FUTURE-READY NETWORKING

INTRODUCTION

IS NOW THE TIME TO INVEST AND FOCUS ON DELIVERING THE NETWORK FOR THE FUTURE?

Enterprise networks are complex, only truly understood by the few who manage and administer them, and berated by the many for whom the problem is always "the network". Throughout the past two years "the network" has withstood the significantly increased demands and pressures of remote work, manufacturing and eCommerce activities.

This sweeping statement belies a complex reality. The corporate network of offices and buildings around the globe have often been dormant as few people have attended the office. And "the network" of which we speak is no longer a singular and proprietary entity, it is a "network of networks" that bridges traditional on premises environments to multiple clouds seamlessly at a global scale.

The requirements of the future network will be dramatically greater than that of the past. What exists today, that has adequately serviced the needs of the recent past must be transformed to meet the performance and experience demands of the future. As technology, operational and commercial landscapes change dramatically, is now the time to invest and focus on delivering the network for the future?

SETTING THE SCENE FOR CHANGE

Enterprise networks are complex and expensive to implement and run. Multiple comms rooms of spaghetti junction cabling typifies many business premises. But networking technology is going through a dramatic transformation, driven by software and automation driving convergence of network functions. There is also dramatic change to the traditional network backbone, fixed circuits giving way to internet-based connectivity. These factors strive to drive down cost, and increase agility, providing flexible services aligned to the business needs. Network uptime is giving way to assurance of network quality, and flexibility of connectivity is mandatory for a business required to support hybrid work, cloud computing and vigilant cyber security.

WORK FROM ANYWHERE, AT SCALE, WITH PHENOMENAL CONSUMER EXPERIENCE

Whilst always a requirement, the concept of work from anywhere is now different than ever before as a result of the COVID-19 pandemic. For users whom their workstyle permits, work from anywhere (home) is compelling for their own preference and benefit, and critically, an accepted mode of work. This is creating a multitude of impacts to the network, not only to enable and equip users to connect (securely!) from home or public WiFi to corporate resources via remote access solutions, but also the impact on existing corporate networks that are now much less utilised, but still represent a material business investment and operational cost to maintain.

To enable hybrid working has required a transformation in the way users work and collaborate, from primarily physical collaboration and asynchronous digital communication, to real time, virtual collaboration and communication, often over longer working hours. Much of the day is spent on Microsoft Teams or Zoom video calls. Even the traditional phone call has given way to video calling - all of which has added huge additional load onto internet and corporate networks.

Since this is a new normal , we must reconsider the mode and principles of remote access. The notion of a traditional VPN, tunnelling all traffic from the client to the corporate data center is outdated in a world where users and businesses rely on internet based services – perhaps even more so than services hosted from on premises data centers. "Zero Trust" is a fundamental operating principle in the face of cyber security threats from every angle (and Zero Trust Network Access (ZTNA) connectivity solutions are evolving legacy VPN based approaches to greatly enhance security and improve the user experience. Traditional architectures of corporate resource access from within the company office, protected by perimeter security solutions are challenged when neither users or applications exist only in static, company owned locations. This dynamic, location independent employee or IT user behaviour is driving the adoption of alternative convergent networking and security frameworks such as SASE as an alternative mode for remote access and enterprise operational security.

Knowledge workers are able (and starting) to return to the office and this brings with it a need to cater for remote working and office working with the requirement and expectation for performant rich collaboration and inherent security. For many users currently the reality is the performance of home WiFi surpasses that of the corporate WiFi. This delta in performance will see frustration turn to resistance in the return to office motion. If we want this to change, the corporate network needs to change.

THIS DELTA IN PERFORMANCE WILL SEE FRUSTRATION TURN TO RESISTANCE IN THE RETURN TO OFFICE MOTION. IF WE WANT THIS TO CHANGE, THE CORPORATE NETWORK NEEDS TO CHANGE.

FUTURE READY CAMPUS AND CORPORATE NETWORKS

Current corporate office networks are relics of the pre-pandemic era. For many WiFi is the default connectivity, which is a positive, but the networks are not scaled for the bandwidth and performance demands of today and tomorrow. We see this in pixelated video and sluggish speech of our office based colleagues, highly frustrating and ironic for those at home on consumer grade broadband which seems to deliver a better experience. Offices need to provide a "best ever wireless" experience if they are to even begin to entice users back with any sort of regularity or scale.

Consumption of public cloud resources is also dramatically different now than it was two years ago. Not just collaboration technologies but a transition to public cloud IaaS and SaaS resources has been underway quietly for many years – and this too accelerated during the pandemic era to underpin or enhance business processes. The stark reality is that in a post pandemic era, many businesses accept that office usage will not return to pre-pandemic levels, so office footprints are and will shrink. Rather than being burdened with expensive fixed lines, internet based connectivity and software driven solutions (SD-WAN) are becoming popular.

Cost reduction is always a key priority, ever more so with stagnated IT budgets, so operational efficiencies must be delivered. We see this in the network with the shift towards software defined networks (SDN), moving from complex configuration on physical switches and routers to centralised policy driven networks with automation at its core. Network deployment and configuration can be administered and pushed out centrally regardless of geography, and policy adherence and vulnerability controls supported by artificial intelligence (AI) and machine learning (ML) technology. The concept of AIOps is starting to come to the fore in several guises – DevOps, SecOps, CloudNetOps – which are changing and enhancing network operating models.

Another factor that is consuming attention is 5G. Though early in its maturity, and limited in availability, what was promised in terms of its throughput and low latency looks like it may deliver in the practice. 5G connectivity for some enterprises is worthy of active consideration and the major telco's are looking to push this out quickly to capture the market, perhaps before the use case, benefit and ROI is fully understood.

There is a potential use case for 5G to support hybrid working, enabling always connected remote workers access to the internet and corporate resources. But perhaps more appealing is the concept of private 5G across a campus environment. A private 5G spectrum across a geographically dispersed campus with the performance and latency benefits is enticing and may provide a new solution to assist with the challenge of legacy debt in existing network infrastructures, or provide the marriage of flexibility and performance to help develop new business ideas. There are particular use cases around healthcare and particularly manufacturing that are in active evaluation – particularly relevant for the transformation of Operational Technology (OT) infrastructures towards industry standard connectivity, and to unlock opportunities in IoT and Edge within the campus and beyond. The opportunity for 5G in IOT and Edge is a topic worthy of its own discussion.

OFFICES NEED TO PROVIDE A "BEST EVER WIRELESS" EXPERIENCE IF THEY ARE TO EVEN BEGIN TO ENTICE USERS BACK WITH ANY SORT OF REGULARITY OR SCALE.

THE NETWORK OF NETWORKS – INTERCONNECTING AND MANAGING CLOUD PLATFORMS

As public cloud emerged, corporate internet links enabled simple connectivity to these cloud resources, inadvertently helping to propagate shadow IT and other issues. There was a dramatic stand-up of cloud resources without much consideration of networking (let alone a range of other factors!). Whilst the initial set up of the cloud resource seemed easy, the reality was that the architecture was highly sub-optimal, often insecure, and for those services that survived the challenge of scaling became very quickly apparent. A modern enterprise will typically consume multiple public clouds, whether infrastructure or SaaS, and so the corporate network becomes a "network of networks" interconnected by the common internet. But each environment will have its own network configuration, each requiring some degree of administration and management. Businesses have complex competing demands to evaluate and trade off- the benefit and efficiency of native solutions and tooling, versus the case for a 3rd party solution to provide an abstraction from cloud lock-in, and to standardise processes for deployment, configuration and management. But this may come at incremental cost and introduce complexity.

Having wrestled with some of these challenges through the virtualisation era, when compute, storage and network disciplines needed to collaborate together, we have matured in recent years to bring engineering and operations closer together via DevOps and similar operating models, such as CloudNetOps which is relevant here. Convergence of technology is pushing (or forcing!) teams closer together to be more effectively in the delivery of services, and have wider spatial awareness of other parts of the technology or operational stack. Automation is imperative in this environment, and we have observed in recent years the technology providers changing from a stance of proprietary closed technology to a recognition of the need to work within broader multi-vendor ecosystems, enabled by APIs and code.

BIGGER STEPS TOWARDS A TRANSFORMED FUTURE NETWORK

For a lot of businesses there can be no doubt that there is significant "heavy lifting" required to ready and transform the network for current and future requirements. Whether this has the mindshare or investment focus or not, the demands for great user experience, performant consumer access to business services and the driver and benefit of cloud adoption are critical business priorities. The network is at the heart of realising those outcomes. And whilst occasionally referred to as "digital plumbing", perhaps a crude analogy, the metaphor works in so much as whilst it might not instantly capture the imagination for focus and priority, the criticality of the "plumbing" is well understood. So then we must act.

There are other emerging themes that warrant consideration and mention. First is the concept of "Network as a Service" (NaaS). The "as a Service" concept is well understood and applied to networking technologies creates opportunities for businesses to consume modern network capabilities without the financial challenges that the transformative activities above would introduce a with downstream operational upside.

There are clearly a range of scenarios for a "NaaS" solution, from the purist, cloud model requiring significant technical maturity, to a commercial and service construct around traditional technology as an extension of traditional managed service arrangements. As is the general argument, the benefit case for "aaS" may suit some types of organisations, but there will also be many for which it won't.

Moving forward toward future network transformations leads to another concept gaining traction and being hyped by the vendors – that being "Intent Based Networking" (IBN). IBN would pull together some of the principles above in terms of automation, cloud and intelligent technologies like AI and ML to action network configuration and policy based on understanding the desired outcome of the network consumer (user, device, or other "thing"). This concept of an intelligent, dynamic network which has the agility, speed and assurance to anticipate and react to the demands placed upon it with limited constraint is a vision for the future where the network becomes invisible and intelligent and at the heart of technology driven business processes and engagement models.

There is a lot to do from where we are today. How much of this vision is required for your business, and how we can better align network capability and outcomes to your business agenda in order to secure the investment in technology and operations required to support continued growth and success?

About Computacenter

Computacenter is a leading independent technology partner, trusted by large corporate and public sector organisations. We help our customers to source, transform and manage their IT infrastructure to deliver digital transformation, enabling users and their business. Computacenter is a public company quoted on the London FTSE 250 (CCC.L) and employs over 17,000 people worldwide.

Computacenter

Computacenter (UK) Ltd
Hatfield Avenue, Hatfield, Hertfordshire AL10 9TW, United Kingdom

computacenter.com
+44 (0)1707 631000