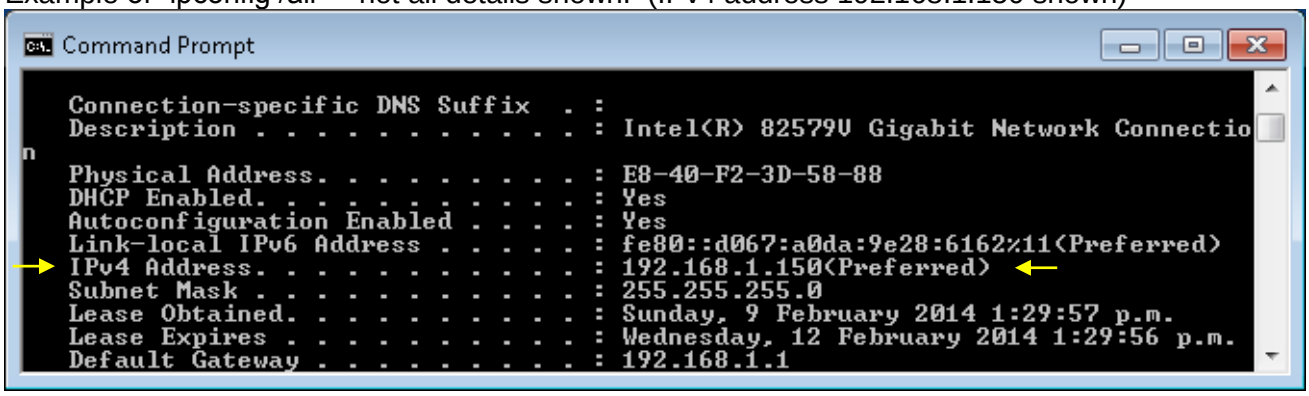
In the window that opens, click on “Details”. The “Network Connection Details” window will show your main IP settings. View the details.



3. The better way (giving more info) to see your automatically assigned TCP/IP settings is to open a Command Prompt and use the “ipconfig /all” command to see/confirm your **IPv4** address and other settings.



Example of "ipconfig /all" – not all details shown. (IPv4 address 192.168.1.150 shown)



In amongst the IPv4 info you will also see IPv6 info. Ignore the IPv6 details for now – we will concentrate on IPv4.

Record your automatically assigned IPv4 settings:

Windows IP Configuration

Host Name: _____ (eg. PAN308-02A)
(This name is not automatically assigned)

Ethernet adapter **Local Area Connection**:

Description: _____

Physical Address: _____

DHCP Enabled: _____ (eg. Yes/No?)

Autoconfiguration Enabled: _____ (eg. Yes/No?)

IPv4 Address: _____ (eg. 192.168.1.102)

Subnet Mask: _____

Lease Obtained: _____

Lease Expires: _____

Default Gateway: _____

DHCP Server: _____

DNS Servers: _____

4. Try to “ping” yourself.

   PING (some say it is short for “Packet Internet Groper”?)

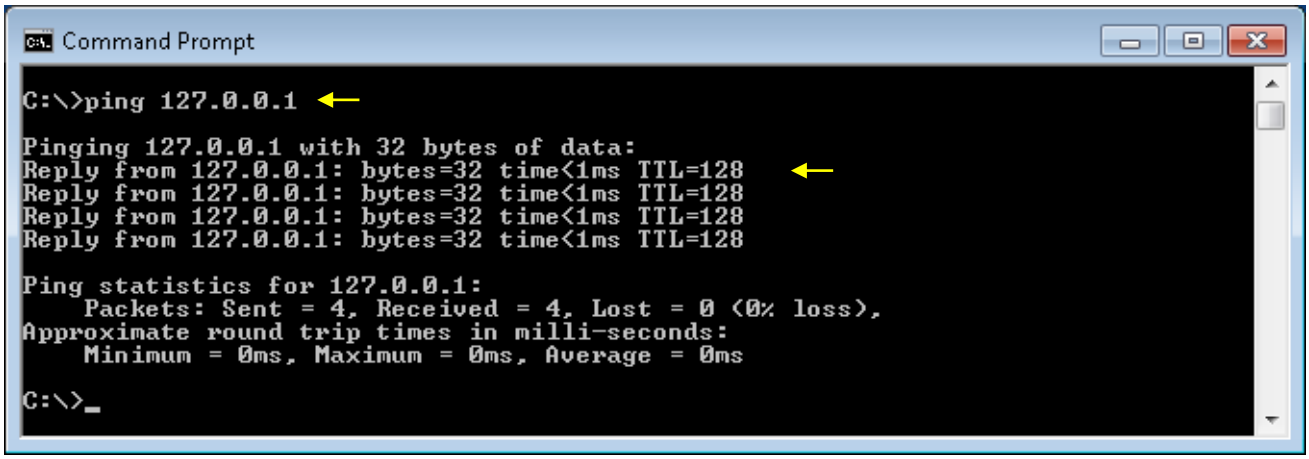
   Ping is a computer network administration utility/command used to test the reachability of a host (ie. computer) on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

   - A ping reply indicates there is connectivity to that address.
   - The ping time (ms) indicates the round trip time for a packet of data to return from the selected address. (The lower the better).

   - “ping 127.0.0.1” This is the localhost address, ie. “this” (your) computer.
   - “ping localhost” This is the localhost name, ie. “this” (your) computer.

     This command checks the TCP/IP protocol stack. If this does not work then no IP communication will work – ie. the TCP/IP protocol stack is not working.

     Every computer has 127.0.0.1 as an address – it is a local loopback test address, no packets actually leave the NIC or go onto the network.



   - “ping 192.168.1.X”
     Where “X” is the address of your PC.

     Packets are sent on the network - to yourself.

5. Try pinging servers on your local network (they should always be running).

   Pandora’s default gateway/proxy server:
   - “ping 192.168.1.1” - by IP address.
   - “ping TMGSVR” - by computer name (the name is not case insensitive).
   - “ping tmgsvr.pandora.local” - by FQDN name (Fully Qualified Domain Name).

Pandora's DNS server (and Domain Controller for the Pandora Domain):

- "ping 192.168.1.10" - by IP address.
- "ping PDC" - by computer name (the name is not case insensitive).
- "ping pdc.pandora.local" - by FQDN name (Fully Qualified Domain Name).

Pandora's File server:

- "ping 192.168.1.20" - by IP address.
- "ping FS1" - by computer name (the name is not case insensitive).
- "ping fs1.pandora.local" - by FQDN name (Fully Qualified Domain Name)

6. Try pinging computers on the Internet.

   - "ping www.google.co.nz" The name of an Internet host (computer).
     Record the IP address that it shows (it represents www.google.co.nz). Ping it.

   - "ping 74.125.237.184"
     This is the IP address that represents the domain name www.google.co.nz. Depending on which Internet Service Provider (ISP) you use, this address may differ slightly from that shown – there are more than one IP addresses for that domain name.

   - "ping 8.8.8.8"
     This is the IP address of Google's DNS server.

7. Try pinging other computers on the local network (they may or may not be running).

   - "ping 192.168.1.Y"
     Where "Y" is the address of your neighbouring student's PC.

   - "ping PAN308-02A"
     The host name (computer name) of your neighbouring student's PC.

     Pinging your neighbour's computer may or may be successful? See notes* below.

*Notes:
For you to be able to communicate (eg. "ping") your neighbour's PC their "Firewall" must permit it. Similarly for others to communicate with your PC, your "Firewall" must permit it.

Simple firewall configuration can be done via "Advanced sharing settings" found in the "Network and Sharing Centre".

In the Advanced Sharing Settings, your current profile will probably be "Domain". Whatever your current profile is, the "Turn network discovery on" option and the "Turn on printer and File Sharing" should both be selected.

We will look at this Advanced Sharing Settings and Firewall settings in a future exercise.

Task 4 – Access the Internet via the Pandora Gateway/Proxy

1. Open up a browser (eg. IE, Firefox or Chrome) and access a web site.
   You access the Internet via a default gateway which is also firewall/proxy server whose IP address is 192.168.1.1

   Before you can access the Internet you must provide Pandora's Proxy server with a username and password. This is done automatically for you because the username/password you used to log onto the Pandora network is what the Proxy server uses for authentication.

   Note:

   - **Your Internet access is logged and monitored!**
   - **You should only access the Internet for course related purposes!**

Task 5 – Ping NetLab (NL) Servers

Recall that the Pandora servers and the NetLab (NL) servers are physically connected to the same network. Pandora servers use IP addresses in the 192.168.1.0/24 **logical** IP network and the NetLab (NL) servers use IP addresses in the 10.100.0.0/16 **logical** IP network.

Your PC is currently on the 192.168.0 IP address range for connecting to the Pandora network and its servers.

1. Ping NetLab's Default Gateway Server
   "ping 10.100.11.3"

2. Ping NetLab's DNS Server
   "ping 10.100.11.1"

   Do the pings work (ie. get a reply)?

   Answer/Explanation: The pings will **not** work.
   Even though your PC is on the same physical network as the NetLab (NL) servers they are on different **"logical"** IP networks. Your currently configured default gateway server/router (192.168.1.1) does not know how to route packets to the 10.100.0.0/16 IP network.

   The Pandora Default Gateway is configured to forward Internet traffic to the Internet but is not configured to route packets destined to the 10.100.0.0/16 private network – packets to 10.100.0.0/16 IP network addresses will be "dropped".

Task 6 – Tracert & Pathping

1. From a command prompt run the command “ping www.google.co.nz”.

   Take a screen shot (Alt – Print Screen) and paste it into a MS Word document.

2. From a command prompt run the command “tracert www.google.co.nz”.
   Observe the path (IP addresses of all the gateways) taken to get to the destination.

   Take a screen shot (Alt – Print Screen) and paste it into a MS Word document.

3. From a command prompt run the command “pathping www.google.co.nz”.
   Observe the information provided.

   Take a screen shot (Alt – Print Screen) and paste it into a MS Word document.

You will later compare the output you record here with the output using the same commands when you are on the NetLab (NL) network.

Part B – NetLab (NL) Network

By default the **standard** Pandora disk's Windows operating system will automatically connect to the Pandora network (IP address in the 192.168.1.0/24 network). We have previously seen how the use of a DHCP server automatically provides your PC's NIC (Network Interface Card) with an IP address and other settings.

In this part of the exercise we will **temporarily** connect to the NetLab (NL) network (IP address in the 10.100.0.0/16 network). This will be done by manually assigning IP address and other settings to the NIC (Network Interface Card).

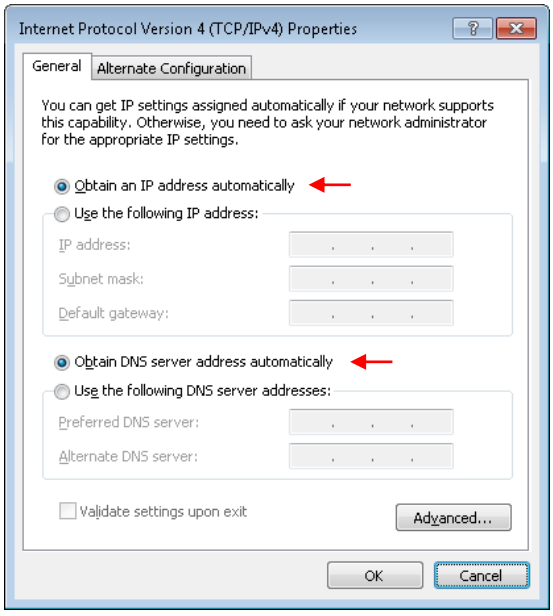
Background
The "Pandora" network's IP address space (ie. 192.168.1.X, with a subnet mask of 255.255.255.0) is too limiting for what we need for the course – only 254 IP addresses are available.

In future exercises when we install our own operating systems and create virtual machines, we will need more addresses than what is provided by the 192.168.1.0 IP network. We will change the IP addresses to a range used by the "NetLab" (NL) network. The "NL" network uses IP addresses in the 10.100.X.X range with a subnet mask of 255.255.0.0. This gives over 65000 IP addresses that can be used on our networks.

IMPORTANT NOTE

Before you continue on with this part of the exercise there is are essential point you must remember.

- Doing this part of the exercise requires students to change the IP settings of the PC.
- Make sure that before you shut down or logoff the computer at the end of the exercise (or if you have to leave part way through the exercise) that **you change the IP settings back to the "original", ie. automatic**.



If these settings are not put back to the original automatic settings, the next user will not be able to logon to the Pandora network!

Task 1 – Static IP Configuration - for the NetLab ("NL") network

1. Set the IP settings to statically/manually assigned and provide the following manually assigned settings.

5003 students in DT303 (Class "**A**"):		use "**21**" for the 3rd octet in the IP address
IP Address:	10.100.**21**.**nn**	where "**nn**" is your PC number
Example only:	10.100.**21**.**6**	for PC number 06
5003 students in DT308 (Class "**B**"):		use "**22**" for the 3rd octet in the IP address
IP Address:	10.100.**22**.**nn**	where "**nn**" is your PC number
Example only:	10.100.**22**.**17**	for PC number 17

All classes use:
Subnet Mask: 255.255.0.0
Gateway: 10.100.11.3

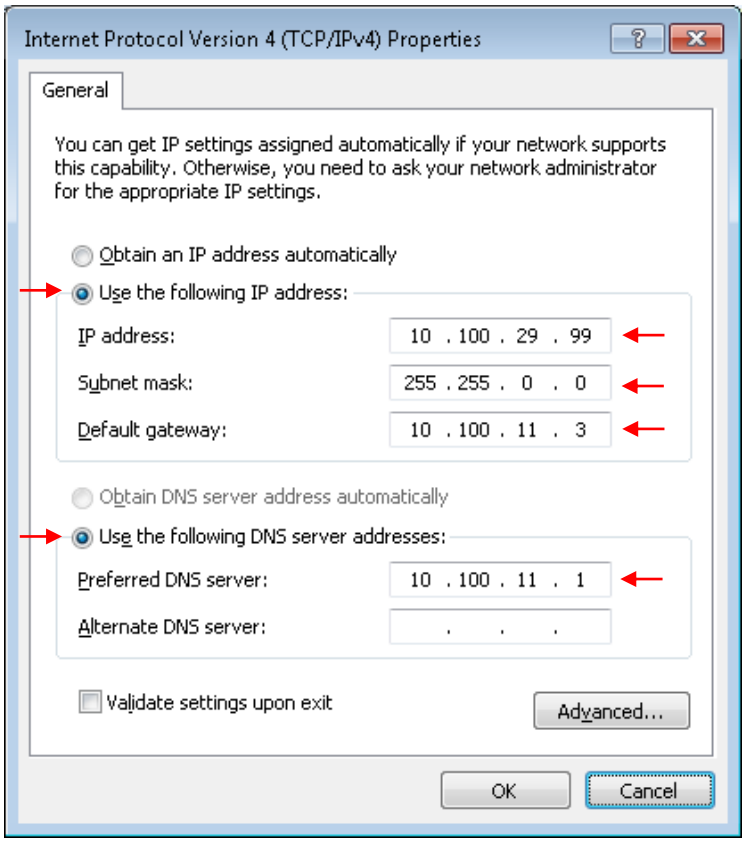
DNS: 10.100.11.1

Note: Record your IP settings!!

This is an example only! >>>

The example IP address 10.100.29.99 in the diagram to the right is typically what the tutor will use for illustrative purposes.

Make sure you use an IP address that conforms to the convention mentioned above.



Note:
In future exercises, when you change network settings you may be prompted with what type of network location you want. If you are prompted always select "Work" (aka Private).

2. Use the “ipconfig /all” command to see/confirm your new IPv4 address and settings.

Record your static/manually assigned <u>IPv4</u> settings:

Windows IP Configuration

Host Name: _____ (eg. PAN308-02A)
(This name is not automatically assigned)

Ethernet adapter **Local Area Connection**:

Description: _____

Physical Address: _____

DHCP Enabled: _____ (e.g. Yes/No?)

Autoconfiguration Enabled: _____ (e.g. Yes/No?)

IPv4 Address: _____ (e.g. 10.100.21.2)

Subnet Mask: _____

Lease Obtained: _____

Lease Expires: _____

Default Gateway: _____

DHCP Server: _____

DNS Servers: _____

Task 2 – Test Connectivity the NetLab ("NL") network

1. Try "pinging" yourself.

   - "ping 127.0.0.1" This is the localhost address, ie. "this" (your) computer.
   - "ping localhost" This is the localhost name, ie. "this" (your) computer.

     This command checks the TCP/IP protocol stack. If this does not work then no IP communication will work – ie. the TCP/IP protocol stack is not working.

     Every computer has 127.0.0.1 as an address – it is a local loopback test address, no packets actually leave the NIC or go onto the network.

   - "ping 10.100.21.X" (for DT303) or "ping 10.100.22.X" (for DT308)
     Where "X" is the address of your PC.

     Ping also your own host (computer) name.
     For example. "ping PAN303-02", "ping PAN308-17" etc.

     Packets are sent on the network - to yourself.

2. Try "pinging servers on the local network (they should always be running).

   The gateway for the NetLab (NL) network:
   - ping 10.100.11.3 - by IP address
   - ping NL-GW - by computer name
   - ping NL-GW.NL.LOCAL - by FQDN (Fully Qualified Domain Name)

   The DNS server for the NetLab (NL) network:
   - ping 10.100.11.1 - by IP address
   - ping NL-DC - by computer name
   - ping NL-DC.NL.LOCAL - by FQDN (Fully Qualified Domain Name)

   The name of the DNS server is "NL-**DC**". This server is also the **D**omain **C**ontroller for the "NL.LOCAL" domain and that's why it has the name "NL-**DC**".

   The File server for the NetLab (NL) network:
   - ping 10.100.11.9 - by IP address
   - ping NL-FS - by computer name
   - ping NL-FS.NL.LOCAL - by FQDN (Fully Qualified Domain Name)

3. Try pinging computers on the Internet.

   - "ping www.google.co.nz" The name of an Internet host (computer).
     Record the IP address that it shows (it represents www.google.co.nz). Ping it.

   - "ping 74.125.237.184"
     This is the IP address that represents the domain name www.google.co.nz. Depending on which Internet Service Provider (ISP) you use, this address may differ slightly from that shown – there are more than one IP addresses for that domain name.

   - ping 8.8.8.8
     This is an Internet host IP address.
     "8.8.8.8" is Google's DNS server and should always be running.

     If pinging an Internet name does not work then "ping 8.8.8.8". If the ping to 8.8.8.8 works then at least you know you have connectivity to the Internet – not being able to ping Internet names may be a DNS (ie. a name resolution) problem rather than a connectivity problem.

4. Try pinging other computers on the local network (they may or may not be running).

   5003 students in DT303 (Class "**A**"):

   ping 10.100.**21**.Y - where "Y" is the address of your neighbouring student's PC. This may or may not be successful?
   ping PAN303-06 - a neighbouring student's computer name (example PC "06" shown). This may or may not be successful?

   5003 students in DT308 (Class "**B**"):

   ping 10.100.**22**.Y - where "Y" is the address of your neighbouring student's PC. This may or may not be successful?
   ping PAN308-17 - a neighbouring student's computer name (example PC "17" shown). This may or may not be successful?

Note

Some useful commands that will be used frequently in this course:
- ipconfig /all
- ping

Remember them – they will be useful in troubleshooting network problems!

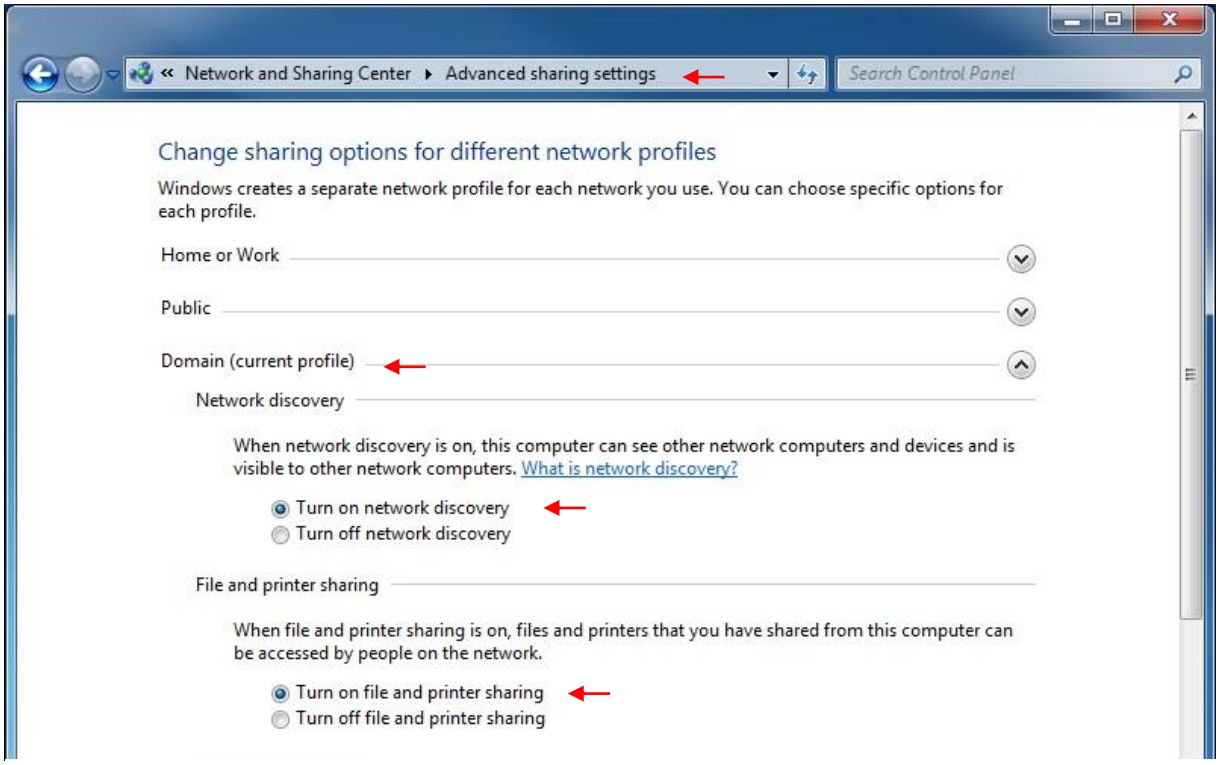
Note:

The following information will be of use later when you install Windows 7 on your own hard disk.

For you to be able to communicate (eg. “ping”) your neighbour’s PC, their “Firewall” must permit it. Similarly for others to communicate with your PC, your “Firewall” must permit it.

Simple “firewall” configuration can be done via “Advanced sharing settings” found in the “Network and Sharing Centre”. Selecting “Turn on network discovery” and “Turn on file and printer sharing” actually open up “ports” in the firewall. These settings will allow your computer to be “pinged” by others and you will also be able to “share” your files (and printers) will other users on the network.

When using your standard Pandora disk your current profile may be “Domain” (because you are logged onto the Pandora domain). When in later exercises you initially install Windows 7 your network location and profile will typically be set to “Work”.



We will look at firewall configuration in more detail in a future exercises.

Task 3 – Access the Internet via the NetLab (NL) Gateway

1. There is no proxy server on the "NetLab/NL" network. To access the Internet via the NetLab/NL network you do need to be "authenticated" with any proxy server – all you need are the correct default gateway (10.100.11.3) and DNS server (10.100.11.1) settings in your TCP/IP configuration.

   Open a browser, eg. IE (Internet Explorer) and visit a web site, eg. http://www.google.co.nz.

   Note:

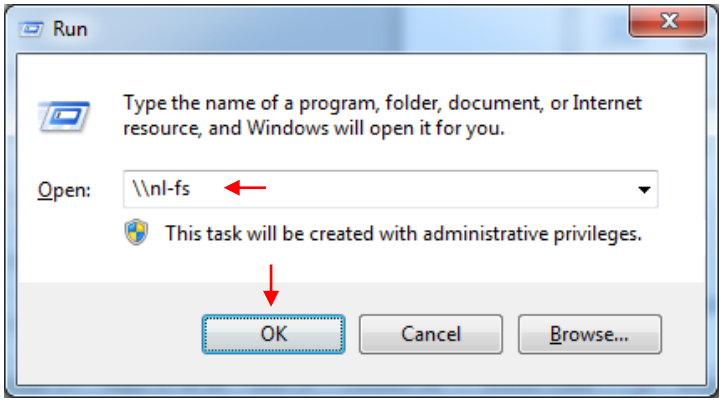
   - **Your Internet access is logged and monitored!**
   - **You should only access the Internet for course related purposes!**

Task 4 – Investigate NetLab's (NL's) Shared Resources

The NetLab (NL) file server with the name "NL-FS" has shared resources (files/folders) for you to access. The tutor will place software on the server for you to use. Unlike the resources on the Pandora file server you will have to connect to the Net Lab file server manually.

1. Previously you pinged the NetLab (NL) file server by IP Address and name.
   Do it again to confirm connectivity, ie.
   - ping 10.100.11.9
   - ping NL-FS

2. Use the "Windows and R" key combination to open the "Run" window.
   In the "Open:" input area type \\NL-FS. This indicates to Windows to go out on the network and discover that computer, ie. computer name "NL-FS" (don't forget to have the two back slashes "\\" in front of the name.



When prompted for user credentials, provide either one of the following:

Username:	**NL-FS**\5003
Password:	5003

The username is "5003" but the "NL-FS\" in front of it indicates that we want to authenticate with a user account on the "NL-FS domain", in this case a user account on the "NL-FS" server.

Username:	**NL**\5003
Password:	5003

Note that will work as well, however an explanation of what it means will have to wait until your networking knowledge develops further.
("NL\" is short for the "NL.LOCAL" domain).

The “Info” folder on the “NL-FS” file server should appear:

Inside the Info folder is a “5003” folder. The “5003” folder may not have much in it at the moment but it will become more populated as the semester progresses.

Task 5 – Ping Pandora Servers

Recall that the Pandora servers and the NetLab (NL) servers are physically connected to the same network. Pandora servers use IP addresses in the 192.168.1.0/24 **logical** IP network and the NetLab (NL) servers use IP addresses in the 10.100.0.0/16 **logical** IP network.

Your PC is currently on the 10.100.0.0 IP address range for connecting to the NetLab (NL) network and its servers.

1. Ping Pandora's Default Gateway Server
   "ping 192.168.1.1"

2. Ping Pandora's DNS Server
   "ping 192.168.1.10"

   Do the pings work (ie. get a reply)?

   Answer/Explanation: The pings will **not** work.
   Even though your PC is on the same physical network as the Pandora servers they are on different **"logical"** IP networks. Your currently configured default gateway server/router (10.100.11.3) does not know how to route packets to the 192.168.1.0/24 IP network.

   The NetLab (NL) Default Gateway is configured to forward Internet traffic to the Internet but is not configured to route packets destined to the 192.168.1.0/24 private network – packets to 192.168.1.0/24 IP network addresses will be "dropped".

Task 6 – Tracert & Pathping

1. From a command prompt run the command "ping www.google.co.nz".

   Take a screen shot (Alt – Print Screen) and paste it into a MS Word document.

2. From a command prompt run the command "tracert www.google.co.nz".
   Observe the path (IP addresses of all the gateways) taken to get to the destination.

   Take a screen shot (Alt – Print Screen) and paste it into a MS Word document.

3. From a command prompt run the command "pathping www.google.co.nz".
   Observe the information provided.

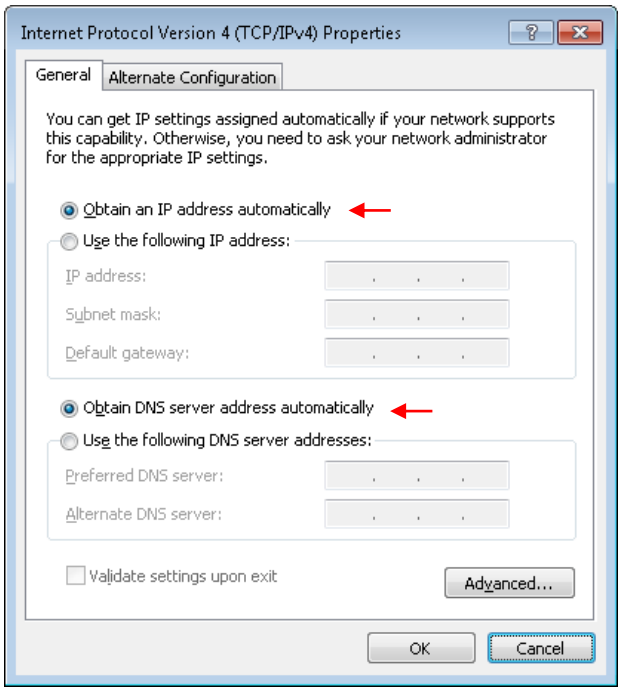
   Take a screen shot (Alt – Print Screen) and paste it into a MS Word document.

Compare the output you record here with the output using the same commands when you were previously on the Pandora network using IP addresses in the 192.168.1.0 range.

The practical part of the exercise is finished!

Make sure that before you shut down or logoff the computer you change the IP settings back to the "original", ie. automatic.

Restart your computer and log onto the Pandora network. If you have any trouble, ask the tutor for assistance.



If these settings are not put back to the original automatic settings, the next student wanting to use the computer will not be able to logon to the Pandora network!

Later in the course you will be working in pairs and setting up your own Peer to Peer network, sharing files/folders and printers on your computer for your partner to access. That is one of the main benefits of a network – sharing resources!

Before the next class think about who will be your partner for future exercises and practical assessments.
