



HUSSARS GAMING GROUP

Series: Hussars Help Hussars

Title: Networking Handbook

A Guide to Setting up a home network

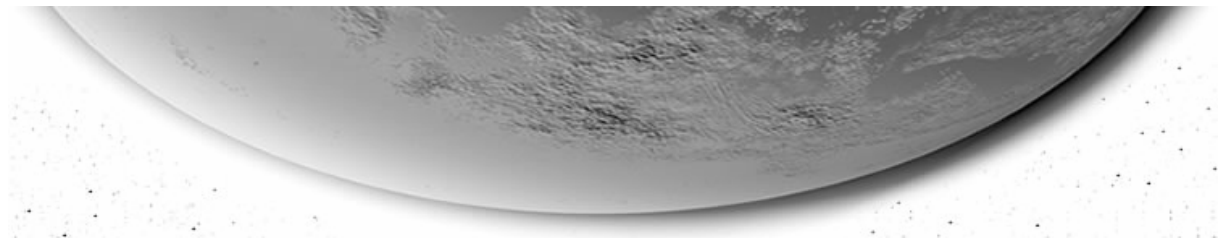
Owner: Simon Brooks

Author: HSeldon

Email: mad_hseldon@hotmail.com

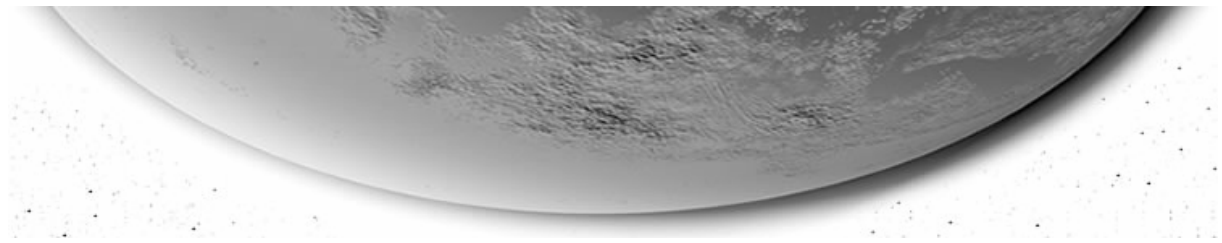
Version: 1.0

Date: 11.6.2003



Contents

1 Document History	3
2 Introduction	4
3 Scenario	5
3.1 Overview	5
3.2 Document Structure	6
4 Internet Access for your LAN	7
4.1 Set up the physical network	7
4.2 Set up the logical networks	7
4.2.1 TCP/IP Basics	8
4.2.2 Automatic TCP/IP Configuration	12
4.3 Deciding on security	15
4.4 Internet Name Resolution	18
5 File and Printer sharing on the LAN	21
5.1 Configuring Computer-Name Resolution	22
5.2 Set up user accounts	25
5.3 Set up shared directories	25
5.4 Testing file sharing	28
5.5 Set up printer sharing	29
5.6 Test printer sharing	29
6 Pings and Lag	29
6.1 Why a ping is not a ping	30
6.2 Links for help and support	32
6.3 Glossary	32



2 Introduction

This document was originally a series of posts on the Hussars message board in answer to distress calls about Internet and local networking being dysfunctional or not working at the same time. In the following I will attempt to shed light on enough networking technology to allow any inclined reader to understand the things that are required for your home network to provide internet access as well as file & printer sharing to all the computers you connect to it. The networking topics we will cover are Internet Protocol Addressing (IP), Routing, Network Address Translation (NAT), Domain Name Servers (DNS), NetBIOS and Windows Internet Name Service (WINS) which is all you need to know to understand what is going on and maybe see what part is missing to make your network be of use instead of causing endless headaches and frustration. Some rules to bear in mind when fixing PCs are

NEVER GIVE UP!

THE PC WILL NOT WIN!

This is a healthy mindset that, although a potential sleep-robber, WILL keep you learning and improving all the time. Once the dark side takes hold, there is no turning back, so stay on it. PCs are dumb and straight forward. Don't let them get the better of you. To make things easier to understand I will use an example configuration that, if not used already, is an easy and universal setup for any home network with a broadband internet connection using for example xDSL (ADSL,SDSL) or a cable modem. In a later version I may include how to provide the same functionality using a modem and Microsoft's Internet Connection Sharing (ICS) technology. The modem could be a 56k analog modem, an internal ISDN card or a USB DSL Modem; they all require the operating system of the PC they are connected to, to handle things that we will make the router do in this initial scenario.

Feel free to give this document to anyone you feel may benefit from it. I ask of you not to change it and not to replace my name with yours as I did write this and I would like to stay in control of what does and does not go in, as well as make sure that the information remains correct and in scope.

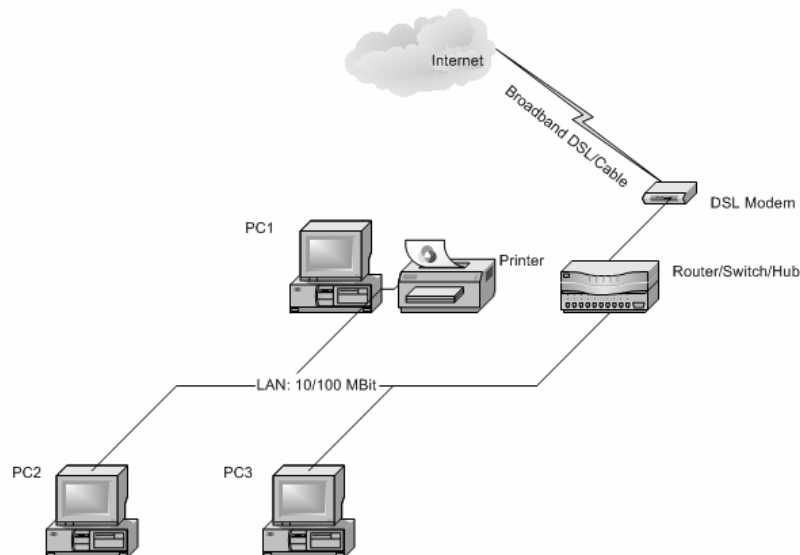
Disclaimer: I am not free of fault, especially in the orthographic department so I will assume typos and grammatical errors forgiven by default. If you spot any technical inaccuracies I'm glad to learn or admit error, so just Email me and point them out. I hereby would like to stress that this document contains information to the best of my knowledge and that you use it at your own risk. I will not be held liable for any damage done to your hard- or software nor for loss of personal data should you decide to implement the content of this tutorial.

3 Scenario

3.1 Overview

Wherever possible I will use diagrams to show you what we are doing. Here's the first one showing a basic home network setup. These pictograms are standard ones and do not show any specific model of hardware so don't be worried if your router looks a little different. Some key points to note are:

- The router is connected to the network, not a single PC
- The printer is connected to a PC via parallel cable
- The DSL modem is shown as a separate device, sometimes its built into the router

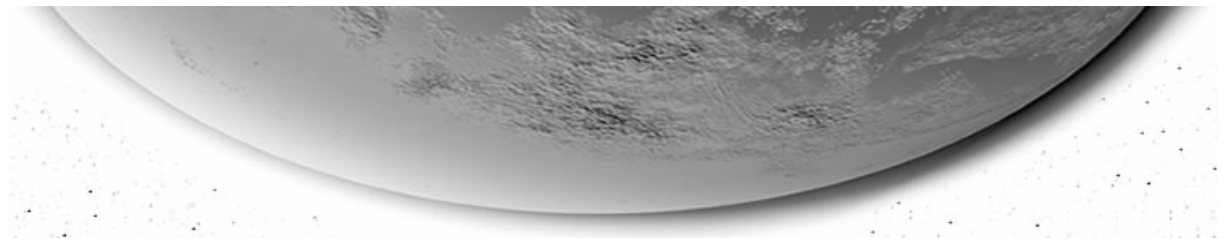


Now for a list of ingredients:

- DSL Modem (usually delivered as part of your DSL starter pack from the ISP)
- DSL Router : combo device router + switch/hub
- PC1 : Running Windows XP (Professional) with a network card or on-board network adapter
- PC2 : Running Windows XP (Home) with a network card or on-board network adapter
- PC3 : Running Windows 98SE with a network card or on-board network adapter

And a list of goals we want to achieve:

- Goal 1: Share the internet connection with all PCs
- Goal 2: Share files between the PCs on the local network
- Goal 3: Make the printer available to all PCs on the local network



3.2 Document Structure

This tutorial is supposed to be structured so its time to tell you what that structure is going to be. We will have chapters that cover the above mentioned goals we want to reach. We will have sections in chapters that each cover a step toward that chapter's goal. If a section gets really complex, I will use a third level and split it into subsections to emphasize coherence and give you places to stop reading and have a look at your own setup to compare.



4 Internet Access for your LAN

The first goal to pursue is make that internet available on all of your PCs. This greatly increases the chance of success on the other goals because you then have the Internet to look up solutions and help or even friendly helpers with. There is a list of places to find help and information in the “Links” chapter near the end of this document.

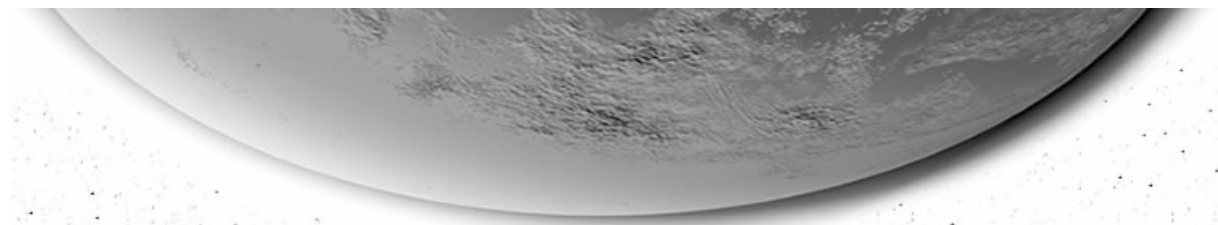
This first goal is also the trickiest because it obviously requires all the basics to be working and so we will go through lots of that in the individual steps. Once this goal is accomplished we will have done most of the work required to reach the second and third goals, which will then just require some operating system settings to be made. Let’s get started already.

4.1 Set up the physical network

First thing to do, which you or the ISP man have already done is to connect the DSL Modem to the ISDN Splitter, or wall socket, whichever you have. Consult your ISP’s docs for the modem on that one. Now connect the DSL Router to your power outlet and the DSL Modem’s network interface marked LAN. Connect each PC’s network card with a normal network cable to the router (switch). A normal cable is one that has 8 wires and in which the colours are in the same order if you hold the plugs next to each other (you may need a magnifying glass to see it properly, I do). If the order of colours is mixed up then you are probably holding a crossover network cable. Crossover leads are useful for connecting two PCs to each other without a hub or switch. They are also usually used when connecting the router to the DSL Modem (if so the cable is provided by your ISP). If the lead in your hands only has 4 wires, then it’s probably an ISDN cable. To make sure the cables are connected properly to the switch look on the back of each PC. Check the network card (or onboard network socket). There are usually two LEDs here, one LINK and one DATA. If your wires are intact and the computers and router are all turned on you should have LINK lit up and DATA flashing irregularly as data crosses the network. If the LEDs are off on any of the PCs, then take a lead from one with working LEDs, you may have a broken network lead. If that doesn’t fix it then plug the lead into a different socket on the router/switch. If this still doesn’t help, you have either not activated the onboard network card in your Computer’s BIOS or your network card is faulty. Assuming all is well we will proceed to the next step.

4.2 Set up the logical networks

Computers use different protocols to communicate over the network. Any Internet-aware computer will use the TCP/IP protocol, commonly called IP. As this protocol is just as suitable for



communications on your home network we will use TCP/IP here too. If you find anything like “NWLink” or “IPX/SPX” or “NetBEUI” on your PC, you can get rid of it unless you have PCs on the network, that are not able to speak TCP/IP.

4.2.1 TCP/IP Basics

When using TCP/IP, computers use IP Addresses to talk to each other. For ease of use Windows can use computer-names on the network and as you know the internet uses URLs like

<http://hussars.org.uk>. Let’s ignore the names for a moment and look at IP Addresses. They are like a street address for your computer. The IP Address contains a street (the network ID) and a house number (the host ID). Both are embedded in a 32bit binary code that we usually translate into decimals so we can read it easily. Example:

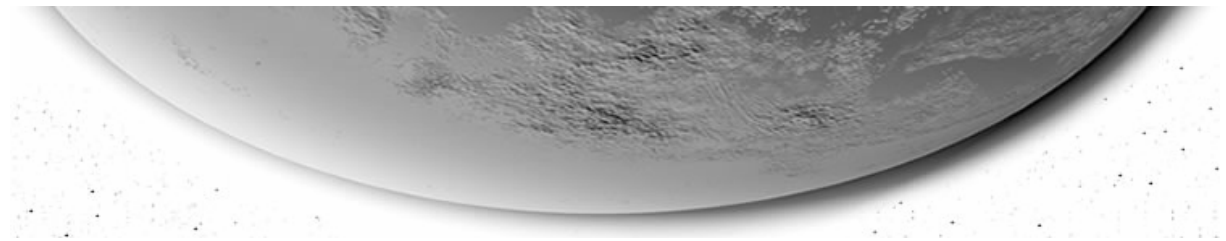
decimal: 192 .168 .100 .1
binary: 11000000.10101000.01100100.00000001

Each 8bit portion (octet) of that binary address is interpreted like this: the left-most bit is worth 128, the next is 64 then 32, 16,8,4,2, and 1. Add the values of the bits set to binary "1" to get the decimal number for an octet above. A computer’s IP configuration consists of:

- IP Address
- Subnet mask
- Default Gateway (optional)
- DNS Server’s IP Address (optional)

I will talk about the other components of a computer’s IP configuration as we go along. Let’s assume our PC2 wants to talk to a computer which has the IP Address 62.123.231.121 (let’s call it PC-Internet) and have a look at how it would do that. Now it’s quite obvious that a computer can only communicate with other computers connected to the same wire (or hub/switch), or with wireless LAN computers in the close vicinity. Following the above example this means that computers can only directly communicate with other computers that live on the same street. To allow different streets to communicate with each other we have routers to connect them. Each router can send data on to any other street on the internet.

Now before PC2 attempts to talk to PC-Internet, PC2 has to determine if it lives on the same street or not. If it does then it will try to talk to PC-Internet directly. If PC2 determines that PC-Internet lives on



another street then it will send all the communication destined for PC-Internet to its local router (our DSL Router) to be forwarded on to the router on the street that PC-Internet lives on. Got that? Good!

How does PC2 determine what street PC-Internet lives on? Well to do that it needs another part of its IP configuration: the Subnet Mask. This is something the computer does internally so it's a binary operation. I'll briefly explain it. The Subnet Mask does two things:

- it tells the computer that all the masked bits make up the network ID (street)
- it *masks* the network ID (street) so that the computer can read the host ID (house number)

This *masking* is done by a binary AND operation on the local IP Address and the subnet mask. Now let's say PC2 is configured like this:

IP Address: 192.168.100.2
Subnet Mask: 255.255.255.0

Translated into binary that looks like this:

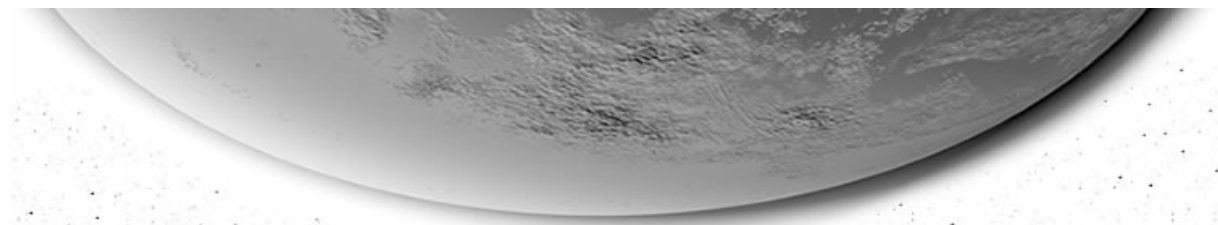
IP Address: 11000000.10101000.01100100.00000001
Subnet Mask: 11111111.11111111.11111111.00000000

This is how the AND operation goes:

1 AND 1 equals 1
1 AND 0 equals 0
0 AND 1 equals 0
0 AND 0 equals 0

So if we do that using the IP Address and the Subnet Mask (first bit of each, AND one to the other, then the second etc..) you can see that any part of the IP Address "covered" or *masked* by the Subnet Mask becomes 0 by default. The rest stays the same.

IP Address: 11000000.10101000.01100100.00000001 AND
Subnet Mask: 11111111.11111111.11111111.00000000 =
Result: 11000000.10101000.01100100.00000000



From counting the number of bits that are set to 1 in the subnet mask our PC2 also knows what its own network ID (street) is, namely the same number of bits in the IP Address starting from the left. PC2s subnet mask has 24 1s. The first 24 bits (starting from the left) of PC2s IP Address are:

11000000.10101000.01100100 or in decimal 192.168.100

The rest of the bits from 25 to 32 are topped up with 0s to make the complete network ID:

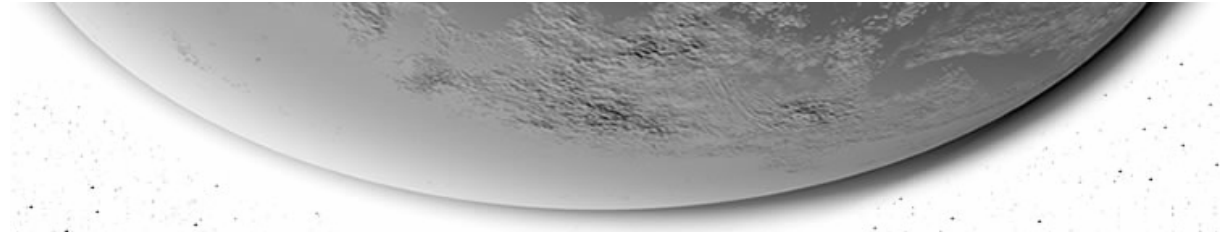
192.168.100.0

Now let's remember what we are trying to do. We are trying to determine if PC-Internet lives on the same wire (street) as we do so what do we do next? We take the IP Address of PC-Internet and check it against our own subnet mask. If we both live on the same street then we both should have the same network ID, right? If we repeat the above operation using PC-Internets IP Address we determine that PC-Internets network ID (street) is 62.123.231.0 and thus quite different from our own. So PC2 now knows it needs to send any communication for PC-Internet to the router. This is where the next part of the IP configuration is used:

Default Gateway: 192.168.100.101

The Default Gateway setting on PC1 PC2 and PC3 needs to be the routers IP Address. The router is a special device in that it lives on at least two streets at the same time; this means it is connected to at least two physical networks. To be able to communicate on both networks and discern between them, it must have two separate IP configurations, one for each network. Our home network is called a "private network". The router is connected to our private network and the Internet, which is a public network. The public network is governed by an independent body that lays down the rules of communication to which each and every device connected to it must adhere. These rules include the prime directive that IP Addresses must be unique (else routers wouldn't be able to tell which instance of a particular IP Address you want to talk to would it?).

As there are not enough 32 bit addresses to supply one to every network device in the world today and also next week, IP Address usage is limited and also governed by this independent body. When we connect to the Internet via an Internet Service Provider (ISP) that ISP gives us exactly one IP Address for communicating with the Internet. This causes a problem for us because we want to connect a total of 4 devices (router and 3 PCs) to it.



The ISP will not give us any more IP Addresses unless we pay serious money for it so we have to make do. I'll explain the solution in a moment. Another rule of the internet is that there are certain IP Addresses what are prohibited from use on the internet. These addresses are reserved for use on private networks. Their being prohibited on the internet allows ISPs to tell their routers to discard any communication using private IP Addresses to prevent accidental connection of computers with duplicate IP Addresses to the internet. Since the reserved addresses are relatively few, they are almost always already in use somewhere else in the world (which in turn is the whole idea). The Address ranges reserved for private use are:

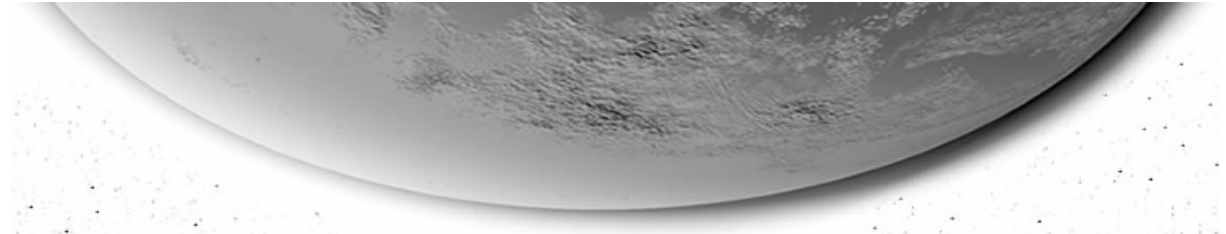
10.0.0.0 - 10.255.255.255

172.16.0.0 – 172.16.255.255

192.168.0.0 - 192.168.255.255

There are other reservations for other purposes but we don't need to know that right now. Now this doesn't really explain our problem yet does it. The IP Address we want to put on our data as the receiver is a public one, and our computer on the private network knows how to send it. Let's think about the destination too though. Any data that PC2 wants to send to PC-Internet is split into network packets (the network will only transmit about 1500bits at a time by protocol specifications). Each packet is stamped with the IP Address of the recipient and also the senders IP Address so that the computer we talk to knows where to send the answers. A-ha, so PC-Internet wants to answer to the IP Address 192.168.100.2 and sends its answer packets to the router on its own street which will dutifully discard them! A Fat lot of good that is!

Now you can see that I chose my examples with care. Our PC2 is using a private IP Address that may not directly talk to the internet. PC-Internet is using an Internet IP Address which brings us back to the solution to this problem. Our router is able to perform what is called NETWORK ADDRESS TRANSLATION. Any communication that PC1 or PC2 or PC3 have for any other streets than their own private one is forwarded to our router which in turn forwards it to another router that is on the destination street. Before forwarding it, our router replaces the sender IP Address with its own Internet IP Address (given to it by our ISP). This way any packets leaving our private network look like they originated from our router, which has a valid public internet IP Address. Bingo, problem solved.



Summary:

Computers use routers to communicate with other networks than their own. Communication is made up of multiple network packets. Network packets originating on the internal network are translated when they pass the router outbound, to look like packets originating from the router itself.

4.2.2 Automatic TCP/IP Configuration

In this I will go into the configuration of our home network a little more and explain where our computers and the router can get an IP configuration from. I have so far just said "let's assume" they have the example configurations, but that won't help you set yours up properly will it?

Let's look at an example configuration for our home network in more detail before we go on. We have already read that an IP Configuration in our example consists of

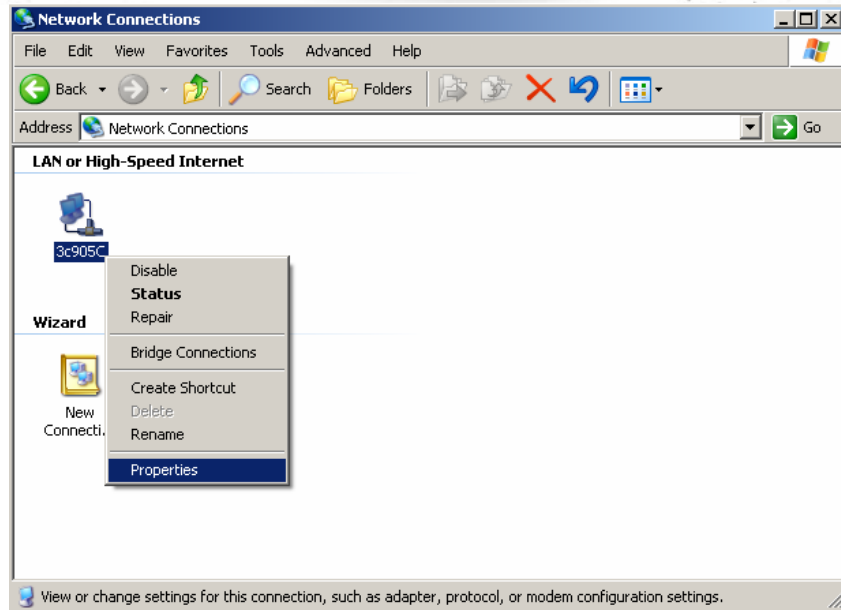
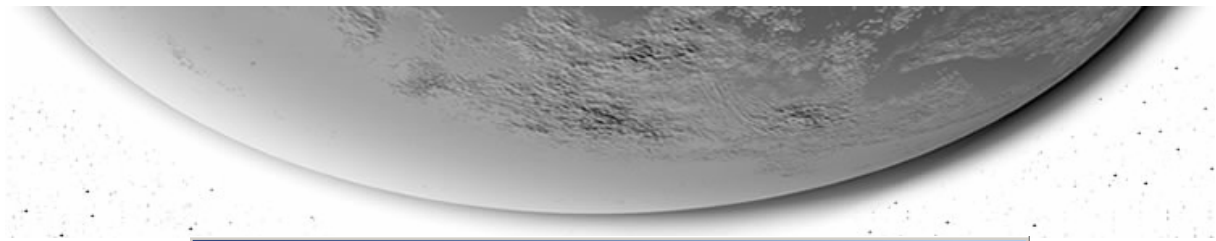
- IP Address

- Subnet Mask

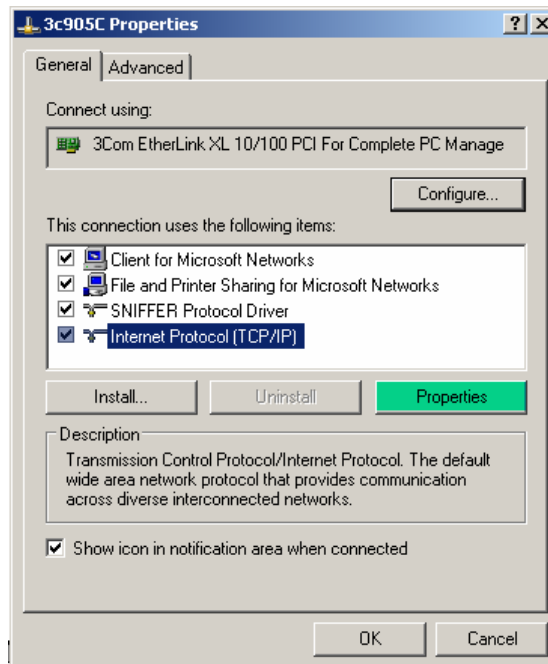
- Default Gateway

- DNS Server

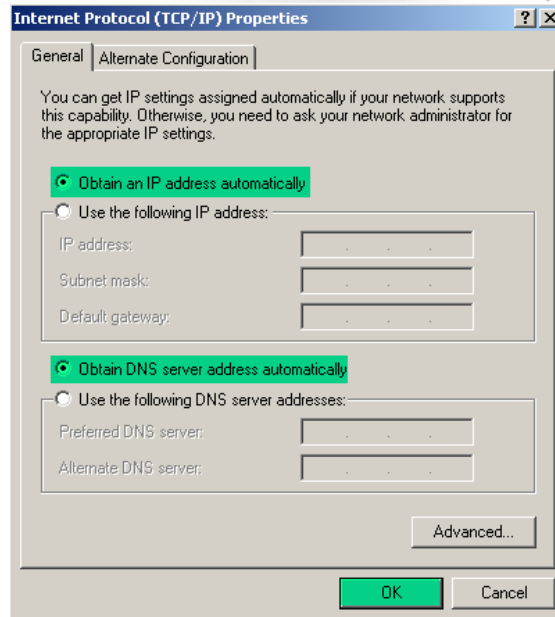
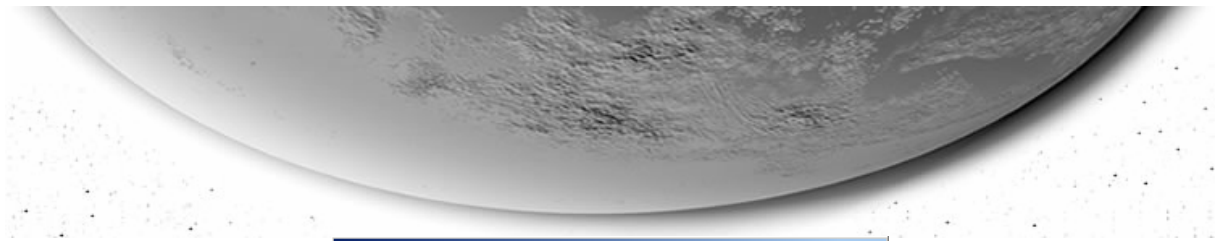
What we haven't covered is where the hell the configuration data comes from. Well of course you can go to "control panel/networks" and select TCP/IP, hit Properties and enter it yourself. This method is prone to errors though and would also make things a little more complicated to configure on the DSL Router. You can assign PC1 PC2 and PC3 each with an individual IP Configuration automatically using a network service called "Dynamic Host Configuration Protocol"(DHCP). This beast understands your needs and your PCs without using IP Addresses. To make this work you may need to activate the DHCP Server service on your DSL Router using the WebAdmin interface that is preconfigured on it. Consult your manual to find this out in more detail. Next you need to go to each of your PCs in turn and click the START button, then SETTINGS, then CONTROL PANEL, then NETWORK CONNECTIONS. In the window that pops up right-click your network card and select PROPERTIES.



Another window pops up. Select INTERNET PROTOCOL from the list and hit PROPERTIES.



Yet another window pops up and you need to make sure both radio buttons on that page are set to "obtained automatically...".



Hit OK a few times to close it all up and you are ready to go.

Note that if you turn on the router after you turn on the PCs, the DHCP Server will not be available and the computers will automatically configure themselves to some 169.254.X.X Addresses on their own. In this situation they will be able to communicate with each other but not with the internet. If you get this problem the easiest thing to do is leave the router on and reboot all the PCs. The less easy thing to do is hit the START button, select RUN and enter CMD, hit enter. In the command prompt that comes up enter

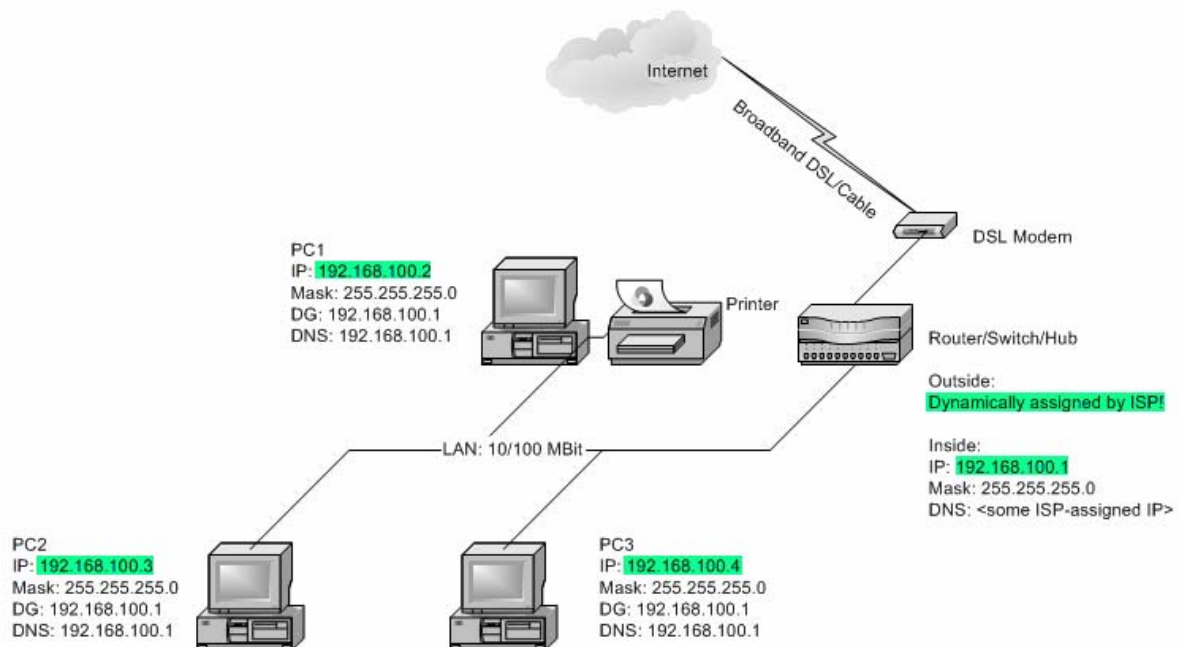
```
IPCONFIG /RELEASE <ENTER>
```

```
IPCONFIG /RENEW <ENTER>
```

To view the current IP configuration type

```
IPCONFIG /ALL <ENTER>
```

So, if you do this right your home network will now be something like this:

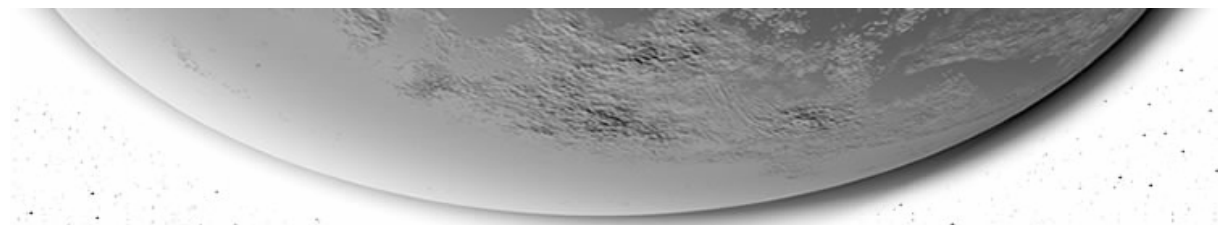


As you hopefully see, our Router will configure the PCs' default gateway to be its own private IP Address. It should also tell your PCs that their DNS Server is its own private IP Address too. The routers Internet-side configuration may change after you turn the router off and on again overnight. Usually only users with cable modems have static IP Addresses. Ok so now we know where the configuration comes from and what it's all for. We also know that the router will silently perform its NAT (Networks Address Translation) for us, but what else does it do? Well it's our boundary to the internet which is full of evil stuff we don't really want snooping around our network so the router is also charged with keeping the riff-raff out in its function as Firewall. Read on!

4.3 Deciding on security

We want protection from the baddies. Baddies can try to connect to our stuff from the outside. Alternatively they can also try and send us something via explicitly desired communication that will call them back from within our private network. Explicitly desired communication means something that you intend to let through your firewall like Email, or WWW or something like that. The safeguard against the first attack is easy and configured by default on our router:

DENY ALL INCOMING CONNECTIONS FROM THE INTERNET SIDE



The first packet of any kind of network communication has special markers on it (flags) telling the recipient that a connection is requested so the firewall has no big problem recognizing these things and ignoring them. The targeted internal PCs will never know anyone tried to contact them and the router does not want to be contacted so ... safe, for now.

The second sort of attack is rather tricky for the attacker to pull off but it's not really hard if the victim is not vigilant and aware of the danger. An attacker trying to do this tries to send you data that makes up an executable program that is run on your PC either by you unwittingly, or by internet explorer (which is very, very, very eager to run anything you throw at it) or some other program the attacker might take his code and run it. Once the attacker's program is running on our PC, he has won and will send whatever he wants off us to himself out of our private network using our friendly routers NAT capabilities. There are two ways to defend against this. One is very safe but a pain in the arse to do, and we will start with it:

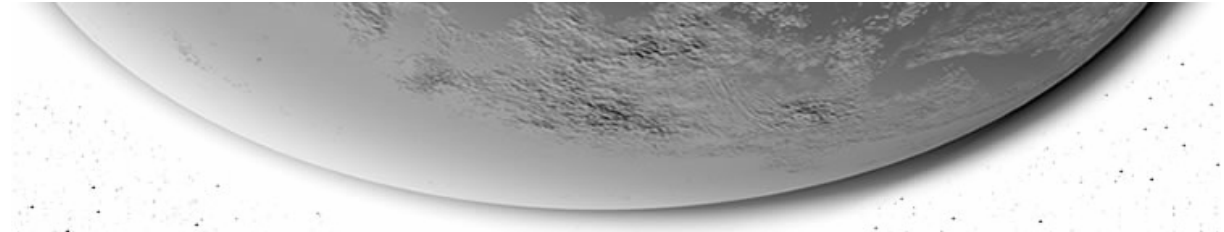
DENY ALL OUTGOING CONNECTIONS FROM THE PRIVATE SIDE

Well yes this would solve it, but it would also completely disconnect our internal PCs from the internet since the router is not listening to us. To make the internet accessible to us using this rule, we would have to tell the router exactly what exceptions there are to this rule, so something like

PERMIT OUTGOING WWW CONNECTIONS FROM THE PRIVATE SIDE

This is still fairly easy because just about every router knows what WWW actually looks like when it's split up into packets on the network. Where this approach gets tricky is when you want to permit BF1942 or other games to get out on the internet. You can bet your bottom \$ that your router has no clue what BF1942 IS, let alone what its network packets look like. Ok now look, I can read minds... you are thinking "What is this man on about, Zone Alarm can do this automatically and for free and even I could use it, what is all this fuss about?!".

HA! Zone Alarm is what you call a Personal Firewall. That's a bit of a dumb name since it's a PC-Firewall not a personal one. Anyway... yes you are right...personal firewalls can see what process (program) is trying to communicate with the internet and can SEE the packets it is sending out so it can make the connection between the two without any real intelligence of its own. Our router is not actually situated ON any of the PCs so it can't see a program called BF1942.EXE throwing out packets, it just sees the packets. So a router is bad, let's use personal firewalls all round? Well yes you could, and tell the router to permit any outgoing connections. This is indeed the safest solution for our home



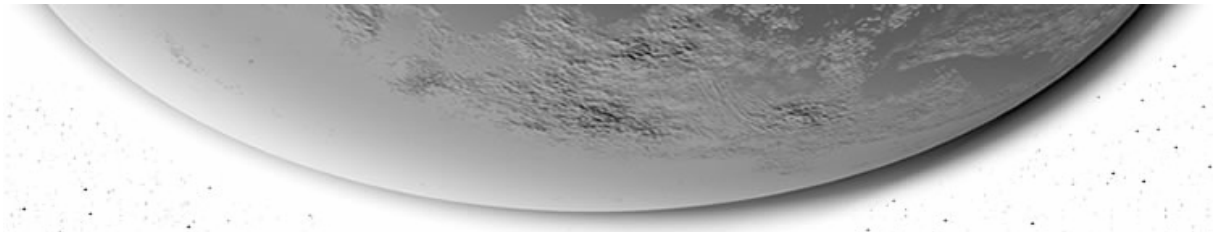
network. It is however a major pain in the arse because our PCs all have one network card over which both internet communication and our local file sharing is done. On local networks you will be doing things that you definitely do not want to have happening between your PC and the internet, but Zone Alarm wont necessarily be able to tell which is which and so an attacker can send a program that calls him back using things that Zone Alarm permits because you need it on your local network. So at the end of the day this is really nothing your average home user wants to worry about when he goes out and buys a new computer game. It all makes personal firewalls on the PCs a lot less useful and the tradeoff security for ease of use gets worse all the time. In this tutorial we will not use personal firewalls on the inside. We tell the router to

PERMIT ALL OUTGOING CONNECTIONS FROM THE INSIDE

..to the internet so we don't have to explain to it what programs want to use the internet using what protocols and what ports etc. The router is smart enough to recognize connections that we started on the inside and remember them so it knows to let the answers back in to the PC that initiated the communication. This approach does however leave us open to attacks launched from our own inside network, so we need to take special care not to let any malicious programs in. These are some simple rules that will protect you from most of the harm lurking out there:

- When using Internet Explorer, run an Antivirus program updated at LEAST once a day!
- When using any kind of FTP, run an Antivirus program updated at LEAST once a day!
- When using any kind of Email, run an Antivirus program updated at LEAST once a day!
- ALWAYS use programs to block popup windows while surfing the web. More often than not they load programs and cookies you don't want on your PC!
- Do NOT EVER accept files from any other program (including ICQ and MSN)
- Regularly scan your PCs and Servers for virulent programs
- NEVER EVER install programs that came free on a CD stuck to a magazine!

Those measures will keep us fairly safe, but as is true on all levels of security, if an attacker really wants to get in, he or she will get in. The level of security we are looking for is one that makes breaking in a lot more effort than anything an attacker could steal would pay for. If you should find something slipped through or assume so because your PC is behaving in a very strange way or just seems bogged down and busy all the time then you may want to run some of these programs to diagnose a possible cause:

- 
- FREE Virus Scanner (does not prevent infection of course, PC-Cillin is the tool of choice for that): <http://housecall.trendmicro.com/>
 - FREEware Adware detector and remover: <http://download.com.com> ; search for “adaware”
 - FREEware tool that will alert you if any program tries to settle down in your PC by telling Windows to autostart it every time it boots up: <http://download.com> ; search for “WinPatrol”

Now then, the next part will explain how <http://hussars.org.uk> and other internet "Addresses" fit into this picture we have of networking.

4.4 Internet Name Resolution

Ok we know what IP Addresses are, what our PCs use them for and how they communicate with the Internet. We know what our router does for us with NAT and its FIREWALL functions and we have understood that an up to date Virus scanner is essential. Now let's get back to networking and see how the World Wide Web fits in the picture. Now we are humans, and as such as by design lazy, forgetful and slow. None of us can remember the IP Addresses of interesting WWW pages we read. Due to the early stages of the internet and peoples foresight of this issue, they came up with addresses that are a lot easier to remember because they are in natural language, usually English. Which you would prefer to remember:

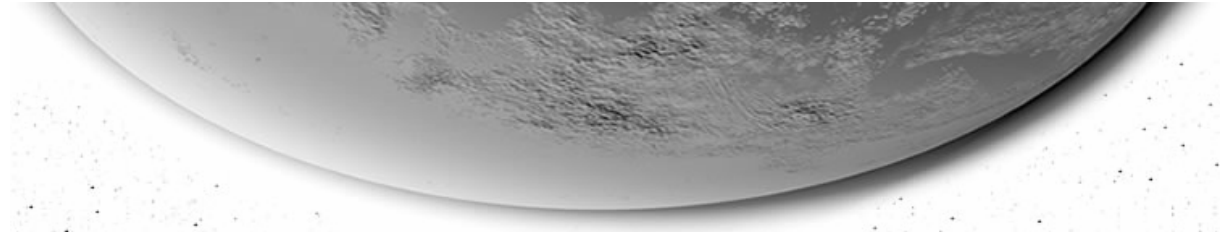
www.battlefield1942.co.uk or

212.123.221.231 (example)

SO, us humans we use names and them, the PCs they use 32bit long numbers and codes. How do the two join up? Now the general term of a computer on a network is "host". Don't ask me why, it's just the way it is. A hosts name is called a hostname. Hostnames and their corresponding IP Addresses are registered and catalogued in the Domain Name Service. If you want to know the IP Address that belongs to a name, you (your PC) ask the Domain Name Service (DNS) Server. That Server will return the IP Address your PC needs to start communication with the computer that owns the name you entered in Internet Explorer. Easy, you can try it out by hitting the START button, then RUN and entering CMD. When the command prompt opens up enter

```
PING www.microsoft.com <ENTER>
```

Your computer will ask DNS for the IP Address and then send 4 small network packets to it each asking for a quick reply so we know it's alive and working. As the replies come in, they are displayed



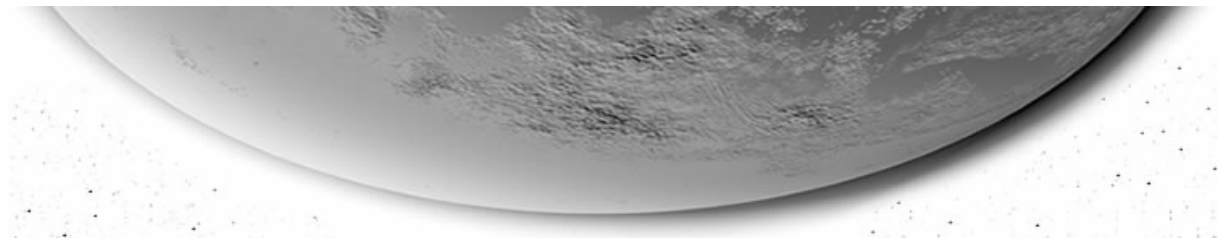
with the time it took for your request to reach it and its reply to reach. There's more about this diagnostic tool in "Ping and Lag" later on. If this fails then your PC either has no DNS Server in its IP configuration, or the server it is trying to use is broken or not reachable. Try PING-ing the DNS Server Address after viewing it with IPCONFIG /ALL. In our case PC2 should have our router as DNS Server. The Router itself doesn't keep a database of names and IPs, but it knows another Server that does so it actually forwards your request and relays the answer back to you (this is called a DNS Proxy Service). You should be able to use the WebAdmin interface for your router to see the DNS Server it was told about by your ISP and then ping that from PC2. Because our router does NAT, we could actually manually set our PC2 to use this ISP DNS Server, but it's not practical because it could change and we would have to notice, get the new address and manually configure it on PC2. It's much easier to tell PC2 to ask the router because the router is automatically informed about changes by the ISP upon every new connection.

I'm going to give you a little additional ramble on DNS names now, if you don't want to know then spin on to the next part! As uniqueness of names is of the same importance as it is with IP Addresses, the names we use must also be unique throughout the Internet. Similar to the IP Addresses, there are also names for private and names for public use. Because there are a damn site more combinations of 255 character long names made up of up to 26 different letters than there are of 32bit Addresses of 1 or 0, it's easiest to reserve the names for public use (remember with IP Addresses the ones for private use are reserved). Let's look at some public names:

www.battlefield1942.co.uk
www.eve-online.com
ftp.germany.microsoft.com
sillybugger.ath.cx

You may be asking yourself what the syntax of these names is since those are all rather different. The answer is connected to another question: How does my computer find a hostname? Is there something like a street in that name like there is in an IP Address? Yes there is. I have been a little inaccurate up until now about names. The above examples are what are called "Fully Qualified Names". An FQN consists of:

- a hostname (www)
- a domain name (eve-online)
- a top-level domain name (com) .. separated by dots.



Domains are similar to streets in function. A DNS Server is responsible for knowing all the hostnames in its Domain. Each top-level DNS Server is responsible for knowing a DNS Server for each of its subdomains. It's a tree structure where a dot "." is the so-called root Domain, the first level is the top-level Domain and the ones we can buy and reserve are subdomains of the different top-level Domains. The names of the top-level Domains define what FQNs are public (resolvable using internet DNS) and what are not. If you ping sillybugger.somedomain.backyard you won't get an IP Address because the top-level domain backyard doesn't exist. You cannot start your own top-level domain, that's another of the internet committee's rules. Once you have bought a domain you can add as many hosts and subdomains as you wish to it. Now you should be able to see how uniqueness of FQNs is guaranteed. The top-level domains are controlled and unique. So any hostname and subdomains in our FQN are automatically unique even if two separate domains contain two hosts with the same hostname. (Confused? Read again!). So if you have a website you want people to be able to reach using Internet Explorer you do this:

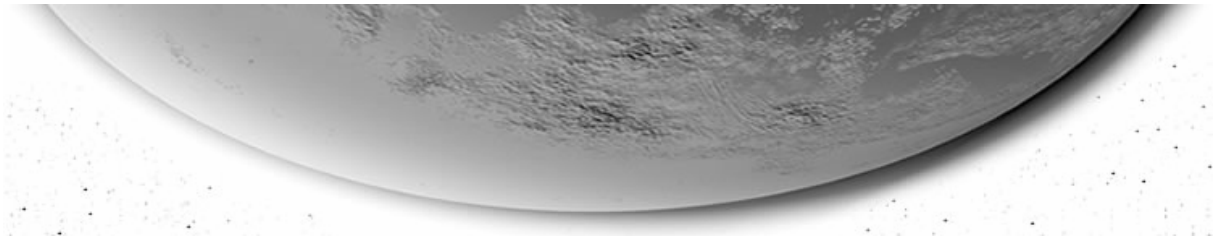
- 1: Buy access to or usage of a Server with a static Internet IP Address
- 2: Reserve a domain name and setup a DNS Server for it OR
- 2b: Reserve a Domain name at your ISP and pay him monthly for DNS upkeep OR
- 2c: Pay to register a hostname in your ISP's domain and let him worry about DNS
- 3: Tell your mates the name..

Let's use a practical example. We are connected to our ISP using our router. Typically our router is also assigned a hostname in the ISP's domain. Let's assume our ISP has this domain: ourisp.com and our router was given the hostname demorouter. Its FQN is

demorouter.ourisp.com

Anyone connected to the Internet can PING it using its IP Address or its name. It's time for an example. Our router received the IP Address of the DNS Server for the ourisp.com domain. What happens when we open Internet Explorer and enter www.eve-online.com?

- Our PC asks the router what the IP Address to this name is (and waits for an answer..)
- Our router in turn asks the DNS Server it was given what the IP is (and waits for an answer..)
- The ourisp DNS Server knows (std DNS Server configuration) the IP Address of the .com TOP-LEVEL Domain's DNS Server and asks it what DNS Server is responsible for hosts in the eve-online domain.

- 
- The ourisp.com DNS Server receives the IP Address of the eve-online DNS Server from the .com DNS Server
 - The ourisp.com DNS Server asks the eve-online DNS Server what IP Address the hostname www has
 - The eve-online DNS Server passes back the IP Address for www.eve-online.com to ourisp DNS Server
 - The ourisp DNS Server passes back the IP Address for www.eve-online.com to our Router
 - our router passes back the IP Address for www.eve-online.com to our PC
 - Our PC translates the name that Internet Explorer wants to talk to into an IP Address and initiates a connection to the IP Address it learned using the TCP/IP and HTTP protocols.

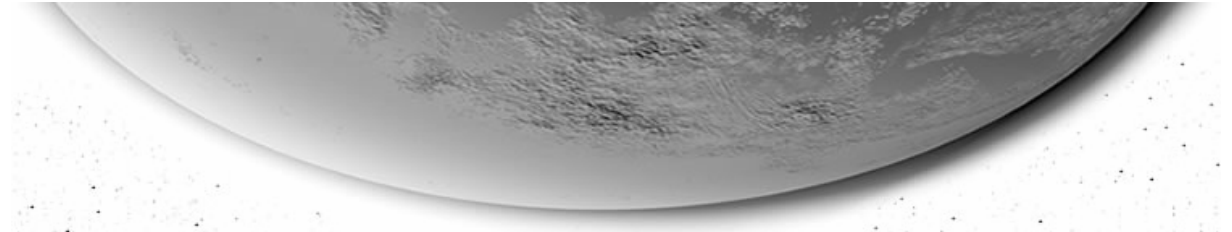
Another example: HSeldon runs a Teamspeak2 Server on PC3 for his mates to connect to. Well HSeldon's Server is of course running on his internal network with a private IP Address so how can that be made reachable from the outside so that even his not so Internet savvy mates can use it without too much tech knowledge and hassle?

- Read Teamspeak manual to find out what PORTS it uses
- Configure ROUTER to accept incoming connection requests on those ports and REDIRECT them to the internal Server whilst NAT-ting the IP addresses to the routers internal IP Address (!)
- Register a DYNAMIC DNS Name with www.dyndns.org and install a program that tells dyndns.org what IP our Router received every time it connects
- Tell mates to tell their TeamSpeak2 client programs to connect to the name that was registered.

You see with a little basic knowledge and free tools you can do a lot of stuff... I hope this little escapade made you curious for more. That's the end of the Internet part of this mega-ramble. The next post will be about communications on our private network and file sharing with Windows XP.

5 File and Printer sharing on the LAN

Now you'd think there's not really much missing in the way of computer-names and IP Addresses and all, and that like Internet Explorer uses DNS and IP, Windows Explorer would work the same way. Well, it doesn't. Once upon a time (not very long ago!), the Internet was something only



available to students at Universities. Dial-In permission to the campus Internet was something you'd kill for and so local networks were isolated ecosystems run on Novell Netware or Windows NT. The Windows world gave birth to a number of services geared to assist networking. As Netware didn't understand TCP/IP (they didn't include it into their OS until about 1998 I think) local networks often spoke IPX/SPX and NetBEUI which are not compatible with IP and DNS. So, that's why local networks developed services that at the end of the day would be made redundant by the open standards used on the Internet. Since Windows 2000 Microsoft operating systems are able to function without NetBIOS. Up until then, including Windows 98 and ME which many of you will probably still be using, NetBIOS was and is essential.

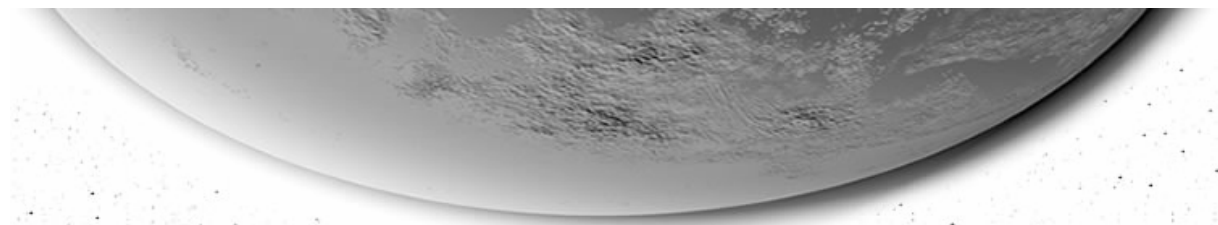
5.1 Configuring Computer-Name Resolution

Microsoft networks do not use HTTP or FTP to transfer data they use NetBIOS mostly, which is an application level protocol that could be used on top of TCP/IP or other network protocols like IPX/SPX or NetBEUI. Quick explanation: computers use network protocols to talk to each other, programs use application layer protocols to communicate with programs. Humans use some sort of abstract language (or a GUI) to communicate with applications.

When a user wants to tell a computer to make a connection to another computer, that user will use a name and not some weird protocol function, so we need to configure the computer so it is able to interpret and translate those names into something they can actually use.

A network packet is like an onion. At the core is the real data that is being transferred, like a text-file. The file itself is transferred over my LAN using Windows Explorer which uses NetBIOS to talk to the Windows Explorer on my Server. My computer talks to the server using TCP/IP. The onion has 2 shells: NetBIOS and TCPIP. Each shell adds its own header to the front of the packet.

When computers talk to each other there is one computer initiating the communication. This computer is called a CLIENT in this situation. The service (program) on the CLIENT computer that makes the connection is called the Workstation Service. The Workstation Service is responsible for any connections using NetBIOS that any program may want. The computer receiving the connection request is called a SERVER and the program that receives and manages connections is called the Server Service. You can see these Services if you right-click on the "My Computer" Icon on your Desktop or your Start Menu (XP) and hit MANAGE, then at the bottom click on the + next to SERVICES AND APPLICATIONS, then click on SERVICES. The right pane of your window will



display all installed services with a short explanation of what they do. So, we know that we want to use windows Explorer to use shares on other PCs of our home network.

We know which service Windows Explorer uses to make connections and transfer data and we know it uses NetBIOS protocol. As with Internet Explorer, there is a HUMAN using windows Explorer and humans needs names to remember instead of IP Addresses so we will be entering computer-names into it to reach shares on other PCs right? Unfortunately NetBIOS does not use FQNs (DNS hostnames), it uses NetBIOS computer-names. This is the computer-name you gave your PC when you installed it. And guess what, DNS cannot translate that name to an IP Address so we need some other way to do this or we won't have a reliable network. To see the computer-name of our PCs we hit the START button and select CONTROL PANEL, and then open SYSTEM. The computer-name has its own tab here. Yes I know it looks like a DNS name and in fact it's both at the same time but I'm not going into that right now. Just take note of our PC names. Our PCs are already named

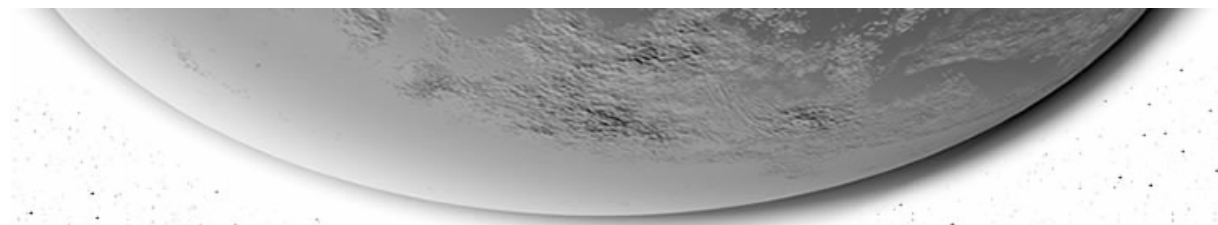
PC1, PC2, PC3

Now we know that these PCs receive their IP configuration automatically from the Routers DHCP Service. This means that they could change over time. In turn this means we need a way to automatically keep track of which computername gets what IP Address. This is done by the Windows Internet Name Service (WINS). This service was named back when MS thought it could force the world to use NetBIOS instead of DNS hostnames, it has nothing to do with the Internet). Now if you are lucky your router can do this also and has already given your PCs a WINS Server address in their IP configuration. If it has you will be able to see it if you open a command prompt and enter

IPCONFIG /ALL

If the WINS Server configuration is empty then we have a problem. Check if your Router can do WINS. If so, use the WebAdmin to activate it and reboot your PCs, they should automatically be told to use it now, in which case our problems are solved. When a PC needs a NetBIOS name resolution it will ask WINS for it and get an IP back. When a PC starts it will actively tell the WINS Server its current name and IP Address so the WINS DB is always up to date. If your router cannot do WINS then we need to get creative and dive deeper into the operating systems legacy parts.

Now in theory Windows computers are able to resolve NetBIOS names on the local network without ANY help. They do this by creating a special network packet. This packet carries the senders IP Address but the recipient is a special one: 0.0.0.0. Packets with this destination in them will be taken



off the network and read by every host that is connected. Routers will not forward these to other networks (if they did you can imagine the Internet would be clogged with name resolution requests) so it stays on the local wire. Inside this packet your computer placed a question:

"What is the IP Address of the computer called PC2?"

All PCs will read this and only the one called PC2 will answer telling us its IP Address so a connection can be established. Now in practice this doesnt always work for reasons in part unknown to me and in part too complex to explain right now. IF you have problems with name resolution on your local network then you will want to manually configure a name resolution on your PCs and edit it whenever their IP addresses change (OR did out an old PC and install windows Server with a WINS Service on it). So how do you know if you have a problem?

- Open Windows Explorer
- Right click on "My network neighborhood"
- Select FIND Computer
- Enter the computer-name to look for ex.: PC3

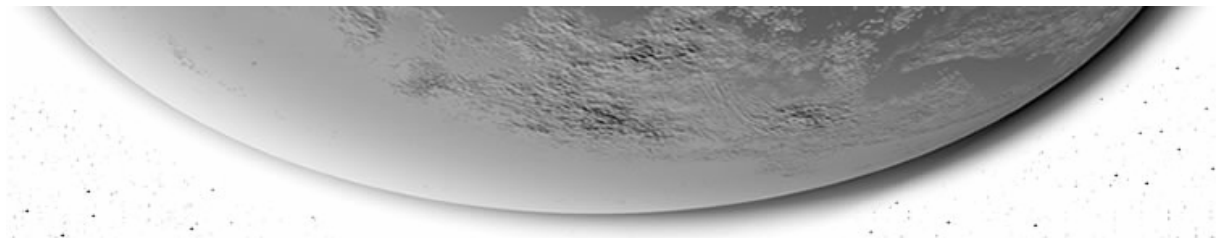
IF NetBIOS name resolution is intact the search will reveal an icon of PC3 which you can right-click and select "Explore" on, revealing a list of the shares available on it. If the search window stays empty then we have a problem either with name resolution or the physical network. A quick PING to PC3s IP Address (192.168.100.3) will reveal if the physical network is ok. If name resolution is the problem you need to edit a text file on your PC. More about that in a min. If the PC3 icon appears but you get a access denied error, everything is ok because we havent set any permissions yet. We will solve this in a bit. So, the file to edit is

C:\WINDOWS\SYSTEM32\DRIVERS\ETC\lmhosts.sam

Scroll to the bottom (read the blurb if you like, it explains what it's all for and what the syntax is) and add a line:

```
192.168.100.3    PC3
```

Then "Save As" filename lmhosts without a suffix! Next you need to go to Windows Explorer and find this file because notepad will automatically add a .txt to the end of that file and it needs removing or it wont work. Check your folder options to make sure you can see the file ending, since it's a "known file type" that has its endings hidden by default. Once this is all done open a CMD prompt and enter



NBTSTAT -r

This activates the name resolution file changes. Next use FIND COMPUTER to search for PC3 again. This must now work unless you mistyped something.

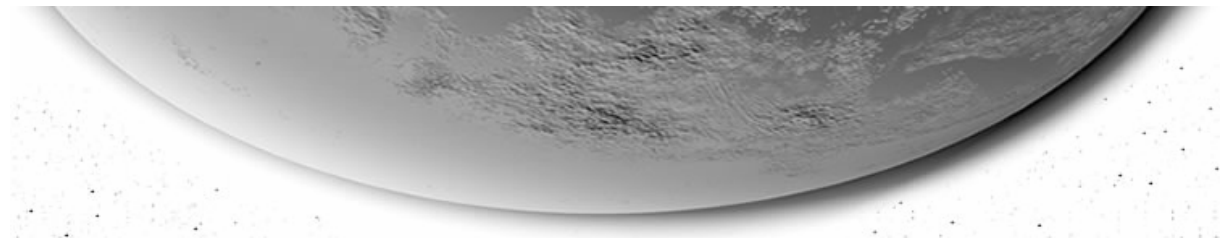
5.2 Set up user accounts

Ok every connection to a computer using Windows XP requires a user accounts authority, else access will be denied. Each Windows XP computer has its own little user database that contains user accounts and user groups. User Accounts as well as User Groups can be assigned access to resources (files, printers, shares, etc). You can permit anyone to connect to your shares by activating a special account called "Guest". When this is active no authorization is required to connect. I recommend you right-click the Guest account and disable it. Where ? Oh yeah, right-click My Computer on your Desktop or in your funky start menu and select MANAGE. On the left hand side find "Local Users and Groups" and hit the + next to it. Now click on Users and hey presto you get a list of user accounts in the right hand pane of your window.

Right-click on the Users container on the left and select NEW USER. Enter BumFluff as username and some password you want to use in the password and confirm password fields. Untick the "User must change password..." option for now and hit create. Repeat this on all three PCs of our example home network. In larger networks you would have a dedicated Server looking after user accounts, and if authorization for access is required, the Server computer would challenge the Client computer for a username and password, which the Server computer would pass on to the Accounts Server to validate. In our little scenario we don't have a central server so to keep stuff easy we will keep user accounts with the same name and password on all three PCs.

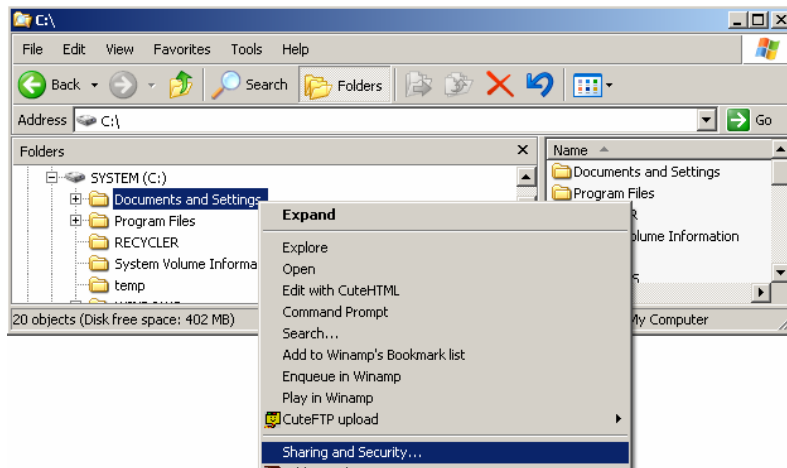
5.3 Set up shared directories

When we share stuff we expect other local network users to be able to connect to our PC, so we need it to be able to perform the SERVER side of connections. Make sure the SERVER service is running (should be). The other PCs will need to have the "Client for Microsoft networks" installed and activated. To check up on this hit START, select CONTROL PANEL, open NETWORK CONNECTIONS. Right-click on your network card and select PROPERTIES. In the window that comes up now, scroll around and locate "Client for Microsoft networks". If its there and ticked yer ok.



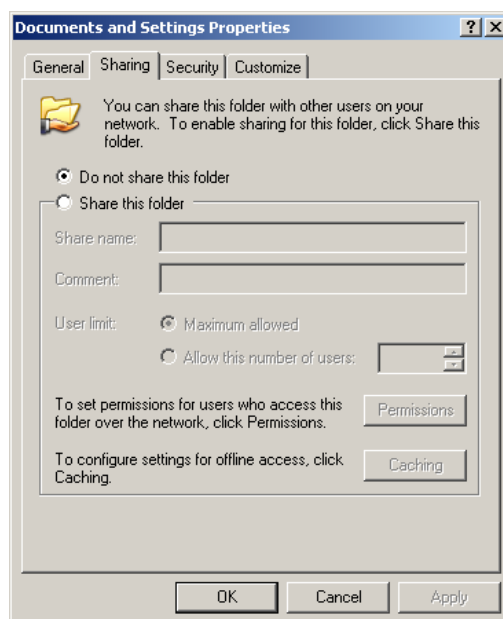
Cancel your way out. If its not there hit ADD and install it.

Open Windows Explorer and navigate to the directory you want to share. Right-click it and select "Sharing and Security".

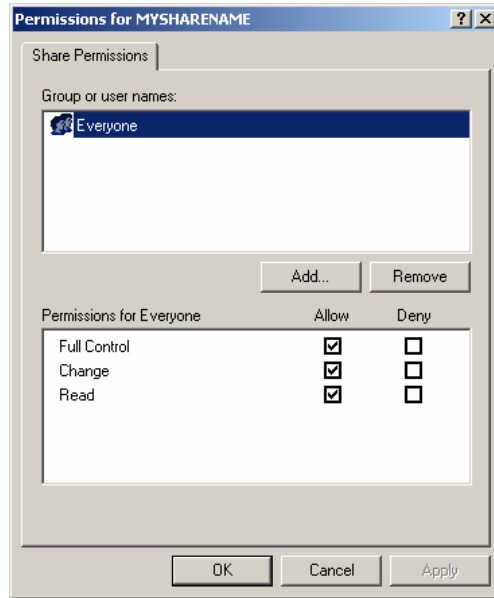


ATTENTION: Windows XP Home Edition differs from the PRO version here. I have never used a Home Edition and I dont intend to so use yer loaf and work this out for yerself or *gosh* read some help. XP Help as well as Windows 2000 help is actually VERY good. Did I mention that Home Edition is a sack of manure? If you can, ditch it and get the Professional version.

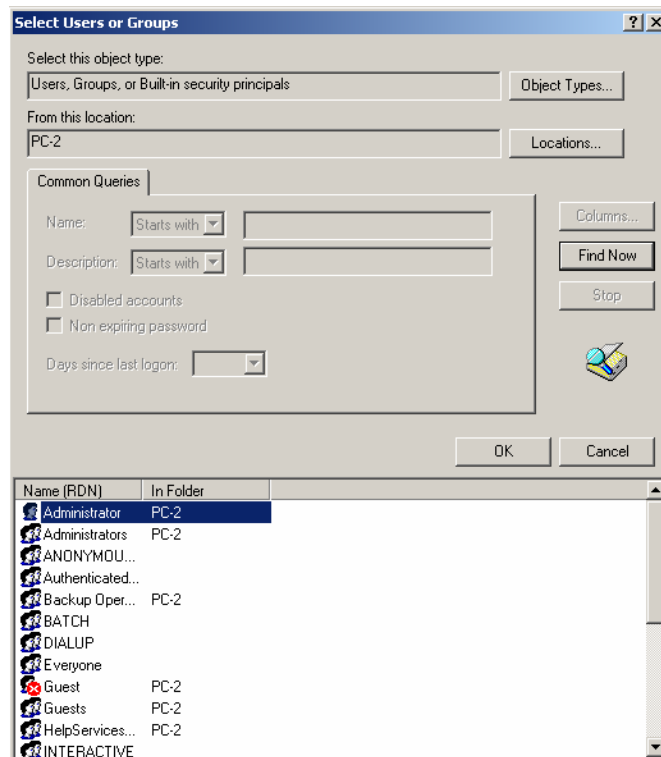
Now a window should have popped up titled "Data Properties" showing you some radio buttons.

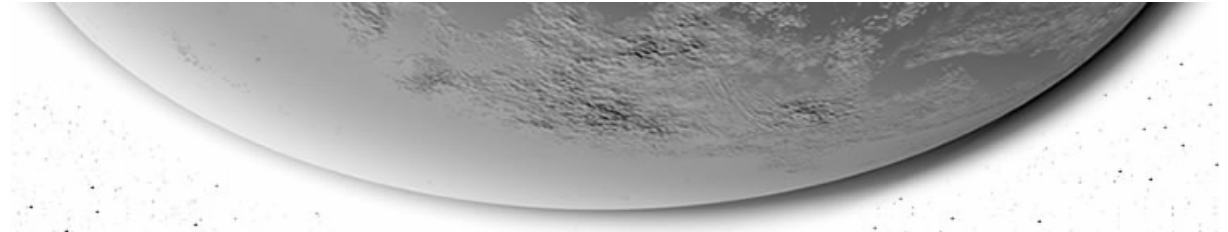


Click the one that says "SHARE THIS FOLDER", then enter a share-name (this name will be visible if somebody FINDs this computer and Explores it. Enter "PC2-Pics" or something that describes the content you are sharing. Add a comment if you wish, but then hit the PERMISSIONS button.



Click "EVERYONE" and hit REMOVE. Cant have that rubbish... tsksk. Now hit the ADD button then in the new window hit ADVANCED, then just hit FIND NOW and the window will fill up with all the computer accounts and groups currently on your computer.





Find the one we just created and highlight it, then hit ok and OK again to add him to the list of admitted user accounts. Next we need to define the type of access this account gets. Usually you will want to give it full control to keep it simple. If its for your wife or kids, make it read only >);). BINGO thats it.

5.4 Testing file sharing

Go to another PC and connect to this share using one of two methods. The first is automatic and easy, the second is more usefull when you know the destination computername and sharename and dont want all the clicking around.

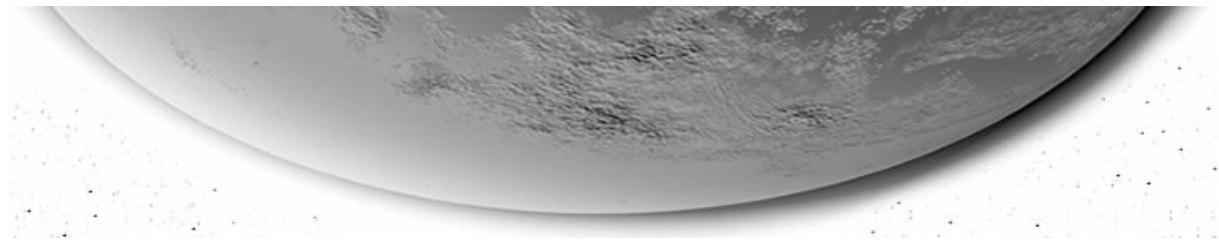
1: Open windows Explorer, right-click the Network Places and select "Search for Cmputers" enter the computername and hit Search. Right click on the computers icon that is hopefully found and select Explore or just click on the + next to it. Right-click on the Sharename and select "Map Network Drive". From here on in its the same for both methods..a window pops up!

2: Open Windows Explorer, open the TOOLS menu and select MAP NETWORK DRIVE. In the window that pops up in the FOLDER field you need to enter the computer and share name in a special format. The format is called Universal Naming Convention or UNC for short. The syntax is [\\<computername>\<sharename>](#) so in our case you need to enter [\\PC2\PC3-Pics](#)

Next select if you want this connection to be automatically made whenever you logon and select a drive letter to use. Now comes the more tricky part. IF you have logged onto your local PC using an account that also exists on the computer you are connecting to, and both accounts have the same password... you can hit OK and everything works fine. If you are NOT logged on to your local PC with an account that also exists on the target computer you WILL get and access denied message. '

IMPORTANT: If you hit OK anyway, your PC will try to connect and upon the Servers challenge your PC will pass through the account and password you are logged on with. Once this has happened you cannot specify another account to authorize this connection until you have logged off and logged back on again. That's the way MS works. So, think before you click. To find out who you are logged on as, hit CTRL-ALT-DEL. Your username is displayed like this

<Computer-name>\<username>



Ok having followed that you might discover you are logged on with an account that does not exist on the target computer which holds the share you are trying to connect to. You can hit the blue text "different user name" and enter a username and password to use for this connection to make it work anyway, but again, only if you haven't already failed a connection to this computer since you last logged on. Enter the username you want to use like this for our example:

```
username: PC3\BumFluff
```

```
password: <whatever you set>
```

5.5 Set up printer sharing

More soon TM

5.6 Test printer sharing

More soon TM

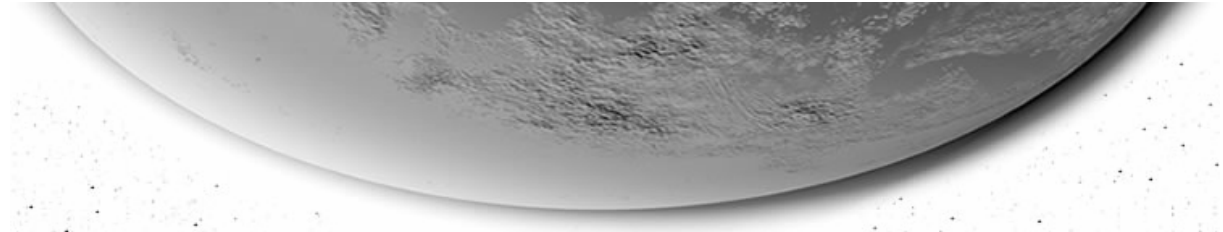
6 Pings and Lag

Let's go back to the things we actually like doing with PCs: games. On a local network games quite happily run and you will not notice any network related problems unless you really try. Playing over the Internet is however a different story. Suddenly the quality of a network connection plays a role in your gaming experience, and of the affected gamers not many really know what makes up the quality of their connections. There are two expressions that we all know: PING and lag.

A PING is not a PING is not a PING! There are a number of things that make up your connection quality. The three basic values of interest are the

- Rate of packet loss
- bandwidth
- Latency (ping time)

Bandwidth is important, no doubt about that. Still, when playing games online it really is the least of your problems. Most games are made to enable players with 56k Modems to play, so they rarely require more than 5-7kB effective bandwidth per second. The only time you may need to worry about this is when you host a game server that other players will connect to (of which BF1942 is by far the hungriest).



Let's look at packet loss. You can have an excellent ping, but if for some reason some of your packets don't make it to the destination you will get disconnects and jumpy opponents at best. Usually packet dropping is due to two things:

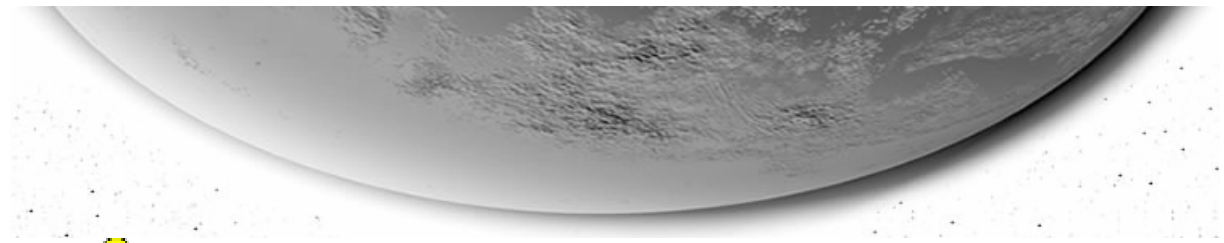
- Hardware errors
- symptom of overloaded hardware

The former would give you good pings *if* you get through, the latter would give you bad pings since even the packets that get through have to "wait in line" to be forwarded towards your destination. Packet loss is the REAL dread. More often than not it will simply disconnect you if it crosses a certain threshold set in the software of the game. The solution to the first problem is to report it to the ISP. They may (or may not) fix it. Usually new BIOS for the router is in order. The latter could also be caused by a router with too little RAM but it could just as easily be caused by congestion coz some other routers have died and a bottleneck exists toward a certain network or area of the Internet. Only time will cure this one =).

6.1 Why a ping is not a ping

A ping is a special type of network packet that contains the request for the recipient to echo it back to the sender. As there is no real data apart from the senders IP Address these packets are rather irrelevant. Some ISPs set their routers to process these packets with a LOW PRIORITY. So you may have a good connection in game in spite of showing an appalling ping time. Game packets are clearly discernable from ping packets to a router they pass through and would be treated with the regular priority for data packets. On the other hand a good ping with a little packet loss might have the opposite effect.

A ping is usually only high due to the number of routers the packets pass through on their way to the destination (a virtual distance). The farther away your destination, the more possible routes there are for a packet to take on the dividing network. That increases the chance of one or some of them having a problem or breaking down. During a game each of your packets may take any of the available paths through the internet, which is one reason why a ping time may fluctuate a lot (paths have different lengths). If a path exceeds a certain maximum length your packet may also be considered too old and hence irrelevant to the application waiting for it. A router would drop these and the effect is packet loss. This prevents packets from circling the net for days when some ISP lets idiots configure their



routers 😊. Now apart from the network connection there are a few other things that might try to screw up your gaming fun.

- The target server: If its CPU isn't macho enough to handle the amount of players trying to play on it, it builds up a queue of "things to do" i.e. process the info coming in from and going out to the players. When this happens ALL players of a server show terrible pings all of a sudden. This has nothing to do with their connections and is usually referred to as "Server lag".
- your Firewall or Router: It may be slow and take a long time to translate your internal packets coming from a PC on your LAN into packets that can travel across the internet (private <-> internet IP Addresses must be kept separate by translation).

If you have a hardware router showing this problem, you should get the latest BIOS (Firmware) for it and upgrade it and/or increase its RAM size. If it's a PC you may want to give it a faster CPU and some more RAM.

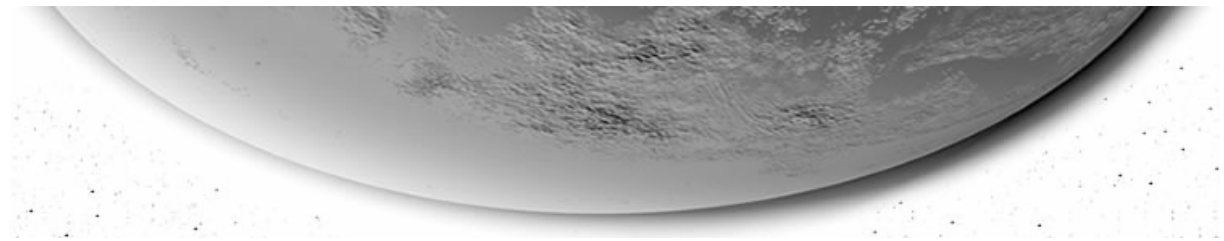
How you are connected to the internet (56k Modem, DSL or cable) is NOT the primary criterion. As long as the game you play doesn't need more effective bandwidth than your connection can deliver, the quality of a gaming connection is dependant on a load of things that I won't go into now. ISDN for instance is from a technical standpoint the FASTEST connection type for online gaming since its infrastructure permits very low latency. In spite of its bandwidth of 7KB/s effective, it is faster than most DSL connections. On broadband connections it is still normal for the routers connecting you to be configured for MASS data transfer rather than FAST data transfer. This has come to ISPs ears and is now being sold to us at an extra cost (although their routers actually have LESS work with it): "Fast Path" is their product name. My ISP offered it to me for 4 EUR a month (!), needless to say I declined.

A Modem (Analog connection) is about the slowest way to connect since it must convert digital signals into analog signals and back, which the others don't have to do. Still, if its route to the server on the internet is clean and its bandwidth is sufficient then there is no reason why it shouldn't outperform a DSL user connecting over a bad network or simply from the other end of the world.

Message:

To those who have 56k Modems: It's a damn site better than my old Lightspeed 2400c (2.4kbit), and its good enough to play online with. To those who slag off 56k users as fun-spoilers and try to push them

Copyright © 2003. All Rights Reserved. Featured trademarks are © of their respective owners.



from servers: You may want to read the above and think before you slag off a modem user. Also remember that broadband is not available everywhere.

7 Appendix

7.1 Links for help and support

<http://www.microsoft.com/technet>

More soon TM

7.2 Glossary

More soon TM