Dispelling the myth: future networks

Steve Masters, VP, Customer Innovation
June 2017
Contents

1. Future networks overview .................................................. 1
2. Why move to future networks? ............................................. 2
3. Customer challenges .......................................................... 3
4. Taking steps towards building a future network ....................... 5
5. Business benefits of future networks ..................................... 7
6. Why BT? ............................................................................. 9
7. Appendix: future network technologies defined .................... 10
1. Future networks overview

Digital transformation is a priority for today’s businesses. It helps open up new opportunities through transforming costs, improving customer experiences, making operational efficiencies and creating new business models.

CIOs implementing a digital transformation strategy are facing new technology challenges and choices. Migrating to new platforms such as cloud, supporting global connectivity (including mobile platforms), and securely managing and making sense of the ever-increasing amount of data, all needs focus.

CIOs that know their organisations need more flexibility and agility to succeed, are already taking advantage of cloud-based IT services and applications. But they are struggling to get their infrastructure to deliver the rapid response, easy collaboration and constant innovation the digital business needs.

Future network technologies offer a new way to build and manage networks that are fit for the digital age – more flexible, affordable, easier to manage and secure.

This paper looks to dispel some of the myths that surround future networks, and how BT’s Dynamic Network Services are delivering future networks that enable you to optimise and transform your network to meet your challenges – today and in the future.

Future network technologies offer a new way to build and manage networks that are fit for the digital age – more flexible, affordable, easier to manage and secure.
2. Why move to future networks?

**Embracing the cloud**

Cloud is the business model of the future for all organisations. Cloud services offer a new way of consuming, developing and locating services in a fast, efficient, flexible and cost-effective way. Newer organisations can quickly set up shop based purely on cloud consumption, and flourish unencumbered by traditional ICT models. More traditional organisations can gain competitive edge and move quickly into new areas or markets by adopting bi-modal ICT practices, allowing new areas of the business to move ahead quickly in its consumption of new cloud services.

**Reducing ICT spend**

Bandwidth demand continues to grow year on year causing organisations to look to cheaper internet services and potentially compromise quality for cost. Large scale adoption of cloud services is also driving more use of low cost public internet services and the subsequent acceptance of those services for business functions.

**Increased flexibility and agility**

Businesses today are dynamic, and cloud adoption gives organisations increased speed and agility. They can turn on new services across the globe, in new geographic areas and new markets very simply and quickly. But network resources typically are out of sync with the cloud capabilities. Typically referred to as the ‘longest pole in the tent’, they set too long a timeframe for delivery to new markets. Customers are looking for parity between network resources and cloud services to bring new locations or branches online in much shorter timeframes. Also new applications such as Machine-to-Machine (M2M) and Internet of Things (IoT) are exerting more pressure on existing network infrastructures, and there’s a need for tighter security and management of end devices.

**Coping with increased demand**

Bandwidth demand is growing significantly year on year. Everything from higher quality imaging to hungrier applications puts pressure on the networks whether they are public or private. With on-demand services difficult to deliver effectively, customers are seeing their network costs potentially growing but not necessarily becoming more flexible.

**Launching new business applications**

As businesses transform, they typically develop new applications on cloud platforms and consume from cloud providers. They are then looking at introducing these new applications in an agile, secure fashion and without impacting existing business applications.
3. Customer challenges

As more applications move to the cloud, businesses push into new and wider geographies and quality is diluted by hybrid.

How do you get from where you are now, to where you want to be?

While it’s clear that digital is now a boardroom priority – and indeed, for many, a competitive imperative – everyone is at a different stage and transforming at different speeds. But wherever you are on the journey, you know it’s crucial to have the right technology environment and service approach underpinning your digital strategy. And that it needs to be flexible, agile, intelligent, cost effective and secure.

Do you really know what applications you’re running?

As the move to the cloud happens, organisations typically experience a reality check on the actual number and complexity of the applications the business is running. Most organisations will then run an application rationalisation programme, and see a need for far greater visibility of specific applications, their performance and the customer or user experience. Tools in this area have historically been disparate, expensive and with a lack of available skills to act on the information provided. As more applications move to the cloud, businesses push into new and wider geographies and quality is diluted by hybrid. There is a greater dependence on, and need for, an integrated toolset with better application visibility and enforcement of corporate polices on approved application use.
Lack of security control in the cloud, regulatory/compliance issues, and lack of cloud usage visibility.

Do you understand the policies and regulatory regimes you need to operate under?

As more personal data travels across cloud infrastructures and potentially unsecured mobile devices, legal frameworks and regulations are rapidly being put in place to protect customer data from exposure. New regulation encourages organisations to build in security by 'design', not by 'default', but business strategy doesn’t always align with security strategy, causing potential gaps and vulnerabilities. CIOs don’t always know exactly what makes up the corporate IT estate and end up spending more time maintaining existing systems than searching for new solutions. And, of course, many are hindered by vulnerable legacy IT.

Do you know how to secure your data and its usage?

CIOs still face three key concerns around cloud: lack of security control in the cloud, regulatory/compliance issues, and lack of cloud usage visibility. As the digital world continues to grow, and traditional security perimeters start to vanish, critical and personal data has become more widely distributed and at risk from threats. The use of shadow IT is becoming more prevalent, with increased risk from insecure cloud services and applications. Moving to the cloud means that visibility and management of user security, endpoints, data and applications needs to be coordinated with a wider set of parties and working cultures in order to protect your data and your customers’ data, regardless of where it resides or where it travels to.

It also means that if customers are not already doing so, they need to understand their security landscape so that they can comply with new regulatory requirements such as GDPR, which comes into effect in May 2018.

Finally, as the attack surface and the amount of telemetry from endpoints, security and network devices grows exponentially, it’s vital that customers are able to make sense of that vast amount of data in real-time so that they can protect their critical assets and data from attack by having actionable intelligence.
4. Taking steps towards building a future network

The journey to building a network infrastructure that will support today’s and tomorrow’s cloud business applications is a complex one. With a range of new technologies to support this, there are some fundamental steps that businesses should be taking now.

Step one

Hybrid networking

One of the first steps you can take is to adopt a strategy to move towards a hybrid networking environment – blending quality of service bandwidth with internet bandwidth. With the demand and growth in bandwidth consumption, the most cost-effective way of achieving this is to expand the capability in a hybrid fashion. With a choice of quality or non-quality routes and with the range of tools available either traditionally (appliance based) or in virtual function format, applications can ultimately be routed by the right route, to get the appropriate quality, at the right time of day, month or week.

For example, hybrid networking could involve offloading certain non-priority traffic to allow appropriate bandwidth for the ERP system to crunch the end of the month numbers.

We offer a hybrid solution which combines a market leading private network with a market leading internet solution, to ensure that your hybrid solution offers the perfect balance of performance and agility, security, scale and cost.

We offer you the building blocks to the perfect hybrid solution.

Step two

Cloud Connect access

Cloud is here and it’s centre stage, with nearly every organisation gaining advantages from cloud services. With 90% of our largest customers planning or already using multiple cloud services, our Connect services allow you to seize the opportunity to implement and realise benefits for your organisation faster than ever.

BT Cloud Connect provides pre-provisioned infrastructure with inbuilt security into leading cloud software as a service (SaaS) providers and infrastructure as a service (IaaS) providers in 13 cities in nine countries. This can allow customers to quickly connect their cloud environments to their corporate networks with either IP or MPLS bandwidth. The service has the appropriate security and acceleration services built in as virtual functions.
Step three

**SD-WAN**

In today’s world, the amount of data moving around the network is just growing and growing, and the lines between business and personal are blurring. We all have multiple devices and use them to connect to applications wherever we are. And that puts a strain on networks.

If your organisation is struggling to get critical applications performing at their best, it’s likely you’re not getting the most out of your network.

Organisations supporting global remote or branch networks should start to categorise their sites into specific site types. In profiling these sites for specific applications, business processes, worker types and personas, we can build a picture of the type of network needed to support this infrastructure.

We have started to build hybrid infrastructures with Cloud Connect access that provide users with access to their cloud-based services. This means we could look to build a picture of how an SD-WAN solution could simplify current, complex, multiple appliance-based locations with a simpler, lightweight, feature-rich solution.

With the ability to connect quickly and securely to base over either quality, internet or 4/5G, new sites can be up and running and generating revenue much quicker than traditional site builds. In many cases the enhanced tooling capabilities embedded with the SD WAN device on site can provide the data analytics for dynamic traffic routing and prioritisation. How the SD-WAN tools work with other cloud usage and management tools is also vital to complete end-to-end diagnostics.

Step four

**A Network Function Virtualisation (NFV) strategy**

NFV is probably the least tangible in the market today due to its position on the development curve. But it is something customers should be thinking about and planning for now.

Organisations should look at the shelf life of their existing estate and ascertain what appliances are going to be ‘end of life’. The viability of the existing estate to run virtual CPE capability should also be assessed, and we can deliver this through our Agile CPE portfolio. For example, some routers have the ability to run blade server cards on which smaller numbers of virtual network functions become viable. The key challenge is balancing the cost of the device with enough processing power to negate any future needs.

At BT, we’ve already taken significant steps to deliver on the promise of NFV/SDN and SD-WAN with our Dynamic Network Services. For example, with our Cloud of Clouds strategy, we’ve provided cloud acceleration and cloud security, giving customers a speedy, secure connection to their cloud apps. Having worked with BT to ascertain the best roadmap to NFV, early pilots should be considered with our capabilities. Depending on location (distance from BT’s edge network) and access (typically fibre), there’s an option for capability to be hosted within BT’s network. This moves the functionality from the branch into the network.
5. Business benefits of future networks

When organisations transform their network into a future network, what benefits will they see? Having deployed a hybrid network with BT’s Dynamic Network Services, our customers find they gain:

**Flexible infrastructure**

Fundamentally, customers will have a secure, flexible infrastructure that can support their current and future cloud migrations. Changes will be more in line with the set-up, take-down, moves, adds and changes of speed and agility that most cloud vendors provide. As the organisation moves more services to the cloud, the infrastructure can flex to accommodate change.

**Simplification**

Using a combination of SD-WAN and NFV, site IT and telecoms domains can be greatly simplified. For new sites, a simpler build can be specified, and for existing sites, complex, multiple appliance-based environments can be simplified with a combination of SD-WAN and NFV capabilities depending on the site size and type.

**Speed and agility**

Using a combination of SD-WAN and NFV, the speed at which new sites can be set up, old sites shut down and the network re-configured increases accordingly. By deploying an SD-WAN device on site, it has the ability to quickly connect in the first instance via either Ethernet/MPLS, Internet or 4/5G, and be configured centrally. There is potential for new branches to be up and running, and generating revenue, in weeks rather than months. As NFV matures, we will have the ability to deliver the x86 hardware to the location and then add, remove or upgrade network functions from a central location. In the example of a BT managed service, virtual acceleration devices could be dragged and dropped in order to triage a network connection suffering unexpected congestion.
Secure and compliant

Using the internet will only ever increase the need for security. It also increases the complexity and challenges around being compliant with new legislation such as GDPR that increases protection of sensitive customer data and carries major financial penalties for breaches, as well as personal consequences at board level if the right prevention steps have not been taken. The evolution to a hybrid WAN environment requires a complete re-think of the security architecture, its scope and the controls applied at the network, application, user and device levels due to the existence of multiple Internet points and remote access gateway needs. This gives rise to the need to understand the existing security landscape and develop a new security strategy to deliver those controls. A well-designed and robust network architecture, where security is designed as the key foundational piece of that architecture will help to protect you. Not only does it need to protect you from threats coming from both outside and inside your organisation, but it should also operate without performance degradation and be flexible enough to support your evolving business. Using a big data analytics service to monitor that network, the endpoints, security controls, users and applications and combining that with third party intelligence information will be key to providing the visibility of those threats so that you can act quickly to pre-empt attacks before they occur or identify and respond in real-time.

Reduction/simplification of ICT skills

SD-WAN solutions are designed to be quickly and simply installed by less skilled staff and auto-discover and connect back to base. With a simplified branch infrastructure, less expertise will be required at remote or branch locations. NFV solutions will ultimately provide the platform to deliver virtual functions, reducing the need for truck rolls and again less expertise required at remote sites. With the move from CLI changes on devices the abstracted management and orchestration capabilities are available to a less technical audience. For example, as part of a BT managed service, sites can be polled on a regular basis, proactively looking for pinch points or application bottlenecks and application traffic can be assigned more bandwidth or re-routed to a higher quality of service.

Cost effectiveness

Hybrid networks provide a cost-effective way of dealing with the increasing demand in bandwidth. By expanding Internet capability, typically provided locally at all sites, application traffic can be routed effectively and according to the agreed SLA. For latency sensitive or real-time applications (e.g. voice and video) the appropriate quality of service bandwidth can be provided. Other lower priority traffic can be offloaded to the Internet and the two routes can be flexed during peak times. Hybrid also offers a more cost-effective way to achieve resilience, and SD-WAN and NFV solutions allow greater management and control of the network with fewer people.

Agreed service levels

BT’s Dynamic Network Services comes with a range of on-board capabilities that provide greater visibility of traffic profiles and application data. These enhanced management capabilities allow us to manage specific business processes far more accurately and maintain greater service levels.

Innovation

As more customers have requirements for M2M connectivity, and more and more IoT endpoints, SD-WAN networks can quickly and easily build over-the-top capability for these new services. SDN overlays can provide persistent connectivity for devices and the appropriate security alternative to IPSec networks.
6. Why BT?

BT has deep experience of the networking business. Our portfolio strategy, the Cloud of Clouds, is a powerful combination of cloud services, IT integration skills, global network and professional security expertise. It allows our customers to connect easily and securely to the applications and data they need, regardless of where they’re hosted or where our customers are based.

We were there at the beginning of several generations of new communication technologies, and SDN/NFV is no exception. We worked on its creation and continue to develop the technology in partnership with other global telcos and leading IT vendors to make sure it delivers for our customers.

Now, with our new secure and resilient networking vision and our Dynamic Network Services roadmap, we’re helping CIOs extend all the flexibility and agility of the cloud to their global communications infrastructure, and build a business that can flourish in the digital age.
7. Appendix: future network technologies defined

**Virtual CPE (V-CPE)**

Typically, the first step towards replacing appliance-based network functions such as routers and firewalls on customer sites. This could be blade server technology deployed in existing capable routing appliances and capable of running a Virtual Network Function such as a firewall or acceleration capability. As services mature, the capability will likely be a generic x86 PC hardware device. Depending on the abundance of high speed fibre, these devices could be located in service provider nodes at the edge of their network (deployable now for limited virtual functions).

**Network Function Virtualisation (NFV)**

In the first instance, these are software or virtual versions of traditional appliance-based network functions such as firewalls, routers, acceleration devices, application management capabilities. They will sit on Virtual CPE, typically either blade servers deployed in traditional appliances or on generic x86 hardware platforms deployed on customer sites or, depending on fibre access, at the service provider edge node.

**Software Defined Wide Area Network (SD-WAN)**

An edge technology with multiple access capability that’s controlled and managed from a central function. Typically, with low or zero touch installation, it will allow connectively by cellular, Internet or traditional WAN (Ethernet/MPLS). It will then allow specific application, policy-based routing, providing application efficiency typically in a hybrid environment. With a range of on-board tools, SD-WAN devices generally provide application visibility and performance, and the ability to dynamically allocate or change application priorities from the central control function (well developed and deployable in the market).

**Software Defined Network (SDN)**

The ability to programme the network from a central control capability and dynamically deploy, increase or decrease bandwidth. Typically deployed within data centres and high-speed fibre networks, but now being deployed within the core of most Network Service Providers. This technology will allow the same (or similar) flexibility in the wide area as the cross-connect does within the data centre.