NETWORKING+

UK set for Terragraph multi-gigabit technology

UK enterprises could soon be offered 10Gbps services using Facebook's Terragraph technology, thanks to a raft of wireless internet providers.

The project is part of Facebook Connectivity, a division of the social media corporation that is responsible for network investments, high-altitude platforms, the Telecom Infra Project (TIP) and other initiatives. Terragraph promises low cost broadband delivery at speeds of over one gigabit, with the potential for over 10 gigabits using license-exempt fixed wireless access (FWA) in the UK by the end of 2020.

Members of trade association, the UK Wireless Internet Service Providers Association (UKWISPA), have met Facebook executives plus officials from equipment makers Siklu, Radwin and Cambium to discuss service launches.

They want to use this for licence-exempt fixed wireless access (FWA) in the UK from later this year, said the association. Siklu, Radwin and Cambium Networks are all set to ship products this year, UKWISPA added.

Facebook has been developing this technology for around five years and has built pilot systems in several countries around the world using prototype equipment. Now, the Silicon Valley giant has attracted a range of global equipment manufacturers to form a whole ecosystem around the technology. One example is global silicon manufacturer, Qualcomm, which has developed a high volume, low cost chipset (802.11AY-based) to enable the high data speeds needed to facilitate Terragraph affordably. This has enabled a range of UKWISPA members to release products in 2020, while others, such as MikroTik and IgniteNet, have been encouraged to commit to joining the community.

David Burns, chairman of UKWISPA, told *Networking+* that the general rule with networking performance is to introduce the fastest speeds possible, "so 10Gbps is a very reasonable goal today" subject to affordability.

"Enterprises invest heavily in communications systems of many types and spend surprising amounts of capital and time investing in bandwidth management methods such as quality of service (QoS)," he said. "Investing in QoS is an admission that the enterprise has insufficient capacity at the right place at the right time. For example, ensuring vital voice services operate smoothly and cleanly at all times is an obvious imperative. But what if this is at the expense of other time and bandwidth sensitive applications that support remote workers?"

Burns added that VPNs and remote desktop services "are also very sensitive to the jitter and latency" typified by over-contended networks "and most QoS techniques crudely reserve minimum data commitment rates".

He continued: "As more workers spend more time out of the office and as more internal and external meetings become online meetings, fast networks will become more important than having desks, chairs and an office to keep them. In the end, 10Gbps of internet connectivity will be far more valuable and cost a lot less than the empty desks abandoned by home workers."

"Facebook recognised that new applications require high speed connectivity and, with data consumption growing at an ever-increasing rate, the demand for broadband cannot be matched by the current ability to build new high-speed networks," added Neeraj Bhatia, product manager at Facebook Connectivity.

Enterprises ready for Terragraph multi-gig tech

Continued from page 1

"With Terragraph, Facebook is creating an ecosystem to address this gap and serve under-connected communities. We helped assemble a technology stack with a range of partners, assisted with spectrum advocacy and the specification of 802.11AY standards, and built an industry ecosystem to realise the potential for this technology."

Terragraph networks are built on very high-speed resilient mesh equipment, where a small low power device is mounted on a building or street furniture and communicates with up to 16 other units on other buildings to form a mesh." Burns said, "this method perfectly complements fibre build out", where the Terragraph mesh fills gaps that would be expensive to install otherwise.

"As a mesh, data can pass in all directions at full speed, meaning upload and download speeds are symmetric and the mesh can tolerate breaks without stopping," he added. "Moreover, it is so fast that it can seamlessly blend with fibre to create a fully hybrid network that suits the local conditions. UKWISPA members are itching to install Terragraph services to help more customers across the country and to upgrade their existing customers to gigabit speeds and complement their fibre plans." ■

Survey reveals 75% of UK firms using AI, but challenges persist

A new survey has revealed that three quarters of UK enterprises are actively leveraging or testing artificial intelligence (AI) today.

The Artificial Intelligence in Europe Survey, conducted by colocation data centre services provider, Interxion, showed that enterprise roadmaps for AI deployment over the next two years are already quite concrete. Despite this, many enterprises are looking to ramp up their AI efforts, but lack the appropriate infrastructure to do so.

It also found that by 2022, 31.4% of UK enterprises intend to use AI for an initial application while a further 19.0% expect to use it in various fields. In addition, around one-third (30.6%) expect to be testing AI in their companies.

"As we continue to shift toward an increasingly digital society, the appetite for AI is growing," said Patrick Lastennet, director of enterprise at Interxion. "By automating processes, delivering new strategic insights, accelerating innovation and improving customer experiences, AI has started to revolutionise industries and UK enterprises are starting to adopt it. As AI use becomes more pervasive, ensuring that the infrastructure is also evolving to properly support the applications will be crucial to future success."

The survey further revealed that infrastructure requirements for implementing AI vary from one industry to another. However, it is clear that for all enterprises, optimising infrastructure

The Artificial Intelligence in Europe Survey, conducted by Interxion, showed that enterprise roadmaps for AI deployment over the next two years are already quite concrete

is critical. Decision makers are seeking solutions to ease the bottlenecks, such as incalculable costs, AI-optimised IT

equipment and experienced personnel.

The Artificial Intelligence in Europe survey polled 500 IT decision makers in the UK. ■

Windstream adds next-gen firewall VNF to SD-WAN offering

Windstream Enterprise, the provider of managed communications solutions, is giving its VMware VeloCloud SD-WAN service a virtual next-generation firewall.

The Arkansas-based firm added next-generation firewall capabilities to is VMware VeloCloud-based SD-WAN service in early August. The new offering aims to fortify customers' WANs from increasingly sophisticated security threats.

"A security breach can be costly and damaging to brand reputation. Even a single incident can inflict long-lasting damage to a company's reputation," said Layne Levine, president at Windstream Enterprise, in a statement. "This new VNF [virtual network function] firewall managed service gives CIOs another tool to secure the networks at all locations without having to endure the time-consuming process of installing and maintaining separate security hardware."

Mike Frane, VP of product management at Windstream, said the firewall is based on a third-party offering, but he didn't disclose which security vendor Windstream was working with.

The firewall is offered as a managed or co-managed service running as a VNF. This allows Windstream to eliminate the need for additional security appliances at the branch. Instead, the firewall will run in tandem with its existing VeloCloud-based SD-WAN offering on VMware's SD-WANEdge appliances.

Furthermore, the firewall will work with Windstream's WE Connect network management portal, which enables customers to manage their network from a single unified interface.

Levine also said that Windstream will continue to roll out new functionality to its managed SD-WAN service to meet customer demand. ■

The firewall is offered as a managed or co-managed service running as a VNF. This allows Windstream to eliminate the need for additional security appliances at the branch

Vodafone and Defra launch 5G-ready NB-IoT forest sensors

Vodafone has partnered with the Department for Environment, Food and Rural Affairs (Defra) and Forest Research - Britain's foremost forestry and tree research organisation – to use a narrowband-IoT (NB-IoT) network to monitor forests the in the north and south of England.

Both networking technologies that will power the industrial Internet of Things over the next five years are narrowband IoT (NB-IoT) and Cat-M (officially known as LTE Cat-M1). In addition, it is predicted that industrial IoT use cases will overtake the likes of wearables, home security and digital home products, by 2025.

The pilot, which is being carried out in Surrey and Northumberland, will use NB-IoT technology, future-proofed to work on 5G networks when available, to monitor how trees respond to environmental changes within the UK's forests.

"Tackling climate change requires radical thinking and our forests will be vital to this," said Anne Sheehan, director at Vodafone Business UK. "Our IoT technology enables us to connect trees and monitor performance, which is a perfect example of how technology can be used in new ways to help create a more sustainable future."

Data is collected from IoT sensors which are attached to the trunks of a number of trees, with data then being transmitted to Defra and Forest Research where the effects of temperature, humidity and soil moisture on tree growth and function will be monitored.

"Trees are a unique natural resource that play a crucial role in combating the biodiversity and climate crises we face," added Malcolm McKee, chief technology officer at Defra. "This exciting partnership uses newly-emerging IoT technologies to improve our understanding of the impacts of environmental change on our nation's forests, which will help inform our policy making. The new technology provides better quality data and importantly, allows us to monitor places that current technologies cannot reach."

The three month trial is now underway in Forestry England's Alice Holt forest, near Farnham in Surrey, along with Harwood forest, near Rothbury in Northumberland.

Meanwhile, Vodafone partnered with Aurrigo, which develops and manufactures autonomous vehicles, to create a driverless transport service from the clubhouse to the opening tee at this year's ISPS Handa Wales Open. Vodafone will provide 4G network connectivity to the shuttles. ■

'IoT devices put workplace privacy at risk'

Almost three quarters (74%) of IT decision makers believe that IoT devices in the enterprise pose a significant threat to workplace privacy, according to new research.

A report from Kollective called Distributed Devices is based on a survey of 270 UK and US-based IT decision makers and claims to explore the challenges and risks of incorporating IoT devices into business ecosystems.

The research investigates how IT teams can ensure all devices at the edge of their networks are reached securely, effectively, and at scale. While the majority (88%) of IT teams said IoT devices will make their workplaces more efficient, there are also substantial concerns regarding the infrastructure required for updating these devices. Failure to update will add significant security risks for businesses, as well as adding to employee privacy concerns.

Kollective's report suggests that this will place significant pressure on IT teams and 88% of respondents said IT departments hold full responsibility for updating and securing these devices. In addition, 90% of respondents said that all IoT updates

While the majority (88%) of IT teams said IoT devices will make their workplaces more efficient, there are also substantial concerns regarding the infrastructure required for updating these devices

should be tested before they are installed.

"The growing prominence of IoT within enterprises has significantly raised the number of entry points for cybercriminals," said Kirk Wolfe, VP of corporate development at Kollective. "In order to maintain workplace privacy and counteract any future threats to businesses across the globe, it's imperative that these devices are updated with the latest security patches – and it's the IT team that's on the front line of defence." ■

Box boosts cloud security with automated classification

Box said an "intelligent, automated classification" will soon be added to Box Shield, the firm's advanced security solution for protecting content in the cloud.

It will now automatically scan files and classify them based on their content to help businesses detect and secure sensitive data. Box Shield is the fastest growing new product in the company's history and security-conscious and highly regulated organisations including NASA use it to secure data in the cloud.

Chief product officer at Box, Varun Parmar explained how businesses are using Box Shield to protect their content from ending up in the wrong hands.

"The sudden shift to remote work has surfaced new security challenges for businesses, making it more critical than ever to keep sensitive data from getting into the wrong hands, Parmar said. "In June alone, Box Shield helped customers protect their content by blocking shared link access to classified files over eight million times and prevented close to a million downloads of classified files. Using advancements in machine learning to automatically apply classification labels as files are uploaded or edited extends Box Shield's ability to enable secure remote work from anywhere. This allows IT and security teams to configure and enforce policies across the enterprise at a new level of scale that would be impossible to tackle manually."

Using advanced machine learning and data leakage prevention capabilities, Box Shield scans files in real-time when they are uploaded, updated, moved or copied to specified folders and automatically classifies them based on admin-defined policies. Businesses can leverage its new automated classification feature to scale their data classification efforts and enforce policies across the enterprise to better comply with GDPR and other regulations. ■

Secure Access solutions keep businesses running

The COVID-19 pandemic has driven a massive shift in workforces everywhere. While work from home had been the exception rather than the rule, it suddenly became standard practice for a variety of industries, including healthcare, education and government.

Secure Access solutions keep businesses running by enabling safe remote computing and connecting people to the data center and cloud applications. The 2020 Remote Work From Home Cybersecurity report examines how enterprises are responding to accelerated WFH adoption during the COVID-19 pandemic and shares key challenges, concerns, strategies and anticipated outcomes.

The report surveyed more than 400 cyber security decision makers, ranging from technical executives to IT security practitioners and representing a balanced cross-section of organizations of varying sizes across multiple industries. 33% of these companies anticipate some positions moving to permanent remote work and over half (55%) plan to increase their budget for secure remote work in the near-term.

But this rapid migration may have elevated the risk profile of corporate network environment. IT may not have been able to keep all endpoints within policy requirements, such as software/anti-virus updates. Many endpoints may have been purchased outside the usual channels and may not be close to your minimum security posture policy. When the workforce inevitably returns to the office, enterprises should consider the risk of these endpoints. Pulse Secure is scheduling a live webcast that explores best practices to help enterprises enable secure access for their workforce, whether they work remotely, or when they connect back into the office. Secure access, continued visibility, protection and productivity continue to be the primary objectives as companies determine their future network necessities and objectives.

Pulse Secure is scheduling a live webcast that explores best practices to help enterprises enable secure access for their workforce, whether they work remotely, or when they connect back into the office. On September 16th (4pm GMT), Teddy Nicoghosian, Director of Technical Marketing will discuss the results of the 2020 Work From Home report and share the benefits for companies when implementing implement Pulse Zero Trust Secure Access for remote and office workers.

Register to attend.

ZERO TRUST REMOTE SECURE ACCESS
for Home and Office Workers

Live Webcast
September 16, 4pm GMT
Register today !

Pulse Secure   www.pulsesecure.net

Ribbon launches Connect offering

Ribbon Communications has launched Ribbon Connect, a portfolio of subscription-based, as-a-service offerings. It supports Microsoft Teams Direct Routing and allows voice-calling capabilities in the Microsoft Teams collaboration platform. Greg Zweig, Ribbon's director of solutions marketing, said the Ribbon Connect portfolio announcement is "100% a result of partner feedback" and "there's a reason" this is a whole portfolio of offers. "Many partners told us they were in different places in their journey to offer Teams-based solutions," he said. Zweig added that the new Ribbon service gets partners to market sooner with a complete offer.

Security specialists release new solution

Cybersecurity specialist SonicWall is launching a new solution combing high-performance firewalls, cloud-native management and on-premise threat analysis to deliver cost-effective security for complex business networks.The Capture Cloud platform combines a number of technologies including SonicOS 7.0 and Network Security Manager (NSM) 2.0, to provide increased visibility, management and control via all-new user interfaces. It stops the attacks that target big networks using its Capture Advanced Threat Protection (ATP) and machine learning technology (RTDMI). The solution also meets corporate, industry and government compliance regulations by keeping data on-premises.

TiKTok to build data centre in Ireland

TikTok, the embattled Chinese video-sharing app that's found itself at the centre of Washington-Beijing tensions, is setting up its first data centre in Europe with a £378m investment in Ireland, the company said. Promising to create hundreds of jobs, improve "the safeguarding and protection of TikTok user data" and shorten loading times for users in Europe, TikTok said that once live, European user data will be stored at that location. The company established its EMEA Trust and Safety Hub in Dublin earlier in the year and said the new investment "signals our long-term commitment to Ireland." It is expected to be operational by early 2022.

Covid-19 exposes UK cyber security vulnerabilities

UK SMEs are at risk of 65,000 cyber security attacks daily – with around 4,500 of these being successful – and the figure could be much higher since the beginning of Covid-19. The findings come from a new report by global recruiter Robert Walters and data provider Vacancysoft – Cybersecurity: Building Business Resilience – which claims that the cost of data breaches to UK companies is around £2.48 million per instance. Highlights of the study are: 65,000 cyber security attacks on UK SMEs daily, 4,500 are successful, data breach costs UK companies £2.48m per instance and 48% of UK companies do not have adequate cybersecurity to support home working.

SD-WAN is key enabler for 'new normal' remote workforces

The Masergy SD-WAN market trends report has revealed that SD-WAN adoption continues to grow – for the third year running - with an ever-increasing interest in managed and co-managed offerings to navigate the complexities of an integrated network and security system. Digital enterprise software-defined network and cloud platform provider Masergy conducted the survey between May 28 and June 3, 2020, questioning 107 executives who held the title of director or above in an IT or IT security-related role and were employed in a multinational organisation. The research revealed the challenges posed in a work-from-home environment during the Covid-19 pandemic. It concluded that it was not surprising to see the transformative impact of SD-WAN and increasingly deployed SASE systems become the new necessity for achieving secure remote access and reliable performance for cloud applications.

'Majority of UK businesses dangerously overconfident over cybersecurity readiness'

Many businesses are at risk from bot attacks—despite an awareness of the problem and a widely held belief that they have the problem under control, according to new research from Netacea, the bot detection and mitigation specialist. The report, The bot management review: The challenge of high awareness and limited understanding, surveyed businesses across the travel, entertainment, e-commerce and financial services sectors. It found a high awareness of how bot attacks could negatively affect a business, with over 70% understanding the most common attacks, including credential stuffing and card cracking, and 76% stating they have been attacked by bots. However, these same businesses revealed that around 15% of their web application resources are taken up by bots. Businesses were also wholly unaware of the marketplaces where their customers' usernames and passwords can be bought and sold, with only 1% of respondents being familiar with them.

Vodafone and Trend Micro offer 'Worry-Free' cyber security

UK telecom giant Vodafone has expanded its business security services to include protection for business customers' laptops and desktops. It has partnered with Trend Micro, adding the security vendor's Worry-Free detection service to its security offering. The aim of is to protect businesses and their employees from online security threats such as ransomware, out-of-date applications and phishing attacks on desktops and laptops. This new service is available to new and existing business customers of all sizes and is compatible across Windows, Mac, Android and iOS devices as well as Microsoft 365, G-Suite, Box, Dropbox and Salesforce cloud services.

Faulty UPS at data centre housing LINX

One of the DCs that houses the London Internet Exchange (LINX) suffered a major service outage affecting customers across the hosting, cloud and telecom sectors. The incident was caused by a faulty UPS system followed by a fire alarm (no fire was reported or recorded) that powered down Equinix's LD8 data centre, a low latency hub that was formerly the Telecity Harbour Exchange. Located on London's Isle of Dogs, the facility caters to hundreds of clients and is positioned close to the city's financial institutions. LINX's members include ISPs such as BT, Sky and Virgin Media.

Word on the web...

Contingency planning: Alan Hayward, sales and marketing manager at SEH, explains three key lessons learned from the Covid-19 crisis...

To read this and other opinions from industry luminaries, visit www.networkingplus.co.uk

Don't think...

...how much you want to reduce your environmental footprint and total operating costs with one standalone solution.

Act!

Get the highest active power needed for your IT applications, with sustainability built in.

Liebert® EXS 10-80 kVA UPS:

- Reduced TCO
- Compact footprint
- Installation flexibility
- High efficiency operation

Vertiv.com/LiebertEXS_N

VERTIV™

Security versus productivity

Iain Shearman, managing director at KCOM, explains what he describes as the 'double-edged sword of the cloud'

As organisations continue on the road to digital transformation, there's a key consideration, which is the extent to which they adopt hybrid multi-cloud technology platforms. This technology approach often brings several benefits to organisations and productivity improvements is most definitely being one of the greatest.

However, it's not always straightforward and adopting the cloud is not without security and implementation risks as it often presents plenty of bugs that need to be resolved. This means that firms are at the mercy of hackers until bugs have been dealt with and 'transformation' is completed. So, as businesses adopt the cloud, what are the strategic challenges they face; how do they keep data safe; and how can firms foster a progressive culture that enables them to evolve while maintaining productivity and IT security?

The modernisation challenge – integrating 'old' with 'new'

It should be natural and obvious but, as organisations integrate new technology alongside legacy infrastructures, they need to ask what their strategy is. Failure to do this could result in irreparable problems down the line. To illustrate my point, in January 2019 the largest collection of breached data in history was discovered, consisting of more than 770 million email addresses and passwords. It serves as a stark reminder of the scale of the problem. These events are increasingly making headlines across the globe and the problem will not disappear.

The size of the organisation is immaterial. Attackers have become so sophisticated that no business can claim to be 100 percent safe. One such sector under attack is retail. It is one of the most targeted industries and entices criminals with a rich pool of data to steal. This is because it's easy to identify individuals and their payment information. Moreover, what makes this scenario worse is that retail is undergoing one of the greatest transformations it has experienced in decades. Therefore, organisations moving to the cloud need to develop a robust and secure cloud strategy.

Security by design

When approaching IT security within this cloud world, it is crucial that organisations consider their attitude and approach. Regardless of size, they need to appreciate that, despite their best efforts, systems will never be entirely secure while threats continue to evolve and they will need to constantly evaluate and improve security.

Within this new mindset, firms need to take a 'security by design' approach, instead of 'by addition'. This is because, to be truly effective, it is insufficient to retrofit cybersecurity into systems. By analogy, when designing an office building, you think about access and cabling and power distribution in advance. The option to retrofit is there. But it is expensive, inefficient and runs the risk of leaving some areas unprotected.

Since cybersecurity is mission critical, it stands to reason that organisations need to provide the due attention and care that it warrants. This means clarifying the separation of layers and functions. In the case of WAN environments, the desired outcome is that they reinforce one another, instead of masking blind spots or creating joints that are a point of weakness, where threats can infiltrate systems.

Engaging the right culture

The concept of a physical office as a perimeter is dated. Most organisations have capabilities to operate virtually and staff can now work from almost anywhere. And, while the cloud is mostly responsible for driving these productivity benefits, it creates security threats too.

Verizon's 2018 Data Breach Investigations Report cites human error as the cause of almost 20 percent of data breaches. Whilst almost 75 percent of attacks are perpetrated from outside an organisation, more than 25 percent involves insiders. Employees are often pinpointed as targets to obtain data, which makes it vital to educate colleagues about cybersecurity.
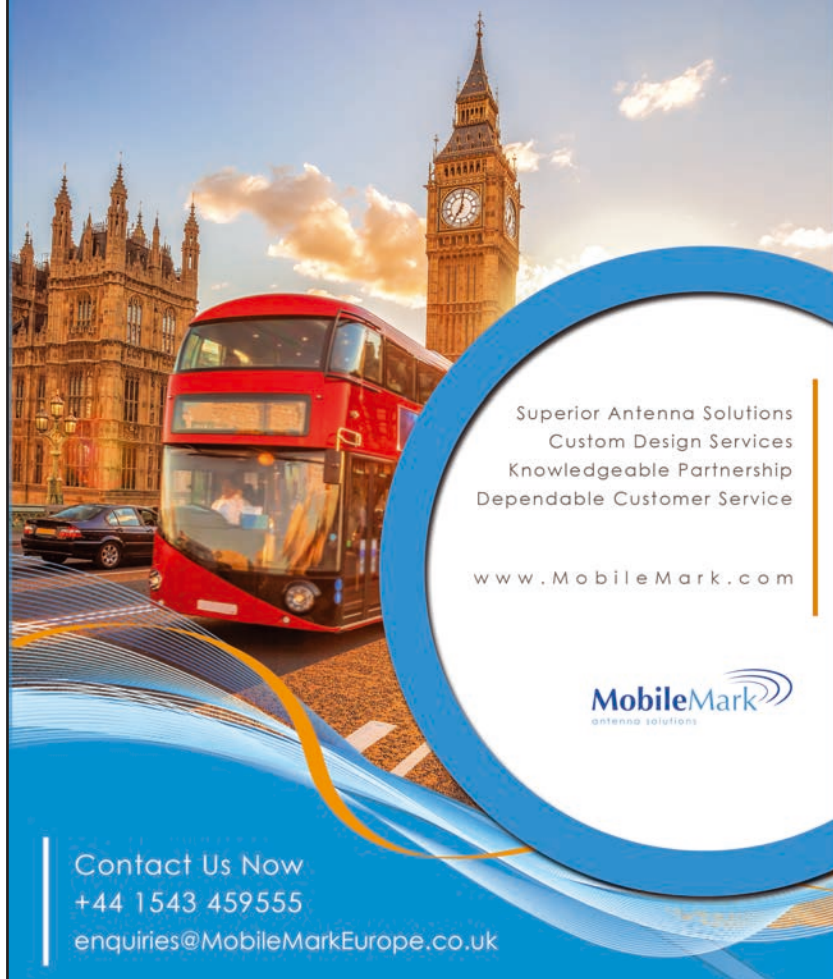
Therefore, security culture within organisations requires strong and meticulous nurturing. If executed effectively, it will transform security from a one-time event into being a positive part of the firm's culture. This is because people are the weakest links in any organisation when it comes to security. And, although computers - for the most part - do as we programme them to, people on the other hand, generally do not. This makes the need for a robust security framework even more necessary.

Within this framework, and cloud-centric world, organisations must continually focus on educating employees about IT security and raise awareness across the entire organisation, not just IT. They need to unify the business to work together to keep information secure. Moreover, helping employees to understand the implications of a cybersecurity attack will also highlight the importance of diligence. An organisation's security will only ever be as strong as its weakest link. This makes it vital to ensure that the technology, culture and people responsible for data are all working to best effect to keep data safe, while the organisation strives to improve its productivity. Every technology and person has a role within a wider cloud strategy.

Iain Shearman, MD, KCOM

Turning data centres green

Vik Malyala, senior vice president, Supermicro

Imagine 350 tons – that's three times the average weight of a blue whale and the amount of e-waste that could be saved annually by typical enterprise data centres. The energy that could be saved would even provide a big city with light. Looking at the reality, only 12% of today's data centres are green. A puzzling number, given that a sustainable approach would not only help the environment by reducing e-waste and consuming less power but also save data centre operators millions of pounds. With data centres playing such an essential role in our data-driven world, the challenge is to align their ecological footprint with sustainability targets.

Today, there are more than eight million data centres. Every year, they not only dispose of tons of hardware but they also account for about 1-1.5% of the global power consumption. This proportion is comparable with the level of carbon emissions of the airline industry around the world (before the pandemic). If the industry is not starting to take actions to reduce these numbers, chances are that in 10 years the energy consumption of data centres could make up more than 10% of the world's electricity supply.

An increasing number of industry leaders and future-oriented companies already develop innovative solutions to approach this issue. However, there are still various missed opportunities when it comes to data centre efficiency. According to a 2019 green data centre survey undertaken by Supermicro, only 12% of today's data centres are designed for optimal power consumption. This can cost operators of data centres up to 400,000 pounds per year, for example, due to older equipment. For 50% of survey respondents the success factors that are more closely associated with green data centres, such as Power Usage Efficiency (PUE) or IT Asset Lifecycles, aren't taken into consideration as measurement, due to the focus for many being on ROI and TCO of the hardware alone without considering the data centre.

Today, data centres don't have to be the "bad guys" in the green discussion anymore. Many businesses don't seem to know all the options they have today. In the past couple of years, the industry has joined the green movement and created optimised server technologies, architectures for data centres and cooling techniques supporting this mission. They allow data centre operators to increase efficiency while reducing energy needs to a minimum. Some of the various technologies are better known than others.

One path towards greener data centres is the implementation of Resource Saving Architecture: it's based on a disaggregated server design that allows individual components to be swapped out or upgraded independently. This eliminates expensive refresh cycles by focusing on upgrading what is needed to make the infrastructure optimized for their workloads, and improves PUE at the data centre level due to better thermal design.

In addition to the disaggregated server design approach, there's also the option to increase the rack power density. Multi-node and Blade systems allow for more servers to be fitted into a smaller space thanks to their shared power supplies and fans (instead of rackmount servers with individual power supplies). It reduces the costs of cooling and can result in efficiency gains of up to 20%.

Dealing with data can work up a sweat – literally. While the average temperature of data centres lies around 23°C–24°C the survey has shown that more than a third of the data centres measure temperatures between 25°C and 29°C. With increasing temperatures rises the risk of overheating the servers which could cause performance degradation and impact user experience negatively. Plus, data centres thrive at colder temperatures. Thus, developing superior techniques to handle the heat - that are effective and sustainable - is crucial.

Free-air cooling is a common solution, whereby outside air is diverted inside the data centre requiring less air conditioner equipment in the server rooms. The energy savings can be significant, varying from 4-5% for every 0.56°C increase in server inlet temperatures. This can translate into savings of up to 12.000 pounds for the largest inlet temperature increase when looking at the annual OPEX savings per rack.

Alternatively, liquid-cooling is gaining popularity and reduces PUE immensely. Compared to more traditional air-cooling, it increases the processing per square foot and can reduce the OPEX by half. The latter due to the removal of provision power needed that would be necessary to keep the fans running.

Cooling and an increased rack power density are essential factors and a good starting point when it comes to optimising data centres from an energy perspective.

Companies must realise how big their impact is on the environment and that both sides benefit from more eco-friendly data centres. With 5G on the forefront and a growing number of IoT devices, it's clear that our data consumption won't reduce – rather the opposite. So, let's make sure we manage a smooth transition towards a world with green data centres.

Keeping the blues and twos connected

The UK can be hit by a terrorist attack or natural disaster with little or no notice - so how equipped are the emergency services should the worst happen? Robert Shepherd finds out

Britain's location in north-western Europe has meant that, luckily, the natural disasters it experiences are, comparatively, not as serious as some of those that routinely strike other parts of the world. However, that's not to say we're immune – after all, the British Isles are prone to storms, floods and of course, terrorist attacks.

Given we could be hit by something anywhere, at any time and likely with little or no warning, its paramount that the emergency services are able to maintain connectivity to save our lives.

Mladen Vratonjić, chair of TCCA, a membership organisation which represents all standard mobile critical communications technologies and complementary applications, says every business, organisation and government should have a business continuity plan to protect operations should they be affected by an unplanned event. The event could be a natural disaster such as an

earthquake or flood, or unnatural such as a terrorist or cyberattack.

"It is often said that there are three 'Rs' of the greatest importance for any critical telecommunications network: resilience, reliability and recovery," he says. "These are achieved through some more 'Rs' - redundancy and robustness. There is no overall standard classification for a mission or business critical network – however mission critical networks are those essential for some mission accomplishment (mostly public safety), and business critical networks serve businesses that cannot operate without reliable communications. To meet those requirements, there are technology standards that have been designed specifically with resilience at their core – these include TETRA, P25, Tetrapol and DMR – all well-established narrowband systems leveraged for both mission and business critical networks around the world.

Earlier this year, the Home Office handed a year-long contract to APD

Communications to develop critical software to integrate blue light organisations and other public services with the forthcoming Emergency Services Network (ESN).

The plan is to replace the UK's existing TETRA-based Airwave network and the Home Office is leading a cross-government programme to deliver it. The rationale behind the decision was to provide police, fire and rescue and ambulance services as well as other public safety organisations with voice and data services. At the time, Mike Isherwood, managing director, APD noted that while he was delighted with the contract because it acknowledges its LTE services, "it will be down to each individual service to make the transition, supported by our software solution".

APD's mission-critical communications and control solutions are used by more than two thirds of UK police forces, as well as other emergency

services organisations.

Indeed, Cambridge-based Sepura supplies TETRA technology to emergency services around the world and a firm official explains the benefits of radio over other methods of communication during a critical situation. "Radio works on an independent infrastructure, so not susceptible to call overload, system failure, etc," says a company spokesman. "It is a robust system, designed to withstand extreme weather. It can also be supported by temporary network infrastructure to support if needed, particularly in remote areas that are often the epicentre of a natural disaster. Critical comms radios are robust and will keep working in hot, wet or dirty environments, and can suffer rough treatment much more than other communication systems. They also use encrypted voice comms to ensure comms are kept confidential." He adds that data applications can be developed

to work over the system to integrate with back office systems. TETRA radio systems also enable co-operation between agencies using that platform – "often police, fire, ambulance, rescue and other emergency response organisations".

Traditionally and unsurprisingly, the largest users have been public safety organisation – police, fire, ambulance, rescue organisations. After all, they need it more than any other group, business or sector.

The Sepura spokesman says the specific requirement for a critical communications platform are where there is a risk to critical national infrastructure, a risk to life, or a risk to business operations. "Where these conditions/risks exist, there is a need for a communications system with greater functionality that can be provided by standard cellular phones or low level radios," he adds.

Another key player in this space is from TCCA member Motorola Solutions, which kits out emergency services around the globe. Ricardo Gonzalez, responsible for the international core strategy (outside the US) points out that Land Mobile Radio (LMR) has long been the best communication method in disaster-stricken or conflict zones. "The evidence for this is that it enables instant, reliable communications with high capacity in areas where cell phone towers are down or even where there are none at all," he adds that despite the fact LMR has been present for some time, it continues to evolve for changing times and many countries are planning to continue to operating their nationwide LMR networks for the next 10-15 years.

So, how is the network maintained and how can the services be guaranteed it will work at a critical hour? On the first point, Gonzalez says that LMR system management has come a long way since the days of analogue-only radios and manual support services. He adds that maintaining today's software-centric LMR system requires a new set of tools and expertise. "This paradigm shift brings its own set of challenges, benefits and considerations. Monitoring a network 24/7 is a heavy burden for many organisations, as their internal IT support staff is simply too small to provide around-the-clock service. These kinds of organisations often partner with an outside service provider who can provide the necessary support," he says.

As far as the second point is concerned, Gonzalez claims that a mission-critical network is purpose-built to withstand multiple failures before communications are affected and is specially designed for multiple levels of active redundancy. Examples he gives are alternative energy solutions for radio base stations such as solar panels, batteries, and generators, as well as alternative linkage between base

So, if the network is safe and it can be deployed in pretty much any situation, is there a question mark surrounding the technology itself?

stations such as satellite or microwave. "When all else fails, our LMR devices will also work in local fall-back-mode if the network does go down," Gonzalez says.

Almost a year after the devastating terrorist attacks that took place in London on in July 2005, Rajant Corporation from the US took part in a critical communications technical demonstration. The goal was to stream video from a tube tunnel back to the surface and Rajant says its system beat other competitors, streaming video back topside within 15 minutes of starting.

Nevertheless, the Sepura spokesman says there are landscapes/terrains/regions where critical comms are more difficult to deploy than others. "Every system deployment is unique," he adds. "Systems have been installed across nations (and indeed allowing interoperability across national borders), on offshore oil rigs, in underground mines, on super-fast train systems, in ski resorts and in locations where buildings are designed to protect from natural disasters. Part of the process of designing a system is to understand where potential problem areas may exist and to mitigate any potential issues with them."

Gonzalez argues that one of the biggest advantages of a modern LMR network is the ability to operate in the most difficult terrain. "That being said, it is extremely important to choose the right kind of technology and form of deployment to fit different kinds of geographies and use cases," he says. "For example, a dense urban area with large amount of users is quite different from remote rural areas. We like to see ourselves as technology partners, helping our customers find the best communication solution to fit their exact needs."

So, if the network is safe and it can be deployed in pretty much any situation, is there a question mark surrounding the

"It is often said that there are three 'Rs' of the greatest importance for any critical telecommunications network: resilience, reliability and recovery."

*Mladen Vratonjić,
chair,
TCCA*

technology itself? Do the handsets/radios need to be updated regularly and just how much of an investment is that? The Sepura spokesman says "it really depends" on how and where the radios are used. "On a less busy site the radios might rarely be upgraded, whereas police users might look to set up a radio much more frequently, based on operations taking place at that time," he says. New innovations are always being brought in to support users in these cases – for example over the air programming, enabling radios to be updated whilst connected to a secure, approved Wi-Fi network, reducing the time radios are out of use."

We've managed to get this far without mentioning 5G. Prior to the introduction of Covid-19 and possibly Brexit, you'd be hard-pressed to find a topic more often talked about that the next generation technology. Of course, the UK has taken one step forward and two steps back with the way the government has handled the Huawei row. However, it's still slated to be with us in the not too distant future and once it is, Ken Gold, director of test, monitoring and analytics at Exfo, which develops test, monitoring and analytics solutions for operators says the new technology brings the promises of more resilience. "5G network slicing would be used to ensure the performance of mission critical services," he says. "Virtualised 5G core and edge networks will accelerate the implementation of required changes. Remote orchestration of new virtual resources as well as changes in traffic routing and moving critical services to the edge will improve service availability and reduce the need for truck rolls—keeping personnel out of the danger zone. Continuous monitoring and orchestration of the services and network will ensure critical services are maintained and the customer's essential communications needs are met."

The good news is we definitely have, or will have, technologies able to handle the very worst situations, but in the words of James Trevelyan, SVP global sales – enterprise at communications solutions provider Speedcast says disasters of any kind are impossible to predict, making short-term communications that connect emergency services throughout every stage of the response efforts critical. "High-speed, uninterrupted connectivity that enables voice, video, data and IoT solutions can be the difference between the success or failure of a disaster situation," he says. "With rapid response

times necessary, communication networks that are quick and easy-to-deploy are imperative.

For many critical communications, satellite remains the method of choice – particularly in areas where the internet access and cell towers have been knocked out as a result of a disaster. Trevelyan adds that as satellite communications become faster, more reliable, cheaper and are able to offer lower latency, disaster recovery operations and critical communications will become more streamlined and tactical than ever before. After all, teams that are better prepared, better equipped and that can work well together in challenging circumstances have a better chance of saving lives than those that are not.

"Low Earth Orbit (LEO) and High Throughput Satellite (HTS) offer first responders a way to establish short-term, easy-to-deploy communications anywhere at any time. "Due to the speed in which emergency services need to react and take control of the situation, solutions that can be brought online within five to 10 minutes and allow them to gain coverage immediately are vital," he continues. "When a disaster strikes, the first action of the emergency services is to create a local hub to re-establish critical communications and ensure they can stay connected through the entire recovery process. Once the disaster response team has established an on-site base, resilient trucks – similar to those used in broadcast – will be driven to the disaster area to create an emergency services network. A quick-deploy antenna mounted to the roof of the truck will be used to provide a satellite link to connect to the nearest cell tower to provide phone services and internet services so responders can better communicate at the scene."

It's a view shared by Martin Jarrold, VP international programme development at GVF, the global trade association for the satellite industry, who says any underlying assumptions that the need for emergency/critical communications in the event of natural disaster only applied to countries with poorly developed, fragile, or vulnerable communications infrastructures have been overwhelmingly challenged in the context of UK flooding, storm damage, and wildfires. "In these contexts, it has been a combination of different, but related, satellite technologies that have been important: communications, navigation, and Earth observation/mapping," he says adding that the Integrating Space Assets for UK Civil Resilience project is part of ESA's Integrated Applica-

tions Promotion (IAP) programme, which develops value-added services by integrating space assets in these areas.

"In the one example of the Saddleworth Moor wildfires, near Manchester, raged for over three weeks in June to July 2018, covering an area of 7 sq. miles of moorland at its peak," Jarrold continues. "Far above the moors a range of satellites invisibly helped to monitor the spread of the fires and coordinate the responses. The EU's Copernicus Emergency Management Service provided detailed maps of the fire, and imagery was also provided by the Airbus UK-operated, UK-built Disaster Monitoring Constellation."

Jarrold says such systems can give responders strong situational awareness using various services in combination, such as "rapid mapping of affected areas using satellite imagery, bolstering resilience of communication networks using satellite communications, enhancing traffic management for evacuations and other activities, coordinating intelligence for asset management, with everything from ambulances and trucks to flood barriers tagged with GPS".

Avanti Communications is a well-established vendor of satellite technology across Europe, the Middle East and Africa. Kyle Whitehill, the company's CEO, says for the first responders and those working in the emergency services, access to secure high-speed connectivity is critical. "Emergency services personnel often rely heavily on mobile internet access," he says. " However, limited network infrastructure, especially in rural and remote locations can affect speeds, reliability and access."

Whitehill cites Avanti's Project HYDRA offering, which provides a secure 4G mobile network that is transportable and enables rapid deployment, whilst ensuring coverage, no matter the location. "HYDRA provides a private and secure high speed 4G overlay network anywhere in the UK," he says. "The project also supports 2G and 3G devices and as it's a completely transportable network and can be deployed wherever it's required.

The service provides a complete small cell network that can operate in both standalone (private) or interconnected (roaming) modes. It has a range of up to 2km and can securely transmit data, make calls without interference and even locate disaster victims using the signal from their mobile phones."

Whitehill explains how Avanti's HTS link delivers end users with up to 60Mbps download and 20Mbps upload speeds and provides full coverage of the UK. "This technology is highly transportable and quickly deployable, both of which are vital criteria for critical situations emergency services," he adds. "Project HYDRA was the world's first hybrid small cell technology combining the latest software and hardware to provide ubiquitous coverage of Ka-band satellite."

Critical to the success of the communications function, however, is the strength of the security culture within the services and its ability to align closely to the security operation within it. Even if the network is in place and the kit is working properly, Trevelyan highlights the need for secure systems for always-on connectivity

"With no knowledge as to when and how a disaster will occur, preparation for connectivity loss is essential," he says. "There's a need to ensure that security has been implemented at every stage to safeguard against any loss of connectivity – particularly those that provide critical services and have a legal obligation to be online at all times. With

a multitude of instances that could cause them to fail, operators need to keep these systems secure and adopt robust and reliable connectivity solutions. In these environments, the Internet of Things (IoT) allows for the systems to check in every second to ensure constant connectivity."

He says power networks predominantly work off terrestrial connections, however all of them will have a diverse technology at all critical sites including solutions such as very-small-aperture-terminal (VSAT) satellite links for critical backups to keep any connections live in the event of a problem with the network. In the event of a disaster, an outage of power could prove detrimental to the UK so operators need to ensure that the systems in place are well-protected and that they have dormant links on standby in preparation for any unprecedented issues.

"High-speed, uninterrupted connectivity that enables voice, video, data and IoT solutions can be the difference between the success or failure of a disaster situation."

*James Trevelyan,
SVP global sales – enterprise
Speedcast*

Let's hope we remain disaster-free for as long as we can, but it's certainly good to know we're in safe hands. ∎

Reaching the city limits

Three English cities get smart with major infrastructure upgrades

CTIL and O2 partner up with iWireless Solutions

Working in partnership with CTIL and O2, iWireless Solutions was asked to design and deliver a world leading, free outdoor Wi-Fi network within the Square Mile. The multi-million-pound project is part of one of the largest investments in wireless infrastructure ever seen in the UK, providing workers, residents and visitors with the ability to access digital rich content in a dense urban environment. This work was inclusive of any column work, such as replacing for suitable height columns, as well as dealing with the power needed to bring the kit live. The existing Wi-Fi solution was insufficient to meet today's data demands, which required the new system to be radically different. iWireless Solutions designed a Wi-Fi system with a dynamic, self- organising, fully resilient, gigabit capable backhaul. This meant the introduction of 28GHz Metnet technology from CCS to create the world's first mesh network of its type and scale. The area, the size of the Square Mile, includes many key London landmarks such as St Pauls, Guildhall and The Gherkin, as well as major transport hubs like Liverpool Street and Cannon Street.

Early January 2017, iWireless Solutions was instructed to start working on the design of this prestigious project, a series of surveys were conducted to understand and model the Wi-Fi coverage and capacity requirements within the Square Mile. The design was created using our bespoke in-house tools which gave further insights to data demand, increased accuracy and supported process automation. This allows us to provide a quick turn around on design amendments due to the ever-changing environment in the City without compromising quality. Through the iWireless design process 9000+ street assets needed to be reviewed, from which a selection of 130+ suitable street locations were to be included within the design, these included streetlighting and CCTV columns of which 30+ required replacement. To achieve fully resilient connectivity with the required density, it was necessary to include a further 20 locations where it was proposed to install bespoke new street columns.

Following the successful design of this landmark wireless network, iWireless Solutions was awarded the deployment of this project: installing, commissioning and optimising the entire wireless network within the Square Mile.

The successful delivery of the final solution was achieved in collaboration with CTIL, O2, Virgin Media and the City to ensure all stakeholders were onboard. Close collaboration with the incumbent street asset contractors (Tyco and JB Riney) ensured work was carried out to the strict client processes and expectations.

SuperConnected Cities Programme helps fund public WiFi in 22 UK cities

There are many towns and cities utilising public Wi-Fi solutions in various forms with ranging areas of coverage both in the UK and worldwide. In fact, pick up any august tech publication or visit a relevant website and you'll see that 'smart cities' or 'connected cities' feature somewhere.

This is very true in many northern English cities, which are investing heavily in various comms technologies in a bid for parity with more affluent parts of the country. Yet while many projects are announced from the rooftops, some cities, councils and other relevant authorities are keener to keep their powder dry. In other words, some information is in the public arena but much of it is not. The following details some that our cities have completed via the SuperConnected Cities Programme and published information about the previous implementation in Barnsley.

Through the SuperConnected Cities Programme, the following 22 UK cities were successful in obtaining funding and have implemented public wi-fi solutions.

Barnsley implemented the following: The Barnsley Free Wi-Fi project was a joint venture by AWTG Ltd and Barnsley Council. AWTG teamed up with Barnsley council to roll-out a free Wi-Fi service to the town centre. AWTG planned, deployed and tested the network and completed the deployment of the free WiFi network in the summer of 2011 and did it for free as a research and development exercise to test off-loading 4G traffic onto wireless. The network was planned to run for a minimum of two years and was hoped to attract shoppers into Barnsley town centre and encourage people to use the Internet to see the benefits that this could have to their everyday lives. AWTG took less than 6 months from conceptualization to going "live" to the public. It was the first ever free network of its kind in the UK. AWTG provided support, monitoring and troubleshooting of the network to provide round the clock availability for the users in Barnsley.

Project connects Sheffield to free, superfast Wi-Fi network

Ruckus Networks, an ARRIS company, got involved in Sheffield City's free-to-use, superfast Wi-Fi project. Working collaboratively with Idaq Networks – it runs the network - and Siklu, a player in millimetre wave radio technology, the project creates a virtual data ring-road around the city, transmitting high-speed capacity between tall buildings, before bringing it down to street level to be used by residents.

The project delivers superfast internet, at 20 gigabits per second (Gbps), to 293 streets in the city and up to 24,000 users can connect simultaneously. The network is free, and at no cost users or to the council who provided exclusive access to street furniture and buildings to install the network. The network can also be leveraged for other commercial opportunities to help fund the service.

As cities across the UK compete to attract tourists and businesses and access the £2.4bn investment announced during the autumn budget for the Transforming Cities Fund, free Wi-Fi is an important part of the equation. "Free Wi-Fi networks are crucial to helping all residents engage with the opportunities available online," explains Mark Gannon, director, business change and information solutions (BCIS), resources portfolio, Sheffield City Council. "We believe we have a responsibility to give all residents the ability to access information and services online so they can carry out tasks such as applying for jobs or benefits. It's also important for supporting our businesses and entrepreneurs as it should increase footfall in the city centre."

The network is future-proofed and has the ability to support future council-led projects such as footfall tracking, traffic management, and smart recycling.

At the centre of the deployment is a unique combination of Ruckus and Siklu technology that helps overcome network interference (a key challenge of smart cities). High-speed fibre is delivered into one building, the point of presence (PoP) site. Idaq Networks then positioned multiple Siklu radios across a network of tall buildings around the city. The fibre connectivity which is brought into the PoP can then be bounced between these buildings, creating fibre through the air, up to distances of 6km.

Siklu radios are then used to deliver these signals down to street level, leveraging shorter buildings and even streetlights, where a high-capacity wireless connection is delivered into a Ruckus Wi-Fi access point, connecting Sheffield's citizens.
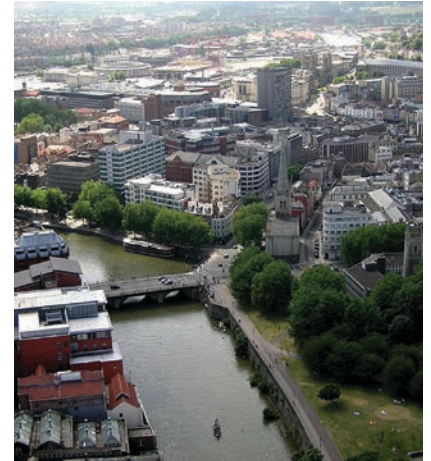
Bristol-is-Open and Zeetta Networks team up

Bristol-is-Open is a project for smart city experimentation in technology and citizen engagement, jointly backed by Bristol City Council and the University of Bristol. The city was recognised as the UK's leading smart city based on the UK Smart Cities index 2017. Then, in 2018, Bristol-is-Open was recognised with the Glomo Smart Cities Award.

Zeetta Networks, a local university spin-out company, has worked closely with Bristol-is-Open using NetOS to manage its smart city network infrastructure.

Bristol-Is-Open's backbone network uses the council-owned fibre-optic network to link several nodes around the city. A variety of wireless access networks branch out from the core fibre network to deliver user data rates up to 1 Gbps using a combination of Wi-Fi, LTE Advanced and – in the future - other more advanced wireless access technologies such as 60 GHz wireless.

Distributed sensors across the city supply the network with information about many aspects of city life including energy, air quality, temperature, humidity and traffic flows. University of Bristol's supercomputing and cloud resources are also connected to the core fibre network to host and analyse information flows, in real-time, providing open, accessible data for the development of a wide range of applications and services to improve the modern urban living and explore solutions on a city-wide scale.

Bristol-is-Open needed a network control and management platform that allowed simplified network operations and programmability to enable smart city experimentation.

NetOS had to support multiple technologies including optical and packet switches, Wi-Fi and a city-wide IoT network.

Flexibility was key for Bristol-is-Open, the ability to set-up and teardown experiments required the rapid reconfiguration capabilities of NetOS.

Barney Smith, CEO of Bristol-Is-Open says Zeetta Networks' technology is pioneering in the world of SDN and NFV technology".

Vassilis Seferidis, CEO of Zeetta Networks adds: "Bristol is leading the way in implementing cutting-edge networking technologies to tackle large-scale urban problems. The ability of Zeetta's NetOS to virtualize and slice different types of network resources including optical, packet and wireless is the catalyst for the exploration of such opportunities."

Bristol-is-Open is part of the EU funded Horizon 2020 project 5G-REPLICATE.

Semantic interoperability

Creating smart cities requires semantic interoperability so apps across different verticals can communicate with each other smoothly and securely

The Internet of Things (IoT) market is expected to be worth $1.1 trillion by 2021, as it continues to expand across different verticals, with China among the fastest developing regions.

By transforming the environment with billions of active devices, the Internet of Things (IoT) will enable countless possibilities from autonomous vehicles to wearable technology, connected health and smarter cities. While the first wave of the future, the smart meter, is implemented in the majority of homes already, other deployments to bring smart services to all aspects of daily life are continuing to pick up pace.

However, for these applications or systems to communicate with each other through the IoT, regardless of their technical specifications or characteristics, semantic interoperability is key to ensure seamless interworking of services.

IoT is a complex system

While the IoT may present a huge opportunity for telcos, it also presents challenges as these technologies are also a prime target for attackers. As a result of this, data breaches are becoming more sophisticated than ever and with varying levels of risk.

In light of this, supporting service domains has never been so important as data will be used in industries such as transportation and public security, making information breaches one of the biggest prohibitors to mass IoT adoption as new security challenges arise with each deployment. Despite these challenges, city authorities have a golden opportunity when it comes to utilising the data generated by smart city applications – enabling them to make enhanced, data driven decisions. The alternative is to operate several silos and absorb the associated costs.

From the perspective of developers and service providers, a complex system such as a smart city requires interoperability across multiple domains, so the horizontal linking of data through a standards-based approach is the key to moving forward.

Smart cities

The IoT offers a prime opportunity for smart cities to implement a convenient way of living through first-of-its-kind innovation. However, none of this is possible without semantic interoperability.

As a national priority mission, smart cities will provide advantages to not only the government, but the whole community including improved transportation, enhanced citizen and government engagement and efficient public utilities. However, governments need to think ahead about how they deliver this and ensure these programmes are to true their value.

A common IoT framework provides cities with the means to connect and communicate with any smart city asset. This can vary from waste management and urban mobility systems to street lighting and monitoring systems designed to protect lives and infrastructure from environmental damage.

With growing demand for smart applications, building the bridge of interoperable IoT systems across global markets is a must to increase efficiency of city-wide actions. Not only this, interoperability can significantly reduce costs in terms of system development, integration and maintenance, and will ensure data is safe and secure. By selecting a horizontal IoT platform, it enables different IoT use cases to be supported by the same platform, eliminating vendor lock-in and ensuring smart city deployments are highly scalable and cost-effective for city authorities.

Transforming to a standardised system within the mass market

oneM2M's horizontal platform is designed to provide a service layer between applications across different verticals and the underlying connectivity networks, supporting end-to-end encryption of data in a secure and controlled manner. The oneM2M standard provides the tools to ensure interoperability across multiple devices on the same platform, which will ultimately improve security by authentication of each application or device.

Going forward with the mass adoption of smart cities, information must be fused together to generate the effectiveness of city-wide actions such as the public service emergency response. Without interoperability boosting the response capabilities of this industry, it could be a potentially life-threatening result and is a must-have on top of IoT data collection and sharing.

Sealing the future of IoT, is oneM2M's latest set of specifications, Release 4, which will continue to create a common language between IoT devices, enabling vertical interoperability, best-in-class security and interworking with legacy IoT standards.

By transforming the environment with billions of active devices, IoT will enable countless possibilities from autonomous vehicles to wearable technology, connected health and smarter cities

Release 4 is being designed to support interworking between a range of industry verticals, including smart cities and Industry 4.0. Together, these factors stimulate the domestic IoT market and will help it grow rapidly as innovation momentum gathers from different enterprises.

To ensure its standardised global implementation within the mass market, oneM2M's global founding partners, including ETSI, TSDSI, TTA, and along with standards body ITU, will ensure that oneM2M is able to satisfy the further security demands of IoT through game-changing collaboration.

A smart city vision

Furthermore, the oneM2M standard is well suited to handle city sensors and the data they generate and is why it is being considered as the national IoT standard for India as part of its smart cities vision. This aims to develop 100 cities across the country by 2023 to make them more citizen friendly and sustainable.

In India, vertically siloed application vendors make up a large percentage of the IoT application environment, particularly in the smart city ecosystem. Following the announcement of the Government of India's smart city vision, proprietary platform providers are continuing to fill the smart cities space.

As a result, cities across India are at risk of being locked into expensive proprietary solutions when deploying and extending their IoT applications. This is driving a deep-er understanding of standards in smart cities across the nation and is why oneM2M, is working with its partner TSDSI and the Centre for Development of Telematics (C-DOT), to raise awareness of the benefits of a standardised IoT framework.

The future is bright with semantic interoperability

With the IoT industry breaking new ground across the sector, we are seeing many endeavours in the research and standards communities to build a more harmonised and semantically interoperable ecosystem. This is why system designers and developers should adopt for a common approach, found in standards like oneM2M, as the basis to build an open and fully flexible interworking system architecture.

As city planners – such as those in India - strive for greater cross-departmental synergies, it is essential that the technologies they select during the procurement process is completed carefully. As a result, long term evolution should be considered with the support of semantic interoperable technologies, to ensure they are not limited as their immediate needs evolve.

Therefore, it is essential that both networks and devices can be used for more than one purpose and this is where standardised IoT frameworks play a pivotal role - paving the way for city authorities to create new features, new ways to manage, govern and live in the city of tomorrow.

Could FWA be the answer to keeping people connected during the global pandemic?

James Bristow, SVP EMEA, Cradlepoint

In the midst of the Covid-19 crisis, it's important to step back and recognise the huge effort being made to limit its potential for disruption. From British Gas using its logistics network to deliver supplies to food banks, to teachers using empty D&T classrooms to make face shields for NHS workers, the pandemic has unleashed a wave of compassion, collaboration and innovation. Combined with our ability to communicate with one another, these factors make us all the more resilient.

Many aspects of daily life have been able to continue while respecting all-important social distancing, thanks in part to the ability to stay connected with family and friends, remain up to date with the latest news and government advice, or work remotely. But whilst things are changing constantly, getting everyone and everything connected can still be a challenge.

New field hospitals and pop-up testing stations are being developed right across the world to fight and control the spread of the disease. Speed and flexibility are key and this need for mobility and rapid deployment means wireline connectivity is a no-go, making enterprise-grade wireless WAN a preferred choice for many of these facilities.

Using 4G LTE cellular networks, FWA has helped remove barriers to getting pop-up facilities connected to high-performance networks in the field without the need for installation by IT professionals. In addition, in-built security measures such as VPN, edge threat detection and content help bolster the security and therefore availability of the network. As a result, healthcare staff can reliably gain access to patient records, transmit valuable data and receive updates in real-time from centralised control hubs, wherever and whenever needed.

Social distancing has made remote working an imperative of business continuity for many organisations. Innovations such as fibre broadband, cloud-based applications and a host of agile collaboration tools have similarly shifted from being useful nice-to-haves to business-critical activities. However, the consumer networks to which home offices are connected lack the security, reliability and manageability characteristics needed to meet the standards of enterprise-class connectivity. This can result in a loss of worker productivity due to reduced network capacity and also risks comprising data security regulations and opening vulnerabilities in the corporate network due to access via an unmanaged, unsecured connection.

Remote workers can rely on plug-in-and-play FWA solutions with all the characteristics of an office-based network already built-in. Not only does this provide them with a high-performance connection separate from their home network, but also enables organisations to centrally monitor, troubleshoot and secure remote access to the corporate network through cloud-based management platforms. For the vast number of households, a separate FWA corporate WAN solution running on a 4G LTE network can provide office-like connectivity separate to the home network.

High-speed home broadband underpins many of the everyday experiences that have now moved online. One of the most crucial is education, as reflected by the UK government's recent promise to supply disadvantaged children in England with free laptops, tablets and 4G wireless routers. This last provision is especially important in light of the UK's digital divide, with internet usage 30% lower amongst lower-income households than

those with an income of £20,000 or more, according to the Oxford Internet Institute.

A similar social initiative is currently being rolled out in the US on the grassroots level. One organisation has converted yellow school buses into mobile high-speed public Wi-Fi hotspots to provide free Wi-Fi to the neighbourhoods of school districts. Fitted with gigabit-class LTE modems, these access points offer sufficient bandwidth for students to gain full access to the learning resources and online content they need. In addition, in-built CJIS-compliant security capabilities, such as threat protection

and content filtering, help minimise the risk of students accidentally downloading malware or accessing dangerous web content. By bringing enterprise-class connectivity to every student, these mobile hotspots are helping to keep students engaged and learning, something which is ever more critical during this period.

We can see the extent to which the coronavirus pandemic would have disrupted daily life had it broken over a decade earlier. Innovations such as smartphones, 3G/4G LTE, fibre broadband and the cloud have proven to be crucial to continuing daily life

during the current crisis, while only having emerged within the last 15 years.

The need for easy-to-deploy networks has ushered in wireless as the defining network medium of our time. Moreover, flexibility, agility and efficiency will continue to be the ingredients of success long after the current crisis ends. It's therefore more important now than ever to cut the cord, consider FWA as the primary source of connectivity, and realise the potential of enterprise-class wireless as the default network paradigm moving forward.

Network attached storage

Michael Cade, senior global technologist, Veeam

IT is the driving force of a modern business. Harnessing it can help companies stay innovative, and make the data they already have work harder to better meet customer needs. As a result, IT teams are under a huge amount of pressure to provide a stable platform for the rest of the business.

This has become especially clear in the past few months, where we've seen a huge change in how digitally-driven many organisations have had to become out of necessity. But data needs and requirements can differ significantly from one organisation to another. One setup can be perfect for one environment, but highly unsuitable for another. It can be difficult to judge the competing factors in play and select a solution that offers the best fit.

Get the best of both worlds

Network Attached Storage (NAS) has been a popular way of storing and sharing data for some time. While it once might have been restricted to a single organisation or location, NAS is today used much more widely, commonly including applications and tasks like virtualisation. Organisations are also using it to store huge amounts of unstructured data, which can be anything outside a database environment – media, text, imagery, or audio.

What's also changed is the sheer amount of data being created every day, which also must be backed up. Both the numbers of and average sizes of files have been growing, alongside a need to often store backups and archives even longer. Backup measures need to be faster and more efficient to catch up to the fact that there's so much more data being manipulated and created every hour.

Minimise the impact of outages

Whatever the specific IT infrastructure decision makers select, they can't forget the need for backup and recovery. It's a matter of when, not if, an outage or system interruption occurs – whether the result of malicious acts, technical faults or even simple human error. They must be prepared to minimise the disruption these situations can create.

Business reputations and customer loyalty are increasingly built on the ability to access and use data in new ways that create value, and any interruption to this can be severely damaging for brand trust and reputation. What's more, smarter data management is also important for remaining legally compliant, particularly when it comes to things like customer and financial data.

Think about the 'why'

In approaching any decision around storage, IT leaders should carefully consider what tools are most effective for them before acting. Adopting the wrong kind of solution can cause major headaches further down the line, or even open the organisation up to data exposure or theft through misconfiguration. IT decision makers must address the 'why' in their planning.

When it comes to backup and recovery, solutions need to be flexible enough to handle the fact that data can often be a mix of structured and unstructured information, stored in a variety of locations and file types. The choice of backup tool must also be scalable – as organisations are often working with terabytes of data at a time, the task of backup must be able to be scheduled and automated if it's going to be of value. Unstructured data can also take significant time to back up, and tools that can offer incremental backups as edits are made can be very useful here.

For many organisations, NAS strategies can strike the perfect balance between performance and cost-effectiveness. Leaders must realise, however, that outages and incidents can take place at any time. By having both behaviours and tools in place to minimise their impact, they can begin to plan for success, rather than playing catch-up.

PRODUCTS

Seagate, incorporated in 1978 as Shugart Technology, says it "prides itself on arming its customers and partners with the right technologies" to help pioneer their business, empowering billions of people and businesses to realise the full potential of their living data every day.This unit from Seagate offers large capacities, along with dual bays for two hard drives. The design allows the Seagate Personal Cloud 2-Bay NAS device to mirror the files from one hard drive to a another, securing files in case one of those drives fails. What's more, it has a plain appearance, which means it can fit easily under a router or on a shelf. In addition, it can work with a plethora of cloud accounts, such as Dropbox and Google Drive. What's more, one can use an app to share content to streamers, such as Chromecast and Roku. *seagate.com*

The single-bay TS-128 is said to be very reliable, while providing remote access, strong app support and a friendly user interface to manage data. One way of describing it is It's akin to an external hard drive with network connectivity. However, this model has no data redundancy – this means copies of files need to be stored elsewhere if you want to keep them safe. Nevertheless, the **QNAP** TS-128 comes with an abundance of easy-to-use software for synchronising files and streaming media to many other compatible devices. *qnap.com*

Western Digital is a San Joe, California-based computer hard disk drive manufacturer and data storage company. It designs, manufactures and sells data technology products, including storage devices, data centre systems and cloud storage services. The company has long had a decent reputation in the hard drive space and it prides itself on producing NAS drives that are polished, reliable and user-friendly. Indeed, the user-friendliness is key if one is just becoming familiar with networked storage. The expert series EX2 Ultra comes with two 3.5-inch drive bays, 1GB of RAM as well as a dual-core 1.3GHz processor. There are also two USB 3.0 ports for plugging in additional drives. What's more, allowing access to different users is simple and transfer speeds are quick. *westerndigital.com*

Drobo is a storage company that's been through a renaissance in that it has decided to deliver products with an emphasis on simplicity. The streamlined 5N2 comes with an intuitive user interface as well as five bays, designed to cater for all storage needs. It also comes with a 1.6GHz CPU and 2GB of RAM, while additional features, such as the HDMI port, are kept down to a minimum. For additional security, the 5N2 has an internal battery to protect against data loss in the event of a power cut, in addition to disaster recovery software. *drobo.com*

Netgear has a solid reputation as a hardware maker in the IT and comms space. This has been strengthened by its strong track record in the manufacturing of NAS drives. The ReadyNAS 214 comes with extra capacity – it has four drive bays rather than two and the disks ones installs can be set up in a variety of ways.

Although not as powerful as some comparable NAS units, the general consensus amongst reviewers is that this piece of kit does all the basics well and Plex support is very much a standout feature. The ReadyCLOUD portal-based user interface and app on PC, Mac, smartphones and tablets make the RN214 a popular choice because of its simplicity and ease of use. *netgear.co.uk*

Synology, based in Taipei, Taiwan, brings to market its DiskStation DS918+. The product is said to be more powerful than most NAS drives in its ballpark. It comes with more memory, a faster processor, as well as twice as many drive bays. In short, it's been described as "a perfect fit for the serious NAS user".

Synology's bundled software is, apparently, capable and straightforward to use. Furthermore, drives can be fitted and removed with ease. Powered by Synology DiskStation Manager (DSM), the DS918+ also offers advanced security measures to protect against sudden data loss and potential security holes. *synology.com*

Toshiba says its 3.5-inch N300 NAS Hard Drive offers unprecedented reliability for NAS and other high-performance storage systems. It is optimized to meet the reliability, endurance, performance and scalability requirements of 24-hour x 7-day high-capacity storage for personal, home office and small business use. The N300 is available in capacities of 4 TB up to 16 TB. They can be used for Network Attached Storage (NAS), desktop RAID and servers, multimedia server storage, private cloud storage same as small business server and storage. Regular hard disk drives without RV sensors can affect the performance of a multi-bay NAS System by generating 'knock-on' vibration. N300 drives ensure high reliability by minimizing vibration effects through their advanced control and sensing technology. Multiple sensors detect the slightest shock and built-in RV sensors also compensate for rotational vibration - eliminating the possibility of 'knock-on' vibration in multi-bay NAS configuration systems. High performance and fast read speed is made possible under high data access loads from multiple users thanks to 512, 256 or 128 MB data buffer. This makes the drive suitable for small businesses and creative professionals looking for solutions to handle high data volumes using multi-RAID NAS environments. The 12 TB, 14 TB and 16 TB N300 NAS Hard Drives use a helium-sealed design, achieving low power consumption while increasing storage density. Toshiba offers a Dynamic Cache Technology, a self-contained cache algorithm with on-board buffer management, optimizes how the cache is allocated during read/write to provide the high-level performance demanded by real-time domains. *toshiba.com*

"Please meet...

Networking+ chats to Kristian Thyregod, VP & GM - EMEA at Silver Peak

What is the best thing about your job?

Working in a disruptive and enabling technology category means that you are collaborating with very smart people. That is a privilege, as conventional wisdom across the board can – and should – be challenged in terms of driving continuous learning and, with that, progress and improvement. On top of that, when you work with an international team, there is always a different take on topics influenced by history and culture.

Who has been your biggest inspiration?

James Edward Hansen, adjunct professor directing the program on climate science, awareness and solutions of the Earth Institute at Columbia University. Professor Hansen helped advance the awareness of global warming approximately 30 years ago – and he is still at it. The ability to, very early on, conceptualise this critical knowledge and then to communicate it widely, and persistently – despite opposition – is an inspirational endeavor in my book. Other than that, I derive quite some inspiration from music – and in that vein, Peter Gabriel.

What is your biggest regret?

I was offered a two-year internship (musician) in a recording studio – yes, the first year would be nothing more than getting coffee, etc. for real musicians, but it would likely have been a great – and maybe formative – experience. However, as it collided with me going to college, I was not able to convince my parents that it would be a really good idea.

If you had to work in a different industry, what would it be?

Maybe music – I play drums and keyboards; granted, these days just for contemplation, relaxation, and fun, but it would certainly have my interest. My favourite drummer is Simon Phillips.

Who was your hero when you were growing up?

My parents albeit both have passed now. We had several traditions in our family – mandatory piano lessons, graduate school, military service for the boys – but my parents mastered inspiring us to always explore and question, if you will, mostly everything; there was always time to jointly seek out answers in encyclopedias and to discuss the findings vividly. My parents also diligently sought to teach us to be respectful of everybody and to treat everybody with dignity and respect.

Which rival do you most admire?

I seek to be informed and mindful relative to our competitors of which there are a few – but, respectfully, I cannot point to any one of them that I particularly admire.

The Beatles or the Rolling Stones?

That is a tricky question, I think; both bands opened so many avenues downstream as these bands inspired a whole host of musicians and bands. However, I am going with The Beatles – and, if you must know – George Harrison.

What would you do with £1m?

Outside of spoiling my wife, I can certainly think of a couple of kit upgrades in my home studio. Obviously, some incremental investments will be knocking on the door,

too – likely in climate protection technologies. And I would also seek to support a couple of my friends and their ventures.

What's the weirdest question you've been asked at an interview?

When I was at business school, I participated in an exchange programme governed by the business school and a number of companies. Through this programme, students were offered short-to-medium-term practical lapses with a variety of companies across multiple industries and sectors. Ultimately, this programme functioned as a talent sourcing vehicle, and helped students and potential future employers to connect. Because of my major, I was "working" in an investment bank – and throughout four semesters, I had but one 15-minute conversation with the CEO during which he asked me: "what would you do if you were me?"

If you could change any UK law, what would it be?

While I am Danish and have lived in Switzerland for the last nine years, earlier in my career, I lived in the UK. While I understand that the European Union can be a cumbersome multinational engagement, I think that more nations banding together is better than fewer nations banding together. I absolutely salute the individual sovereign state's rights and attributes and will defend these vigorously every day of the week, but I do think that the challenges we face are better engaged and dealt with by as many of us together as possible. And I think that it is a worthy endeavor to participate and thus influence the European Union – and, personally, I am saddened that the UK has decided to leave."