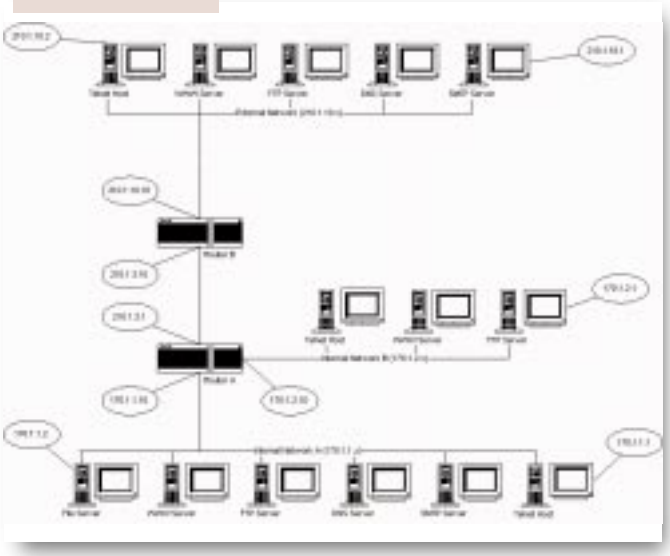
Route it out

Routers are the key to transporting data over a network. Bob Walder hitches a ride.

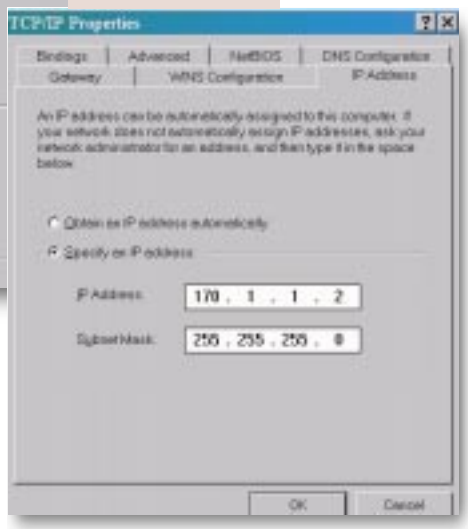
In past issues I've covered the mysteries of IP addressing and the differences between bridges, routers and switches. This month I'm going to try and pull things together by explaining how routers use IP addresses and subnet masks to determine where your data packets finish up. We'll also learn the significance of that magic parameter in your Windows protocol set-up, the default gateway.

Take a look at our network diagram [Fig 1]. This basically attempts to show a corporate network with two segments joined by router A; segment B uses the addresses 170.1.2.x and segment A uses addresses 170.1.1.x. The netmask for all of these is 255.255.255.0, and if you cast your mind back to the previous piece on IP subnetting, you will recall that segment A can consist of addresses 170.1.1.1 to 170.1.1.254, while segment B addresses the range from 170.1.2.1 to 170.1.2.254. Only the final octet changes within each subnet with this netmask (as indicated by the final 0), so as soon as the third octet changes (from 1 for subnet A to 2 for subnet B) it indicates to any router that the device is on a different subnet.

▼ **Fig 1** Network diagram displaying the role of a router



◄ **Fig 2** Setting the default gateway through Windows



▼ **Fig 3** Setting up an IP address and netmask

Configure it out

So, how do we configure devices on segment A? The file server at the end would have an IP address of 170.1.1.2, a netmask of 255.255.255.0, and a default gateway of 170.1.1.10 [Fig 2]. The default gateway points to the port of the router that is attached to the local subnet. If the file server (170.1.1.2) communicates with the Telnet host (170.1.1.1), the fact that the first three numbers are the same tells it that the destination machine is on the same subnet, and it is not necessary to bother with the default gateway. Our source machine thus uses something called ARP (Address Resolution Protocol) to determine the MAC address of the destination machine (it needs this in order to transmit the packet). The file server sends out an ARP broadcast with the IP address of the Telnet host, and the Telnet machine responds with its own MAC address. To prevent too much of this sort of traffic, each machine keeps such resolved addresses in an ARP cache for future reference. Once the MAC address has been resolved, direct communication can begin between the machines.

Now say our file server wants to communicate with the FTP server on segment B. This time it compares IP addresses and sees that 170.1.2.1 is actually on a different subnet to 170.1.1.2, because the third number of the address is different. At this point, it knows the packet needs to be handled by a device that knows more about the network topology than it does — the router (or default gateway). So, it ARPs for the MAC address of the default gateway, which is 170.1.1.10 in this case, and sends the packet on its way.

Routers are incredibly complex devices, but what they do can be boiled down quite simply: they direct traffic. Like a traffic cop, the router takes packets in from its various ports, checks on their destinations, and sends them off to the appropriate outgoing port. In our case, the router spots that 170.1.2.1 is actually on its second port

by comparing addresses and netmasks again, and so it sends the packet directly to the FTP server.

Two's company

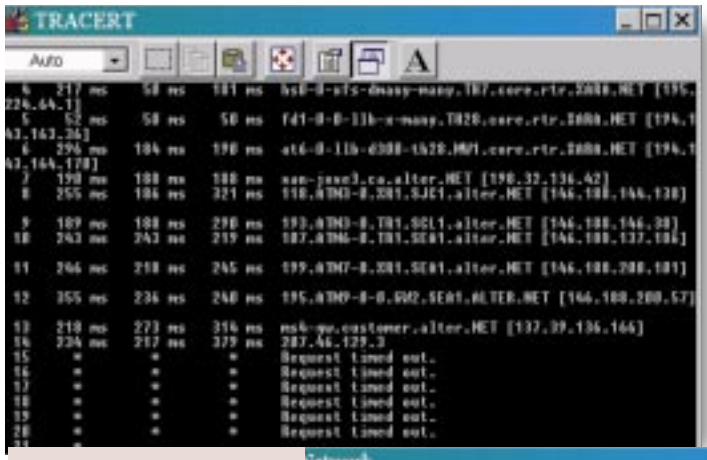
OK, so that has dealt with routing packets within an organisation where the addresses are known. When it comes to connecting our network to the internet, however, there is more than one router involved. In fact, there are millions of the things spread around the world, but we are particularly interested in two: the one at our site and the one at our ISP. Of course, if you wanted to attach a small network to the internet, you could use a proxy server and have all your users go through that: this way, you can often get away with a single-user dial-up account to support a small network. However, we are assuming here that you have opted for a full-routed connection, and so you have to make sure that your router and the ISP router know about each other.

Your ISP will provide you with an address and netmask for the router at its own site [Fig 3, p271] and this is what you need to enter into your own router to enable it to speak to the outside world. What you do, in fact, is create another subnet, this time between the external port of your router and your ISP. In our diagram, this small subnet consists of just two devices: the external port of our router is 210.1.3.1, and the appropriate port of the ISP router is 210.1.3.10. What we effectively do is tell our router that its default gateway is 210.1.3.10, and that is where it will send all the packets it doesn't know how to deal with directly.

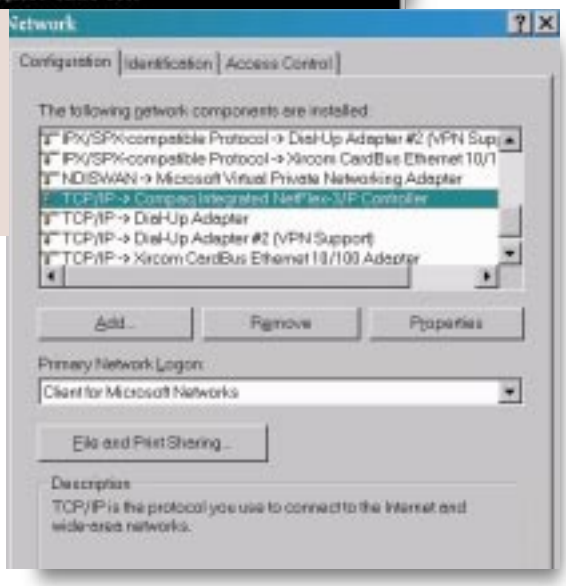
The right address

OK, so now our file server wants to communicate with the SMTP server 210.1.10.1 somewhere on the internet (in this case it is actually at our ISP, to keep things simple). It compares IP addresses and determines that the device is not on the local subnet, and so sends it to the default gateway address. Router A checks the address and notes that it doesn't correspond to any of the subnets attached to it directly. So if the router is stumped, what does it do? It sends it to its own default gateway (210.1.3.10), just as the file server did.

Now router B has the packet, and it takes a look at the IP address and sees that 210.1.10.1 is actually on the same subnet as its internal port — 210.1.10.10. It can thus ARP for the MAC address of the SMTP server and deliver the packet directly. Each time a packet traverses a router in this way it's known as a "hop", and the number of hops a packet has to make determines how quickly you receive your data.



▲FIG 4
A SAMPLE TRACERT OUTPUT



▶NETWORKING CONFIGURATION APPLET FROM THE CONTROL PANEL

Try dropping to a DOS box under Windows and typing TRACERT MICROSOFT.COM. You'll get a display similar to that shown here [Fig 4], with each hop represented by a new router. As you can see, it is sometimes a long, tortuous and slow route to Microsoft!

RIP it up

Of course, given the size of the internet, or even a large corporate network, routers need more than just a 'default gateway' to go on if packets are to find their way from point A to point B some time this week. Routers learn about the network automatically using something called RIP — Routing Information Protocol. This is used to allow routers to tell each other about the segments they are attached to and the addresses they know about. This is done by 'advertising' what they know across the network, whereupon each of them listens and updates its own routing tables accordingly. This is what makes the internet so resilient. Should any router fail for whatever reason, it will stop advertising and the routers that were communicating with it directly will start to find other ways around it. This dynamic change in network topology is completely automatic and is called 'convergence'. Finally, it's also possible to 'tell' a router about a specific route between two points, and these are called 'static routes'.

Hopefully, between this and the IP addressing/subnetting tutorial you have enough information to create your own IP network and get it attached to the internet. If you want to delve into TCP/IP a lot deeper than I have the space to here, you could do worse than check out the book *Windows NT TCP/IP* by Karanjit Siyan (ISBN 1-56205-887-8). Published by New Riders, it costs £26.95 from Computer Manuals (0121 706 6000).

PCW CONTACTS

Bob Walder can be contacted via the PCW editorial office(address, p10) or email networks@pcw.co.uk