# Connecting your LAN to the outside world

***To enable communication across many different boundaries a WAN is of paramount importance. WANs are becoming easier to set up and maintain and are much more accessible.***

A local area network is all very well, but as the name implies it's local and there's likely to come a time when you want to communicate beyond the limits of your own department, building or campus. That inevitably means buying and installing extra hardware and software, although Wide Area Networks (WANs), like LANs, are something you can set up and maintain yourself. Not only that, the technology involved is becoming more accessible and affordable.

**Altogether now**

Having said that, though, a modicum of know-how is required and exactly what you need for this job is going to depend on where your networks are located and how far apart. If you just want to hook your LAN into another elsewhere in the same building, for example, a simple bridge or an Ethernet switch might be all that's needed, and that's no more difficult than expanding a single LAN. The only thing to watch out for is the distances involved as using structured UTP cabling, for instance, you're limited to a maximum of 500 metres from one end of the backbone (the network cable that links all your LANs together) to another.

For systems bigger than this the best alternative is FDDI, using optical fibre rather than copper cable to connect hubs together, because it can cover greater distances, the EIA/TIA specification listing 2km as a maximum. But you'll need additional hardware in the form of FDDI uplinks in your hubs and, of course, the optical cable that joins everything together. You'll also need to look at just where you locate all the hubs and switches, to make sure the network is segmented efficiently. And on a very big network, routers and VLAN software might be needed to further optimise the bandwidth available.

Routers will be needed if you then want to join remote networks together, such devices adding the ability to link networks using dial-up, ISDN and leased lines. And which of these you use will depend on the amount of bandwidth required, and how much you can afford to pay for it.

In terms of bandwidth, leased lines offer the most, and do so at a fixed cost, so they're ideal for heavily used links that need to be available all the time. In contrast ISDN is like an ordinary dial-up phone line--the more you use it the more you pay, but with more bandwidth and the added benefit that what you don't use doesn't cost anything. To this end ISDN has grown in popularity over the last couple of years and there are now lots of cheap ISDN routers to choose from. Sophisticated spoofing mechanisms built into these further help reduce call costs, filtering out routine broadcasts between NetWare LANs, for example. And you can get routers able to aggregate multiple lines together to provide the bandwidth you need.

That leaves the good old dial-up line at the bottom of the bandwidth pile, and as such, limited to connecting small networks. Traditional analogue lines aren't totally redundant as you can use them to support mobile users. For that you need little more than ordinary modems and suitable software, although for a lot of users dedicated remote access servers are a better alternative.

## The Internet connection

So much for linking your own private networks and their users together. On top of that you might also want to provide access to networks in other organisations, add public email facilities, and perhaps publish information and provide users with access to the World-Wide Web. That means connecting your LAN to the Internet. And for that two things are required--a physical connection to the Net, and the software that allows users to send and receive information across it.

For all but the largest of organisations the connection will be supplied by one of the many Internet service providers, such as CompuServe, Demon, Pipex, and the like. All you have to do is connect to their network, and they, in turn, provide the connection to the Internet, which is just how it works when you want to gain personal access. And in much the same way you could use an ordinary modem to dial into the service provider. But the bandwidth available would be pretty limited, which means this is only an alternative for a small number of users or for email only access.

In this case you're back to considering either ISDN or a leased line, with much the same bandwidth and cost implication as when using these to link private LANs together. The hardware's the same, too, with most companies opting for one of the many ISDN routers for their link to the Internet, because of the lower costs, the spoofing and filtering options, and the ability to add extra bandwidth quickly and easily if it's needed.

Then it's down to the software side of things and the main concern here has to be the protocol support needed to allow users to send and receive data over the Internet. The trouble is the Internet uses TCP/IP, where you might be using IPX, NetBIOS or NetBEUI on your LANs. The obvious answer is to equip each and every user with their own IP stack. There are lots of these around, and a good Microsoft implementation is included as standard with Windows 95 and NT. But then you've got to manage the IP addresses involved, and that means obtaining a large enough block of addresses from the service provider and making sure these are distributed correctly. You might end up having to configure a Dynamic

Host Configuration Protocol server to automatically assign addresses, particularly if you've a large number to look after, and the whole thing can get both expensive and messy.

As an alternative you could implement a gateway, with just one system (usually a server) having an IP stack and communicating with the Internet using TCP/IP. The other users send and receive data using IPX or whatever other protocols are used on the LAN, the gateway handling the translation to and from IP as required. Novell includes just such a gateway as part of the latest IntranetWare package, which means user workstations don't have to be changed at all. Other software gateways for use with both NT and NetWare are also available and you can get dedicated hardware gateways, such as Instant Internet from Bay Networks, which provide similar facilities, and that are equally easy to setup and run.

## Keeping it to yourself

Of course, as soon as you connect your LAN to the Internet you immediately open it up to intruders: for instance, if you can see them, they can definitely see you. Therefore some kind of protection is required. An IP gateway, like that included with IntranetWare, provides some security, but you might also want to set limits on exactly which networks different users on a private WAN are allowed to access--and almost certainly when they can surf the Internet and what kind of sites they can browse.

There are a number of ways of meeting all these needs, starting with the simple filtering options to be found in the hardware used to join LANs together. Using such facilities in a router or switch it's possible, for instance, to stop particular workstations or even whole LANs from communicating across a WAN link, barring access to other networks and the Internet altogether, if required. As simple and effective as these filtering options are, however, they're something of a sledgehammer when what most people want is a much more flexible, and much easier to manage, mechanism for controlling access to their LAN.

The best way of going about this is to add a firewall, which usually involves extra hardware or software, or sometimes both, capable of monitoring traffic as it passes in and out of your network. Again most of these will let you set up filters to limit the users, workstations, and networks allowed to communicate across the firewall barrier in both directions. But that's not all they provide--rather, the more sophisticated will offer additional proxy services, where the firewall accesses the local network in response to outside requests, and the Internet in response to local calls. These so-called 'application-level gateways' or 'proxy servers' will have substitutes for all the more common services, such as Telnet and FTP, and if someone tries to access your LAN or the Internet using a non-proxied service they won't be allowed through. You can even tailor the proxy applications and further control exactly what users are allowed to do with each one, even when they can use them.

Firewalls and proxy servers that provide these facilities are available in lots of different guises with more being ported to the NT platform rather than Unix, their more traditional home. And it's worth looking for those that can also act as IP gateways, as the firewall host is the ideal location for software that can handle the address translation we talked about earlier, making Internet access simpler as well as more secure.

## Staying in control

Having read this you might decide that connecting your LAN to the outside world simply isn't worth all the bother, but it really needn't be that difficult if you take it step by step. The hardware and software involved is no more complex than that needed for local networks. Some careful planning is called for, however, as the links between networks can all too soon become bottlenecks, slowing down everyone on the network, whether they access remote networks or not. Tools to monitor and manage a WAN are also important considerations, and in this respect it's worth reading the feature on managing the network later in this supplement.

And if you're still not convinced don't miss out on the benefits of wide area communications, as you can always take the really easy route and buy a connection into one of the many public networks, like those run by IBM and BT for instance. Like the Internet, these span the world, but provide a far higher level of security and guaranteed bandwidth, and with no need to install or manage your own WAN infrastructure at all.

# Managing the network

***Once you've installed networks in remote sites and added switches and routers to segment the network, you need to monitor and fine-tune the system to keep it optimised.***

A network is much like a car in that buying it is only the beginning. You then have the day-to-day maintenance of it to consider. The cost of ownership of a network can be astronomical if not kept in check. An effective network management strategy will do just that.

There are two sides to managing a network: control and monitoring. Controlling the network is about making the adjustments to keep things running smoothly. Monitoring is watching what's happening on the network and identifying where problems are. You can then take corrective action where necessary.

If your network is managed properly, you can save time, money and headaches with slow response times and lost connections. Just tuning the network, without the need to install faster networking or increase segmentation, can solve many bandwidth problems. Even if you do upgrade your network, careful management can ensure you're making the most of your investment.

## Controlling your network

You can take control of your network in a number of ways: using the console connections for network infrastructure components like switches and routers; using a proprietary management; or using standards-based management. The console connections on networking devices are designed for the initial setup, and to use these for day-to-day management would be time consuming and inefficient. Likewise, proprietary management packages are fine, as long as all your networking infrastructure is from the same manufacturer, something which is unlikely.

For an heterogeneous enterprise network, standards-based management is by far the most efficient choice. The Simple Network Management Protocol (SNMP) is a standard protocol that can control everything from hubs to workstations. Unfortunately, it's not as simple as the name implies. SNMP involves a system of management information bases (MIBs) that contain details of the devices on the network, alerts when something goes wrong, and traps that notify network management stations (NMSs) of the network's status. A network management station will usually be a PC with a management package, such as HP OpenView, IBM NetView or Novell ManageWise.

The object properties held in a MIB describe the functions of a device. Standard MIBs are available for many devices, such as PCs, switches, bridges and routers. Manufacturers can also write their own MIBs to allow custom features to be managed through SNMP. When a new device is added to the network, its MIB must be compiled into the NMS to allow it to recognise the device.

This will only provide a basic level of management. For more sophisticated control, OpenView and NetView support plug-in applications for specific devices. These are supplied by the hardware vendor, and can provide access to all the features in the device. Very often you find that a representation of the front panel is used, showing all the indicators you'd see on the actual device.

## Effective monitoring

Control is only half the story. To effectively manage your network you need to know what's happening on the wires. This is where statistics collection comes in. By taking samples of network traffic and analysing them for patterns, you can see which applications or nodes are using most bandwidth, and whether the network is segmented evenly. The standard method of statistics collection is called RMON. Just like SNMP, RMON is a client/server environment. Probes reside in network nodes: either specialised devices, or included in hubs, switches and routers. An RMON package is used to tell the probes which information to collect and to retrieve this information when needed. The same NMS will often be used to analyse RMON statistics as monitor SNMP traps, and most packages are now capable of interrogating RMON probes. The statistics these probes can collect vary, depending on which RMON groups have been implemented. One probe is needed for each network segment you want to analyse, and some devices might only have one built-in probe. On a switched network, you should analyse each segment for utilisation; if one segment is more heavily used than the others, then consider moving some of the machines from that segment to another.

RMON can also be used to spot other sources of problems. For example, Windows 95 loads NetBEUI by default when a network adapter is added. NetBEUI is suited to peer-to-peer networks, and you're unlikely to use it on an enterprise network. By tallying the MAC address of any machines transmitting NetBEUI broadcasts with your records, you can trace the offending machines and remove the protocol. However, you'd also be able to tell how much of the overall network traffic is NetBEUI, and whether it's responsible for slow responses. Like any line of business, it's important to act on the information you receive in order to get the full benefit. Self-configuring networks might be on the horizon, but they haven't arrived yet.

Most networks need management--only the smallest can get away without it. Careful management will ensure that your investment in network infrastructure isn't lost. View the time spent in managing the network as you would the time spent checking the oil on your car: it could save a very large problem later on.