**Institute of Technology Tralee**

**Computing Department**

**TCP/IP Settings and a**

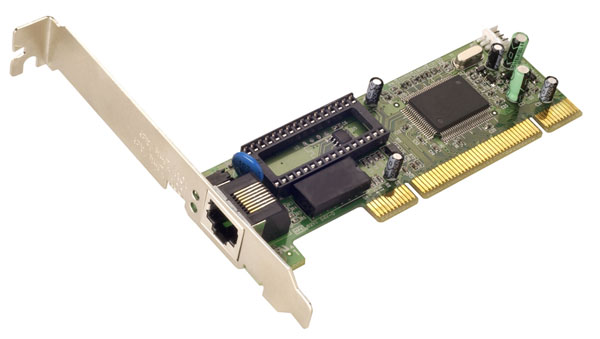
**Peer-to-Peer Connection**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Lab 1**

**What is a Network Interface Card (NIC)?**

A NIC is a fairly complex networking hardware device containing the necessary circuitry to enable a PC to **interface** with a network. The NIC hardware on its own is not enough to allow network connection – this is also dependent on NIC software (drivers and configuration files) and the installation of appropriate network **protocol**(s).



PCI Bus Edge Connector

RJ-45 Connector

**Modern PCI Bus NIC card with RJ-45 8-pin connector.**

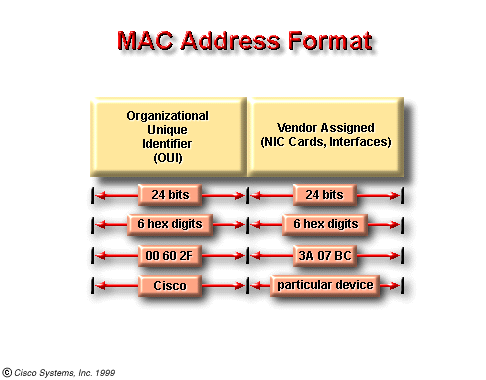
Today, a network card is often integrated into the main mother board of the PC.

**NIC Functions**

The electronic signals that represent bits on the network and the media used are commonly referred to as **physical layer** (**layer 1**) entities.

With just signals and media, there is no particular structure to how data is transferred from place to place. The data is sent as a sequence of bits along the cable but what happens if there is some noise that disrupts some of the bits, or what if some of the bits get lost or what if the intended destination for the bits cannot been located? How can the machines actually find each other on the network? The NIC has a major role to play in this respect.

A NIC is normally considered to be a **data-link layer** (layer 2) device and it allows networked computers to be identified uniquely by what is called a **MAC** **address** (Medium Access Control). A MAC address is a burnt-in or hardware or physical address.



A MAC address is **48 bits long** containing a total of 12 Hexadecimal (base 16) digits. One half of the address is assigned by the IEEE and identifies the manufacturer or vendor comprising the *Organizational Unique Identifier* (*OUI*) (an example of such a manufacturer would be 3Com) and the rest comprises the *interface serial number* and is assigned by the specific vendor of the card.

Worldwide, every computer, whether it is attached to a network or not, has a unique **physical (MAC) address,** provided it has a NIC installed. No two physical addresses are the same. This physical address is programmed into the ROM of the NIC itself and so is a **permanent** address. If a NIC is replaced in a computer the physical address of the machine changes to that of the new MAC address

There are two formats for MAC addresses: 0000.0c12.3456 or 00-00-0c-12-34-56.

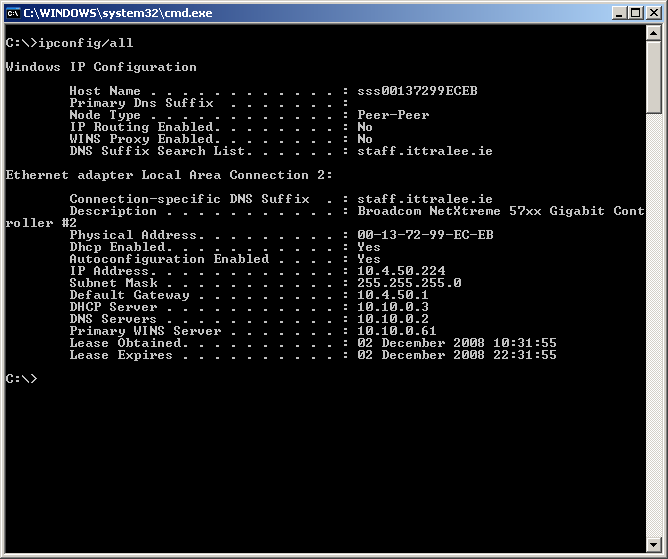
**Exercise**: Find out the physical MAC address and logical IP address associated with your machine and write them down.

In Win 7 we have numerous utilities to find this information. Today we will use **ipconfig.exe**.

1. Bring up the Command Prompt window.
2. Go to Start and type in cmd in the search box to bring up the Command Prompt).
3. Type **ipconfig/all** at the command prompt **-** This utility tells you some IP configuration information associated with the NIC installed on your machine.
4. **MAC Address: 00:24:E8:FC:DA:A5**
5. **IP Address: 10:5.23.145**



Browse through the details and you should see a “**Physical Address**” field. This identifies the MAC or adapter address of the NIC installed on your machine. Your MAC address should be unique so compare it to some of the people next to you to make sure that is the case.



On an **Ethernet** network, when one device wants to send data to another device, it can open a communication pathway to the other device by using its MAC address. When a source sends data out on a network, the data carries the MAC address of its intended destination. As this data travels along the network media, the NIC in each device on the network checks to see if its MAC address matches the physical destination address carried by the data packet. If no match is made, the NIC ignores the data packet and it continues along the network to the next station.

However, when a match is made, the NIC makes a copy of the data packet, and places this copy in the computer, where it resides at the data link layer. The original data packet continues along the network where other NICs will be able to look at it to determine if a match can be made. As data travels along the wire, the NIC in each station checks it. The NIC verifies the destination address in the packet header to determine if the packet is properly addressed. When the data passes its destination station, the NIC for that station makes a copy, takes the data out of its “envelope” and passes it to the computer.

MAC addresses are vital to the functioning of a computer network. They provide a way for computers to identify themselves; they give hosts a permanent, unique name, and the number of possible addresses is not going to run out anytime soon, since there are 248 possible MAC address names (281,474,976,710,656 possible combinations – over 281 trillion!)

**Physical versus Logical Addressing**

MAC addresses do, however, have one major disadvantage. They have no structure, are unrelated to each other, and are considered *flat address spaces*. Different vendors have different OUIs, but they're like RSI numbers. As soon as the network grows to more than just a few computers, this disadvantage becomes a real problem.

In computer networks **IP** (Internet Protocol) **addressing** provides a structured approach to addressing. This addressing scheme uses a 32 bit (moving to 128 bits with IPv6 **unique** address which, rather than being permanently associated with a NIC like a MAC address, is instead **software based** (is a **logical address**). Write down your IP address and compare it to those close to you.

**What kind of NIC are you using?**

**Exercises**: Find out what kind of NIC you are using with WinXP/Win7

Go to **Start->Control Panel->System->Hardware->Device Manager->Network adapters**. Record as much information as you can about the NIC installed on your machine – Manufacturer, Model Speed of Data transfer etc.

## Testing the TCP/IP installation and the NIC using the Ping utility

The overall goal of the NIC is to connect you to the network. **TCP/IP** is the suite of protocols most commonly used nowadays for both intra-network and inter-network usage. Once the card and TCP/IP has been installed you can easily test them using a networking program called **ping** that is very often used by networking professionals to test network connections. Ping can also be used to determine if the network itself is operating and you can even use it to determine things like delays on networks and whether a particular machine on the network is “alive” or not.

## Ping

Ping is an **application** **layer** entity (layer 7), and comes with the installation of the TCP/IP suite of protocols on your machine. It uses **ICMP** (Internet Control Message Protocol) to send an **ECHO\_REQUEST** to elicit an ICMP **ECHO\_RESPONSE** from a specified host. This essentially means that ping sends a message to a machine and requests a response from that machine. It waits for the response for a particular amount of time and then displays the amount of time the response took.

## Exercise: Test to see if TCP/IP is installed properly by carrying out the following simple test. Launch the Command prompt utility and enter the command

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

The information here, simply means that the host machine you are testing, the one having an IP address of 127.0.0.1 (this is a very special IP address called the loopback address and means the local host i.e. the machine you are actually running the ping ICMP ECHO\_REQUEST from) has TCP/IP installed properly on it. Note in the default case here 4 packets of information each holding 32 bytes of information have been sent and the response time in each case is very low indeed (less than 10ms) as you might expect. The TTL is the so-called **Time-To-Live** field. This is a useful piece of information in its own right because it indicates the number of routers the packet had to go through in order to reach the source machine. Here the TTL is originally 128 (the default) and the final TTL value indicated is also 128 that indicates that the packets did not go through any routers at all (true indeed). If, for example, the value of TTL was 126 then it would indicate that 2 routers were traversed by the ECHO\_RESPONSE packets. The TTL value itself can be altered as can many other of the ping parameters. In this case no packets were dropped along the way – when testing out connections on a network with ping and if many dropped packets are discovered it means trouble, possibly a very congested network.

## Exercise: Test to see if your NIC is installed properly by carrying out the following simple test. Launch DOS prompt utility and enter the command

## ping *hostname*

## where *hostname* is the IP address number of a few machines in the R200 lab. Get this information from your colleagues using the information they wrote down earlier.

## Exercise: Test to see if you can connect to the IP address www.microsoft.com using ping. Note that you may have a problem here. If so, it means that ping requests outside of the college intranet are barred by the college firewall software. This is pretty normal behavior and does not mean that there is a problem with either Microsoft’s server machine or with the college network – it is more of a security issue. Many Internet servers frown upon the use of ping as it can be used maliciously to keep Internet connections alive by pinging “forever”. This obviously eats up server time.

## Exercise: Creating your own 2-PC hubless LAN using a UTP cable and NICs under Win7.

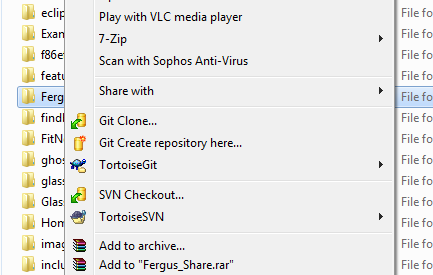
We are going form a simple peer-to-peer network and try to share files across this simple network.

Copy this lab to the local Desktop and then disconnect the PC from the college network.

You will be creating your own simple LAN containing just 2 PCs connected by a **UTP cable**. Normally a *crossover* cable is used to connect devices that have similar interfaces (2 PCs in this case) but we have autosensing NIC’s on the PC in R200 so a *straight-through* UTP cable will also work in this instance.

***Before you connect the PC’s with the cable complete the following tasks***

1. Create a new folder on the C: drive and call it *myname*\_share (use your name). Copy some arbitrary files into this folder.
2. Right click on the folder and select the Share with option and choose Specific people from the drop down menu.

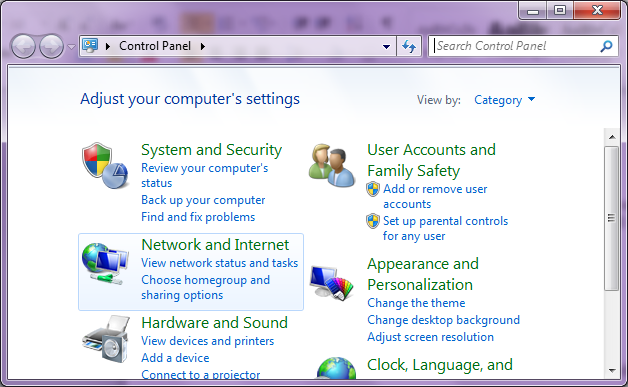


1. Enter the t-number of the person that you want share with and select share.

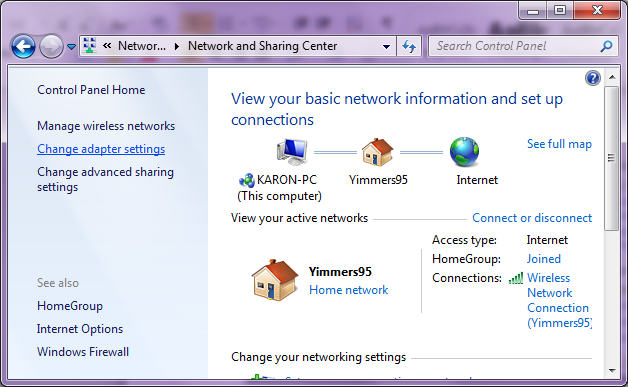
CHANGE IP ADDRESSING SETTINGS

We are going to connect the two PCs but first we will change their network settings.

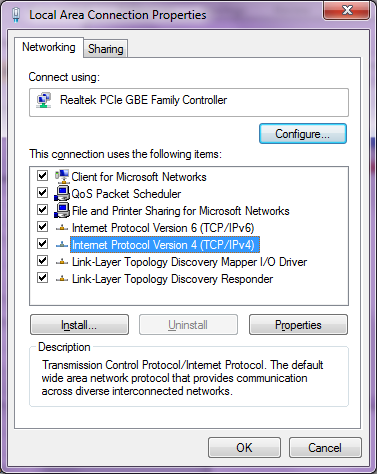
1. Normally in the college the DHCP server dynamically assigns each computer an IP address – in this instance we are going to assign a **static** IP address to each machine.
2. Disconnect the network cable from the college network at the wall or bench network socket.
3. Click **Start** -> Control Panel -> Network and Internet-> View network status and tasks



1. Select Change adapter settings



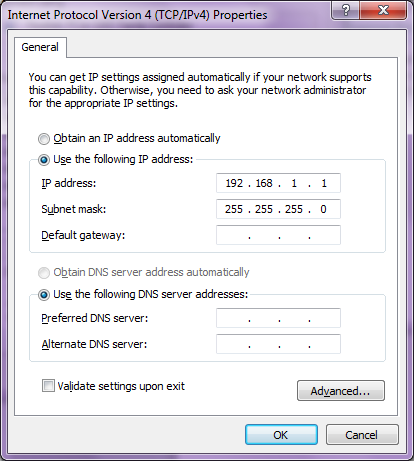
1. Double click on Local Area Connection - there May be more than one connection – make sure you select this one.
2. In the protocols list click on **Internet Protocol Version 4 (TCP/IPv4)**



1. Select **Properties**

The Network automatically assigns IP addresses to the computer dynamically – we want to set a static IP address on both machines for this practical. Click on **Use the following IP address** and set the following addresses on the two connected machines.

1. Enter the IP address 192.168.1.1 for one machine and 192.168.1.2 for the other machine.
2. Enter the Subnet Mask 255.255.255.0 for both machines. The other entries are not important today.



You have to close all these setting windows before the IP address changes take effect.

1. Bring up the **Command Prompt** and use **ipconfig/all** to make sure the IP address has changes to the correct value on each PC.
2. Use one of the existing network cables to connect both PCs together.
3. Try to ping each PC on the other side of the link.
4. Try mapping the shared folder on the other PC to say Drive Z:

You may need the other student’s T-number to do this.

You should now be able to see the files in the folder on the other PC.

On completion, re-join the college network by resetting the ip address to being dynamically assigned.

Delete the shared folder you created.