

Now and Next - Connect

How connectivity can help businesses
now and looking ahead to the future



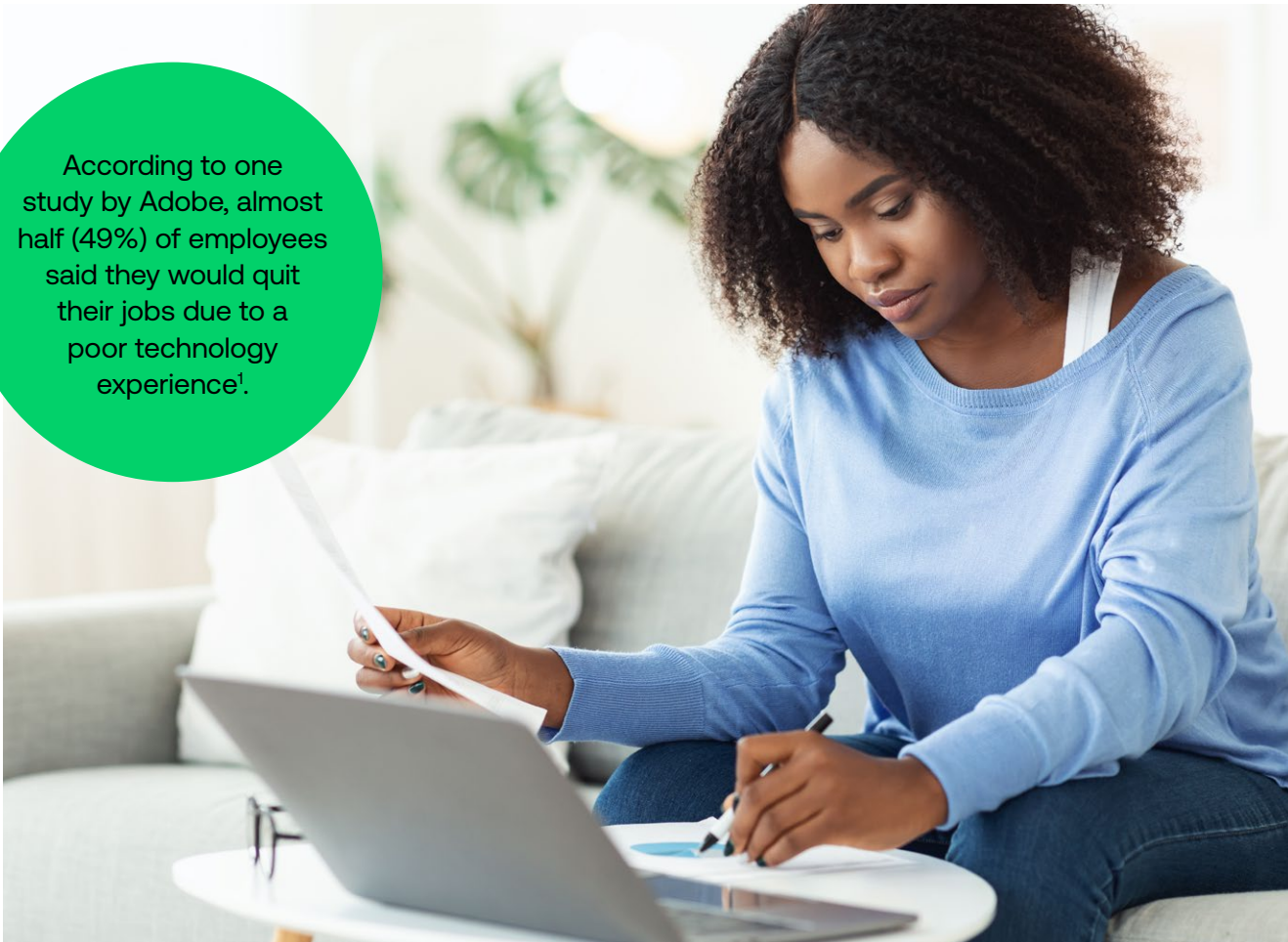
Putting connectivity at the heart of the organisation

The importance of effective connectivity

Whether it's working from home, on the move, or in the office, reliable connectivity is the bedrock of modern productivity. Connectivity has a direct impact on business productivity because the more time people spend waiting for data to be processed, dialling back into calls, or waiting on the phone to speak to IT Support, the less time they're spending on the activities that make up their jobs. Poor connectivity is also a huge source of frustration at work that impacts not only the employee experience but also retention.

Currently, many organisations will have some kind of dedicated physical WAN, like IPVPN or MPLS. With the accelerated use of cloud apps and tools as well as wider digital transformation initiatives, there is a drive towards changing the underlying connectivity infrastructure. At the same time, employees and customers say they do not really care what that infrastructure looks like so long as it works.

Powerful communications tools which work over mobile and on-site are key to keeping connected, allowing employees to collaborate effortlessly with your customers and each other 24/7, wherever they choose to work from.

A woman with dark curly hair, wearing a light blue sweater, is sitting on a white sofa. She is looking down at a document she is holding in her left hand, while her right hand is on a laptop keyboard. The background is a bright, modern living room with a white sofa and a potted plant.

According to one study by Adobe, almost half (49%) of employees said they would quit their jobs due to a poor technology experience¹.

1. [Adobe study](#)

Next generation connectivity looks beyond traditional WAN

There are options such as SD-WAN, hybrid with MPLS or through-internet enabled by building blocks such as Ethernet and fibre. Blending some of these forms of connectivity infrastructure can give you a robust, reliable, high performing and cost-effective network.

Cellular connectivity – whether 4G or 5G – should also be a key consideration for businesses connectivity infrastructure. It's particularly useful in sites that are difficult to access with traditional fixed connectivity. Or where rapid set-up of sites is required, such as for retail stores or construction sites. Or for new connectivity requirements like disparate IoT sensors.

Private cellular networks

There is also huge potential for businesses to utilise private cellular networks. These are custom-built networks designed to provide dedicated, secure connectivity across their sites. To-date, these have predominantly relied on 4G connectivity.

But with the introduction of 5G, there are opportunities to develop new use cases thanks to the higher speeds and far lower latency compared to 4G. These next-gen features are critical for deriving value at scale from applications like autonomous vehicles, robotics, AI and automation. In turn, the rewards from such investments will be increases in productivity, operational efficiency, and better health and safety practices.

As with the roll out of any new connectivity technology – whether that is SD-WAN or 4G IoT or 5G private networks – the promised benefits are intrinsically dependent on the degree to which that connectivity is secure.



SD-WAN



4G IoT



5G private networks

How things could change back at the office

Despite the shift towards hybrid or remote working, there is still the good old office or physical workplace to consider. In particular, how might these new ways of working put a burden on your legacy office infrastructure. Many employees have more devices now than they when they 'left' the office at the start of the global pandemic. They have, no doubt, become used to using them in different ways like calling via Teams, Webex or Zoom more than they ever would have done before. This has worked fine from home, where traffic routes straight through the internet and so (a) the quality of the session is generally good and (b) it doesn't create an overhead for the LAN.

But with wholesale changes in how people use technology (and the demands to use it as part of everyday tasks), bringing employees back to the office may place a much greater load on the traditional connectivity infrastructure. Rethinking how people can connect at work could involve investing in higher-bandwidth WiFi.

Or reconfiguring WAPs that were set up pre-pandemic and now need to reflect a change in working practices, such as the increase hybrid working, collaboration via video calls and people using multiple devices at work.

Changing role of the service provider

Service providers have always had more in their locker than the core connectivity infrastructure. They have provided many of the managed services that made that connectivity work for individual business requirements. Yet an increasing number of organisations are investigating ways to gain more visibility or control over their network services.



Moving from legacy networks

This can be addressed – in part – by moving from legacy networks such as MPLS to SD-WAN, which offers visibility and control at the application layer. Being ‘software defined’, it also promises the ability to make swift changes to service. Deciding on the right level of control over the network is still highly dependent on what the organisation needs. If you opt for a fully managed service from your service provider, it offers an increased level of security and peace of mind knowing that your network is in safe hands. There is, of course, the associated management costs as well as the need to live with the provider’s timescales for MACs. In some cases, it may be preferable to take back some level of control or acquire the ability to make changes yourselves. If you are minded to do so and look after certain elements ‘in-house’ there are some key considerations for co-management:

- Define what will be managed in-house and what will be managed by the service provider, with clear roles and responsibilities
- Consider the best ways this approach can add value (Perhaps your service provider can take away the more labour intensive tasks to free up your internal teams for other important projects, which will involve amended SLAs and terms and conditions to ensure both parties are protected, along with adjusted pricing and potentially a rate card for agreed activities)
- Agree roll-back processes in the event anything goes wrong
- Ensure you’ve got the right platforms in place and that the right people have the right level of access to those platforms
- Assess whether you have the necessary in-house skills to support the day-to-day management of the network (The savings from not paying for a fully managed service could soon be overcome by the costs and resources required to manage tasks and retain those skills)
- Ask if your service provider could help to keep your people up to date with their training and consider joint training initiatives that build on the understanding on both sides of the partnership
- Agree methodologies and processes such as how will you deal with different situations, who will resolve them and what with the SLAs look like
- Introduce a change control board for both parties to participate in

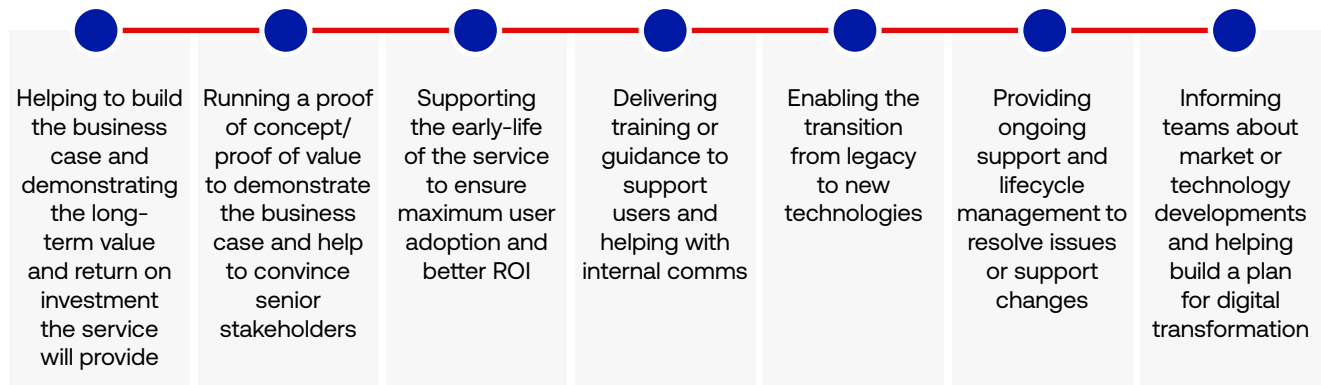
Future considerations for connectivity

Plenty of organisations made rapid investments at the beginning of the global pandemic to get people set up and able to work from home quickly. However, uncertainty about the best ways of working moving forwards means some of those organisations are delaying investment decisions and rolling over current contracts while they assess their options.

Weighing up the costs and benefits

It's important to weigh up the cost/benefit of investment compared with the cost/benefit of doing nothing. Instead of seeing their service provider as a supplier, those looking for longer-term value and additional support in making the right investment decisions are placing more faith in service providers. For service providers then, it is no longer enough to just sell connectivity or connectivity services.

They must be in a position to offer support across every stage of the contract lifespan:



Progressive customers expect a service provider to remain relevant in order to become a truly trusted partner. One area that service providers can demonstrate this is through advice on connectivity and beyond. Since connectivity, collaboration and security are all interlinked, it is rare that a decision in one area does not affect what happens somewhere else. The role of a trusted advisor is further enhanced by advice on what investments the organisation should be prepared to make in the coming months and years.

The role of machine learning and AI

The connectivity networks of the future will use advanced algorithms and smart analytics driven by machine learning and AI. They will use these technologies to self-triage, self-heal and self-optimize, ensuring critical traffic, i.e. services and applications, are optimized. AI will automatically monitor network data using real-time insights into the users, devices and applications, speeding up troubleshooting and ensuring optimal network performance.

By using AI in this way, service providers should be well-placed to bring together experience in managing the wider network with your own pool of knowledge to add value. For example, enabling your own network to self-manage and optimize via automated processes will free up your IT team to address real business problems or facilitate internal innovation. This also opens the door for lower operating costs by reducing the internal resources required for network management.

The importance of security

As the use of automation improves and expands into most areas of connectivity, security will become critically important. With workers using a wider range of devices, network and endpoint security should adapt to changing habits and workstyles. AI-powered, cloud-based endpoint security can keep you ahead of real-time threats, following the user rather than the network and applying a security blueprint anywhere on any device, enforcing a consistent security policy at all times.

Your organisation will need to liaise with its service provider to coordinate sophisticated approaches to potential cyber threats, such as integrating the threat-hunting skills of the provider's SOC analysts.

The connectivity networks of the future will use advanced algorithms and smart analytics driven by machine learning and AI.



Want to talk?

By working with you, we can help you and your people achieve more – right now and well into the future. We'll go beyond being just your connectivity provider. Instead, we'll respond to what your organisation needs as your digital business partner.

Talk to your account manager today or call us on **0800 955 5590**

For more insight into how your business can leverage technology to solve problems now and into the future, discover more in the Now and Next series:

Now and Next – Empower



Now and Next – Protect



Glossary

AI – Artificial Intelligence

IPVPN – Internet Protocol Virtual Private Network

MACs – Moves, Adds, Changes

MPLs – Multiprotocol Label Switching

SD-WAN – Software-defined Wide Area Networks

SLAs – Service Level Agreements

SOC – Security Operations Centre

WAN – Wide Area Network

WAP – Wireless Access Points

© Virgin Media Limited and/or Telefonica UK Limited 2022. Any intellectual property contained within this document is either used under licence or is owned by Virgin Media Limited and/or Telefonica UK Limited. 20220922