Networking

WHITE PAPER

Is your network fit for
the demands of today,
let alone tomorrow?

Is your network fit for the demands of today, let alone tomorrow?

While the rest of your infrastructure has been undergoing a radical transformation over the last 8–10 years, especially in the areas of server virtualisation and storage provision, the underlying networking hardware has mostly stayed the same. This white paper looks to discuss the functional requirements of your network both today and tomorrow, as IT undergoes its largest shift yet into the mobile/cloud era.

The basics

We are going to start by looking at the underlying business requirements of your Local Area Network (LAN) today. We will then look at the current developments in technology and consider the changes required to make your LAN fit for purpose and the technologies available for us to make these changes.

The key business requirements of a LAN today can be summarised as follows:

- Highly available
- Secure
- Mobile
- Seamless

Let's break each of these open to understand what they really mean.

Highly available

Access to the IT infrastructure and the internet is business-critical to most organisations. If a user can't access their data, applications and networked services, such as printers, it is going to severely impact them being able to do their job. Therefore, network resiliency and redundancy is paramount in the design of any network. We therefore need to consider, as part of our business continuity planning, what is the impact to the business of a complete or partial network failure. Several different scenarios should be considered on a case by case basis, utilising a Business Impact Analysis methodology to quantify the effect on the business of different failures. By understanding a breakdown of the failure scenarios, you will be able to design the correct architecture for your network to ensure it meets your specific requirements. When we talk about resilience in your network we need to be thinking edge to edge, all the way from the internet connections, routers and firewalls through to your core network and onto the edge. While it would take the most stringent of business requirements to make each endpoint connection fully resilient, all other areas commonly do need to be highly available. However, today you would be surprised by how many small-to-medium-sized businesses lack this availability within their network, when the technology available today makes this easily achievable.

Secure

We are currently seeing large-scale increases in cyber-attacks, personalised to gain entry to your business data. While there are many considerations as to how we can ultimately secure your environment, we need to start by looking at the very basics within your infrastructure – and this starts with your network. In this white paper we are focusing mainly on the internal network; however, it goes without saying that perimeter security should be a major consideration. Your firewalls should be fully featured, fit for purpose, patched and, of course, highly available.

For many businesses perimeter security is where IT security on their network starts and ends. This is often likened to how an egg is made up – being hard on the outside, but soft on the inside. Unfortunately, many cyber-attackers take advantage of this oversight by using innocent-looking, email-borne payloads or even social engineering to reach inside your organisation's perimeter defences, enabling cyber-criminals to take control of less well-protected devices. This allows them to roam freely within your network. Incidentally, it is often far easier to gain access to users' devices within your network than to break in through your secure perimeter network. When considering our internal networks, we should be considering how we can increase security within the network. There are several ways in which we can achieve this and we will be covering them later in this white paper.

Mobile

You may very well be asking: "How can I make my LAN mobile?" By the nature of the name, it is local to your business. However, in today's mobile-first world this is exactly what users demand, wherever and whenever your users demand access to their applications and data. The LAN needs to support this. Internet access is today often classed as all but a basic human right, and while you may invest in delivering quick and reliable wired access to your network, users have come also to expect performant and reliable wireless access. Wi-Fi inside your organisation is something that has often been treated as a second-class citizen. In many cases it started in meeting rooms to provide internet access for your guests, and then slowly spread to common areas and beyond. Today wireless network access is the predominant way our users will be

ComputerWorld recommend considering firewall devices from Barracuda and SonicWall when considering edge security.

connecting, especially as many devices no longer have wired network connections. Gone are the days where a user will only be utilising the single PC you place on their desk – these have probably largely been replaced with laptops and, whether IT like it or not, they will also be using one or more mobile devices, which in many cases are owned personally. The thought of delivering corporate network access over a wireless network raises alarm bells for many businesses. However, with modern technology it is often easier to deliver a more secure wireless network than a wired one. Of course, this isn't where our mobile LAN access ends: we also need to be considering secure access from outside of our organisations. This is an area of technology that is also currently being revolutionised, where per device VPN access was the only option in the past, remote desktop solutions and per application VPN solutions by the likes of VMware are now seen as the defined standard. This challenge will be the subject of another white paper.

Seamless

The life of a network manager is a hard one. Do you remember the last time you were congratulated for providing a fast and reliable network? No? We didn't think so. You will only ever hear about the problems the users have and you are seldom, if ever, congratulated for the times it works. The users expect the network to be available whether it is wired or wireless. They expect to be able to connect quickly and easily and they expect it to be so fast and seamless that they don't even think about speed. In addition to this, there is the growing demand for ever-increasing bandwidth and the need to keep your data safe by implementing more security than ever before. There is no doubt about it that the task of delivering a seamless network is a difficult one and is potentially going to be our hardest task when considering the re-architecture of your network.

Where is the technology going?

Now we understand what the user wants we need to look where the technology is going. As a network architect we need to blend these potentially very different needs together. The art of success when designing your network will focus firmly on getting this mix correct.

Core and edge network

The concept of a core and edge network has its origins in the days of the mainframe computer. The core is the central switches where your servers connect and where all the magic happens in terms of routing and security, the edge being the remote switches that are located around your premises that enable users to connect their devices. This topology goes against many of the goals we may have in terms of delivery performance. The first issue is that our servers themselves are no longer physical: they are now virtual entities running on clusters of host servers within our data centres. Because of this we are seeing an increase in the so-called 'East to West' traffic travelling between these virtual servers. However, we are still trying to manage the networking tasks of these servers with physical core switches. In addition to this, rather than just delivering the security functionality within the network core, there is an increasing demand to deliver this protection at the edge of our networks. This requires edge switches that support routing and other security functionality.

In addition to the increased bandwidth requirement of traditional server environments, the advent of hyper-converged solutions that require the network to support significant storage workloads mean that 'East to West' traffic increases further, with many solutions demanding a minimum of 10GB networking. Whether you are currently considering a hyper-

converged infrastructure or not, the current trend is very much indicating that this is the way forward for your virtual infrastructure and, to cope with this growing demand, we also should ensure that alongside 10GB connectivity we have the ability to uplink at higher speeds such as 40GB.
Bandwidth requirements to the desktop are also increasing. While most technology today is designed where possible to be thin to the edge to allow mobile and cloud working, we are seeing users needing to be more creative, using a vast array of technologies within strategic departments such as marketing, as well as specific industry related tasks like CAD. As such, along with a decrease in costs, we are seeing GB connectivity at the edge become much more common.

The end of hardware defined networking?

In the past, as we have implemented and upgraded our network's infrastructure, the software that has delivered the new functionality has come embedded in the new switching hardware. This has resulted in a 'rip and replace' mentality, as every time we need to deliver new networking functionality we need to replace the hardware. Now, for the first time, we are seeing this approach change as, in the same way as we have previously seen with server virtualisation, network virtualisation is becoming a reality.

Software Defined Networking and Open Networking revolutionised network design by allowing you to invest in smart-switching hardware that has a small hypervisor layer, allowing you to run and change the switch operating system and applications to meet your business needs. The good news about this new trend is investing in these solutions today needn't be costly or lock you into one software-defined switch provider. Manufacturers like Dell offer open networking-capable switches with their own familiar switching operating system without a premium on the price. Later when there is a further business case for a particular open networking software you are able to simply license, download and install the switch operating system of your choice on your open networking capable switch. Popular open networking vendors today include Big Switch and Cumulus.

Virtualisation aware

As our servers have radically changed from physical to virtual over the last 5-10 years, our networks haven't kept up pace. The number of physical servers connected to our core switching is likely to have reduced; however we now have many more connections to virtual switches without the same functionality and management of our physical switches. One of the next major trends we are seeing within networking is to fully embrace virtualisation, to add layers of intelligence, management and control closer to these virtual workloads and ultimately improve security.
Technologies like VMware NSX allow you to move core network tasks like routing, load-balancing and firewalls into the virtualisation stack, allowing improvements in performance, enhanced security with micro-segmentation (more details on this below) and automation of the provision of complex network designs. All of this is achievable without massive changes in hardware and configuration to your existing core network.

What is micro-segmentation and why do I need it?

We have already discussed the increase in cyber-attacks and the fact that the perimeter of our network is secure while the inside is soft, much like an egg. With an increase in attacks from within we need to change this, starting with our virtual infrastructure. VMware NSX introduces a concept of micro-segmentation: think of this as a firewall for each of your servers or workloads. While this may have previously been possible with complex physical network design, the cost and management involved would have been excessive. With NSX we can centrally manage these from one interface: ultimately introducing a much tighter layer of security, meaning one system being compromised no longer means a free rein to your internal network.

Wireless networking

As we all know, the need for wireless connectivity is growing daily. Every day we are reading or hearing about new autonomous systems that will run on wireless networks – not to mention that all personal devices in today's market offer wireless connectivity as standard. A lot of the newer personal devices don't even offer network ports anymore. This can mean alarm bells to a lot of businesses.

Wireless networking is still a pretty undertrained area for most IT departments as it used to be plug and play with a standard key and maybe internet access only. However, due to the growing demand of wireless devices, IT departments have a duty of care to provide reliable Wi-Fi for a growing number of devices and at the same time are challenged with keeping it all secure. With most IT departments being asked to do more with less time and even staff, consideration should go into designing a wireless network that is easily accessible with little input from the IT team. This is where we are seeing a huge growth in self-service portals for wireless access. There are companies in existence now that just specialise in creating on-boarding portals for the wireless infrastructure to make it easier for the department and its users.

When considering wireless solutions now, IT departments don't have to worry about coverage: they have to worry about capacity, security and ease of use. If the right amount of time is invested into designing and covering those three topics, IT teams can sit back and enjoy the customer paradise of good wireless.

Our top tips when considering an update for your wireless network include:

1. Ensure you undertake a wireless site survey to ensure optimal placement of the access points. Common mistakes include the installation of too many access points resulting in poor performance and interference.

2. Ensure your wireless network is secure. This should be a key priority, probably slightly above user experience. With thanks to the recent developments in wireless standards it is now possible to have both performance and encryption for your traffic, delivering optimal user experience and high levels of enterprise security. Maybe it's time to update your old, outdated wireless network?

3. How you get your users and possibly guests onto your wireless network is a big consideration. Understand who is going to be using your wireless network and look at suitable solutions to ensure secure but easy on-boarding. There are many solutions available for your corporate devices that allow centralised policies to be deployed – and for your guests or public, on-boarding portals will probably be the right way to go. Depending on your business this may even offer you marketing opportunities.

4. Understanding the applications and use cases will be critical to designing an enterprise-ready wireless network. Without this information, it is likely that you will struggle.

Areas of expertise

Virtualisation & Cloud

We design, deliver and protect custom-built virtualised solutions – bringing our customers the latest technology that allows them to focus on where their business is going, not just where it is!

Networking

We provide fast and secure networks for enterprises of all sizes and across all sectors, from education to heavy industry.

Microsoft Technology

Nobody knows more about how to maximise your Microsoft investment than ComputerWorld's engineers, most of which are MCSE-qualified or greater. Our team has been offering expert Microsoft solutions since day one and bring to the table an unparalleled amount of experience, whether you're looking to migrate to Office 365 or for traditional Microsoft services.

Desktop Transformation

IT departments are finding ever-increasing demand to deliver the flexible working environments their employees need to fully optimise their output. We work alongside industry leaders in business mobility to help businesses realise the true potential of their workforce and to combat Shadow IT.

Security

ComputerWorld's security consultants have all of the expert knowledge and certifications needed to offer businesses the most robust solutions for all aspects of IT security. We work in close partnership with some of the industry's most respected hardware and software vendors.

To find out more about how to future-proof your network, contact ComputerWorld today:

enquiries@computerworld.co.uk

01454 338 338

Apex House
Turner Drive
Westerleigh Business Park
Yate
Bristol
BS37 5YX

www.computerworld.co.uk

COMPUTER WORLD

Helping Businesses Define Tomorrow™

www.computerworld.co.uk | 01454 338 338