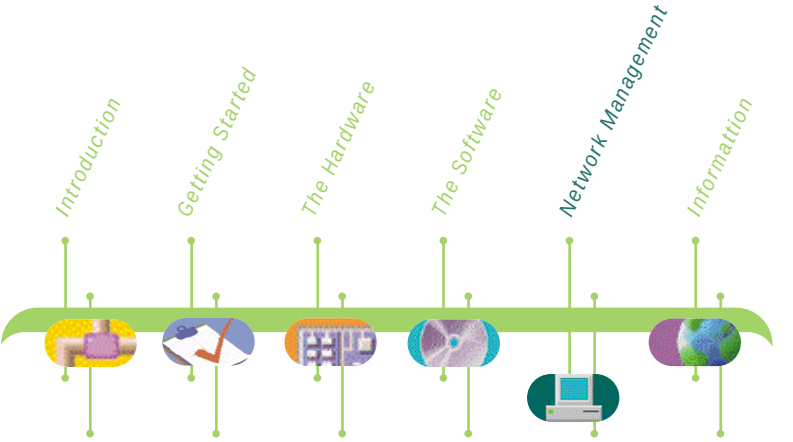

Introduction
Getting Started
The Hardware
The Software
Network Management
Informattion

Windows file sharing

Windows to Windows

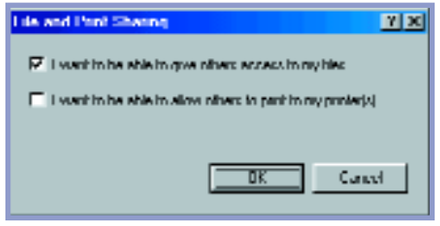
Basic drive or directory sharing in Windows 95 or Windows 98 is very simple, once you have networking installed and you're using the same protocol as everyone else on the LAN.

ONE

Go to Network Properties, double-click Network on the Control Panel, or right-click Network Neighborhood and select Properties.

TWO

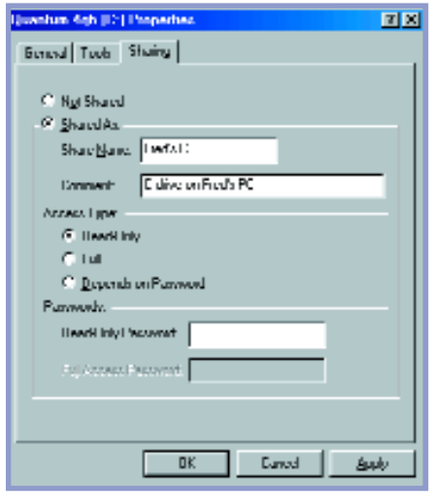
Click the 'File and Print Sharing' button, then select the first option, and the second if you also want to share your printer. You'll be able to share your drives after you reboot.



THREE

Right-click the file or the folder that you want to share and then select the Sharing option.

You can choose how this drive or folder will appear to others on the network, and grant different levels of access. You can even specify passwords for read-only and full access.



FOUR

If you put '$' at the end of your Share Name, you'll make it a 'hidden resource', which can only be accessed over the network if you know its name. To do this, you have to right-click Network Neighborhood and select 'Map Network Drive', then type the drive's full path in as shown:

Note the double-backslash before the name of the computer the drive is on.

Now the drive will appear as drive X; the 'reconnect at logon' option will automatically re-map it whenever you restart Windows.

FIVE

If a drive *isn't* hidden, it's much easier to map. Any drives on a remote machine viewed from Network Neighborhood can be right-clicked and will have their own 'Map Network Drive' option, which works the same way but saves the typing.

NT specifics

Sharing drives in Windows NT is more complex. NT has 'user permissions' — levels of access that can be allocated flexibly to various users, who can be grouped in different ways. This is dealt with in more detail in the Software chapter.

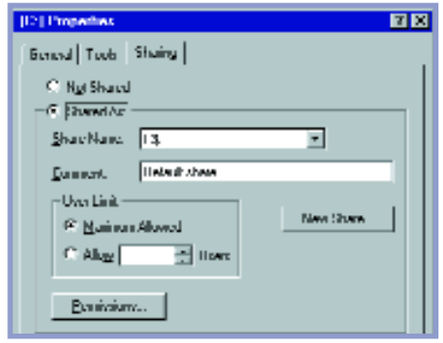
ONE

To change the drive sharing settings you need to be logged on as an Administrator or have administrator-level permissions.

By default, all of the drives on an NT machine with networking set up properly will have the drive-in-the-hand icon Windows 95/98 uses to indicate a shared drive; this icon indicates the standard Administrator-level share access. These drives are not actually accessible over the network, yet.

TWO

If you right-click a drive and select 'Sharing' you'll see a window like this:



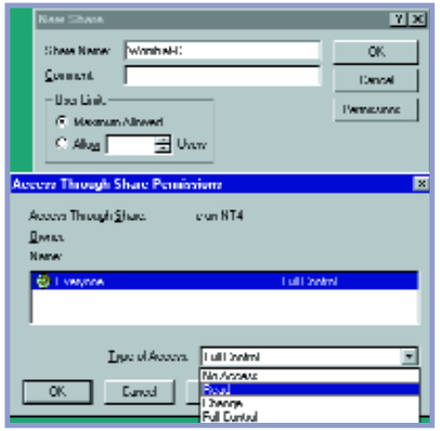
The dollar sign at the end of the Share Name makes this drive invisible to the network. You'll need to create a 'New Share' to make the drive remotely accessible. Do not attempt to remove the standard Administrator Shares.

THREE

By default, NT sets up new Shares so everyone who can log on to the computer has read access to the Share. You can set this basic permission or you can define individual users. Select Add to see a list of all of the computer's defined groups.

The Show Users button adds individual users to the list. Select the group or user whose access you want to define and make a choice from the Type of Access drop-down menu.

Full Control lets the user do all file operations; Change allows users to modify existing files, but they can't add or delete files; Read grants read-only access. Press the Add button to make the change.



FOUR

For a Windows 95/98 user to access shared drives on an NT computer, they have to be defined as a User on the NT computer (again, check the Software chapter for instructions). They also have to log on to 95/98 with the user name and password defined on the NT machine.

If the user name/password combination isn't defined on the NT machine they won't be able to log on, unless the NT machine has the Guest account enabled (also covered in the Software chapter). If it does, an incorrect logon will automatically grant Guest access.

Windows to Macintosh

Apple Macintosh networks generally use either the AppleTalk protocol or TCP/IP. In either instance, Windows NT Server can talk directly to Macs by installing its Services for Macintosh. Windows 95/Windows 98 to Macintosh connections require extra software installed on the Windows boxes or on the Macs.

PC MACLAN, from Miramar Systems (http://www.miramarsys.com/), lets you connect Windows 95/98 machines to AppleTalk via a LAN, a modem or even the Internet. Shared files and printers are accessible both ways, from Windows to Mac and Mac to Windows.

The Macs need to be running AppleShare IP 5.0 or an Apple Remote Access (ARA) 3.0-compatible PPP remote access host for direct modem connections in order to share resources over the Internet, but they don't need any special reconfiguration for plain LAN applications.

Windows to Linux

Linux is capable of using Microsoft's own Server Message Block (SMB) protocol that Windows uses to handle its file and print sharing over networks. As a result, a Linux machine will appear as just another Windows box with shareable and accessible resources.

Accessing these resources is performed in exactly the same way as you would access shared resources on a Windows machine.

From the Windows side you don't have to do anything to access a Linux machine. Configuring a Linux machine to use the SMB protocol is covered later on in this chapter under the Linux section on page 102.

Windows Web serving

IF YOU WANT TO MAKE a local intranet Web site which is accessible to other machines on your LAN, you don't need special server software. If you put your HTML pages in a shared directory or drive, anybody on the network can open the files in their Web browser. They can use the site as if it were on the Internet, only, probably, much faster.

If you actually want people to be able to have HyperText Transfer Protocol (HTTP, the standard World Wide Web protocol) access to your locally stored site, though, you'll need to install Web server software. This software enables a computer to deal with HTTP and File Transfer Protocol (FTP) requests, whether they come from the local network or the Internet. The computer must have a static IP address, which your Internet Service Provider can assign for a fee, if you want a domain name (for example your-company.com, yourgroup.org).

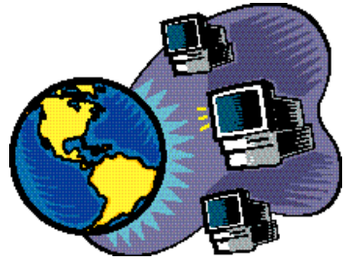
Web serving is an inherent feature of Windows NT Server and Linux, but needs to be added to Windows 95/98. If you're seriously thinking of hosting a real company Web page from your LAN, though, think again. There are better ways to do it.

Web servers are some of the most powerful computers in business use today. They have to be, because even if most of their visitors are only on small modem links, all of those couple-of-kilobyte-per-second connections add up very quickly.

For this reason, running any sort of serious Web server yourself is not a good idea for a small business. For proper Web serving, you'll need a fast, permanent connection to the Internet — a modem, or even several modems, will not be nearly fast enough for more than a couple of people to view the site at once. The computer also needs to be switched on all the time. It is also not a good idea if you're running Windows 95 or 98.

Windows 95/98 is slow, which means you'll need a fairly expensive PC for the Web server even if the only people logging on are your three sales staff. Windows 95 and 98 are also unstable; your site may be down more than it's up. If you're going to do local Web serving, Windows NT Server can handle it, but it is expensive, slow and not overly stable. Macintoshes are reasonably unlikely to crash, but aren't designed as high-load Web appliances. Linux is a much better bet; cheaper hardware and free operating system and software. But you still have to pay for the connection.

A cost-effective alternative is to pay somebody else to host the site for you; they take care of the expensive Net connection, redundant servers and automatic backups, and so on. There are lots of companies that



do this; a good place to start is Virtual Servers (www.vservers.com). Local site hosting really isn't practical when you consider that fast, reliable remote hosting costs from well under $100 a month — which is a great deal less than what you'd pay just for the *connection* if you did it yourself.

This doesn't mean that ordinary Web server software, even for Windows 95/98, is useless. For a start, running a Web server is an effective if somewhat roundabout way of moving files between dissimilar systems on a LAN.

If the server supports File Transfer Protocol (FTP) and all the machines have TCP/IP installed, you can use any FTP client program to copy files from, say, a Macintosh to a Windows 98 machine, even though neither of those computers is aware of the other's shared drives.

If all you need to do is shift the occasional file from place to place, this does the job. If you don't want to install FTP server software on every machine that needs to receive the files, you can use just one machine as a 'drop box', and have other computers FTPing files to and from it.

For undemanding purposes, Microsoft's Personal Web Server for Windows 95/98 does the job fairly well. It has the considerable advantage of being bundled with Microsoft products such as its site authoring package Frontpage.

You'll need to have TCP/IP installed — which you probably already have, courtesy of Dial-Up Networking. Personal Web Server will show up in your Network Properties and as a Control Panel item. Once it's been told where to put files, your computer will be accessible via HTTP and, optionally, FTP as well; http://[your IP address] will bring up the Personal Web Server administration pages and let you set everything up.

Your new Web server will be accessible locally on your LAN from the Internet by anybody that knows your IP address. With an ordinary dialup connection, your IP address changes every time you connect. This makes hosting a site on your machine impractical.

Many ISPs allow you a moderate-sized home page on their servers, which is much more sensible. It's somewhat slower to update a remote Web site (you should modify a local copy and then upload it when your changes are complete), but that's the only real disadvantage.

Modem sharing

The easiest way to set up modem sharing under Windows is to use software such as the popular products WinGate and SyGate. These programs allow you to share the Internet connection of a PC quickly and easily and automatically handle forwarding and retrieving packets coming from client machines without any additional configuration.

All you need to do for the client machines to gain access to the Internet is set the server machine as a gateway in TCP/IP properties and configure the DNS settings accordingly. For more information see 'Internet sharing hardware' on page 41.

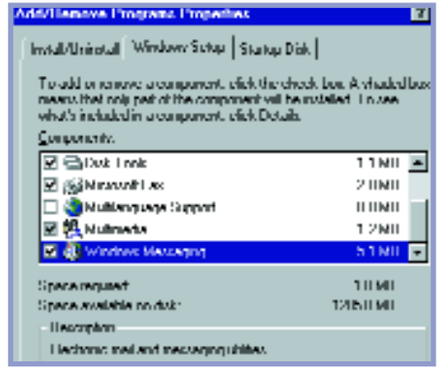
Windows mail serving

A LOCAL EMAIL SERVER IS a useful addition to any LAN where shouting across the office is not a practical means of communication. In a pinch, you can use Internet email, but only if everyone has Internet access; sending messages thousands of kilometres in order to get them to the next cubicle, however, is not the most practical solution.

Again, Windows 95/98 is capable of handling the job as long as you don't expect too much in the way of performance and can put up with a crash every couple of days. Windows NT Server is better, but is expensive; it is designed to deliver much more server than most networks need. Macs are also quite good; they are easier to set up and pretty reliable. But, using a Mac as an email server is a bit of a waste. Linux is, again, the winner for efficiency and price; unlike the Microsoft options it has email serving built in.

Microsoft Exchange (Windows Messaging in later versions), is a popular choice for local network Windows mail serving because it comes free with Windows 95 and 98. If you're running an undemanding local email system, Exchange/Messaging will do the job.

In Windows 95, you install Exchange from the standard Add/Remove Programs item in the Control Panel; it's in the Windows Setup tab with all the other standard Windows components. In plain 95 it's called Microsoft Exchange and in Windows 95 Release B it's Windows Messaging. Exchange is no longer a supported part of Windows 98, but it's still on the disk in the tools\oldwin95\message subdirectory, where it languishes with the similarly unsupported but functional Microsoft Fax.



Windows NT contains Workgroup Postoffice, which works the same way; it's listed as Microsoft Mail and you install it from the Mail Control Panel item.

In brief, setting up Exchange involves installing it on the machine you want to be the mail server first. You have to cancel out of the original configuration procedure after Exchange has been installed in order to open the new Microsoft Mail Postoffice item that will appear in Control Panel. You can then set up a 'Postoffice' file somewhere on a shared drive on that machine; this is where all of the messages are stored. You then open the Postoffice configuration program again to 'Administer' the new Postoffice and define users and passwords. After this, you can open the other new Control Panel item, Mail, and configure Exchange.

All the remote clients have to use 'Map Network Drive' to assign a local drive letter to the drive the Postoffice is on, so they can find it via the 'Browse' option during setup.

Better options

The big names in serious Windows email software are Microsoft's full Exchange Server package and IBM's Lotus Notes. Neither of these is likely to be affordable for small office users. Fortunately, there are lots of shareware and a few freeware mail servers for 95/98; WinFiles.com has a list at http://www.winfiles.com/apps/98/servers-mail.html, and there's another good list at http://www.emailman.com/win/servers.html.

A good place to start is VPOP3 (http://www.pscs.co.uk/software/vpop3.html), which is a full-featured, easy-to-set-up shareware server.

Windows monitoring

ON LARGE NETWORKS IT'S A GOOD IDEA to run a management package to monitor performance, so you know when a link is going bad or when something is amiss — such as an overloaded server. On smaller networks this is unnecessary because small network problems are generally quite easy to identify and fix.

Windows 95 and 98 have two standard programs to view network status — Net Watcher and System Monitor. If they aren't already installed (they live in Accessories —> System Tools from the Start menu), you can add them by running Add/Remove Programs from the Control Panel. (Select the Windows Setup tab and check them in the Accessories or System Tools section, depending on the version of Windows.) Net Watcher lets you view what you have shared and who's looking at it, but it can't perform traffic analysis.

System Monitor is more useful for problem spotting. The 98 version has a few more features, including the ability to show statistics for the Dial-Up Adapter, as shown above. Both versions can report on LAN performance, although they haven't much idea what computers — other than your own — are doing. They only report on what's coming to you or going from you, not what other computers are saying to each other.

Windows NT's industrial-strength equivalent is Performance Monitor, which is sufficient to diagnose many network problems, provided they impinge on the server. In a network with an NT server, most problems that don't have an obvious cause — a faulty cable or a computer that clearly needs a faster connection — are the result of an improper server setup or a lack of speed or storage to perform the task. Performance Monitor can also be set up to sound an alert if any resource or performance figure gets too low. It also has extensive reporting options, database export features and other bells and whistles.

More advanced network analysis software, often referred to as a 'sniffer', can keep an eye on the activities of everything on the network. Sniffers can directly spot malformed data and other problems, rather than leaving you to figure them out from the symptoms or under the impression that your network is *meant* to be slow. If you want a decent sniffer for Windows, though, you're talking thousands of dollars, and again they're of no use for smaller networks. Like so many other serious network administration tasks, this is one that's much better performed by a Linux box running free software.

The next step up is a full-blown protocol analyser, which is a standalone piece of hardware often based on a PC to some extent. It is an essential part of a professional network troubleshooter's arsenal and generally makes a Windows sniffer package look like a bargain-basement special. Since nearly all small network problems can be solved by swapping suspect components out until the problem goes away, or by updating a driver, all this is only of academic interest to most LAN builders.

Network gaming

WHEN MICROSOFT ANNOUNCED THAT Windows 95 was going to become the computer gaming operating system of choice, most people's response was disbelief. But Bill Gates' prediction came true. These days when people cart their computers around to build an impromptu LAN and shoot each other either personally or via armies of tiny troops, Windows 95 or 98 is the OS they're running.

Fortunately, Windows makes it quite easy for even beginners to get a plug-and-go network up and running. It isn't quite as simple as setting up an office LAN, but it's close.

ONE

NetBEUI is an excellent protocol for office networking, but it bombs out for many network games, which prefer IPX/SPX or, more recently, TCP/IP. So you'll need one or both of these protocols installed for your network card. If you only want them for multiplayer gaming, make sure you turn off all the bindings in their Properties windows, and say No to the dialog box which asks if you'd like to change your mind.

The bindings allow Windows to use these protocols for regular network communication as well as the raw data transfer the games require; redundant bindings waste memory.

TWO

If you're using IPX/SPX, make sure the Frame Type is the same on all machines, as mentioned in 'Windows pitfalls' in the Software chapter. The default Auto setting may or may not work. There's no other configuration needed for IPX/SPX, which makes it quite painless to set up even new players' machines.

THREE

If you're using TCP/IP, you'll need to decide on an address scheme for everyone, as detailed in the 'Picking your IP address' sidebox in the Software chapter. Write the details down on paper so latecomers to the game don't force people to get shot by all and sundry while they switch back to the desktop and hunt down the text file containing the magic numbers.

FOUR

One of the classic Windows network gaming annoyances is periodic pauses. These are caused by Windows 95 machines with misconfigured TCP/IP which are set to obtain an IP address from a nonexistent DCHP server. If the 95 machine is on a TCP/IP network with no DCHP server, it should have an IP address manually set. If it isn't on a TCP/IP network, you should delete the TCP/IP binding for its network card. If it was formerly on a TCP/IP network but you've plugged it into a different network for gaming (and it's going back to the office in the morning . . .), temporarily give it a random IP address (1.1.1.1 is fine, as long as nothing else on the network has the same address), then reset it to get its address from the server when you've finished playing.

FIVE

Keep spare network cables and, if you're using 10Base2, T-pieces and terminators on hand. Spare powerboards, keyboards, mouses and even monitors are helpful, too. If you are the host, do not rely on your visitors to bring essential hardware with them, as the network gamer is a forgetful creature at best.

Dedicated gaming

If you have a *lot* of people coming to a LAN party, network problems will probably be outweighed by other considerations, such as whether the venue can handle 40 computers that each draw 200W. Fortunately, network games don't actually throw around a great deal of data; they push the limits of a modem, but a 10BaseT or even 10Base2 network has more than 300 times the bandwidth of a 28.8Kbps modem, and therefore will remain silky smooth for everyone until about 40 computers are connected. After that, it's time to add a switch and segment the network (see the Information chapter for more information on switches). You could also just split it into more than one LAN — after all, it isn't very likely that you will have 60 people playing in any single game, although that day is fast approaching.

For big networks like this, it's also important to run 'dedicated servers' — game servers that run on a separate machine. Since a server doesn't run all the fancy game graphics, several game servers can run on one quite modestly powered machine. All the hot first-person shooter games have dedicated server versions. Like any server, a computer running several games at once will have a lot of data going to and from it and may thus require a dedicated 100Mbit connection from a switch, otherwise ensure that you have a 100Mbit hub and use 100Mbit cards on the server and on all the game client PCs.

Quake 3 is a multiplayer-only game currently in development. It is likely to be the single most common reason gamers flock to each others' abodes to play on home-made LANs.

If you're using dedicated server machines, you can simplify the TCP/IP setup if you can make the server a DHCP server too, allowing it to hand out IP addresses. It's much simpler for people to set their computers to get an address automatically than to pick an address from a list and cross it out or use some other manual system.

Windows NT and Linux can perform DHCP natively; Windows 95 and 98 can do it too, with any of a number of packages, including WinGate and SyGate (which are mentioned in the Hardware chapter).

Mac file sharing

Mac to Mac

Sharing files between two Macs is a piece of cake once you've taken care of the physical connection, though a little forethought is necessary for security. The only time you can overlook security is if you are the only person using the computers (if you are running a personal network between your desktop and notebook machines for example).

A good rule of thumb is to give people access only to those things they need. So you could collect all the files you intend to share into one enclosing folder, then share that whole folder with users who need access to all the files. You could share particular subfolders (or even individual files) with those who only need to use a subset of them. You can take this idea one step further and create a separate volume on your hard disk to hold everything you're going to share. This makes it even easier to check that other users don't have access to your private files and don't 'accidentally' trash your System Folder.

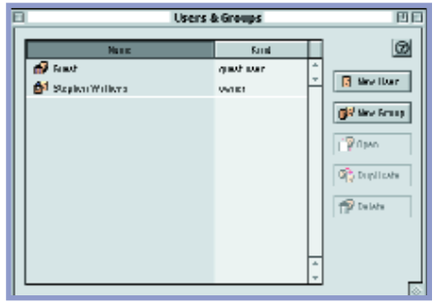
Access controls in Mac OS revolve around the Users & Groups control panel. This is where you create users (in this context you might find it easier to think of a user as an account) and groups (collections of users that are to have similar access rights).

Unless you are happy with the idea of letting all other users connect to your Mac as Guest, you should set everyone up as a separate user, even if you make them all members of the same group. That way, everyone has their own password, so you don't need to change the password when an individual leaves your organisation. Instead, you just delete the corresponding user from Users & Groups.

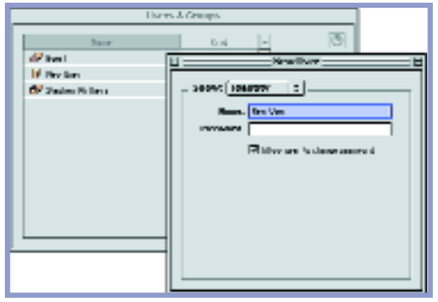
It is particularly important to get Users & Groups settings and file sharing privileges set correctly if you have an Internet gateway, because some Internet applications use them to control access by all users. In particular, make sure that the Guest user doesn't have access to more than you intend.

ONE

Open Users & Groups (Apple menu, Control Panels, Users & Groups).

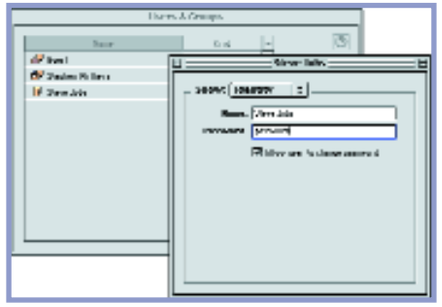


TWO



Click the New User button, and a new window called New User appears.

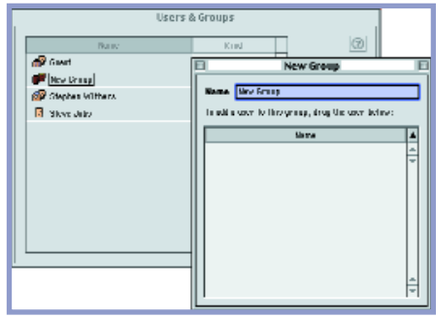
Type in the user's name (the window title will change to whatever user name you specify) and a password. If you *don't* want the user to be able to change this password, uncheck 'Allow user to change password'.



THREE

Close the window and you'll see the new user in the Users & Groups list.

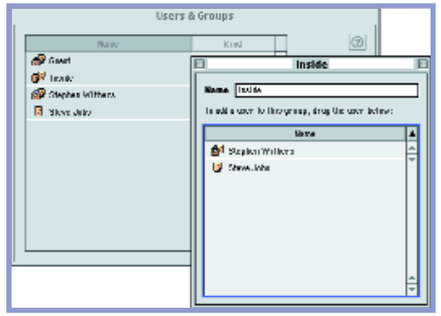
Click the New Group button, and give your new group a meaningful name.



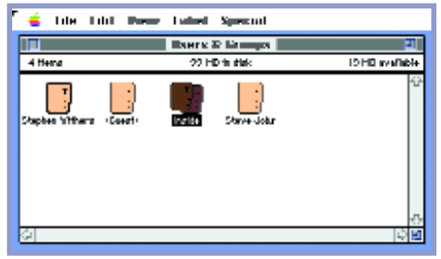
It's your network, so you can use whatever names you like, but you'll find it easier if the group names reflect their purpose. In a domestic environment, you might have Adults and Kids groups, in a small business it might be Owners and Employees.

FOUR

Having created the group, add users to it by dragging their icons either into the lower part of the group window (if it is open) or onto the group's icon in the main Users & Groups window.



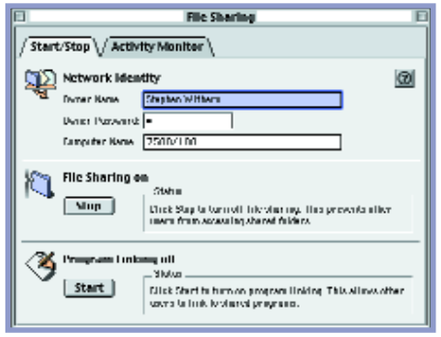
The procedure is basically similar in Mac OS 7.6, although the interface looks different



and menu commands are used instead of buttons.

FIVE

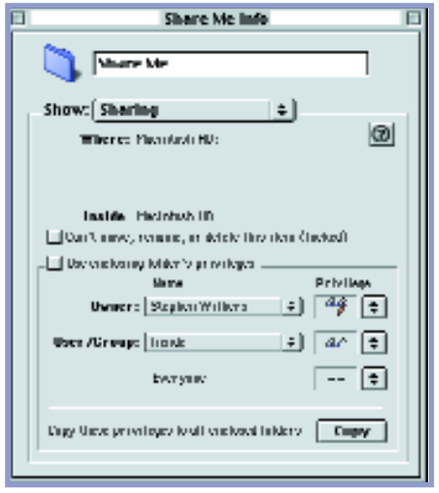
Now that we've created some users and groups, it's time to start sharing some files. Open the File Sharing control panel, ensure that the Computer Name is still set to something sensible, and click the Start button in the middle (File Sharing Off) pane. The label will change to File Sharing starting up and then to File Sharing On. The folder icon next to the label will also change to show a network connection attached to the folder.



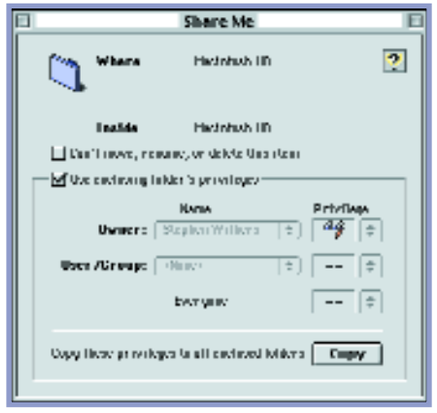
SIX

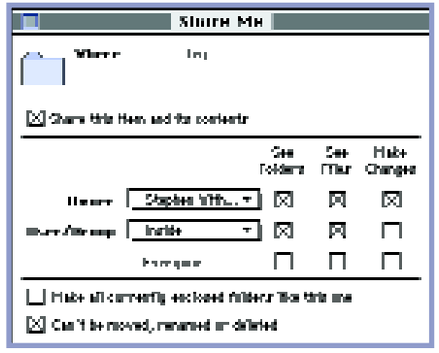
This is where things vary according to the version of Mac OS that's in use. If it's 8.5, select the folder you want to share and choose Get Info from the File menu. Select Sharing from the Show: pop-up menu. By default, the folder inherits the settings of the folder or volume that encloses it. To change this, you must uncheck the Use enclosing folder's privileges box. You can then use the pop-up menus to set privileges for the owner, individual users and groups, and everyone. These menus use small icons to indicate the privileges. A pair of spectacles means read access, a pencil means write access, and two dashes mean no access. The allowable combinations are read and write, read only write only, and none.

Generally speaking, you would use default owner privilege of read and write, and everyone privilege of none, and set particular user or group privileges to whatever is appropriate for the content. Note that a write-only folder is a dropbox: the folder is visible to users with that privilege and they can drop items into it, but they can't see inside. Before closing the window, you may want to click the Copy button at the lower right corner to copy these privileges to all the folders contained within this one. This can be a time saver if they are appropriate to most of the subfolders.



If you're using 8.0 or 8.1, select the folder and choose Sharing from the File menu. Setting privileges is otherwise the same as for 8.5.





Mac OS 7.6 uses an older privileges model. Select the folder and choose Sharing from the File menu. There are still separate privileges for the owner, a particular user or group, and everyone, but the See Folders, See Files and Make Changes settings are individually controlled, giving slightly finer control than 8.x does. (Note also that the File Sharing control panel is called Sharing Setup in 7.6.)

SEVEN

File Sharing does add to the load on your computer, and in some circumstances it can noticeably slow other operations. There are three basic steps you can take to minimise this effect. First, don't leave File Sharing running unless you actually want to share files. The most convenient way to start and stop File Sharing is via the Automated Tasks item in the Apple menu. As long as you've selected Submenus On in the Apple Menu Items control panel, you'll have direct access to Apple, Automated Tasks, Start File Sharing and Stop File Sharing. This is much more convenient than opening the File Sharing control panel and clicking the Start/Stop button each time.

Second, don't share more items than really necessary. This is fairly easy to achieve if you follow the advice above and keep everything you're going to share in one folder.

Third, consider using a separate computer as a file server for shared items. In most SOHO environments, it doesn't need to be particularly powerful. Consider using a hand-me-down Mac (such as a Quadra if you've

upgraded to Power Macs) or buy a used machine if you're on a tight budget. Running AppleShare (Apple's network server application for Mac OS) or even Mac OS X Server (the first stage of Apple's 'modern operating system' strategy, based on technology acquired as part of the purchase of NeXT) on a dedicated Mac is a possibility, but more appropriate in larger environments.

Another approach is to use a cheap 'Lintel' (Linux on Intel) computer as a file server. You don't need frills such as a large monitor or a fancy graphics card, just a decent PC with plenty of disk space and an Ethernet card. The operating system is free and so is the netatalk software (see page 101) that provides Mac-style file services.

EIGHT

To use items shared by another computer, start in the Chooser. Click on the AppleShare icon in the left-hand pane to reveal the names of the Macs that are currently sharing files (along with those of any other AFP servers) in the right-hand pane. Double-click on the name of the server you want to use, and — after providing a valid user name and password — you'll be presented with a list of the available volumes. Double-click on the appropriate volume to mount it on your desktop.

Mac to Windows

If you want to add a Windows-based computer to a Mac peer-to-peer network, you'll need proprietary software for the Windows machines. It is easier with server-based networks. Current versions of AppleShare include SMB support, so as far as Windows is concerned, they appear as just another server.

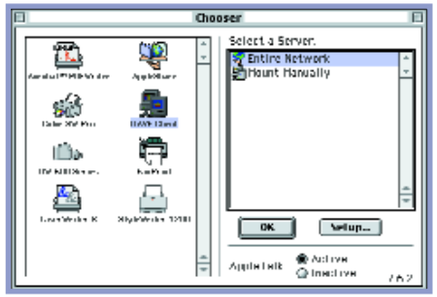
In a peer-to-peer network, your basic choices are between Miramar's PC MACLAN (which comes in various flavours for the different versions of Windows, and is distributed by Conexus) and COPS' COPSTalk (distributed by Macsimise). MACLAN is a good choice because it provides both client and server functions, whereas COPSTalk is only a client — it doesn't let you share a Windows disk with the Macs on the network. Incidentally, PC MACLAN for Windows 95 Version 6.2 *is* compatible with Windows 98, despite its name. PC MACLAN for Windows 95/98 Version 7.2 has extra features, but isn't required for Windows 98.

If you're going in the other direction — adding a Mac to a Windows network — you'll need DAVE from Thursby Software Systems (distributed by Streetwise Software). This piece of software does a neat job of putting a Mac-style face on an SMB network. The SMB servers show up in the Chooser, and once you've mounted or selected them, they function as if they were their native Mac equivalents. A trial version is available, but you need an individual activation key from the company, which can be obtained from http://www.thursby.com/eval/. It's also a good idea to download the documentation from http://www.thursby.com/DAVE2/.

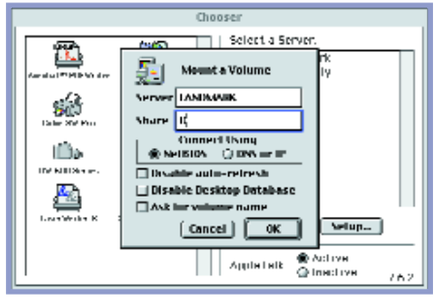
DAVE installs with traditional Macintosh ease, but a restart is necessary as it includes some extensions. You should also ensure that the TCP/IP control panel is configured for your LAN rather than dialup access to an ISP, and that file sharing is correctly configured at the Windows end.

Once that's done, open the NetBIOS control panel and type or paste in your name and licence (evaluation) number. Then type in an appropriate name for your computer and the name of the workgroup it is joining into the Control Panel itself.

Once DAVE is configured, you can open the Chooser and click the DAVE Client icon.



You can then double-click Mount Manually and enter the names of the computer and the shared folder you want to use.



If you double-click Entire Network you can browse the network as if you were in Windows' Network Neighbourhood.

If you need to share items on the Macintosh with Windows, open the DAVE Sharing control panel and click the radio button to turn on File and Print Services. Click the Sharing button to specify the volumes or folders you want to share. Click Add to add and Remove to delete items from the list. When adding, you'll get the

chance to specify read/write and read-only passwords, plus the share name for the item.

Mac to Linux

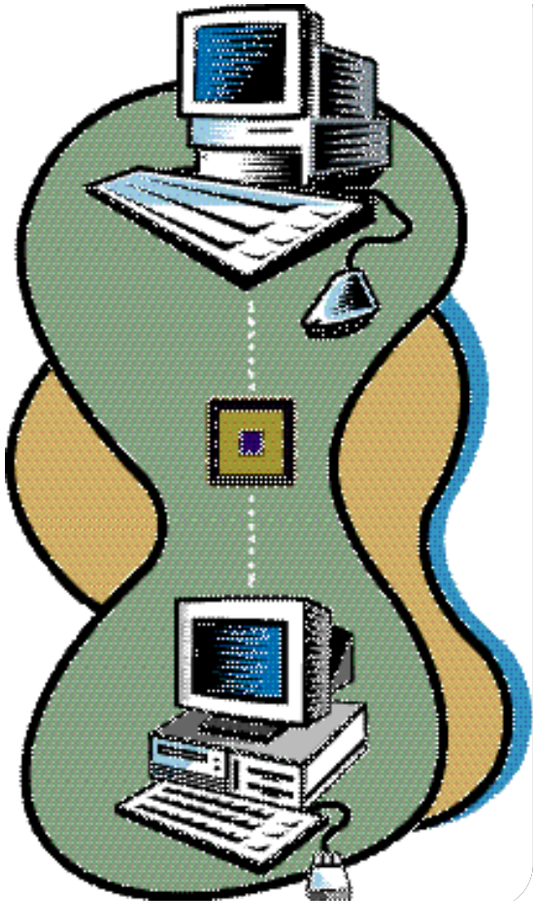
Networking Macintoshes and Linux systems is straightforward and you have several choices.

For a Mac-centric network, install 'netatalk' and 'afpfs' on the Linux system. Since the software is free, it's probably the most sensible approach, even if you're only connecting one Macintosh.

If you're already providing SMB services from Linux with Samba, you could run DAVE (see page 91 above) on the Mac, but remember that it is a commercial program. If you have more money than time, or if you're paying someone to look after your Linux server, DAVE could be the way to go.

While there used to be a selection of NFS clients for the Macintosh, the only current product available is Ascend's IntragyAccess, which does a lot more than just NFS and is aimed squarely at the corporate market.

Depending on the application, protocols such as HTTP or FTP running over TCP/IP may be ideal, allowing the use of standard programs (such as Web browsers) with a native look and feel at each end.



Mac Internet serving

A SOHO ENVIRONMENT DOESN'T put much strain on a Web server, so it doesn't make a huge difference what hardware you choose, as long as it meets the requirements of the software and the operating system version that you require.

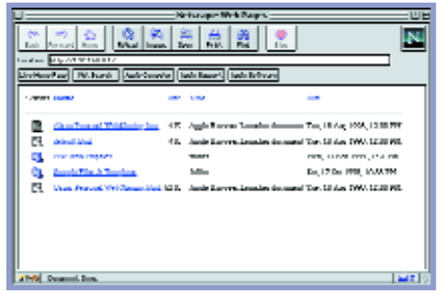
As programs increasingly require Open Transport rather than 'classic networking', it's likely you'll need at least a 68030-based Mac.

On the other hand, if you're going to open the server to the outside world, you'll be pleased to know that recent Macintoshes are able to support high hit rates easily.

If peer-to-peer networking with File Sharing works for you, then Web Sharing probably will do too.

Using Web Sharing is simple — so simple, we've already described the basics in the section on testing your TCP/IP LAN (see page 68) — but there are three settings you may want to alter.

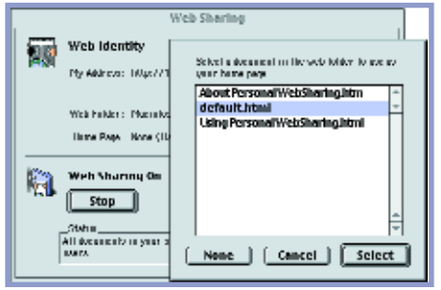
The default location for the folder that Web Sharing will publish is Web Folder on your startup disk. If you have multiple hard disks, it might help to move it onto one of the others, either to save space or help performance a little (especially if you're using virtual memory).



Just click the Select button on the Web Folder: line, and navigate to the required folder.

The second setting controls what is served. The default is to use Personal NetFinder, which generates an FTP-style page *unless* there is a file called index.html in the folder, in which case that is used as the home page.

If you click on the Select button on the Home Page: line of the control panel, Web



Sharing allows you to choose among the HTML files in the currently specified Web Folder.

Finally, you have the choice of giving everyone read-only access to your Web Folder, or using the File Sharing settings to control access (which means File Sharing must be active alongside Web Sharing). Stick with the default unless you only want certain people to be able to access particular pages.

If you outgrow Web Sharing, consider NetPresenz, one of the most widely used Mac Web servers. Created by Western Australia-based Stairways Software (which also gave us Anarchie and Internet Config), this $10 shareware program is even used by corporate customers such as Apple and Optus.

Mail serving

The situation with mail servers is very similar to Web servers. If you are only supporting a few users, you don't need fancy hardware. It is normally reasonable to run the mail server on the same computer as other network services or to dedicate a hand-me-down Mac to this function.

A selection of standards-based mail servers are available from various companies, and AppleShare IP includes a mail server.

Stalker Internet Mail Server is free, but according to the company is only suitable for use with permanent connections. The same company's Communigate server handles intermittent connections and is still free for up to five users.

Beyond that, prices are still pretty reasonable. The only snag is that if you want to use it with normal POP/SMTP mail clients, you need the add-on POP/SMTP module. This module adds a 'free trial' notice to your messages until you pay the $US100 licence fee.

News serving

AppleShare IP includes a news server, but if you aren't using it, try Stairways' RumorMill (shareware, $35).

Installation and setup are straightforward — the 'quickstart' document gives just eight steps and, providing you aren't selecting many newsgroups, the process only takes a few minutes.

The only warning here is that while RumorMill can import an existing list of newsgroups from your Newswatcher (or one of its derivatives) preferences file, it's quite possible that it will contain more groups than RumorMill is able to display. You can also use RumorMill to run local (private) newsgroups.

Mac modem sharing

IN A SMALL INSTALLATION, it can be handy to share one modem among a few computers. Problems can arise if the users are likely to download large files or perform other bandwidth-intensive tasks simultaneously, but for routine Web browsing, email, and so on, the performance will generally be acceptable.

While it is possible to share an Internet connection across a LocalTalk network (for example when connecting older Macs that lack built-in Ethernet), this presents a slight complication. If the computer that's acting as the gateway isn't a Power Macintosh (or clone), it should be either an AV model or be fitted with a third-party, high-speed serial card. The design of the serial ports on other 680x0 models means the modem port can't drive modern modems at full speed at the same time as handling the AppleTalk protocol through the printer port.

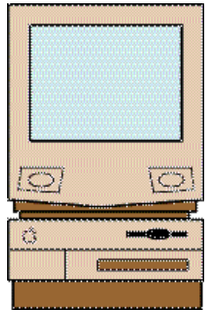
A variety of software is available for modem sharing. The best known (and most prolific) supplier is Vicomsoft (represented in Australia by Fosh and 1World Systems). Vicomsoft SurfDoubler supports just two computers. It's a relatively cheap and easy way of allowing a Mac and one other computer (which could but needn't be a Mac) to share a single modem and connection to an ISP.

VicomSoft SoftRouter Plus not only extends this idea to a larger number of computers, it also integrates a firewall, a remote access server, a DHCP server and other functions. The Vicomsoft Internet Gateway (VIG) goes one step further by adding the CyberNOT Web site filter to prevent access to inappropriate sites.

It is reportedly a bad idea to run SoftRouter Plus or VIG on a Mac that is also running another network service such as a Web server, as this results in poor performance due to the multiple handling of network packets. However, Australian company T&B Brodhurst-Hill has identified a way around the problem using a second Ethernet interface — see http://www.tandb.com.au/internet/.

Sustainable Softworks offers IPNetRouter. It's cheap ($US89 for one gateway with an unlimited number of users) and you can try the actual program for 21 days before you buy. Step-by-step instructions for setting up IPNetRouter are available at Sustainable Softworks Web site (see http://www.sustworks.com/products/ipnr/gettingstarted/Guide.html).

If you have a spare 680x0-based Mac, consider installing the NetBSD (http://www.netbsd.org/) operating system and configuring it as a gateway — but you're then entering the realm of Unix which is covered elsewhere in this pocketbook.



Mac monitoring

A VARIETY OF MAC-BASED TOOLS are available to help you keep tabs on your network and in some cases tweak its performance. Following is a selection arranged in alphabetical order by vendor.

The ag group's AGNetTools (which is distributed by Conexus) includes Ping, Pingscan, Traceroute, Namelookup, Namescan (finds the names associated with each of a range of IP addresses), Whois, Finger, Networkinfo (Open Transport information), Portscan, Servicescan and Throughputtool (calculates throughput for http and ftp servers).

The company also offers NetMeter, a real-time SNMP monitor; Skyline/Satellite, which collects and analyses network utilisation statistics from one or more Ethernet segments using AppleTalk or IP; and EtherPeek, an Ethernet packet analyser which can decode IP, AppleTalk, IPX/SPX, SMB and other major protocols.

Dartmouth College's MacPing sends ICMP or AppleTalk echo packets to multiple devices in parallel and then displays the result. According to the software's developers, this parallel testing can help isolate network problems. A 30-day demo version is available.

Once you get to the stage of running multiple servers and routers, Dartmouth's InterMapper can automatically generate a network diagram and report changes, heavy traffic and failures via audible alerts or email.

Neon Software's free OT Tool lets you ping, traceroute and query DNS information, and offers a few other functions. The company's commercial products are more suited to larger networks. These include Ethernet and LocalTalk versions of the NetMinder traffic analyser LANSurveyor, for automatic network mapping and monitoring (including Mac system configuration, software inventory, and remote file updating) and RouterCheck for monitoring AppleTalk routers.

From the same stable, IPNetMonitor is a $US20 collection of tools to help monitor TCP/IP networks. It includes Ping, Traceroute, Name Server Lookup, Whois, Finger, Monitor, TCP Info, Connection List and Address Scan.

Stairways Software's Mac TCP Watcher 2.0 is a $10 shareware utility that reports on the current TCP connections of the Mac it's running on, sends UDP and TCP echos and Pings, and replies to UDP and TCP echos. This means you can run Mac TCP Watcher on two or more Macs to make sure they are communicating. The program also tests DNSes and provides the Traceroute function.

WhatRoute (http://crash.ihug.co.nz/~bryanc/) is a freeware tool that performs the traceroute function. It can be useful when your network expands sufficiently to require routers, or when you just want to know where the bottleneck is between you and an Internet server. It also carries out Ping tests, and DNS, Finger and Whois queries.

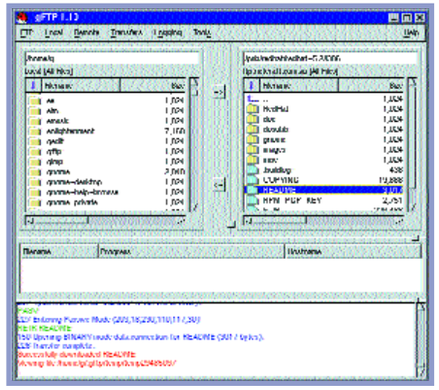
Linux file sharing

Linux to Linux

Linux is an inherently networked operating system. A standard installation comes with server and client tools for file sharing, web serving, email, remote management, and more.

There are two main methods of file sharing between two Linux computers. The first is with FTP, the File Transfer Protocol, used across many platforms including Unix, Windows and Mac. The second is a method specific to Unix machines known as NFS, the Network File System.

NFS lets you access the disks on a remote Linux computer as if they were local disks — if you wanted to edit a file on a remote machine using FTP, you would need to download the file, edit it, then upload it again. The disadvantages of NFS are that it requires more setup work and that large file transfers take longer than FTP.



The Gnome FTP client supports simultaneous downloads, resumption of interrupted file transfer, file transfer queues, and much more. Handy for transferring files between machines on a LAN or across the Internet.

ONE

To set up an NFS server, you need the nfs-server and portmap packages installed. Some distributions install these automatically, but if not you should find them included with your distribution.

TWO

Next you need to define the directories that you want to 'export' (serve) and the hosts you want them to go to. You do this with the /etc/exports file, which looks something like this:

```
/mnt/cdrom   client1(ro)
/            client2(rw,no_root_squash)
```

This example indicates that 'client1' (the name of a machine on the network) should be allowed to access the /mnt/cdrom directory through NFS and that it should have read-only access. This is useful when sharing a CD-ROM drive across the network.

The second line indicates that client2 should be allowed to access the entire file system through NFS. It can write as well as read and it has root access (this is not usually allowed for security reasons).

Note that this example shouldn't be used if you don't completely trust the owner of client2 (or for that matter, anyone on a network between the server and the client),

since they can read or write any file on the NFS server.

THREE

Whenever you modify /etc/exports, you need to tell the NFS server that the export list has changed. To do this, you can use the command:

```
/etc/rc.d/init.d/nfs restart
```

FOUR

Now that the server is configured, you can try getting the client to mount the file system. To do this, you first need to decide which directory the file system will appear in. The directory must exist and it is preferable that it is empty (otherwise any files located there will disappear until the file system is unmounted). Presuming that the NFS server is called 'nfs-server', you can type this to mount the remote CD-ROM on nfs-server from client1 into the local /mnt/cdrom directory:

```
mount nfs-server:/mnt/cdrom/mnt/cdrom
```

You can now access the remote CD-ROM as if it were attached to your local computer. If the mount is unsuccessful, it may be a result of one of these problems:

- If the portmap server is not running, the error message will be:

```
mount clntudp_create: RPC: Port mapper failure
- RPC: Unable to receive
```

- If the NFS server (or the associated mountd server) is not running, the error message displayed will be:

```
mount clntudp_create: RPC: Program not
registered
```

The error 'mount failed, reason given by server: Permission denied' means that NFS is running, but either the client is not allowed to access that directory or the client's host name is not recognised. If that's the case, then a more informative error message may be logged on the server in the /var/log/messages file (type `tail /var/log/messages` to check). If the host name isn't recognised, you'll need to add the name of the host and its IP address in the /etc/hosts file.

FIVE

As with other file systems, you can unmount an NFS file system by typing `umount` followed by the mount point (`umount /mnt/cdrom` for the above example).

Also like regular file systems, you can automatically mount NFS file systems when you boot. This can be useful, for example, if you want to share home directories between machines, in which case you could put an entry such as this in /etc/fstab:

```
nfs-server:/home  /home  nfs  defaults
```

When mounting or using an NFS file system the default client keeps retrying if the server is down. Because of the design of NFS, it is possible for a server to be rebooted without the clients losing their connection; they will just wait until the server is back up.

Linux to Mac

As mentioned in the Mac section on file sharing, you can easily network Linux and Mac machines with the addition of the 'netalk' and 'afpfs' package available from ftp://ftp.u.washington.edu/public/asun; just follow the installation instructions, be sure to edit the Makefile, and make sure netatalk is tailored to your specific requirements. Then do the following:

ONE

After compilation add the following lines to your /etc/services file:

```
rtmp        1/ddp    # Routing Table
                       Maintenance Protocol
nbp         2/ddp    # Name Binding Protocol
echo        4/ddp    # AppleTalk Echo Protocol
zip         6/ddp    # Zone Information
                       Protocol

afpovertcp  548/tcp  # AFP over TCP
afpovertcp  548/udp
```

TWO

Next, copy the conf/atalkd.conf file to /usr/local/atalk/etc/. This file tailors how the AppleTalk interface communicates between the kernel AppleTalk module and netatalk.

THREE

Copy the config/afpd.conf file to /usr/local/atalk/etc/. This file sets Appleshare IP server options and for the most part the defaults here will work just fine.

FOUR

Lastly, copy the conf/AppleVolumes .default file and conf/AppleVolumes.system file to /usr/local/atalk/etc/. These files list volume-to-path mappings and type/creator mappings. You'll need to tailor these files to create Linux directories you want visible to Mac systems across the network.

FIVE

Once everything has been installed and configured, you need to make sure that AppleTalk support is compiled into your kernel.

Most distributions have it running by default as a module when you install Linux, but if not you can follow the normal kernel compilation procedure and add AppleTalk support to the kernel.

SIX

Finally, you need to start the server by running `/usr/local/atalk/etc/afpd -F /usr/local/atalk/etc/afpd.conf`. You can set this to load automatically at boot time by adding this command to your rc.local file.

Given that both Linux and Mac support the Windows SMB protocol, it's just as easy to add SMB support to the Macintosh using DAVE (covered on page 91) so that the Linux box is accessible to both Windows and Mac machines. This will save you time should you wish access to both platforms over your network.

Linux to Windows

The most convenient way to share files between Linux and Windows machines is by using Windows' own SMB (Server Message Block) protocol. SMB is implemented under Linux using the Australian-developed Samba server, and is automatically installed by most Linux distributions.

Samba only supports SMB over TCP/IP, so you should remove the IPX and NetBEUI protocols from the Windows clients, unless they are being used for other purposes.

The initial setup of Samba will involve modifying the /etc/smb.conf file to specify which workgroup your computer should belong to, as well as which directories should be shared; whether 'user' or 'share' level security should be used; and whether encrypted passwords should be used. Samba has plenty of other configurable options you can adjust, but the default /etc/smb.conf file provides reasonable defaults initially.

The workgroup name should match the workgroup to which the Windows PC belongs. You can find this by opening the Windows Control Panel, selecting Network and then clicking on the Identification tab. The default workgroup is 'MYGROUP' — just change this to the name of your workgroup.

The default smb.conf defines only one share called 'homes', which allows anyone with an account on the server to access their home directory by using their login name as the share name. Other shares can be defined in smb.conf by putting the share name in square brackets, followed by options to set parameters such as which directory the share relates to, whether the share is read/only or read/write, and so on. Here is an example share definition:

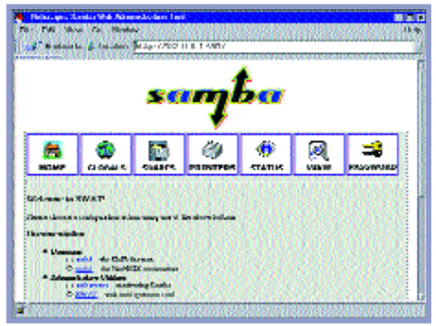
```
[tmp]
  comment = Temporary file space
  path = /tmp
  read only = no
  public = yes
```

Other share options available are described in the smb.conf manual page and in the smb.conf file itself.

Before trying to use Samba, you'll also need to decide whether to use 'user' or 'share'-level security (defined by the 'security=' option in smb.conf). The difference between the two is that share-level security associates passwords with particular shares, whereas user-level security associates passwords with particular users. In general, if your Windows login names match your Linux user names you should use user-level security; if your Windows and Linux user names don't correspond then share-level security will be easier to set up. This is equivalent to 'guest' access under Windows (anyone can access the share if it doesn't have a password set).

After making any necessary changes to your smb.conf file, you should check its syntax by running testparm before starting Samba.

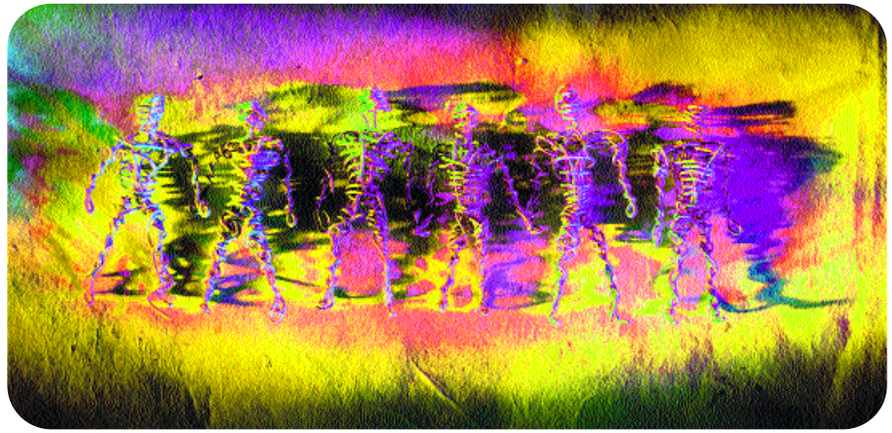
Recent versions of Windows default to requiring encrypted passwords to access SMB servers. Samba supports encrypted passwords, but you will need to set up SMB passwords for users that will be logging on; instructions to do this can be found in the Samba documentation file ENCRYPTION.txt. The alternative to using encrypted passwords is to tell Windows that it should accept plain-text passwords. You can do this by copying the appropriate PlainPassword.reg file from the Samba documentation (/usr/doc/samba-*) to the Windows machine and double-clicking on it.



SWAT: The Samba Web Administration Tool lets you configure Samba using a Web-based interface.

After starting Samba, the Windows Network Neighbourhood should show the Linux server. When you double-click on that, it should produce a list of shares. If something goes wrong, you should read the DIAGNOSIS.txt file supplied in the Samba documentation. This is a step-by-step guide to test whether the Samba server is working, and offers advice on how to fix problems.

Finally, to make things easier you can install SWAT, Samba's Web-based administration tool packaged with Samba 2.0 and above (which is included in most distributions). SWAT allows you to tweak Samba's settings through your Web browser and restart the server on the fly.



Linux Web serving

MOST DISTRIBUTIONS COME WITH the Apache Web server built in and running automatically. Any files that you place in the /home/httpd/html directory will subsequently be made available through the Web server.

The Apache manual is automatically installed in /home/httpd/html/manual, so you can access it by pointing your Web browser at http://your-server/manual/.

If you have a network with Windows machines, you may find it convenient to run Samba so that updates to the Web pages can easily be made through a shared directory. If only one user needs access to the Web pages, you can place the following lines in your /etc/smb.conf file to create a 'Web' share which only they can access:

```
[Web]
  path = /home/httpd/html
  writeable = yes
  valid users = bob
```

You would also need to change the Linux permissions so that the user 'bob' is the owner of everything in /home/httpd/html by typing:

```
chown -R bob /home/httpd/html
```

If you want multiple users to be able to modify the Web content, you can add them to the 'valid users' list, but you will also need to specify 'force user' so that all accesses to the files in /home/httpd/html will be performed as the nominated owner:

```
[Web]
  path = /home/httpd/html
  writeable = yes
  valid users = bob, cheryl, jack
  force user = bob
```

Apache is highly configurable through the httpd.conf, srm.conf and access.conf files in the /etc/httpd/conf directory.

As an example, if you want to modify the page that is displayed when a non-existant document is requested, you would add the following line to your srm.conf file (404 is the error code for 'Document not found'):

```
ErrorDocument 404 /missing.html
```

Whenever you change one of Apache's configuration files, you need to tell Apache to reread its files by sending it a 'signal' with the kill command.

You'll need to know the process ID of Apache; this number is stored in /var/run/httpd.pid (or as otherwise configured in your httpd.conf file). To find out the process ID and restart Apache with one command you can type:

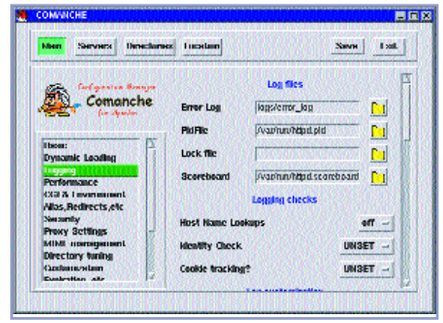
```
kill -USR1 `cat /var/run/httpd.pid`
```

'USR1' is the signal for a 'graceful restart'. You can also use the 'HUP' signal to restart Apache immediately, but this will abort any connections Apache is currently servicing without waiting for them to finish like 'USR1' will.

Apache performance

In its default configuration, Apache can easily saturate a 10M Ethernet with a low-end Pentium machine, so performance is generally not a concern unless you are running CPU or disk-intensive scripts or programs to serve dynamic content. In most cases, the limiting factor will be the speed of the network connection between the Web server and the browser. The amount of RAM the Web server has is the next most important consideration; the more data that can be cached in RAM, the faster the server will appear to run.

As with Samba, a more convenient front end called Comanche (COnfiguration MANager for apaCHE) is available to configure Apache. Some distributions come with it pre-installed, otherwise you can find it at http://comanche.com.dtu.dk/comanche.



Comanche: The Configuration Manager for Apache lets you configure Apache easily.

Linux network monitoring

The 'netstat' (network status) command can be used to display a variety of information about current network connections and interfaces. Here are a few commonly used netstat switches:

Command	Displays
netstat -atu | grep LISTEN	Services that are being provided by the server
netstat -t	Active connections
netstat -r	Routing table

The '-n' switch can be used with any of the above netstat commands to display IP addresses and port numbers instead of host names and port names.

INTERNET SERVICES AND THEIR CORRESPONDING PACKAGES	
Telnet	inetd, tcp_wrappers, telnet
FTP	inetd, tcp_wrappers, ftp, wu-ftpd
HTTP	apache
NFS	portmap, nfs-server
SMB	samba
SMTP	sendmail
POP-3	imap
IMAP	imap

Linux mail serving

SMTP EMAIL WITH LINUX IS MOST commonly implemented using a package called sendmail, which lets Linux send and receive mail to/from other SMTP clients or servers over a network. To allow mail clients such as Eudora or Netscape Communicator to read mail, it is also necessary to install a POP-3/IMAP server. These servers are included in the 'sendmail' and 'imap' packages with most Linux distributions.

By default, sendmail will only accept mail addressed to your server's exact name. For example, 'your-server.company.com.au', not simply 'company.com.au'. If you want the server to accept email for a domain name or host names apart from its own, add the name to /etc/sendmail.cw on a new line and restart sendmail.

If a user has a valid account and password, sendmail will accept email for that user, and the imap server will allow the user to access their mail. If you only need local email, no other configuration should be necessary, but if you want to send/receive mail from the Internet, you'll need to configure a couple of other items.

The default sendmail configuration with Linux is designed to prevent spammers from using your server to relay their messages. However, this means that you do need to let sendmail know the IP addresses of any clients which will be using it as their 'SMTP server'. In /etc/mail/ip_allow, place the IP addresses or network numbers one per line; then restart Sendmail for the changes to take effect.

If you can't receive mail directly because you don't have a permanent Internet connection with a fixed IP address, you can use 'fetchmail' to retrieve email from your ISP's POP-3 or IMAP server. To deliver mail to a single account (such as yourname@your-isp.net.au), create a .fetchmail file in your home directory with the following contents:

```
poll mail.isp.net.au
protocol pop3
user username with password secret is bob here
```

Substitute *mail.isp.net.au* with your ISP's POP-3/IMAP server name, *username* and *secret* with the POP user name and password, and *bob* with the account name on your machine where you want the mail delivered.

You'll also need to set permissions on .fetchmail so that the mail password can't be read by anyone else: chmod 600 .fetchmailrc or chmod go-rwx .fetchmailrc will do the trick.

If your ISP is delivering mail for many users into the same mailbox (such as for anyuser@your-company.com.au), then you can have fetchmail distribute the mail into multiple local mailboxes as such:

```
poll mail.isp.net.au
protocol pop3
localdomains your-company.com.au
user username with password secret to * here
```

Once you have the .fetchmailrc file set up, just type 'fetchmail' to fetch your mail, or automate the process by placing the 'fetchmail' command in the /etc/ppp/ip-up script.

Linux modem sharing

MULTIPLE COMPUTERS CAN SHARE a single connection to an ISP with a single IP address using the IP Masquerading feature of Linux. With IP Masquerading, any communication from a computer on your LAN to the Internet has its IP packets rewritten so that they appear to originate from the Linux server dialled into the ISP. The server keeps track of the connections originated internally so that when reply packets come back in, the server can forward the packets to the correct computer on your LAN.

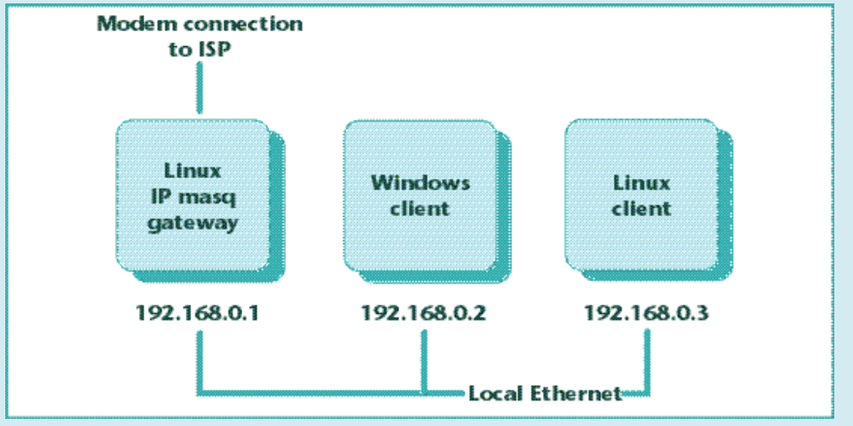
Linux includes all the kernel features which are required for IP Masquerading, but if you are going to compile your own kernel, you will need the IP forwarding/gatewaying, IP firewalling, IP masquerading, and IP 'always defragment' options turned on.

Once you have LAN networking and a connection to your ISP working separately (using the PPP tools or network configuration tools that came with your Linux distribution), you then need to enable IP forwarding and masquerading.

IP forwarding is configured in Linux with the /etc/sysconfig/network file. Change 'FORWARD_IPV4=NO' to 'FORWARD_IPV4=YES' and restart the network by running '/etc/rc.d/init.d/network restart'.

You can enable IP masquerading by first running this command to turn off any forwarding unless otherwise directed ('IP FireWall ADMinistration set Forwarding

Modem sharing using IP masquerading



Policy to deny'):

```
/sbin/ipfwadm -F -p deny
```

The following command then turns on masquerading ('Add Masquerade rule from Source 192.168.0.0/24 to Destination 0.0.0.0/0'):

```
/sbin/ipfwadm -F -a m -S 10.0.0.0/24 -D
                                0.0.0.0/0
```

You'll need to change the source, 192.168.0.0/24, to match your LAN network number and netmask. Destination 0.0.0.0/0 refers to any IP address.

Now you can test access from a machine on your LAN by pinging a site on the Internet. If it doesn't work, check the following:

- The 'Gateway' setting on the client needs to be set to the IP address of your Linux server.
- The 'DNS server' setting on the client needs to be set to the IP address of your ISP's DNS server.

Some protocols (such as FTP, RealAudio and IRC) have special masquerading requirements and need 'helper' modules; you can see a list of these in the /lib/modules/*(kernel-version)*/ipv4 directory. To load the IRC module, type:

```
/sbin/modprobe ip_masq_irc
```

You can use similar commands to load the other masquerading modules.

The ipfwadm and modprobe commands above only affect your networking until you reboot, so once you have it working you'll want the commands to come into effect every time you boot.

To do this, place all the commands at the end of your /etc/rc.d/rc.local file; this script is executed near the end of the Linux boot sequence.

Remote access

Remote access is one of the most useful abilities of a networked Linux system. By running a Telnet server, you can log in from another networked machine and access the server as if you were in front of it. When you type telnet**, you will be connected to the computer and will then be presented with a login prompt.**

At this point, everything will work as if you are logging in from the console, expect for two main differences: you won't be able to run 'startx' or other X applications unless you are running an X server locally, and it won't be possible to log in as root directly. You'll need to log in as a normal user instead, then use the 'su' command to become root. By using telnet to log in to a Linux machine you can remotely perform any administration task in the same way as if you were accessing the machine directly.