

I believe in evolution!

So often in visiting new customers I see networks that have evolved over time from a simple way of linking two computers together into a complex tangle of spaghetti-like wiring held together by the proverbial string and sticky tape. Often these networks are causing real performance problems now; they always pose a risk of serious failure for the future. Because they consist of wiring largely hidden from view and boxes with obscure functions, they are ignored until they go wrong.

I also believe in intelligent design.

Intelligent design starts with an understanding of real world needs for capability, for reliability and resilience, and for performance and security. As ever the design process is littered with choices and trade-offs – performance versus cost, accessibility versus security, resilience versus simplicity.

Choices, choices, choices

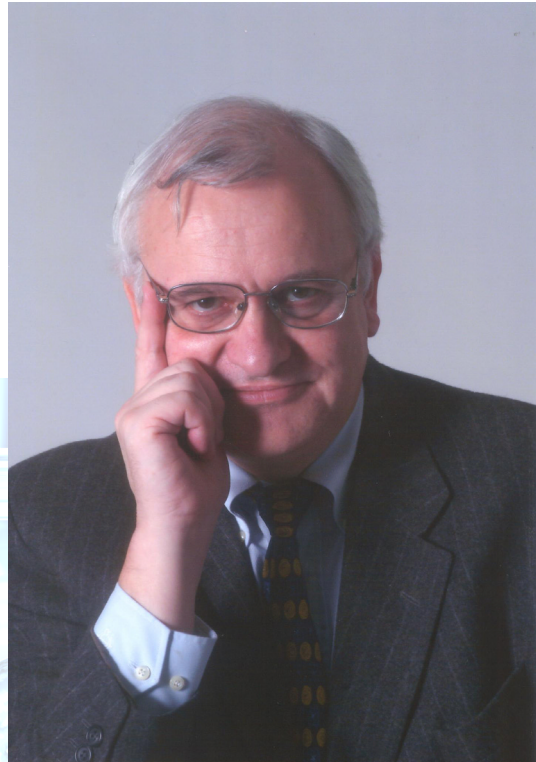
Once the requirements are understood, thoughts move on to considering the choice of technology. TCP/IP is almost bound to be the main choice today, but underlying it are technologies that are changing as fast as ever. Within buildings, cabling may need to be replaced to achieve speed and reliability. It needs to be specified correctly and properly installed if it is to deliver what is required of it. The necessary switches and routers need to be correctly specified and configured to control network traffic. Maybe a wireless capability is needed?

Routes we can go by

Between buildings there are further options with ISDN, ADSL, SDSL, 'traditional' leased line, and even wireless and satellite links. At this stage some thought needs to be given to resilience. Most of these technologies offer highly reliable means of communication. However, they do sometimes break and consideration must be given to the costs incurred if, for example a branch office is unable to communicate with headquarters for a significant period.

There's more

There is not space here to cover network security. Suffice to say that it is vital that security is addressed as a part of the design process. As a bare minimum no unencrypted data traffic should go outside the premises. And give a great deal of thought to the physical security of the network infrastructure. Both malicious and well-meaning interference with networking components can cause havoc with the network.



Finally give some thought as to how the operation of the network will be monitored. Given its importance in many organisations it could well be worth investing in a network monitoring service to ensure that you or your service provider are alerted to any potential problems before they occur, or at least that you know about them before your users do.

This article was originally published in the Newbury Weekly News Business Review in January 2007.

Charles Zealey is a consultant working with business professionals helping them to improve their organisation's productivity and effectiveness with the use of Information Technology. Typically a return on investment can be achieved with 6-12 months. To access help sheets go to www.itsolve.co.uk/HelpSheets/. For a free half-hour consultation on business IT issues phone 01635 869863 or email lisa@itsolve.co.uk.

This article is © Copyright ITSolve Ltd 2006-7. All rights reserved. You may copy or distribute this article in full as long as this copyright statement and full information about contacting the author is preserved. The author is Charles Zealey, ITSolve Ltd., charles@itsolve.co.uk. Telephone : 01635 869863.

To subscribe to our newsletter, IT in Focus, email subscribe-it-in-focus@itsolve.co.uk. To 'unsubscribe' email unsubscribe-it-in-focus@itsolve.co.uk using the same email address as that from which you originally subscribed.

We keep our subscriber list in confidential. Whilst we aim to ensure that all out-going mail is scanned for viruses we recommend that you ensure that you are fully protected against all forms of malware attack. We only send our general bulletins to those we understand have given their express permission to receive them. ITSolve Ltd never release, sell or give a subscriber's e-mail address to any party outside of the organisation, except when referring business between individual subscribers. Our subscribers only receive email messages that contain requested information, new monthly articles or announcements of new services.

