Network Design Planning

Introduction

The past 30 years have seen remarkable growth in the size and reach of computer networks in the workplace; and more recently in the home. Technical innovation has driven this growth: improved standards have allowed faster speeds to pass along both copper and fibre cables, wireless networks have become ubiquitous, new devices with their own embedded network capabilities (the internet of things, IOT).

In tandem with this technical innovation, the demand for network capacity has increased as ever more data is created – content is richer (much of it to be consumed in real time), software applications can now generate enormous data flows, massive database store more and more relating to every aspect of our businesses and our lives. All this data needs to be moved around the organisation, reliably and effortlessly in a way that maintains its integrity while keeping it safe and secure.

There is nothing to indicate that this trend of growing data 'throughput' will abate; if anything, it seems more likely to accelerate further as demand for new and faster services grows and we enter the era of the IOT (Internet of Things).

It's therefore quite important to get the design of your computer network right if these important benefits are to be realised, and reliability assured.

This article provides some general advice on planning a network.

By Ohmega1982

Stock illustration ID: 109197839

Hand write LAN diagram on the Touchscreen Interface.

Designing for Growth

The demands on a network will inevitably increase over time, so it is important to plan for how the network will grow both in terms of the number of devices and the demands that each will make. It would be reasonable to design your network to last for at least five years ahead.

By Ohmega1982

Stock illustration ID: 127086326

Business lady write web service diagram on the whiteboard.

Of even more importance is the structured cabling upon which your network will run. Although the choice of network equipment (switches, routers and wireless access points etc) has a major impact on the maximum throughput of your network, adding extra capacity here is much easier than changes to the physical network layer. The physical cabling, which is much more difficult to upgrade or replace, should be designed to for at least 10-15 years ahead, acting as the plumbing for the next two to three generations of network equipment. Measures such as redundant fibre backbone links, spare network outlets, cabling for future WAP installation, leading edge technology cables, all cost relatively little upfront but will quickly pay for themselves if needed down the line.

Network Segmentation

Most modern networks carry a range of network traffic. As this will be mainly IP based, each device will be broadcasting on that network – and as the network grows with more devices added a significant amount of resources would be spent listening to the broadcast traffic. Just as a crowded room with many conversations makes it harder to hear and be heard, so with a network. Each device would be interrupted – albeit momentarily – by conversations it needs no part of. The solution is to segment with VLANs (Virtual LANs)– making one type of network traffic visible only to devices on the same VLAN.

By Profit_Image

Stock illustration ID: 542469955

VLAN in the form of binary code, 3D illustration

This has 2 consequences at the design stage.

- First and most obvious, it's important to decide which devices need to be on the same VLAN, and therefore how many VLAN are needed. In many cases this is simple – CCTV cameras for example, need to be on the same VLAN as the NVR recording device. A BMS Head End computer will be constantly monitoring the temperature sensors and heating controllers. It doesn't matter where devices on a VLAN are, a VLAN is a service separation only; independent of location (building or floor level).

- The second design consideration is more complex. While we've gone to the trouble of segmenting our traffic, we won't want to stop all traffic passing between VLANs. A building's CCTV system might need to talk to the Access Control System so that when a visitor buzzes

for entry, video is switched to the front desk. A router device can allow this to happen in some circumstances, but these rules need to be set up quite carefully to avoid security issues (see below). The alternative, which his not normally recommended, would be to allow any traffic to flow between VLANs – this is simple to do but can represent a security risk.

Security

Network security is a broad topic, but there are a few basic considerations at the design stage that can make a difference.

By Maksim Kabakou

Stock illustration ID: 149243228

Protection concept: computer keyboard with word Network Security or

- A Firewall device – one that is sized correctly for the network is an essential element of any network design. As well as defending against attacks from outside (Denial of Service) a firewall can provide Antivirus protection - stopping malicious infections from being carried within email attachments – and detecting the presence of malware installed on site. Prices vary enormously, largely depending on the anticipated level of traffic and the degree of protection required; thorough the vetting of traffic the more power will be needed.

- The physical security of network equipment is easy to overlook yet it is a vital first step. The room housing the core equipment, firewall and patch panels should be secured with a swipe card or similar, cabinets should be lockable and of good quality.

- Physical security is important also at the network edge; for example, riser cabinets used to house edge switches should be secured, again with a quality lockable cabinet.

- Wireless networks present their own unique security challenges; most modern commercial wireless access points are very secure, however are intrinsically more vulnerable to attack. A wireless network that are open to the public, or to visitors, should be segregated in its own ‘DMZ’.

Reliability

An unreliable network will disrupt a wide variety of services; therefore, its design should try to minimise as many potential failures as possible by:

By Raywoo
Stock photo ID: 171968426
Computer system robustness concept words written on white paper

- Design the physical later with redundant backbone links – careful consideration to the routing of these links can deliver additional resilience by diverging through different risers etc

- Consider high availability (hot standby) systems for key items: core switches and firewalls typically are single points of failure that can bring down an entire network
- Select quality network equipment – it is more expensive and may not seem to do any more than generic equipment, but the support service is normally much better
- Consider equipment that can accommodate a backup power supply
- Including sufficient backup power and smoothing for all core networking equipment
- A secondary Internet service should be configured as an automatic failover – particularly if essential services (voice, and security systems) are IP based
- Purchase adequate support service from your network supplier for your needs – think of this as an insurance policy; although a good supplier will include an annual health check with their support to proactively spot problems before they cause serious concern
- Maintain backups of all your network configurations; your supplier should provide these upon completion – you (or your maintainer) will need them in the event equipment has to be replaced