

# **NETWORK MANAGEMENT FOR THE SMALL TO MEDIUM USER**

## **THE FACTORS THAT DRIVE RISK AND REWARD**

### **1. BACKGROUND AND WHERE WE ARE NOW**

During the 1980's the growth of PC's and the flexibility of the software predicated the need for sharing files and for access to shared devices – printers etc. We also saw the shift of resources in that more staff were provided with a desktop terminals to undertake the computerised tasks that made up their daily work – i.e. billing systems, word processing and customer data-base management.

In addition, we saw in the need for a single desktop device (PC) to be capable of running a wide range of applications, with large main-frame systems being accessed from the PC, not a dedicated terminal.

This drove the fortunes of the original **network** operating systems such as Novell Netware. The Netware product was the first to utilise a shared server base operating system and this was the fore-runner of the current networking platforms.

#### **Microsoft Windows**

With the adoption of Windows as the common basis to access software that was Microsoft based rather than proprietary to a hardware device, such as IBM or DEC, we saw the need for these PC's to be connected over higher speed and greater access connectivity options.

Windows introduced the platforms that brought new levels of ease of use and drove hard the need for everyone to have a PC on their desk. During the 1990's, vast amounts of money were spent on desktop equipment.

Windows has also introduced a level of dependency on one supplier that is unprecedented in the evolution of the IT industry.

#### **LAN Connectivity**

In the main, the market defined Ethernet networks as the de-facto method to connect PC's, printers and resources. The industry focus moved to developing high speed and enhanced physical cabling structures, so that now we have the systems we use today.

Challenges to the cabling systems have gone away, with the latest drive to Wireless being based on adaptation of the Ethernet protocols.

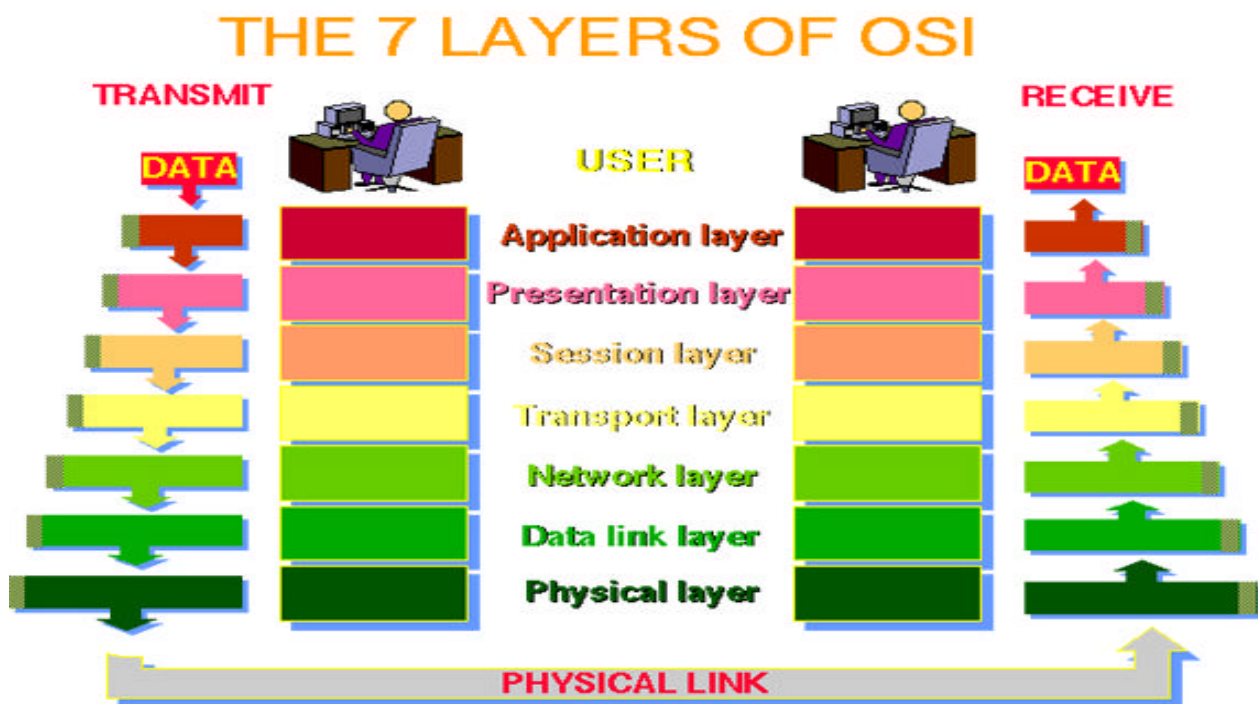
We now have proper industry standards for LAN connectivity and design, thus there is a solid platform basis for the installation of a LAN. By far the majority of the market uses 10 base T Ethernet networks, with servers, routers and other resources connected; and this design is the backbone for most corporate LAN systems.

## WAN and the 7 Layer Model

Even in the 1980's, users needed access to other networks or computers. This was done by basic leased lines which had no specific network protocols, thus the computers themselves were responsible for managing file transfer.

The next generation of connectivity was based on simple network protocols, such as X25. The X25 protocol used packets and headers / footers for the first time to both ensure data delivery and to format data as part of the WAN application, rather than the computer running the communication exchange.

X25 developed further but the growth of Ethernet, servers and the need for "seamless" data transfers drove the market to evolve towards a platform of standards that would be used by everyone. The solution was the OSI 7 Layer Model – shown below: -



This basis allowed for the development of the protocols that enabled to Network Layer (layer 3) to operate; and for hardware suppliers to focus on the technology to build packets and handle addressing, with maximum efficiency and lower cost.

Initial protocols for LAN / WAN access included TCP (Transmission Control Protocol) which were focused on delivering server to server connectivity.

However, the growth of WAN connectivity evolved differently and separately to LAN's and management technology did not integrate, thus making users face two different basis for managing their network resources.

## The Internet

In addition to the issues raised above for sever to server (gateway based) communication, it was inevitable that users would want to access devices and hosts themselves. In other words, a single PC to connect across a myriad of many systems and host facilities.

This became the basis to develop the Internet.

The Internet Protocol was designed to create a Network of Networks (the "Internet") and required that TCP became enhanced to become TCP/IP.

Individual machines are first connected to a LAN (Ethernet or Token Ring). TCP/IP shares the LAN with other uses (a Novell file server, Windows for Workgroups peer systems). One device provides the TCP/IP connection between the LAN and the rest of the world.

### **The Growth of E-Mail**

Another effect of a PC at every desk with common software everywhere and LAN / WAN access for all, is that electronic exchange of files can be quickly organised.

E-mail can be organised across a number of server based networks and the growth of e-mail was a natural development of the above.

In almost every case, e-mail is now the de-facto method of undertaking file transfer or basic information exchange between departments, companies and the world. An e-mail response to a customer / user inquiry is very much a standard way of getting information.

E-mail servers are now bigger, more complex and the greatest use of network resources, in that e-mail has become a priority for network design and redundancy. Security and virus management is also a major risk to e-mail performance.

### **The Issues**

The issues for Network Design are now massive. Considerations even a small to medium network (100 – 1000 devices) include: -

- Client / Server issues
- Shared software and application rights
- Network cabling and physical issues
- Security – LAN and WAN
- Addressing protocols and integrity
- Routing design and redundancy
- Disaster recovery
- User and device tracking
- E-Mail server access / rules
- Performance and device management
- Web server design and control

## **2. DRIVERS FOR CHANGE**

If the rise of e-mail, faster Internet connection and faster PC processors were not enough, the needs of the users and the drivers for change keep coming.

Some areas that are looming to make the current network open to change are –

## Voice Over IP (VOIP)

Networks now operate with high speed (100 meg) structured cabling and this infrastructure provides a platform for more traffic – as a rule. The current trend from network equipment suppliers is for the (potentially) spare bandwidth to be used to carry voice traffic, using IP based call routing and IP telephone handsets.

The rationale for this trend is based on: -

- **Economies of scale** – by using already installed network access infrastructure;
- **Improved redundancy / re-routing options** – IP is a redundant protocol by design, as it always looks for an alternative path;
- **User addressing flexibility** – mobile staff can load up all their user settings including voice profiles;
- **Next generation technology** – which improves integration with other systems, such as CRM and user interface applications.

The issues with the implementation of VOIP in practice are: -

- **How to model traffic profiles;**
- **How to ensure call quality** – VOIP is a packet based technology that can use considerable bandwidth – a typical voice call over IP can use up to 768K of bandwidth;
- **QOS call routing** – especially in a WAN context:
- **Network management** – who “owns” the voice user?

A typical SME user has delayed with the implementation of VOIP. At this time, VOIP equipment is not so costly and the pressure to investigate VOIP is very strong.

It is likely that savings are possible, but the challenge is to ensure that the current infrastructure is capable of coping with the new voice traffic; and how the new voice user base will be managed.

## Security

All businesses are very concerned with network security and the issues are ever-changing in terms of keeping up with SPAM, Fire-Walls and Virus checkers. This paper cannot address the details of these.

The area that can easily be over-looked is the reliable and up-to-date audit of the equipment that is connected to the network. This area causes massive concerns and is often a highly time consuming task.

In recent times, software has been available that will reliably discover and detail: -

- What devices are connected or exist within the network / or sub-networks
- Which devices (may) need upgrading
- Validate OS and firmware levels
- Validate hardware configurations
- Discover names of devices
- Discover the model numbers of the devices
- Discover the chassis serial numbers
- Chassis modules with serial numbers

With this data in hand, options can be explored very easily and new areas of security risk can be planned with confidence.

### **Wireless and Bluetooth**

New hand-held devices (PDA's and Mobile handsets) and Note-Book PC's are more frequently provided with Bluetooth and/or wireless access and the impact of this means connection to server based systems. Typical applications are e-mail and calendar access.

These devices may not running the same level of virus checkers and firewall controls – as a rule.

Furthermore, the wide ranging deployment of hand-held devices that enable access to secure networks also means that traffic profiles for this new range of users is not modelled in the original design and configuration of the network.

One other issue is that the Wireless device can be stolen – thus if access is not carefully tracked, un-authorized users can be live on the network, this is rather like losing your house keys and not having the locks changed.

### **Storage and Secure Recovery Planning**

Networks can fail and disasters will happen. In many cases the trend has shifted away from physical DAT or tape based restoration and back-up towards Storage Area Networks or Network Accessed Storage solution.

This involves the applications and user profiles being “mirrored” or duplicated on an outsourced remote storage device, often via a service provider.

The issues here for network management are quiet clear, namely: -

- **How dynamic is the storage facility** – real time or under a routine?
- **How is the SAN built** – i.e. is the SAN always on-line or only enabled when running a routine?
- **What is the restoration plan** – how is restoration enabled?
- **Who “owns” the DR plan** – often the IT manager / Chief Information Officer.

Network management in this case is highly relevant, as the failure of services or management alarms may often be the first indication of a problem.

### **3. RISKS HAVING STARTED TO CHANGE**

In many cases, the changes that are being considered by most network managers – especially in the SME field – are based on priorities that are driven by business issues. Money and retaining a competitive edge are key to the change priority.

The overall issues with any change are to do with the network being capable of supporting the change and; how much (if any) investment or cost is required to make the change a success.

No network manager is willing to either undertake a change that will jeopardise existing users or undertake a poorly researched change. Indeed, doing so is a certain way to get noticed!

In real terms, the challenges facing most network managers are all around the impact on their particular infrastructure whilst balancing the expense associated with change against the risks of failure. This translates into a risk analysis process, which can be fundamentally affected by the lack of solid base information about the existing infrastructure.

Almost all the respected consultancy firms and the experts in the field of network design recognise the value of having reliable and trustworthy information to start with.

In addition, any change will be subject to the following risks: -

- **Reliable traffic modelling** – does the new application / enhancement produce unacceptable traffic levels or adverse performance issues?
- **Security issues** – are we adding an increased risk or opening a door to risk?
- **New storage or restoration issues** – does the business face increased storage or restoration problems from the new application; and most important of all;
- **What is the back-out or “Fall-Back” plan?**

In regard to the risk analysis, all changes must be implemented with due consideration to back-out or a “fall-back plan. In almost every case, a change without the option to recover back to the original specification is a massive mistake.

In general terms the old analogy is very true – “If it is not broken, do not fix it”!

#### 4. REWARDS THROUGH GOOD MANAGEMENT

Good management is a process and inherent in the business, as much as it is the software or tools required to provide information to the network manager. However, the best software used for network management will provide: -

- **Clear and “at-a-glance” graphical displays** – especially for key information and data, such as packets sent, bandwidth used and packets lost;
- **Ease of use** – the software should be user-friendly and easy for all involved in the network management process to use;
- **Reliable** – the information provided should be taken for granted and not need any other processing to become useful;
- **Real-time** – the dynamics of network management mean that real-time data is much more useful and relevant than data that is trawled and then needs to be processed to be useful;
- **Low overhead** – software that has high maintenance cost or has a high training overhead is often not updated and falls behind the up to date needs of the business.
- **Flexible** – as we all know, networks change, thus the management software must be flexible to adapt to the changing needs of the business.

In most cases within the SME market, the management software need be Windows based and a Unix based system means heavy investment, which may not be returned through the benefits received.

In addition, the software is just a tool for the overall management process and must be able to be adapted fast, so that all concerned with running a successful management system get the just rewards associated with the overall management strategy.

## 5. CONCLUSIONS

Users will always face demands for change and history has taught us that change is best undertaken when proper planning is in place.

The conclusions from this paper are; -

- Understand fully the current structure and network facilities **before** any fundamental change is undertaken;
- Network management is a process that involves more than tools and software, to achieve a solid management approach;
- The most simple expansion or enhancement to a well designed network can bring about major disruption – always have a fall-back plan;
- Use of differing technology can create design and traffic modelling problems – always analyse the current basis and then design with solid base information.

## 6 ABOUT CODIMA

Codima is a European software provider with a world-class portfolio of network and service management products.

We solve problems such as: -


- ❑ **How to control network resources – in “real-time”**
- ❑ **How diagnose network utilisation conflicts**
- ❑ **How to find and document network assets / risks**
- ❑ **How to discover and map resources / equipment**
- ❑ **and delivering value**

Our focus is based on: -

- \* Ease of use – highly graphical real-time data
- \* Low running costs – no need for expensive professional services or committed bandwidth
- \* Responding to user demands – either through expanding database updates or developing software to work in new applications – e.g. Voice Over IP (VOIP)

Our HQ is based in Central London, with offices in the US; Northern-Europe and France. From this office infrastructure, Codima supports an extensive distribution channel throughout the world and we are committed to working with partners to reach end users of our products.

Whilst our company is young, we have a very mature product suite. This is because we have managed to acquire a number of technologies from others and quickly integrated them to provide a high-value and innovative product set.



All of the unique technology we provide is highly complementary and delivers an extensive set of functionalities for network and IT services management. We have specifically developed links between products so as to extend their respective functionalities and to deliver a unique set of benefits.

Codima has positioned our products at attractive price levels, so that the large number of SME companies that also need to manage and control their networks, can benefit from technology that has previously been the “tool set” of large enterprises.