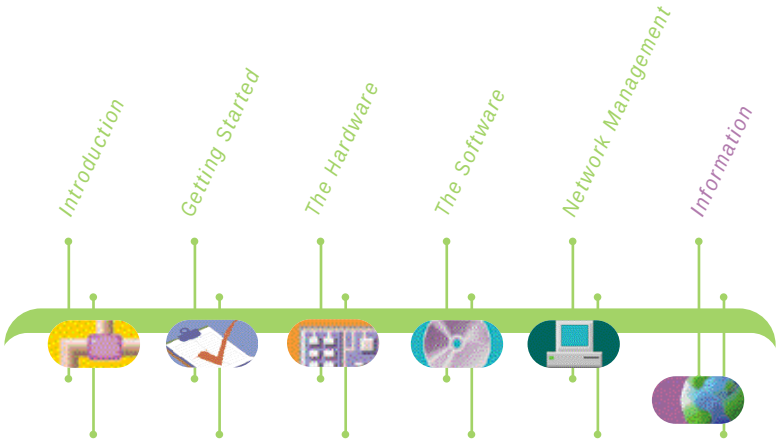


Information

Bigger and faster

FOR THOSE INTERESTED IN the greater networking model at large, the following information will cover the hardware and methods that make up the big networks of the world. Chances are you won't be dealing with any of this, but it's interesting to know exactly how networks such as the Internet are constructed.

Bridges, switches and routers

There are limitations to the size of a network before you need extra hardware. A 10Base2 segment can only be 185m long, and can only accommodate 30 computers. For many applications, this is fine, so you can get away with a network card costing $40 or less in each machine and a few $10 cables. But 185m can be used up surprisingly quickly in standard 'into the wall and up through the ceiling' cable installations.

If you need more length, a repeater lets you join 10Base2 segments together. The Ethernet spec allows for up to four repeaters in a network — which, for the mathematically disinclined, means five segments — but only three of these segments can be 'populated' (have computers connected to them). Therefore the maximum 10Base2 cable length using repeaters is 925m, 555m of which can be used for up to 90 computers.

This rule applies to 10BaseT as well, because every 10BaseT hub acts as a repeater. This can result in rather complex layout diagrams, but the basic rule is easy to remember: the path between any two computers must not include more than four repeaters or hubs, or more than three populated cable segments.

Having 90 computers connected a Ethernet, though, is not a good ea unless each of them doesn't se the network much. Ten megabits per second between 90 machines, all trying to move data at once, would give each computer a theoretical maxium bandwidth of about 14K per econd. Since there'd be collisions galore from all that simultaneous chatter, the real bandwidth would be much lower, and the network would grind to a halt.

To cut down the chatter you to either increase the total shareable bandwidth by switching to 100Mbit Fast Ethernet (which won't actually help all that much; the network will probably still be painfully slow), or chop the network up into smaller segments, so that traffic only escapes a segment when it's actually addressed to a computer on the outside. Dividing your LAN up like this is called 'internetworking'. It allows big networks to be both faster and physically larger, as it overcomes the maximum cable run problems.

To get around the maximum number of repeaters problem, you can use bridges, which can be either a standalone device or an appropriately configured computer with two network cards. Bridges are more expensive than repeaters, but they allow you to extend your network without breaking the rules. They intelligently filter and forward data based on the machine it's intended for. The bridge knows which machine addresses are on each side of it, and blocks the passage of traffic addressed to a section of network which does not contain the intended recipient of the data. When calculating legal routes, you can reset your repeater count to zero if the data path goes through a bridge.

The Ethernet specification does not allow more than seven bridges on a network. Bridges traditionally have only two ports, but they can have more, and so can connect to more than two network segments. By using multi-port bridges, you can have the maximum number of computers permitted on an Ethernet network, which is 1,024.

Bridges can even solve problems as a result of being connected in loops. If left uncorrected, a loop would cause instant and hopeless congestion as every bridge retransmitted everything it received to every other bridge in the loop, and then got it retransmitted back, ad infinitum. The bridges deal with this by arranging themselves into a 'spanning tree'; they very quickly shut down connections between bridges until all of the loops are eliminated. This allows redundant network wiring; if one cable is cut, the bridges sort out the problem and create a new tree using a previously ignored cable.

Routers are like bridges, only more functional. They do the same data filtering, but can also connect completely different networks to each other, allowing, for example, an office network to be connected to the Internet. With the use of routers, there's no practical limit to the number of machines you can network.

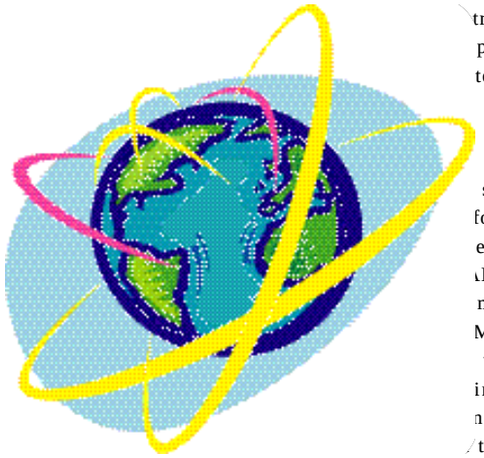
Switches are harder to define. In fact, these days there are all sorts of devices designed to move data from one network to another, with many advanced features, and their names are a highly unreliable guide to what the device actually does.

An expandable switch, with 16 10BaseT/100BaseT ports installed.

A switch is essentially a really intelligent hub; or, in its simplest form, maybe just a multi-port bridge. Essentially, switches are a creation of marketing departments; there may be some differences between them and previous devices under the surface, but from an operational point of view they're the same as earlier bridges and routers, only faster.

All bridges and many switches can only connect networks which could connect anyway — through a hub, in the case of 10/100BaseT, or just by hooking them together, in the case of 10Base2.

They allow you to connect more computers than you would otherwise be able to, and they let you make better use of the speed of your network by cutting chatter. All of the computers still have to be set up as if they were on the same network — same protocols, same subnet for TCP/IP, and so on.



Some switches (referred to as 'Layer 3 switches') and all routers, however, can overcome this. They connect networks together, like a bridge, but are a great deal smarter.

Routers and Layer 3 switches analyse incoming data and modify it, if necessary, so it's redirected to another router or to its initially intended destination. This allows routers to send packets from one kind of network across another kind of network on their way to a destination network, which can be yet another type, via more routers if necessary. As long as the routers know what computers live where, they can figure out the necessary route themselves.

Full-blown routers are distinguished by their ability to maintain a database of other router addresses, allowing them to manage transfer of data around very large and plex networks — most notably, the ternet. Each router, essentially, knows enough to get the data one step closer to where it has to go and hand it off to another router. Some Layer 3 switches can do this, and should therefore really be called routers; others are esigned to work only with ordinary ANs and smaller WANs, which makes m cheaper.

Many routers and fancier switches are used for Media Access conversions — ing networks with different physical nections as well as different protocols, token ring and Ethernet for example.

How to make networks faster

A NETWORK'S BANDWIDTH REPRESENTS how much data it can move per second. In a plain 10Mbit Ethernet LAN, that bandwidth is 10Mbps, or just over 1M per second. The actual amount of real data throughput is considerably lower, because a lot of bandwidth is taken up by the extra formatting information tacked onto the data to be sent. But if you just look at the bits being sent, the total number per second — assuming no collisions — is 10 million.

Things become more complicated when you start playing with bridges and switches on larger networks. Both of these devices, after a brief learning period, forward traffic only to network segments that actually contain the computer to which the traffic is addressed. Depending on the network, you may get a larger performance gain from segmenting a 10Mbit network than from upgrading it to 100Mbit.

If you have a 10BaseT network with, say, 32 computers, you could add an eight-port bridge or switch with a four-port hub hanging off each port. This chops the network into eight segments of four computers each, which means that each computer can yammer all it likes to its three segment companions without cutting into the 10Mbit bandwidth of any of the other segments. If a given computer does talk to a machine on a different segment, it will only take up bandwidth on those two segments, leaving half of the network untouched.

Segmented networks can therefore offer impressive 'aggregate bandwidth' — the total amount of data that can be moved around the network by various machines talking to each other at once. High aggregate bandwidth does not, in this case, indicate higher bandwidth available to any one network conversation. But this is usually OK, as for most operations the transfer rate provided by a 10Mbit network is adequate, provided you can get most or all of it for yourself.

If two machines conduct a 10Mbit conversation between two ports on the bridge or switch that segments this 32-computer network, and another two conduct a similar conversation on each of the other three pairs of ports, the network will be saturated (any extra traffic will produce collisions and slow the LAN down) and an aggregate bandwidth of only 40Mbps will have been achieved.

On the other hand, if computers on the network happen to only talk to other computers on their own segment, the lack of inter-segment network pollution means the aggregate bandwidth available will be 80Mbps. The worst case scenario arises if three segments all want to talk to the fourth at once; in this situation they have to share the fourth segment's bandwidth, and the network's aggregate bandwidth drops back to 10Mbps.

In this case, an eight-segment 10Mbps network clearly offers significantly less bandwidth, under all circumstances, than an unsegmented 100Mbps LAN. But if you double the number of segments to 16, so each one serves only two computers, the aggregate bandwidth figures in the above

examples jump to 80 and 160 respectively, and the chance of everyone concentrating on one segment falls.

If there's one computer that commonly attracts lots of traffic — a file server, for instance — it can be given a segment to itself, and can even be given a 100BaseT network card and be connected to a 10/100MBps dual-mode switch. Switches are available with only one or two 100BaseT ports, the rest being 10BaseT, for exactly this purpose. This gives the high-demand computer a dedicated 100Mbit connection to the whole of the rest of the network, even though any given other computer can only move 10Mbps.

If the 31 other computers all try to access the file server now, they're sharing 100Mbps between them instead of 10, and will still receive data at a decent rate. Because bridges and switches prevent collisions between traffic originating on different network segments, if ten 10Mbps computers simultaneously request data from the 100Mbps server (and everything else happens to shut up), they'll each get data about as fast as their network cards can handle it, without a single collision.

They will, in fact, perform just as well in this situation as if they were networked to the server with 100BaseT all the way.

An important factor is the internal or 'backplane' bandwidth of your bridge or switch. To avoid causing bottleneck problems at moments of high network use, you need a backplane bandwidth equal to the aggregate bandwidth of all of a device's ports. If a bridge, switch or router has this much

backplane bandwidth, all of its ports can operate at full speed all of the time, and the 'data pipe' inside the device is wide enough to let all of the data through.

When there are no switches, bridges or routers to worry about, only repeaters (remember, a standard 10BaseT hub is a repeater), network performance is easy to work out. Everything shares. It isn't quite as simple as that, however; in a collision no data gets sent by anyone, so when the network is saturated the total useful throughput can be much less than the total bandwidth of the network — but at least it doesn't matter who's talking to whom. A given number of connections will result in a given aggregate bandwidth.

Now, if you haven't been sufficiently confused so far, you're well on your way to becoming a networking guru. For the most part you won't need to concern yourself with the complexities of large networks, but it's always handy to know just how they work and where your smaller network fits in with the big picture.

Technical glossary

AppleTalk: The networking protocol built into all Apple Macintosh computers and laser printers. Very simple to use — automatic, even — but not as fast for demanding applications as other protocols.

Bus: A kind of network topology. The bus configuration, as used by 10Base2, has all the devices on the network connected in parallel to one cable. This 'cable' is really made up of separate cable segments joined at the T-pieces, but electrically speaking it can be treated as one wire. Any computer can be disconnected from this bus without affecting connectivity for everything else, but if the cable is interrupted anywhere, the whole network goes down.

Category: Twisted pair cable such as that used by 10BaseT and 100BaseT is available in various specification levels or 'categories'. 100BaseT requires Category 5 cable, often referred to as 'Cat 5'. 10BaseT will work with lower grade, thinner cable, but a lot of installers use Cat 5 cable anyway because it costs little more and makes it easy to upgrade. Make sure the cable you use really is Category 5 cable, not just something labelled 'Category 5 quality'. Incidentally, all coaxial network cable can be referred to as 'Category 6', but since this makes no distinction between the different kinds used by 10Base2 and 10Base5, the term is seldom used. Fibre-optic cable is Category 7.

Client/server: The client/server network architecture defines every device on the net-

work as either a client or a server. Separate processes running on one computer can also be designated as clients or severs. Servers are typically powerful computers, or processes running on powerful computers, which handle data storage (file servers), printing (print servers) or network traffic (network servers). Clients are the computers which are used for whatever the network is actually set up to do, and get their resources from the servers. Client/server architectures are much less common today, because ordinary desktop computers have enough power to provide server functions on an ad-hoc basis for other computers or themselves. Large networks still need servers, though, to keep the operation of the network orderly and handle very demanding tasks. See also Peer-to-peer.

Collision: When two devices on a baseband network like Ethernet try to send data at the same time, they talk over each other and cause a collision. When a collision occurs, every device that's trying to send data pauses

for a brief, random period and tries again. This simple system works less and less well as more and more computers are added to a network, which is why segmenting big networks with bridges and/or switches is a good idea.

Datagram: See Packet.

Duplex: In computer communications there are three kinds of connection between two devices. The first is simplex, in which data can only flow one way. Half duplex is the system used by regular Ethernet; data can flow either way, but only one way at a time. Full duplex allows data flow in both directions at once. Ethernet supports full duplex operation, but only between two devices over twisted pair cables. Regular 10BaseT or 100BaseT cable has two physical pairs of wires in it, which in full duplex operation can be used for full bandwidth data transfer in both directions — one wire pair per direction. This works because when there are only two devices involved, collisions are impossible. The second wire pair is normally needed for collision detection. Full duplex doubles the aggregate bandwidth of a connection, but doesn't greatly increase performance unless both devices send a lot of data. Many network transactions involve a lot of data going one way and only a little going the other, so there isn't much performance difference.

Ethernet: The hugely popular system first promoted in 1980 which is now the de facto standard for most networks. The most popular versions of Ethernet are 10Base2 and 10BaseT, running at 10Mbps over coaxial and unshielded twisted pair cable respectively, and 100BaseT, running at 100Mbps over unshielded twisted pair.

Firewall: A hardware and/or software system that aims to prevent unauthorised traffic into or out of a private network. Firewall functions are often included in other products, such as software that allows computers on a TCP/IP LAN to access the Internet.

FTP: File Transfer Protocol, a protocol which allows one system (the client) to transfer files to and from another (the server) over a TCP/IP network. FTP servers are widely used on the Web for file downloads; URLs which point to a file on an FTP server start with 'ftp:'.

Heterogenous network: A network composed of computers and other network devices made by different manufacturers. A LAN with IBM-compatible computers and Apple Macintoshes on it, for example, is heterogenous.

Hub: A common connection point for network devices. In Ethernet parlance, a hub is a multi-port repeater.

HTTP: Short for HyperText Transfer Protocol, HTTP is the TCP/IP protocol used by the World Wide Web. HTTP covers message formatting and transmission standards, and also tells Web servers and browsers how to respond to different commands. Giving your browser a URL that starts with 'http:' tells it to send an HTTP request for that URL and display what it receives in return. There are different versions of HTTP; currently, most servers support HTTP v1.1, which allows a 'persistent connection', in which one connection can be made between a browser and a server and multiple files transferred, whereas with HTTP v1.0 a new connection has to be made for every file. See also S-HTTP.

IMAP: Internet Message Access Protocol, a protocol used for retrieving email messages from a server by a client (your email software). IMAP is a younger protocol than the more commonly used POP, and the current version (IMAP4) supports extended features like keyword searching email messages which are still on the server.

Intranet: A TCP/IP network accessible only by members of a particular organisation, usually a company. Intranets can have various Internet services hosted locally — Web servers, mail servers, FTP and so on. Intranets have the advantage that they can use the same cheap or free software that works on the Internet, rather than expensive and possibly inferior proprietary systems.

IP address: A unique identifying number for a node on a TCP/IP network. Every computer on the network must either have an IP address assigned to it by a server, or have a 'static' address manually entered. IP addresses contain four numbers separated by full stops, and each number can be from 0 to 255. See TCP/IP.

IPX: Internetwork Packet Exchange, a networking protocol used by the Novell NetWare operating systems.

ISP: Internet Service Provider, a company that provides Internet access to its customers via modems or other means. ISPs are occasionally referred to as Internet Access Providers (IAPs).

NetBEUI: Short for NetBIOS Enhanced User Interface, and pronounced 'net-booey'. An enhanced version of Novell's old NetBIOS protocol, and an excellent choice for small office networks.

Network Interface Card: Normally shortened to NIC, this is the technical term for what everyone simply calls a network card. The NIC is the board you put in your computer which connects the computer to a network. They are almost always made for a particular kind of network and media, although Ethernet cards commonly have connectors for 10Base2 and 10BaseT.

NNTP: Network News Transport Protocol, the protocol used for distributing, posting, receiving and acquiring information on Usenet newsgroup messages.

Node: The correct word for a processing location on a network. Things other than computers can be connected to networks — printers, traffic handling devices, and so on.

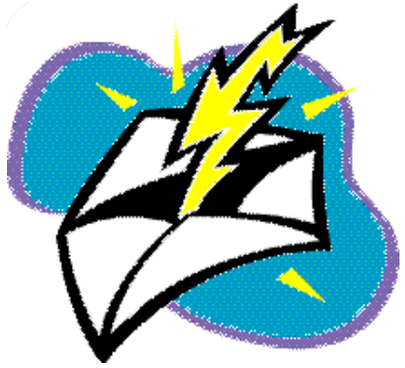
Packet:
A unit of data transmitted over a packet switching network. Packets contain a destination address in addition to their data, can travel by different paths to their destination and can also be assembled into a complete message when they've been received. On IP networks like the Internet, packets are often referred to as 'datagrams'.

Packet switching: A networking system in which messages are chopped up into packets before sending. If errors occur, only the packets that failed to arrive need to be re-sent, not the whole message. Packet switching allows networking hardware to be used very efficiently, as the extra bandwidth used by the packetisation of the data is offset by the reduced resends and absence of dedicated connections between points.

PC: Personal computer. In popular parlance, and for the purposes of this Pocketbook, PC is shorthand for 'IBM-compatible personal computer'. Although a Macintosh is also a personal computer, chances are when someone says PC they mean an IBM-compatible machine. On the other hand, if they actually use the phrase 'personal computer' instead of the acronym, they're probably using the more general definition.

Peer-to-peer: A network architecture in which every computer has broadly equal abilities and tasks. Most smaller networks are peer-to-peer, a system that works well because ordinary computers are now much more powerful than they used to be, and also because current operating systems make basic network administration quite simple. See also Client/server.

POP: In email parlance, POP stands for Post Office Protocol, a protocol commonly used to retrieve email from a mail server. The other common protocol for this purpose is IMAP. Two versions of POP are currently in common use — POP2 and POP3. Higher-numbered POP versions are not compatible with lower-numbered ones. POP can also stand for Point Of Presence, a location in which you can locally call an ISP or telephone company for a given service. An ISP with local Sydney, Melbourne and Brisbane



phone numbers can be said to have three Points Of Presence.

Port: In network-hardware parlance, a port is a socket to which a cable can be attached, as in 'a 12-port switch'. In network-software parlance, a port is the end of a logical connection in a TCP/IP or UDP network. Different services a computer can provide have different port numbers; for instance, port 80 is used for HTTP traffic. When one computer connects to another over the network, it specifies the port number with which it's trying to communicate to indicate what it's trying to do.

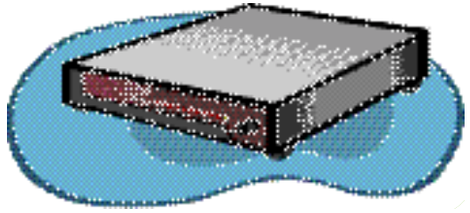
Repeater: A network appliance that takes data in one port, amplifies it and retransmits it from one or more other ports. Repeaters allow network cables to be longer, but do nothing to control network traffic.

S-HTTP: An extension to HTTP, not supported by all browsers or servers, which allows secure (encrypted) data transmission over the World Wide Web. S-HTTP allows HTTP messages to be exchanged securely, making it possible to use a Web site without your actions being easily comprehensible if intercepted by a third party. See also SSL.

SMB: Server Message Block, a message format that Microsoft operating systems use when sharing files, directories or devices. SMB is used by other systems to enable compatibility with Microsoft networks; Samba, for instance, lets Unix machines use SMB.

SMTP: Simple Mail Transfer Protocol, the usual protocol for sending email messages between servers, and also commonly used to send messages from the mail client (your email program) to the server. SMTP can operate over various network protocols, but it's usually used with TCP. Email is retrieved from the mail server by the client with the IMAP or POP protocols.

Sniffer: A program or device that monitors network traffic. Sniffers of various kinds are



used for management purposes on larger networks, to spot problems quickly and figure out how to optimise performance. Sniffers can also be used for illicit purposes; they are very difficult to detect. Sniffers on a TCP/IP network are referred to as 'packet sniffers'.

SSL: Secure Sockets Layer is an Internet security protocol originally developed by Netscape and supported by many browsers and Web servers. SSL uses a private key to encrypt transmitted data, creating an encrypted channel between the client and the server over which any amount of data can be transmitted. URLs which use SSL start with 'https:' instead of 'http:'. See also S-HTTP.

TCP/IP: This is short for Transmission Control Protocol/Internet Protocol, and consists of a collection of network protocols used by the Internet, more advanced networks and more recent network games. TCP/IP is capable of much more than simpler protocols like NetBEUI, but is more complex to set up.

Token Ring: If uncapitalised, token ring denotes any network with a ring topology which uses a circulating 'token' to regulate data transfer. When capitalised, it denotes IBM's implementation of the idea, which never achieved the popularity of Ethernet.

UDP: User Datagram Protocol, a collection of protocols which, like TCP, can be layered on top of the basic Internet Protocol (IP) to transport data. UDP is simple but unreliable — it provides no built-in error handling, unlike TCP.

URL: Uniform Resource Locator (originally Universal Resource Locator). The URL system is the de facto standard for indicating the location of something on the Internet, be it a file, a video stream or a newsgroup. URLs are most commonly encountered on the World Wide Web, and they take the form of a protocol name, a colon, and then some kind of address, as in http://www.server/com/webpage.html or mailto:foo@bar.net. URLs may include such things as an FTP server user name and password, or strings to be passed to a program (when using a search engine, for instance).

WAN: Wide Area Network. Any computer network that covers a large geographical area and is composed, typically, of more than one Local Area Network. A WAN can be composed of a multiplicity of network systems. The Internet is the biggest WAN in the world, both in geographical extent and number of nodes.

Web resources

WHEN YOU'RE IN NEED OF more infor or you're looking to download the late and tools, the following list should pro with a great place to start.

Windows

http://support.microsoft.com/suppor articles/q192/5/34.asp

Microsoft's Troubleshooting Windows 9 Network Connection Problems knowled base article. Microsoft troubleshooting guides are well known for failing to cover peculiar problems. Fortunately, most network problems *aren't* very peculiar, and this handy document will help you sort them out with the minimum amount of hair-pulling.

http://www.ezlinkusb.com

USB networking by itself isn't suitable for anything more than a very small LAN, because the adapters are both rather slower and considerably more expensive than ordinary 10Mbit Ethernet cards. It is, however, a great, simple way to connect a recent-model Windows PC to a network without opening the case.

http://www.diamondmm.com/homefree

Diamond Multimedia's wireless network system. Homefree was the first low-cost wireless networking solution, and remains the cheapest. Its performance is slow compared with plain 10Mbit Ethernet, and it doesn't deal too well with obstructions and distance, but you can't beat the price.

http://www.proxim.com

Symphony, Proxim's wireless network system. Proxim's wireless networking system is more expensive than Diamond's Homefree, and isn't any faster, but it works more reliably in real world situations where running cables isn't possible.

http://www.miramarsys.com/index.htm

PC MACLAN, from Miramar Systems. Connect Windows 95/98 computers to an AppleTalk network via a LAN, a modem or even the Internet. Shared files and printers are accessible from both Windows to Mac and Mac to Windows, and for plain LAN applications you don't need to do a thing to the Macs on the network.

http://client235.subnet62.depauw.edu/dfsoft/html/server_watch.html
Server Watch: notifies you when one of several multiplayer games is launched on your network. If you're a system administrator who wants to keep an eye on the frivolous activities of people on your Windows network, this program will let you know when someone's goofing off. It's also handy, of course, if you just want to join in!

http://www.wingate.com
WinGate proxy: The most popular Windows proxy server software, for sharing one Internet connection among many networked computers.

http://www.sygate.com
SyGate proxy: More recent, more features and arguably better than WinGate, SyGate is gaining fast in the Windows Net-connection-sharing market.

http://www.pscs.co.uk/software/vpop3.html
A VPOP3 Windows mail server — full-featured, easy to configure Windows mail server package, for proper Internet mail serving on your network, whether it's connected to the Internet or not.

http://www.vservers.com
Virtual Servers: front-running Web hosting company. The Web hosting market is crowded with low-cost options, but Virtual Servers is easy to work with and contains comprehensive online help and support services. It also has a long track record of reliability, which makes it less likely that your site will mysteriously disappear.

http://www.microsoft.com/msdownload/downlabc.htm
Complete list of Microsoft free patches and upgrades. Forget cryptic searches and fishing through the forest of links in the Microsoft maze. This is allegedly a comprehensive list of the company's downloadable patches and upgrades. If the one you need isn't here, you're on your own.

http://www.microsoft.com/ntserver/nts/exec/vendors/freeshare/Mail.asp
http://www.microsoft.com/ntserver/nts/exec/vendors/freeshare/Web.asp
Microsoft's list of downloadable freeware, shareware and demo Windows NT mail and Web servers. Want to find a cheap or free NT mail or Web server? Here's the source. If you've already shelled out for NT, you probably feel you've done enough spending for the time being.

http://www.winfiles.com/apps/98/servers-mail.html
WinFiles.com's list of Windows 95/98 mail server software.

http://www.emailman.com/win/servers.html
EMailman's list of Windows 95/98 mail server software.

Mac

http://www.dartmouth.edu/netsoftware
Dartmouth College: home of MacPing, InterMapper and other useful networking software. Some items are free or shareware, others are commercially licensed.

http://www.experts-exchange.com/comp/mac/networks
The Experts Exchange Mac networking Q&A area. The Experts Exchange 'self-help' model is basically that users trade points for information on message boards. Answering questions earns you points, which can be used to view answers to other questions. Even if you don't provide any answers, you can ask a limited number of questions each month. An excellent resource for those new to networking.

http://www.macsimise.com.au
Macsimise: Australian distributor of network hardware from companies including COPSTalk, Sonnet and Sonic. Online catalogue includes recommended retail prices.

http://www.macwindows.com
Macwindows is a leading site for useful information and news concerning Mac-Windows interworking.

http://www.miramarsys.com
Miramar Systems: developer of PC MACLAN, which allows Windows clients to participate in an AppleTalk network.

http://www.neon.com
Neon Software: home of OTTool, LANSurveyor and other network utilities. Click the Demos link at the foot of the home page for the downloadable demos and free items.

http://www.sustworks.com
Softworks: home of IPNetRouter, a low-cost IP router (Internet gateway), and other network utilities.

http://www.sonicsys.com
Sonic Systems: manufacturer of network hardware and software. Distributed in Australia by Macsimise (see above).

http://www.stairways.com
Stairways Software: home of the NetPresenz Web server, the RumorMill news server and other highly-regarded Mac network programs and utilities such as Mac TCP Watcher.

http://www.stalker.com
Stalker: developer of the Communigate integrated messaging system and the Stalker Internet Mail Server.

http://www.starnine.com
StarNine home page. WebSTAR is one of the leading Web servers for Mac OS.

http://www.streetwise.net.au
Streetwise Software: local supplier of Thursby's DAVE (see below).

http://www.tandb.com.au/internet
T&B Brodhurst-Hillm: some useful material on setting up Mac-based intranets and Internet connections, especially on Internet routing.

http://www.tenon.com
Tenon Intersystems: developer of WebTen, a Web server with "unmatched features and unmatched performance", according to the company.

http://3macs.nowonder.com/network/index.html
Three Macs and a Printer: a useful guide to setting up small Mac networks.

http://www.thursby.com
Thursby Software Systems: developer of DAVE, which lets a Macintosh participate in Windows-style networks. COPSTalk has also recently been acquired by Thursby from COPS, and can also be found here.

http://www.vicomsoft.com
Vicomsoft: developer of Macintosh and Windows Internet gateways (including Web caching), remote access servers and other software.

Linux

http://cesdis.gsfc.nasa.gov/linux/drivers
The Linux Ethernet Card Drivers site is the primary site for information on and updates to the Linux Ethernet device drivers. Linux has driver support for all mass-market PCI Ethernet chips and this site is the place to go if you find your NIC isn't supported out of the box by your Linux distribution.

http://mirror.aarnet.edu.au/linux/sunsite/docs/HOWTO
This HOWTO archive contains all the HOWTOs you need for networking, including the Ethernet, NET-3, Network-Overview and IP Masquerading HOWTOs. These are excellent, easy-to-follow step-by-step guides to Linux networking.

http://www.loonie.net/~eschenk/diald.html
The Diald site has extensive information on Diald, the PPP Dial-on-Demand daemon. Diald allows you to configure Linux to bring up a PPP connection on demand and bring it down when not in use, completely and seamlessly automating PPP access for users accessing the Internet through a PPP connection.

http://ethereal.zing.org
Ethereal is a network protocol analyzer for Unix. You can examine data from a live network, or from a capture file on disk. One of the goals of the project is to have an application that is similar in functionality to Network Associates' NetXRay or the AG Group's EtherPeek. Although these are both excellent products, neither of them runs under Unix.

http://www.tuxedo.org/~esr/fetchmail
Fetchmail is a full-featured, robust, well-documented remote-mail retrieval and forwarding utility intended to be used over on-demand TCP/IP links (such as SLIP or PPP connections). It supports every remote-mail protocol now in use on the Internet: POP2, POP3, RPOP, APOP, KPOP, all flavors of IMAP, and ESMTP ETRN. It can even support IPv6 and IPSEC.

ftp://prep.ai.mit.edu/pub/gnu/wget
GNU Wget automatically retrieves files via HTTP or FTP. A very handy tool for automating downloads.

http://www.uk.research.att.com/vnc/index.html
Virtual Network Computing: in essence, this is a remote display system which enables you to view a computing 'desktop' environment not only on the machine on which it is

running, but from anywhere on the Internet as well as from a wide variety of machine architectures.

http://www.newwave.net/~masneyb
The gFTP homepage. gFTP is a free multithreaded FTP client for *NIX based machines running X11R6 or later. It uses a GTK front end and provides features such as resuming interrupted transfers and drag and drop downloading.

http://www.apache.org
The Apache home page. Apache is the world's most popular Web server, and is the driving force behind Web serving on the Internet.

http://www.samba.org.au/samba
The Samba home page. Samba provides Windows SMB services for Linux, and is said to outperform Windows NT for file and print serving.

http://www.freshmeat.net
Freshmeat is the central source for new Linux files. If you want to see what's new in Linux development, or you're looking for a particular application, Freshmeat will have it.

The Pocketbook CD

THE POCKETBOOK CD CONTAINS a large selection of server and client software for Windows, Mac and Linux. You'll also find fix packs for Windows NT and Mac OS as well as other handy programs such as chat tools and browsers. If you're using Windows, simply insert the CD into your CD-ROM and it will load the default page automatically. If you're using Mac or Linux, simply open the file 'DEFAULT.HTM' in the root of the CD using your favourite browser.

Highlights of the CD include:

Windows

FTP tools	WS_FTP LE 4.60, NetLoad 3.8d, CuteFTP 3.0b15
Telnet	CRT, J-Term PRO 1.1.3, NetTerm 4.2a
Ping and analysis tools	Ping Plotter 2.03, TJPing Pro 1.2.1
DNS lookup	CyberKit 2.4a, NIC-O'matic 1.71
File sharing	ICE.NFS 1.5.2, ZanNet 1.0
Log analysers	WebTrends 4.5, FastStats 2.52
FTP servers	WAR FTP Daemon 1.7, FTP Serv-U 2.5
Web servers	Sambar Server 4.2,Xitami 2.4c3
Mail servers	FTGate 2.1.2.1, Mdaemon 2.75
Chat servers	IRCPlus 1.1, WircSrv 5.07
Miscellaneous servers	CU-SeeMe, WebBoard 3.0

Mac

FTP tools	Anarchie Pro, Transmit
Telnet	BetterTelnet, dataComet
Ping and analysis tools	MacPing
Chat tools	Ircle
FTP servers	Hotline FTP Server 1.0, NetPresenz 4.1
Web servers	Quid Pro Quo 2.1.2, EasyServe
Mail servers	Eudora Intrernet Mail Server 2.2
Chat servers	HotLine Server (PPC) 1.2.3

Linux

FTP tools	gFTP
FTP servers	glFTPd 1.16, Pro FTPd 1.2.0, WU-FTPD 2.4.2

Web servers	Apache, Xitami 2.4c3, thttpd 2.04
Mail servers	VxMail 1.39, IMAP Server 4.5
Chat servers	IRCd 2.1, Naken Chat 1.03
SMB servers	Samba 2.03
Miscellaneous servers	Dnews 5.0, INN

Disclaimer

All software and documentation on the cover CD is provided as is, with no explicit or implied warranties. *APC* cannot be held liable for any damage that may occur as a result of using the software or documentation provided. Further, *APC* cannot provide technical support for the software products contained on the CD. *APC* will, however, replace faulty CDs. Just send the faulty CD to Level 8, 54 Park St, Sydney NSW 2000, include a return name and address, and we'll send out a replacement CD.

The Networking Pocketbook

If you have any criticisms or comments about the Networking Pocketbook, feel free to email the Pocketbook team at pocketbooks@acp.com.au. If you have any suggestions for future Pocketbooks, such as a specific topic you'd like to see covered, email us at the address above and tell us what you have in mind.