Standard practice

Don't worry about implementing TCP/IP on an NT network. Andrew Ward offers sound advice.

TCP/IP has been the default networking protocol for Windows NT for some time and is now virtually the standard protocol used on any network. But many people from a Windows for Workgroups or PC background, rather than Unix or enterprise, are unsure about how to implement it on a Windows NT network.

For larger networks, you really need to read one of the many books on the subject and go for the whole gamut of DHCP, DNS servers and so on. For a small network with only a handful of machines on a single network segment, TCP/IP with Windows NT is extremely easy. Never believe anyone who insists that you need to implement and maintain the horrendous old-fashioned HOSTS or LMHOSTS file mechanism, or use WINS, or add other protocols besides TCP/IP.

If you have a server which you are going to rely on as being available all the time, you can save a huge amount of hassle by using DHCP, but unless you know that the server is going to be there whenever you need to use the network, it's safer to use manual IP addressing.

There are several IP address ranges specifically reserved to be used on internal networks (such as 192.168.0.1 to 192.168.255.254) and you should use one of these. You don't need to worry about DNS on a small network.

If you intend to access the internet and you don't have your own real internet IP addresses, it is quite safe to use one of the reserved ranges as long as your net access device, be it a Linux system or a dedicated router, implements masquerading, NAT (Network Address Translation) or a similar scheme. Then, DNS resolution for internet sites will be taken care of by your ISP and you can usually use the same device as your DHCP server. Within your own network, however, you'll want to refer to servers and other systems by their usual names — SATURN, MARS, VENUS — or whatever nomenclature you've chosen, which are actually the NetBIOS names.

This will prepare you for Windows 2000 implementations

If you don't use DNS or haven't set up a HOSTS file, nor implemented the NetBEUI protocol you may well be wondering how this works. The answer is B-node broadcasts or, more specifically, Microsoft Enhanced B-node broadcasts.

Let's say you want to access a resource on the machine known as VEGAS. What happens is that your workstation first looks in the local cache for this name. Only if it can't find it does it send out a broadcast, known as a B-node broadcast, on the local network specifying the NetBIOS name you want to resolve. The system named VEGAS will respond with its IP number and then your workstation can store this information in the local NetBIOS Name Cache for future use. Interestingly, if the remote system doesn't respond, which probably means it's not working, you're not really going to get much further anyway, and Windows NT will look in the LMHOSTS file.

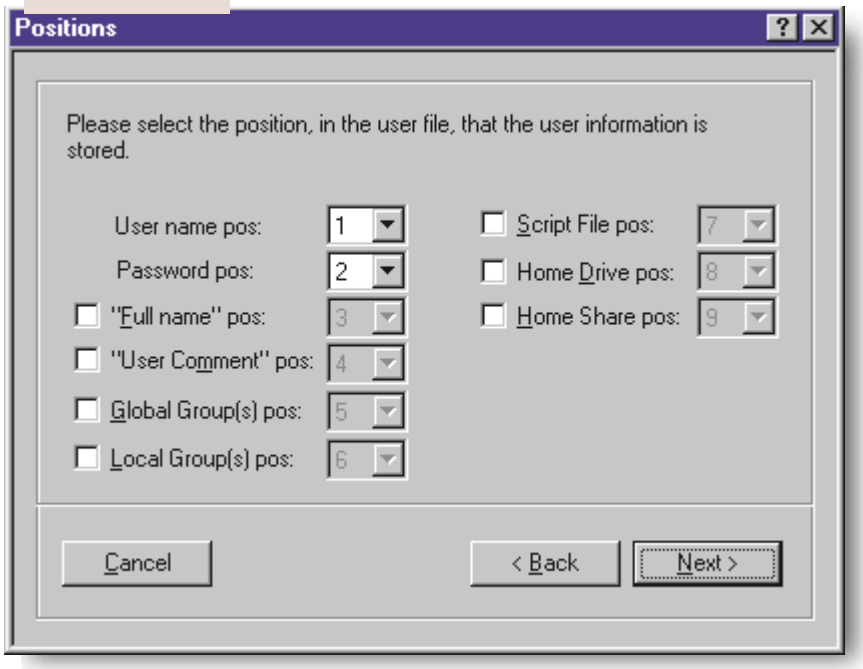
On small networks, this scheme works well, but as soon as you introduce multiple subnetworks and routing you enter into all sorts of complications — for example, B-node broadcasts are not normally passed on by routers and the whole thing falls apart. By the way, don't worry about the network traffic generated by these broadcasts. It only happens the first time you reference an external NetBIOS name following a reboot.

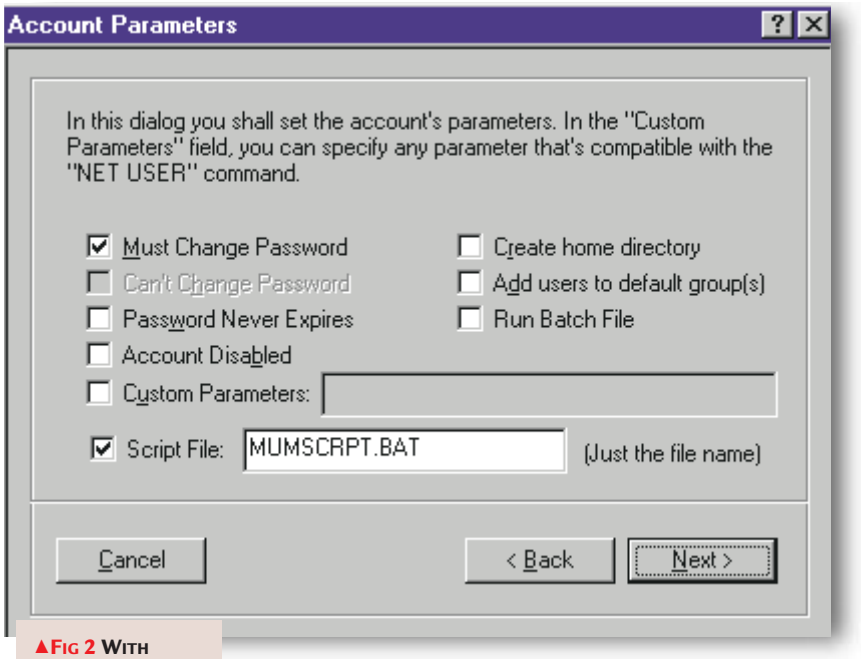
When you do get to a larger network you're probably better off avoiding NetBIOS names altogether and using DNS-style machine names and a DNS server. Apart from anything else, this will prepare you for Windows 2000 implementations where the forthcoming Active Directory structure mirrors the domain naming scheme.

Network oddities

Networking hardware is unreliable even in the normal course of events when there's nothing specifically wrong. Software has to be able to cope with this unreliability by carrying out retries and

▼ FIG 1 ADDING USERS TO THE NT SAM USING NMUM





▲Fig 2 With NMUM, you can specify the various user options required

Windows NT does this very well — sometimes rather too well — and many people have problems with what appear to be obscure network errors.

For instance, a problem readers frequently come up with is that while it's possible to see a remote system when browsing the network, they get an error when they try to do something more adventurous like connecting to a share. They may even be able to establish a connection but then receive errors when transferring huge amounts of data, when backing up over the network, say.

The problem they're running into here is that even though there is an underlying network hardware problem with the cabling, or maybe one or more of the network cards, the software is able to mask it sufficiently well that at first sight the network appears to be working.

A useful tip is that if you can see a machine when browsing, you shouldn't automatically assume that the network is fully working. You shouldn't be afraid to try changing network cabling and network cards.

Adding users

James Roberts-Thomson is one of several readers who have pointed out that the Resource Kit ADDUSERS command is an excellent way to add user accounts from a CSV (comma-delimited) file of user names. ADDUSERS will also dump existing account details from the SAM, although without showing passwords. In fact, the dump feature is immensely helpful because it shows you the file format and headings you need to use when creating your own file of additional user names.

Another option is to delete existing accounts. Hence, with the help of a few cute scripts, someone working in an academic environment, say, could easily construct a mechanism to clean out all leavers and set up accounts for those starting a new course.

Another tool which can be useful in these circumstances is NMUM, or Multiple User Manager for Windows NT [Figs 1&2], written by Anders Wahlin. Its features include these abilities:

- Creating multiple users from a text file, including home directories etc
- Changing password for /disable /rename /enable multiple users from a text file
- Dumping information about the accounts/groups/shares into a text file
- Sharing multiple directories using their names
- Adding/removing multiple users/groups to and from the ACL of multiple files/directories

For those who prefer a GUI tool with wizards to the command-line world, NMUM is a boon. It takes you step-by-step through the options to create files from user information in the SAM, or vice-versa. NMUM can be downloaded from www.winsite.com/info/pc/winnt/sysutil/nmum25.exe.

Changing drives

Another hint from James Roberts-Thomson would be of help when changing drives. (To refresh your memory, the original problem was the easiest way to back up the registry on a system where the hard drive is going to be replaced).

The Resource Kit includes two utilities, REGBACK and REGREST, which make backing up the registry much easier. Specifically, REGBACK [Fig 3] will backup the registry live and online and you can then use REGREST to restore as much as required to a new installation.

Finding the phantoms

Many people have experienced problems with routers (or the built-in DUN auto-dial) being brought online by phantom events. In my own case, the ISDN router log tells me that one of the systems on my network brings the router up at midnight and at 4am every day, but I can't fathom out why.

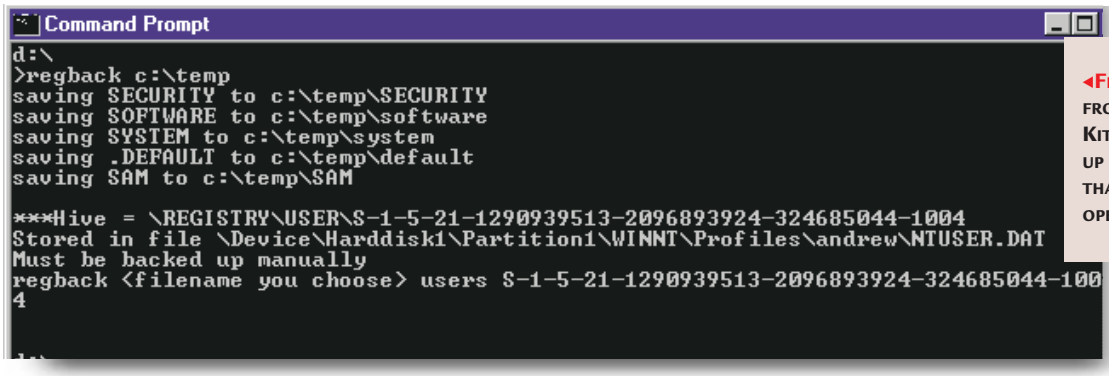
Reader Peter Edgley has thrown some light on a few of the phantom accesses he's been experiencing. When he checks the log of his ZyXel Prestige 100 router he notices that some of the packets causing the router to come up include the ASCII text WORKGROUP. And, like most of us, he has a workgroup called, er, WORKGROUP.

Unfortunately, not all routers will log the packet contents, so not everyone will be able to use this technique to track down errant processes. But if you can, you have a number of techniques at your disposal to prevent phantoms.

There are techniques at your disposal to prevent phantoms

Firstly, be sure that you've turned off anything optional you can find, such as the ability to route NetBIOS packets. Then you can use the filtering facilities of the router, suggests Peter. Decode the source and destination addresses, the packet type and the port numbers from the packet header and then create a filter based on this information.

Peter's other suggestion has prevented the WORKGROUP packets



◂FIG 3 REGBACK FROM THE RESOURCE KIT WILL ONLY BACK UP REGISTRY HIVES THAT ARE CURRENTLY OPEN AND IN USE

from bringing up the router, although one suspects that turning off NetBIOS routing would achieve the same thing. What he has done is to manually add an entry to the HOSTS file on the Windows NT system with an entry referring WORKGROUP to the local machine or any address on the local subnet. For example:

```
192.168.169.2 WORKGROUP
```

Another reader, Chris Bennett, has written in with some observations on the causes of phantom dialling. In certain circumstances, some Office applications, have a habit of storing document and template references as UNC filenames. This is fine until you move the document elsewhere on the network — say to the other end of a dialup link. Then, when you open the document, even though it is now actually stored on the local hard drive it will cause accesses across the network. Similarly, when setting up shortcuts on a roaming desktop be sure that they, too, do not explicitly reference applications on the machine on which the desktop was originally configured but use a relative reference that will work entirely locally.

Please continue to write in with any causes of phantom dial-ups you've identified.

Exploring

If you work from within the Windows NT Explorer, rather than the command prompt, you have a problem once you find a file that you want to edit, unless the file type is already associated with an editor such as Notepad.

From the command line you can just type in 'edit filename.type' but unless Notepad is already associated with the file type in question, you're stuck with the tedious 'Open with...' dialog.

To overcome this problem, there are two ways which allow you to easily edit files using the menu you get when you right-click on a filename.

The first technique uses the SendTo menu. Simply by adding shortcuts to your SendTo directory — which will be located somewhere like 'D:\WINNT\Profiles\andrew\SendTo' — you can extend the SendTo menu at will. I've added a shortcut to Notepad but named it '01 Notepad' so that it always appears first in the list (the list is shown in alphabetic order).

This works for any file type but requires that you wind down to the Send To submenu. An alternative procedure will add an entry to the standard right-click menu, thus avoiding this step. Simply copy the text shown in Fig 4 into a file called, say, EDIT.REG and then double-click on this filename to cause the information to be entered into the registry. Of course, you'll have to change the path to NOTEPAD.EXE to match your system. Unfortunately, using %SystemRoot% in this context doesn't work. This creates an association for unknown file types so, where an association already exists for a particular type, 'Open with Notepad' won't appear automatically. To force it to appear, hold down the shift key before you click the right mouse button.

SUBST again

In the February issue, I pointed out how if you wanted to avoid maintaining vast numbers of shares on your server to support personal user directories you could use the SUBST command with the %username% argument in users' logon profile. Reader Chris Ahchay has sent further information on the SUBST command, observing first of all that it can use the environment variable %LogonServer%. So, your user profile command could be something like the following which is, of course, far more generic than my previous example:

```
SUBST F: %LogonServer%\↙
UserShares\%UserName%
```

(↙ Code string continues)

On the down side, Chris points out that SUBST mappings are retained after logout — associated with the workstation rather than the logged-on user — until the next reboot. If this is undesirable, remember that NTFS permissions will prevent a different user accessing a drive mapped by a previous one, Chris suggests including the code shown in Fig 5 within login scripts.

[FIG 4]

A right-click menu item for editing files with notepad

```
[HKEY_CLASSES_ROOT\Unknown\shell\Open with Notepad]
[HKEY_CLASSES_ROOT\Unknown\shell\Open with Notepad\command]
@="D:\\WINNT\\notepad.exe %1"
```

[FIG 5]

Deleting SUBST drives at login time

```
SUBST | FIND "F:" > NUL:
IF NOT ERRORLEVEL 1 GOTO SubstDrive
SUBST F: /D
:SubstDrive
SUBST F: \\VEGAS\UserShares\%UserName%
```

PCW CONTACTS

Andrew Ward can be contacted via the PCW editorial office (address, p14) or email NT@pcw.co.uk