Introduction to TCP/IP

Introduction to TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of protocols devised back in the 1970's to allow communication between hosts. It was designed to be flexible and expandable, although
at the moment is supposedly nearing breaking point for reasons that I will explain later.
Because of the popularity of the Internet it is available on practically every computer type and operating system, and can scale from handling connections of all speeds, from modems right up to huge multi megabit fast international connections. This makes it very suitable for handling the varying performance levels across the Internet.

1. The Basics.

Every device connected to the internet has one IP address. By "device" I mean a box of electronics that accesses or provides resources, routes information around the superhighway etc. Such devices include client computers, servers, routers (devices that connect one network to another network and pass information between them) etc.
The IP address is in the form of a number aaa.bbb.ccc.ddd where each octet (each set of 3 digits) is a whole number between 0 and 255. Thus, the theoretical range is from 0.0.0.0 to 255.255.255.255. The reason that the number count does not go up to 999 is because these numbers are interpreted in binary (base 2) by the computer, and 255 is the highest number that can be obtained in 1 byte of information. (if you want more information on binary arithmetic and why this is so, please look in any book on computer science above GCSE level or maths at A level, or use the Windows Calculator in Scientific mode).
Nearby the IP address configuration option is an entry for the subnet mask. This defines the scope of the local network, because it is ANDed with the IP address to perform a binary AND to determine the size of the local network. For example:

IP address 192.168.2.3 (binary: 11000000 . 10101000 . 00000010 . 00000011)
AND 255.255.255.0 (binary: 11111111 . 11111111 . 11111111 . 00000000)
Using the basic knowledge that 1 AND 1 is 1, 1 AND 0 is 0, 0 and 1 is 0 and 0 AND 0 is 0 we have the result that the network is anything starting with 192.168.2
Thus, the local network can have 255 hosts starting with 192.168.2.

The IP address is divided into two parts defined on the Subnet mask. The Network ID is the part defined by the subnet mask - 192.168.2 in the above case, and the host ID as the 3 to define the individual host on the network.

IP addresses are given various classes, which define the IP address range and subnet mask that should be used, and these are defined globally in international standards.

1. Class A addresses have the first octet between 1 and 126
2. Class B addresses have the first octet between 128 and 191
3. Class C addresses have the first octet between 192 and 223.

You will notice that there are gaps, notably 127 and anything over 224. These will be discussed in section 2.

Subnet masks may seem redundant as specific networks can easily be determined by looking at the IP setup, but the subnet mask can be used to further divide a single network.

1.1 TTL (Time To Live)

Every packet of data using IP has what is called a TTL figure – a time to live. This defines the maximum life of the data packet in milliseconds. This is important because it is possible that a packet of data may never reach its intended destination, and forever wander around the TCP/IP network using up bandwidth. Every time the packet passes through a routing device, the figure in the TTL header is reduced by the number of milliseconds since the last route, and if the TTL figure is zero or less, then the packet will be discarded rather than forwarded. You can see the TTL figure using the Ping.exe program detailed in section 6.1.

1.2 Default Gateway (Sometimes called a Default Router)

The Default Gateway is the IP address to which packets that are destined for a network outside the current one are sent. It is typically the address of a router. This entry is optional, because on many networks, especially private ones, there will be no router. Take a look at section 2 for details on private networks.

2. Reserved Addresses

The network starting with 127 has a specific purpose: it is what is called the loopback address.
This is because it is used to refer to the current computer. There is only one valid IP address within the 127.x.x.x range, which is 127.0.0.1. Thus, any software that uses TCP/IP can operate on a computer not physically connected to a network. Note that the IP address assigned is used in addition to the loopback address, so "localhost" and "the local DNS name" refer to the same system, the only difference being that localhost requests don't need to go onto the network and use up bandwidth.

2.1 Private Networks

Each class of IP address has a range that is reserved for use by private networks:

Class	Address range	Largest Subnet Mask permitted
A	10.x.x.x	255.0.0.0
B	172.16.x.x	255.240.0.0
C	192.168.x.x	255.255.0.0

This means that there can be multiple occurrences of addresses within the Internet because routers are configured so that addresses within those ranges won't be forwarded. This is because there are many networks, which don't have globally visible IP addresses (i.e. addresses outside these ranges), but still need the ability to maintain a TCP/IP network on its computers. A typical use for such things is a small company or home network, with an internet connection through a proxy server.
The address range from 224.0.0.0 through to 255.255.255.255 are multicast addresses. These are used for broadcasting the same information to multiple computers at the same time.

3. Ports and Services

If each device on the internet only provided one service, then just connecting to its IP address would be sufficient. However, many provide multiple services, such as web servers, ftp servers, SMTP and POP3 email servers and usenet news servers as examples.
In order to differentiate between different services on the same server, the concept of a port is used.
Think of a port as a logical connector, not quite dissimilar to the cables at the back of the PC. It is not, however, a physical connector, it is only a number.
Different services use different ports, so when a connection is opened, it is not to a specific IP address, but to a specific port on a specific IP address. Below, please find a list of common ports and services:

Service	Port	Comments
FTP data transfer	20	Used for data transfer of FTP files
FTP control	21	Used for controlling FTP data transfers
Telnet	23	Used for accessing a remote console of a device, normally for administration purposes.
SMTP mail transfer	25	Used for sending email around TCP/IP networks.
DNS service	53	Used for converting names to IP addresses and vice versa
Bootp/DHCP	67	Remote network configuration –You can't have both on the same network
Trivial FTP	69	Like FTP, but simpler and less secure. Is frequently used for providing remote bootup facilities for diskless workstations.
Finger	79	Used for obtaining information about user accounts on a specific host. Rare now on publicly accessible systems because of security implications.
web servers (http)	80	A web server.
POP3 Mail	110	Used for downloading email from ISP into email package
Usenet News	119	
NTP time synchronisation	123	Used for time synchronisation across a network.
NetBios Session	139	Used in MS Windows networking plus compatible (eg Samba on Linux)
SSL Web connections	443	Used in e-commerce secure web transactions.
IRC Chat sessions	6667 and 6669	Used by IRC Chat servers and client software.

There are many other ports which are in frequent use - for a fuller list take a look at c:\windows\services on a Windows computer (but don't change anything) or a good book on TCP/IP. A port can be any number between 0 and 65535, and a lot of the recent viruses or trojans use ports fairly high up in the range which aren't yet reserved for use by any particular application. The phrase "Service" relates to a background process running on the computer, which may or may not service connections to one or more ports on the machine. This is the term used on Win32 systems including NT and 2000. Unix/Linux systems use the name "daemon" for the same thing, and Novell Netware uses NLM's (Novell Loadable Modules). Socket connections are connections between one machine on one port to another machine on a port, and is quite a normal way of communicating over a TCP/IP network. Many ports have been reserved for use by specific applications, for example the Sybase Adaptive Server Anywhere database engine runs on port 2638 by default, but there are many that are free to be used as you wish. However, something has to be running, listening for connections on a port to enable connections to it. As an example, a machine without a POP3 server running won't permit connections to port 110 by default as there is nothing 'listening' to accept the connection. The numbers listed above are default ports, accepted widely. However, there is no reason why a system administrator could not use non default ports for increased security, but it would be harder to debug if problems occurred, and it would be an extra administrative burden altering the settings in client software such as email clients.

3.1 The ShieldsUp test at http://grc.com

The ShieldsUp server at http://grc.com attempts to connect to some of the ports on your computer with important services running, as it 'knows' your computers' IP address from the web site access logs.

In order to make a successful connection, the client computer needs to have a piece of software running which uses that port – e.g. a mail server for ports 25 and 110, or a file server on port 139.

If nothing is running on a particular port then no connection can be made to it.

4. Firewalls

What a firewall does is hide the fact that some ports are open by intercepting incoming connections before they open based on a set of rules - you might want to permit connections to some services on some machines, such as port 80 on a web server. They can also do further things to make networks secure such as Network Address Translation (NAT), which means using a private or invalid range of IP addresses, and have the router or firewall convert them to valid ones on going out according to a predefined set of rules. It can also block incoming connections to DNS and other servers, which can make it difficult to find out how the network is structured, or what servers are running.

A firewall can be one of three types:

A dedicated hardware device into which the network connects on one side, and the external connection on the other side. This can be another network, a dialup connection through modem or ISDN, or a connector for ADSL or a cable modem.

A piece of software running on a dedicated computer sitting between the private network and the internet connection through which all traffic has to pass. Such software here includes Firewall-1 from Checkpoint software.

A small piece of software running fairly low down in the TCP/IP stack on a non dedicated computer, commonly referred to as a personal firewall. Such software in the latter category includes ZoneAlarm and Symantec AtGuard.

It is worth noting that a firewall must be configured correctly, otherwise it may allow traffic through that should be blocked. There used to be, although it still exists to a lesser extent now a "We've got a firewall so we're safe from internet attacks" mentality which is not true. A firewall will also not stop certain attacks, such as recent viruses sending messages to everybody in Outlook address books if sending external mail is permitted.

5. Assigning of IP addresses.

Apart from the private IP address ranges, which anybody can use, addresses are assigned globally by an organisation called IANA (The Internet Assigned Names and Numbers Authority). This organisation assigns blocks of IP addresses to companies, including ISP's.

It is up to each companies IT staff how they use the addresses given, whether they give fixed addresses to each device, or use a DHCP server to disseminate IP address information to each computer on a network. It goes without saying that the DHCP server must have a fixed IP address as it cannot assign one to itself, and that there can only be one DHCP server on a particular network at a particular time otherwise confusion will reign.

5.1 DHCP servers (DHCP stands for Dynamic Host Configuration Protocol)

A DHCP server is a computer running a service or a specialist device, which is used to distribute IP address, subnet mask, router and other TCP/IP configuration information to the clients etc.

This is used to centralise control in environments, to ensure a consistent configuration across all machines whilst ensuring that IP addresses remain unique amongst their clients. Another reason for the popularity of DHCP servers is because the addresses are not assigned to a particular computer on a permanent basis is that addresses can be reused.

This is because DHCP works on a lease time defined by the server, towards the end of which the computer must renew it to ensure that it still remains active. Should it not be done so the address joins the pool of unused addresses. This is important, as due to the recent exponential growth of the internet, there is a shortage of addresses available. There are ways around this, a common way of which will be discussed in section 7 on Proxy servers.

5.2 BOOTP (Bootstrap Protocol)

Related to DHCP mentioned back on page 1 is BOOTP. This is an older version of the same type of protocol which only assigns addresses, not other information, and the assignment was permanent. It has been superseded now in all but the most specialised of circumstances by DHCP.

6. TCP/IP utilities and tools.

Many tools and utilities are available as standard to help administrators manage TCP/IP networks, diagnose faults and track down bottlenecks. Many of these you may have heard of and used, but didn't understand what was being done. All of the tools mentioned here are command line tools, designed to be run from a DOS window/NT command prompt unless otherwise mentioned.

6.1 Ping (PING.EXE)

Ping is the most common TCP/IP diagnostics tool, and is used to determine whether a particular host is available. The syntax is ping <hostname> or ping <IP address>. It will either return a "Successful access in xxx milliseconds" type, or "Host unreachable". If accessing a machine by name doesn't work, but by IP address does, then the DNS servers are not configured properly or the remote DNS server is not working.

If a "ping localhost" or "ping 127.0.0.1" comes back as a failure, then TCP/IP networking on the local computer is not working properly and needs looking at.

Ping attempts to connect to port 7 on the remote computer and wait for a reply. Just because a ping fails it doesn't mean that the host is down though, because many routers/firewalls are configured to block ping requests for security reasons.

6.2 Traceroute (TRACERT.exe)

If ping just tells you if the final host is accessible, traceroute (tracert.exe in Win32 systems) is used to determine where along the internet the bottleneck is. Syntax is tracert <hostname> or tracert <ip address>. On Unix systems the command is traceroute in full, the shortened name on Win32 systems is necessary for the 8+3 command names for historical reasons from DOS.

It will show the path that it is going through the various networks and the hosts through which it passes, and you will be able to see how fast each segment of the network is, and where the block is in place.

Don't be surprised if you perform it more than once for the same host that the results are different, as this is part of the way that the internet is designed and different packets may well go different ways as changes on the internet are reflected to the end user.

6.3 Finger (finger.exe)

Finger is a tool only supplied with Windows NT/2000, although versions for other operating systems are available from many of the freeware download sites on the internet. It is used to determine information about a particular user, the syntax is finger <username@hostname.domain>. Don't be surprised though if such connections are blocked because the informed can tell use the output of finger to tell them about users on the server, and sometimes its operating system by looking at the format of the messages displayed. In fact, running a finger process on a publicly accessible server is rare these days.

6.4 NSLookup (nslookup.exe)

NSLookup.exe is a tool available only on Windows NT for looking up IP addresses and returning the host names associated with it, and returning the IP addresses associated with a hostname. The syntax is nslookup <ip

address> or nslookup <hostname.domain>. As with finger, some networks will have blocked external access to their DNS servers for security reasons.

6.5 IPConfig (ipconfig.exe) and WinIPCFG (Winipcfg.exe)

IPConfig is a tool for the Win32 family of operating systems that shows the complete TCP/IP configuration of the local computer on screen, including many configuration options that aren't here. It will tell you the addresses of DHCP and DNS servers, routers etc and is a very useful tool for troubleshooting network problems as it puts all the useful information in one place. There is a Windows based version of this tool called Winipcfg (use Start -> Run -> Winipcfg). Both IPConfig and Winipcfg allow you to release and request new addresses from a DHCP Server.

6.6 Telnet (telnet.exe)

Although Telnet is primarily a means of accessing a remote computer, typically for administration purposes, it has its uses for problem diagnosis. Although it by default connects to port 23 for telnet, it can also connect to any port on the system by changing a configuration switch. Syntax is telnet hostname port#. If port# is omitted, 23 is assumed. Telnet is valuable as an administrative/diagnostic tool because it allows users to connect to a specific port and viewing the communications between the server and client machines. Many other devices such as print servers and routers have built in telnet systems for administration.

Unlike other tools mentioned here telnet is a Windows program under Win95/98/NT/ME but has reverted to a command line tool in Win2000 but don't ask me why.

The Microsoft telnet client as supplied however has many flaws, as it doesn't support a particularly wide range of terminal types and is prone to the stepladder effect. This is where text doesn't move down to the next line at the end, and you end up with lines that start the character after the last one on the line above.

As with others, many excellent freeware tools are available from numerous Internet download sites but my own particular preference is for a program called Tera Term Pro available at many sites.

6.7 Whois

If Finger allows you to find out about users on a specific host, whois allows you to find out which company/organisation owns a particular domain. No whois tool is supplied as standard with any Microsoft operating system, but as always free tools are available on the internet.

6.8 Port Scanners

A port scanner is the name for a tool that attempts to connect to multiple ports on a specific host or group of hosts and is the general name for tools such as the ShieldsUp web site. As with Whois, none are supplied as standard with Windows, but free versions are available on the internet. My own preference is for TCPScan available for free on the internet, but as always others are available. These can also help find other security holes that you didn't know about, or processes running on machines.

6.9 Other Tools

There are other tools that are available, but I think they would rather blind a TCP/IP beginner with science further so I won't go into detail. However, I will tell you about a program called NetLab, which is a swiss army knife of TCP/IP tools combining ping, traceroute, finger, NSLookup, whois, time synchronisation and a port scanner into a single Windows' package, and is well worth downloading and keeping to hand. As it is freeware you can't really go very far wrong. The home page is at http://members.tripod.com/~adanil/ or search for it on tucows.com or Nonags.com.

For other tools, the Network Tools facilities at Demon Internet provide facilities for NSLookup, whois and searching of other TCP/IP related information at www.demon.net. You don't have to be a customer of Demon Internet to use them.

6.10 Web based Administration tools

The exponential increase in use of the world wide web has led to a significant increase in web savvy users, and so many manufacturers of network connected hardware devices now have a web based administration interface such as storage arrays, print servers and routers. Even some user applications/operating systems now have a web administration interface to make things easier for the novice administrator. Such systems include Linuxconf, which runs on port 98 and permits most of the administrative tasks that a user would want to use on a Linux server/workstation. To find these, which are often undocumented and well hidden, run a port scanner against the machine. If you find any unidentified open ports, use a web browser to connect to it with the syntax http://machinename:port for example http://linuxbox:98 to connect to port 98 on a machine called linuxbox.

7. Proxy Servers

A proxy server is a server that does something for a client computer. Proxy servers are commonly used for several reasons:

1. To allow a network, notably those on a private IP address range to share an internet connection through a dial up facility within a small network. There are many proxy server packages available, such including WinProxy and NetProxy amongst the small and simple packages, right up to MS Proxy server at the complex level, or packages such as Squid on a Unix machine.
2. Cache and store frequently accessed content, thus reducing internet requests to access the pages or download files, especially if you have a low bandwidth connection or pay for connection time perhaps on a dialup or ISDN connection.
3. The final reason for using a proxy server is to provide some form of security to the network, both in terms of blocking access to undesirable web sites etc, and also any potential hackers following the connection back would find the proxy machine first rather than the client computer, a lot more difficult to break into than if it is a Windows PC direct. Having said that, no proxy server is 100% secure.

Proxies are configured through the Internet control panel’s Connections page on a per connection basis, because different ISP’s use different servers, and using a server not local to your connection can and probably will significantly slow down your connection.

Proxy servers typically run on port 8000 or 8080 on the host computer, although Squid runs on 3128 by default, so the chances if you have incoming connections from such a port it is a proxy server making the connection.

In general, if a proxy server is available it is a good idea to use it, but should it be overloaded, e.g. if you have a consistently slower than expected connection than it could be the server that becomes a bottleneck and it may be an idea to remove it if possible.

8. Special cases

In the world of TCP/IP networking, the above are all well and good, but there comes a time when having a “standard” setup is just not enough. This section covers some of the more common of the specialised setups.

8.1 Multi homed systems

Many servers have multiple network interfaces to increase the bandwidth into / out of the system. A typical 100Mbit network card although it would suffice for many personal and low traffic web/ftp sites, assuming that the rest of the server was up to the job, could find the bandwidth overloaded if the site had a major advertising campaign, for example.. One easy way of adding extra bandwidth is to add extra network interfaces to the server and have the router switch between different addresses to allow each one to take some of the load. A multi homed system is simply one with more than one network adaptor, and these are typically on different networks. Multi homed systems can act as a router between networks, but need special configuration in the operating system and it is generally better to use a proper dedicated router if available.

8.2 Load balancing and clustering

Sometimes there comes a time when having a single server to host a site is not enough. Sites such as Yahoo.com, Altavista.com and Microsoft.com have thousands of servers worldwide. Load balancing is the act of having the same resources hosted on multiple servers, and use a fancy DNS configuration to switch the load between them. The most common way is Round Robin, in which each site has a list of IP addresses associated with it. As each request comes into the DNS server it gives out a different address, going through the list until the last one is used when it reverts to the first. The difficulty with this approach is that the content has to be mirrored on all servers involved, and it makes analysing log files very difficult as all servers’ have to be taken into consideration at the same time.

Clustering is a slightly different approach to solving the same problem and it also involves adding a second server, absolutely identical to the first. It involves setting up a dedicated high speed connection between the two. What happens is that all writes/updates are reflected on both machines, but reads are done only on one, alternating between the two. The systems are so tightly integrated that they appear as a single machine for the purposes of administration, and what must be done to one is done to the other. Although I mention two, there is no reason why there cannot be more than two servers clustered together.

8.3 Microsoft TCP/IP enhancements over the ISO standards.

As usual with many things, Mr. Gates has seen fit to add his own proprietary bits and pieces to the standard definitions. Whilst this approach has its advantages in that their implementation is customised for applications under Windows, it makes a mockery of international standards and also makes it difficult to transfer knowledge gained from other platforms.

8.3.1 WINS

The main enhancement Microsoft has added is WINS, the Windows Internet Naming Services. DNS servers are used on the internet to translate names to IP addresses and vice versa, and are absolutely essential as if you had to remember IP addresses of servers rather than URL's or names it would be a lot more difficult to use. They are so important it is wise to put multiple entries in if they are available.

As Windows computers have names which have nothing to do with their DNS names – look at the TCP/IP Identification tab for details, Microsoft figured that you should be able to use standard TCP/IP tools with these names as well as the DNS names. Without WINS, name resolution within a purely MS windows network is done by broadcasts – sending messages to every computer on the local network asking "Are you host xxx?" and waiting until a reply is received. This is both wasteful of bandwidth and time consuming, for a computer. What a WINS server does is provide a DNS type lookup and reference for these names, plus a centralised control for the administrator.

8.4 Bindings

Bindings are used when there is more than one network connector used in a computer such as a modem for internet connection and a network card for accessing other machines on a network. If the computer in question runs several services, such as a POP3 and SMTP email server for the network, then obviously this has to be running TCP/IP on both the network card and the Dial-Up adapter for the modem connection. Assume that the IPX protocol has to be installed for legacy applications, ranging from old versions of the Novell NetWare client software through to playing networked Doom, then both have to be installed. However, it is wasteful to have IPX running on the modem link, represented as the PPP adapter in the Networks control panel, because no dial up connection will use the combination. So, from the network control panel, the entry "Dial-Up adapter -> IPX/SPX Compatible protocol" can be safely deleted.

If the computer runs File and Printer Sharing for Microsoft networks to make available some of its disk shares to the network, then there is no point having that running on the Dial-Up adapter either, unless you want disk shares to be visible to the internet. Use the Bindings tab to make sure that it only runs on the network adapter. By default MS Windows binds every adapter to every protocol and service, but this is not often the best thing to do and it is worth spending time getting this section correct, if only to save bandwidth and close off potential security holes.

9. Protocols other than TCP/IP

Although at the moment the world revolves around TCP/IP and all others can be forgotten in the context of the internet, other protocols such as IPX/SPX for NetWare and NetBIOS are widely used, and can't be forgotten in terms of general networking. NetBIOS is a simple broadcast type system as per Windows networking without the WINS server as all that is configured is the name of the machine and any resources on it. NetBIOS's main disadvantage is that it doesn't route at all, so it won't work on a system of any size. IPX is another common protocol. It is very easy to configure because it just needs to be installed, the computer given a name, bound to the network card and client and forgotten about. Like TCP/IP, IPX (IP with Extensions) is a routable protocol that can cope with huge numbers of machines but needs only one configuration parameter (called the Frame Type) unlike TCP/IP which has seemingly hundreds.

References

Microsoft Windows NT 4.0 Workstation Resource Kit, Microsoft Press, 1996.

Running Linux 1st edn. by Matt Welsh and Lar Kaufman, O'Reilly and Associates, 1995.

Revision History

1.0: 16-18 March 2001. Original version

1.1: 24 March 2001. Added section 1.1 on TTL and 1.2 on the Default router. Added items to section 3 to cover the fact that not all ports are in use on any machine. Added section 6.10 on web administration tools.

1.2: 15 April 2001. Rewrote certain sections to remove information specific to the setup of its original recipient and to remove assumptions about any prior knowledge of TCP/IP.

1.3: 1 June 2001. Rewrote section on Subnet masks. A few minor bug corrections elsewhere.

Glossary

Note that not all of this information is described above.

Bandwidth
The 'size' of a network connection, which determines the maximum amount of data that can be transmitted or received at any one point in time.

Binding
A connection between a protocol and an adapter, whether it be a network card or a modem. Bindings in Windows are managed through the Network control panel.

BOOTP: Bootstrap Protocol.
An old way of configuring remotely certain IP address settings. Now superseded by DHCP in all but the most specialised of circumstances.

Class A IP address
IP addresses with the first octet between 1 and 126.

Class B IP address
IP addresses with the first octet between 128 and 191.

Class C IP address
IP addresses with the first octet between 192 and 223.

Clustering
The act of having multiple servers configured so that they are treated as one for the purposes of administration and management.

Cybercafé
A café that provides access to the internet in addition to providing food/drinks for sale and consumption on the premises.

Daemon
The term for a background process on a Unix/Linux type system.

DHCP: Dynamic Host Configuration Protocol.
The most up to date way of having centralised control and administration of IP configuration information.

Default gateway
The default IP address to which traffic not on the current network is sent.

Default router
See Default gateway.

Dial-Up access
Access to the internet, typically for home or small business users provided by dialling up an ISP using a modem.

DNS
The Domain Name System. Used for translating names to IP addresses and vice versa and is an essential part of any TCP/IP network.

Domain
In the Internet/DNS meaning of the word, in the URL www.mywebsite.co.uk, mywebsite.co.uk is the domain. They are hierarchically allocated by the named administrators, so the mywebsite.co.uk is assigned by the owner of .co.uk, and co.uk is assigned by the owner of .uk.

Dynamic Host Configuration Protocol: See DHCP

Finger

A program for obtaining information about specific users on a host.

Firewall
A piece of software or dedicated hardware used to prohibit access to certain port/host combinations.

ftp: File Transfer Protocol
A way of transferring files between hosts on a TCP/IP network.

Host
Any device on the internet.

Host ID
The part of the IP address that identifies the specific host on the network.

Intranet
Use of internet protocols and software within a company/organisation for its own private use.

IP
Internet Protocol – the part of TCP/IP that provides for data transfer between hosts.

IP Address
The address(es) assigned to a particular host to allow it to communicate on a TCP/IP network. They are in the form of a dotted quad aaa.bbb.ccc.ddd where each number is between 0 and 255.

IRC: Internet Relay Chat
A way of communicating in real time with multiple people across a TCP/IP network.

ISP: Internet Service Provider
A company that provides access to the internet for its customers.

Linuxconf
A piece of software for the Linux operating system used to make administration easier. It has a built in web server interface.

Load balancing
The process of having multiple servers host the same resources and the load shared between them, invisibly to the end user.

Loopback IP address
The IP address 127.0.0.1 with DNS name “localhost,” used to access resources on the local computer without using network bandwidth.

Modem
A device used to connect a computer to a telephone line, and convert the digital signals used in the computer to the analogue ones used by a telephone system and vice versa.

Multi homed system
A device with more than one network adaptor and thus IP address. It may be possible to act as a router if the server software allows it.

Multicast IP addresses
The IP addresses above 224.0.0.0 used for sending data to multiple hosts at once.

NAT: Network Address Translation
A piece of software in a firewall or proxy server that can translate invalid or private ranges of IP addresses to valid ones as data packets flow through it.

Network ID
The part of the IP address that determines the maximum number of hosts which can connect to it.

Network Address Translation
See NAT.

NLM (Netware Loadable Module)
A background process or foreground program for running on Novell's Netware operating system.

NSLOOKUP
A program on Windows NT or Windows 2000, used for querying the DNS system. Short for Name Service Lookup.

Packet
An item of data for transmission in a network, together with the destination and other information such as its TTL figure.

Ping
A program used to determine if a specific host is currently accessible.

Private IP address
An IP address in the range of 10.x.x.x, 172.16.x.x or 192.168.x.x which will not route by default.

Port
A logical number between 0 and 65535 used to differentiate between connections to services running on the same host.

Port scanner
A piece of software that will access a range of ports on a host or network to determine if any security vulnerabilities exist.

Postmaster
A person or team of people in charge of an email server.

Proxy server
A server that connects to a service on behalf of another server.

Round Robin
A way of implementing load balancing, by having the DNS distribute different IP addresses for a site as different requests for it come in.

Router
A device used for connecting two networks together.

Service
Microsoft's name for a background process running on a Windows 95/98/NT/2000/Me computer.

ShieldsUp
A web based port scanner provided by Gibson Research Corporation located at the http://grc.com/ web site.

Subnet mask.
Used to determine the size of the network ID from the host ID by ANDing it with the IP address.

SMTP
Simple Mail Transfer Protocol. One protocol running on top of TCP/IP used to deliver email between servers.

SSL (Secure Sockets Layer)
A way of encrypting data, often used in e-commerce, to encrypt data transmission between hosts on the internet.

TCP: Transmission Control Protocol.
The part of TCP/IP that ensures data transmission is reliable – i.e. successful receipt of packets are acknowledged.

TCP/IP: Transmission Control Protocol/Internet Protocol.
The suite of protocols invented in the 1970's used on the internet and most computer systems available today.

Telnet
A protocol running on TCP/IP that allows remote access to a system console. Is often used to host remote administration systems for network attached devices such as storage arrays, print servers, routers etc.

Tftp: Trivial FTP.
A simplified version of the FTP protocol in which many functions have been removed. TFTP is mostly used for remote configuration.

Time to live
A setting in an IP packet used to determine the maximum life of a packet in milliseconds.

TLD: Top Level Domain
A domain without anything after it in the address, such as com, edu or uk.

Traceroute
A program used to find out the route between the current host and another. Syntax is tracert <hostname> or tracert <ip address>.

Trivial ftp: See TFTP

TTL: See Time To Live.

Web server:
A program used to accept connections to port 80 on a system and return web pages (HTML). This may be a daemon, an NLM or a service depending upon the host operating system.

Webmaster:
A person or team of people responsible for the maintenance and administration of a web site. Usually has an email address of webmaster@domain.

Whois
A process used for finding out the owner of a particular internet domain.

Win32
Generic term to refer to all 32 bit operating systems by Microsoft in the Windows family. It currently consists of Windows 95, 98, NT, 2000 and Me. Soon it will be extended to include the forthcoming Windows XP.

WINS (Windows Internet Naming Service).
The Windows Internet Naming Service. Microsoft's enhancement to TCP/IP to allow it to provide a centralised name lookup of hosts on a Windows network.