Doyle Research

Next-Generation WAN: Connecting, People, Places, and Things

By: Lee Doyle, Principal Analyst at Doyle Research

Sponsored by Cradlepoint

Executive Summary

A paramount goal for many of today's leading IT organizations is to enable Digital Transformation (DX) within their business operations. This means companies need to connect more people, places and things than ever before. Today's enterprise wide area networks (WANs) are decades old in design and technology — and were not built to handle such diverse and distributed requirements. As a result, the enterprise WAN must be transformed to accommodate DX and its underlying enablers, which include cloud, mobility and the Internet of Things (IoT) — a reality that is challenging companies of all sizes across many industries.

A new set of cloud-delivered and Software-defined Networking (SDN) technologies, including Software-defined WAN (SD-WAN) and Software-defined Perimeter (SD-Perimeter), are well suited to meet these next-generation WAN requirements. SD-WAN provides branch and mobile networks with secure, flexible and resilient connectivity utilizing a hybrid of wired and wireless Internet broadband links, as well as legacy MPLS. For mobile users and IoT, SD-Perimeter is a host-based architecture that creates a "dark cloud" over the Internet to connect, isolate and secure mobile and IoT devices anywhere.

As more traffic shifts from private networks to the public Internet, 4G LTE is rapidly becoming the connection of choice for primary and failover links due to its pervasiveness, ease of deployment, and reliability. This trend is expected to accelerate as Gigabit LTE and 5G fixed and mobile services enter commercial availability starting in 2018.

Cradlepoint's industry leadership in 4G LTE network solutions and new Elastic Edge^{SM} strategy uniquely position the company to deliver next-generation WAN solutions for connecting people, places and things anywhere. The Cradlepoint NetCloud platform powers the company's portfolio of 4G LTE-enabled routers and provides cloud-based management, SDN and virtualized network functions. With NetCloud, enterprises can connect fixed and mobile sites, remote workforces and IoT devices — on premises and in the field — with software-defined overlays that stretch across wired and wireless Internet broadband links. Everything is simply managed through a single pane of glass with end-to-end visibility, security and control.

Digital Transformation is Driving WAN Transformation

Businesses of all sizes and across many industries are in the midst of Digital Transformation (DX) as they seek to improve operational efficiencies, capitalize on new opportunities, and respond faster to changing market conditions and competitive pressures. IT organizations are grappling with the many effects of DX: supporting expanding global operations, shifting of workloads to the public cloud, adoption of SaaS and UCaaS applications, workforce mobilization, and the proliferation of IoT devices — including kiosks, digital signage, video capture and surveillance, sensors and other connected devices (see Figure 1 below). To meet the needs of the new "Connected Enterprise," the enterprise WAN needs transformation to become more secure, elastic and reliable.

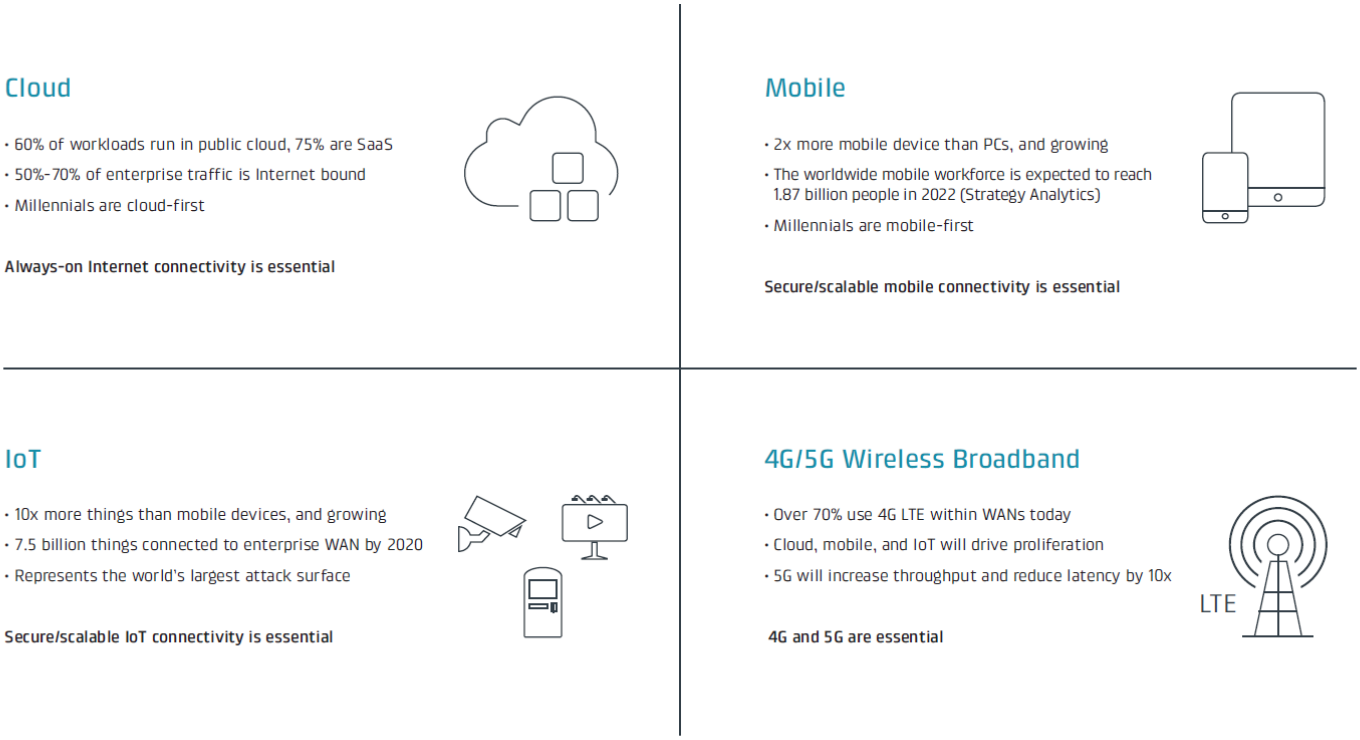

Figure-1: Digital Transformation Related Trends

The traditional enterprise WAN was designed primarily to connect distributed sites and provide secure access to centralized business applications and data using private network services, such as MPLS, and was built on architectures and technologies that are more than two decades old. In the wake of DX, companies are dramatically increasing the number of network endpoints as they connect to more people, places and things than ever before. Additionally, bandwidth requirements have increased significantly and shifted as more traffic is moving off private networks and onto the public Internet, creating a new set of visibility, availability, security and quality of experience challenges.

The new Connected Enterprise requires a next generation of WAN connectivity that extends beyond fixed sites to vehicles, mobile workforces and a plethora of M2M and IoT devices. Moreover, this new WAN will need to capitalize on wired and wireless Internet broadband services, such as cable, DSL and 4G LTE to meet pervasive connectivity, economic and performance requirements.

Requirements of the Next-Generation WAN

The enterprise WAN is experiencing exponential change in the volume, velocity and variety of endpoint connections to connect people, places and things, traffic shifting from the intranet to the Internet, new security paradigms, pervasive mobility and increased utilization of 4G LTE. These changes represent a nexus of requirements that demand an entirely new architectural approach to building and managing the next-generation WAN (NG-WAN).

Support for Enterprise IoT

IoT is emerging as a key technology enabler for DX by leveraging data from sensors and connected devices to provide actionable insights and automated processes, which can improve operational efficiency, increase customer satisfaction, and lead to higher profitability. IoT will soon be widespread with 85% of businesses planning to implement IoT by 2019 (AT&T). The explosive growth in Connected Enterprise WAN devices (7.5 billion by 2020) means that IoT customers need intelligent, scalable infrastructure at the edge of the network.

Multiple WAN Connections

What cloud, mobility and IoT have in common is that they are Internet-derived and, together with video and unified communications applications, they are driving more network traffic at the WAN edge than ever before — saturating expensive MPLS links. As a result, many organizations are augmenting, and even replacing, their expensive MPLS networks with wired and wireless Internet broadband connections, such as cable, DSL, carrier Ethernet and 4G LTE. By comparison, Internet broadband can be as much as 90 percent less expensive than MPLS. As more applications and workloads are cloud-delivered, NG-WANs must be always-on. While multiple wired broadband links can statistically improve availability, 4G LTE is required to provide path diversity into buildings and achieve a truly non-stop network.

New Security Paradigm

With the pervasive connectivity of NG-WANs, network security has become a top-tier IT concern due to an increased attack surface, the diversity of endpoint devices and growth in Internet-bound traffic. Addressing these new challenges requires a fresh approach to network security. As more traffic shifts from the corporate Intranet to the Internet, the traditional paradigm of “tromboning” branch traffic through a centralized security firewall and Internet gateway no longer makes sense. Instead, these security services need to virtualize and distributed to the branch to enable direct Internet access.

Moreover, remote users are increasingly accessing cloud and SaaS applications from 4G LTE, public WiFi hotspots and other third-party networks, bypassing critical security infrastructure such as VPN gateways and Active Directory domains. This requires a new, perimeter-centric overlay security model across the public Internet that is capable of extending domain services anywhere. Connecting many thousands of IoT devices to existing enterprise networks has given rise to a new specter of security breaches, which have already affected numerous high-profile brands. Here too, a perimeter-secured overlay allows IoT devices to be connected over 4G LTE, WiFi or Ethernet while being obfuscated and isolated from underlying third-party networks and the Internet.

Simplified and Unified Management

IT organizations within highly distributed enterprises spend a significant amount of their time deploying branch sites, remote access and IoT devices as well as dealing with network outages, user access problems, asset monitoring and application performance issues. This problem is exacerbated by the fact that more fixed and temporary sites, users, vehicles and IoT devices are being connected to the enterprise every day. To address this daunting challenge, NG-WANs require simplified and unified management and control planes that provide a single pane of glass for network operations, administration and management. This includes configuration, zero-touch deployment, orchestration, automation and advanced remote troubleshooting capabilities. To ensure optimal application performance, especially at critical branch sites, NG-WANs also require the ability to steer traffic across multiple wired and wireless links based on real-time performance measurements and dynamic policy control.

Pathway to Gigabit LTE and 5G

Today's LTE Advanced networks are capable of theoretical speeds up to 600Mpbs (download) and 30-100Mbps in the real world, and they are not slowing down. Gigabit LTE is expected to be commercially available in early 2018, followed by early 5G deployments in 2019. One of the key benefits of using LTE as the primary WAN for highly distributed branch networks is that a company can deploy a nationwide network with just a couple of cellular carrier partnerships as opposed to tens — or even hundreds — of wireline Internet Service Providers (ISPs). With these advancements and benefits, LTE is poised to become the preferred infrastructure in NG-WANs.

Building a Software-Defined NG-WAN for Connecting People, Places and Things

To meet the demands of DX and support the volume, variety and veracity of endpoints connections across people, places and things, NG-WANs will need to more agile, intelligent and policy-controlled. In other words, they need to be more software-defined and cloud-enabled. However, the NG-WAN will require multiple software-defined architectures to span all the connectivity requirements of fixed branch and mobile networks (SD-WAN) and remote workforces and IoT (Software-defined Perimeter).

SD-WAN

SD-WAN uses SDN, dynamic policy and orchestration technologies to connect remote networks within fixed branches and mobile sites (e.g. in-vehicle networks in school buses and police cars) to the corporate intranet or Internet. It allows multiple wireline and/or wireless links (e.g. MPLS, Internet broadband and 4G LTE) to be combined into a hybrid WAN and leverages real-time policy and orchestration to select the optimal physical path for each specific application (see Figure-2).

One of the defining attributes of SD-WAN is the ability to automatically select the optimal path for any type of traffic at any moment in time and steer it accordingly — providing elastic bandwidth, Quality-of-Service and resiliency. Additionally, most SD-WAN implementations have unified control and management planes that simplify and automate common management functions such as router deployments (i.e. zero touch), configuration of secure overlays and dissemination of policies.

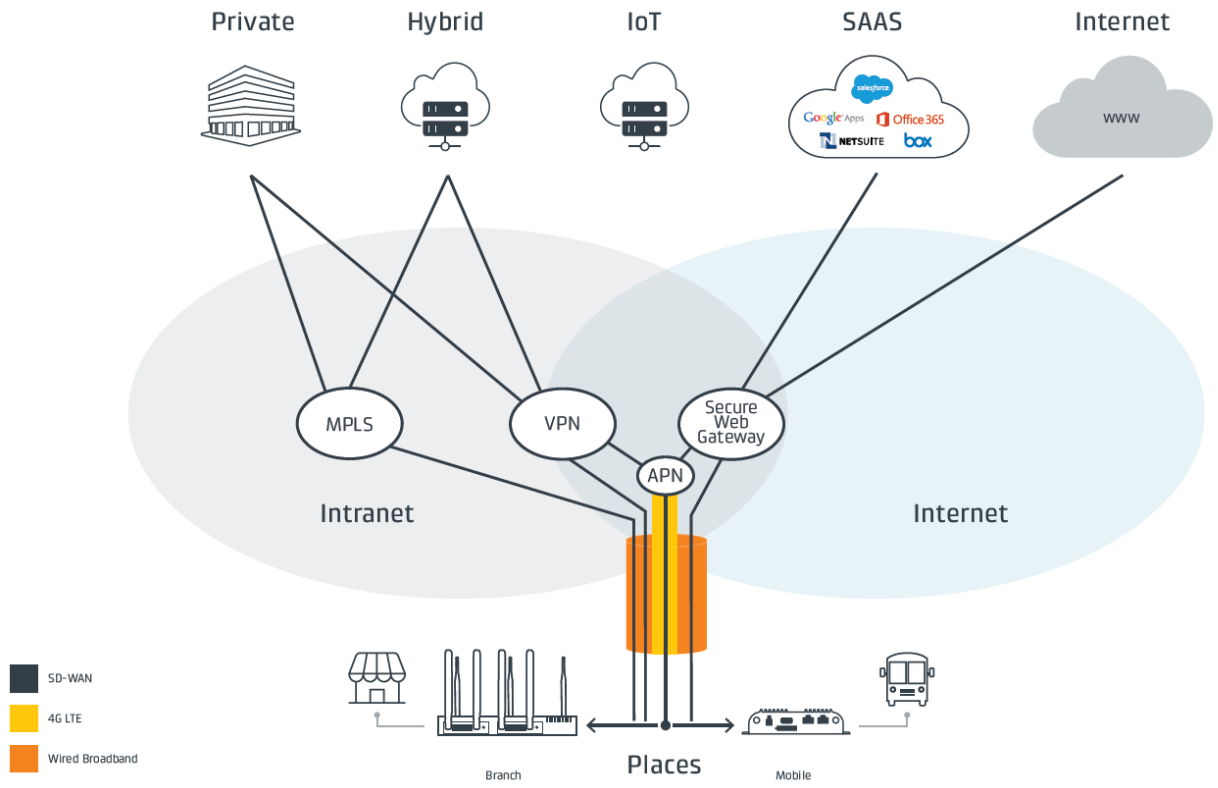

Figure-2: SD-WAN Topology

SD-Perimeter

In contrast to SD-WAN, SD-Perimeter is a cloud-based Network-as-a-Service that uses a perimeter-secured, private overlay network to connect discrete mobile and IoT devices over the Internet to servers and applications within the corporate intranet and public cloud. Each secure overlay, called a Virtual Cloud Network (VCN), has its own private IP address space so that its completely obscured from the underlying Internet (you can't attack what you can't see). For traffic that needs to egress to the Internet, such as web or SaaS application traffic, a secure gateway function with integrated overlay-to-underlay address translation is provided (Secure Cloud Gateway).

The SD-Perimeter service leverages a variety of SDN and cloud technologies, including: data planes deployed within public cloud data centers to serve as global points of presence, network virtualization, end-to-end encryption, micro services-based virtual network functions, invitation-only network access control, and fine-grain policy control that enables firewalling, filtering and micro-segmentation to precisely control communications to and from endpoints. SD-Perimeter also utilizes unified control and management planes to provide self-organizing, self-healing and self-optimization capabilities, and to enable the automatic distribution of perimeter policies across data planes.

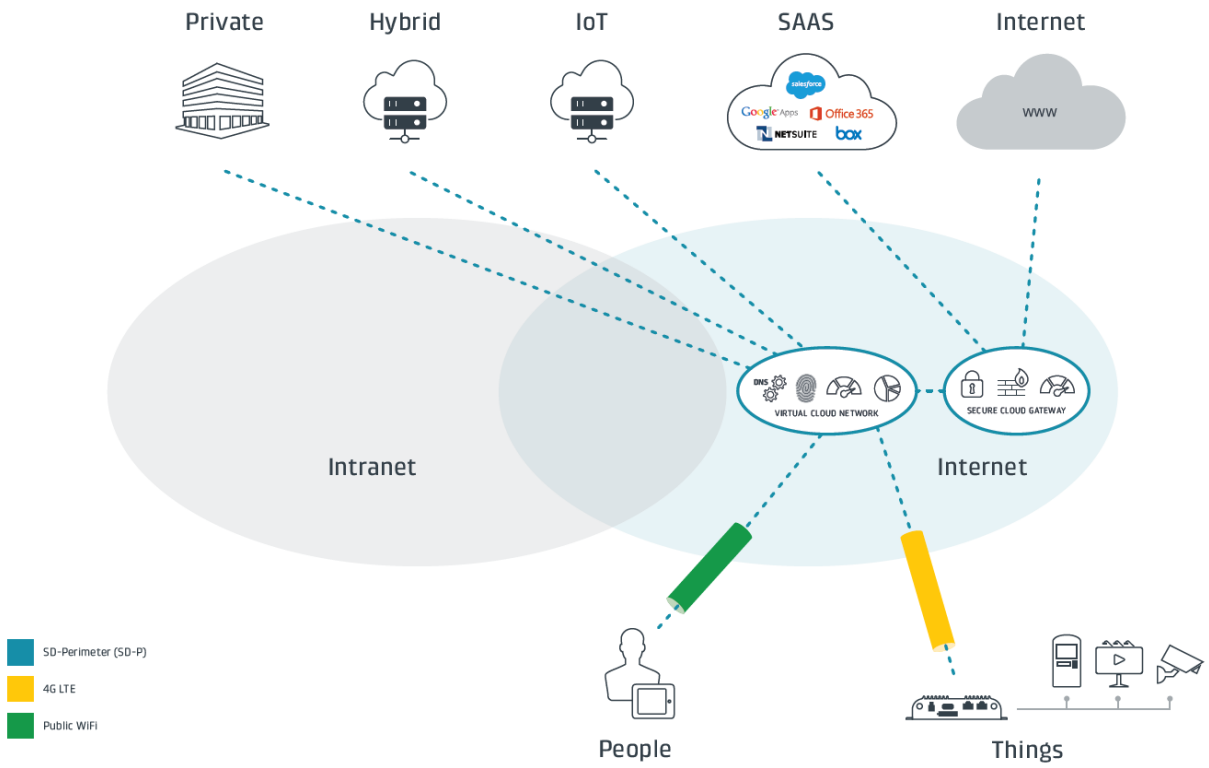

Figure-3: SD-Perimeter Topology

Cradlepoint NG-WAN Strategy — The Elastic Edge

Cradlepoint is an industry pioneer and leader in providing cloud-based, LTE-optimized network solutions for connecting people, places and things over wired and wireless broadband. Today, more than 17,000 enterprise and government organizations around the world rely on Cradlepoint products to keep their distributed sites, workforces, vehicles, and M2M/IoT devices always connected and protected.

To support the demands of the Connected Enterprise, NG-WANs must support much a greater **volume** of connections, **velocity** of change, and **variation** of endpoints than ever before. To address this need for more *elasticity* at the WAN edge, Cradlepoint has developed its Elastic Edge strategy that combines cloud management and orchestration; SD-WAN and SD-Perimeter architectures; industry-leading 4G LTE with a built-in pathway to gigabit LTE and 5G; virtualized network functions (e.g. third-party security integrations); and edge computing capabilities with purpose-built appliances for branch, mobile and M2M/IoT deployments. A key enabler of this strategy is Cradlepoint NetCloud (see Figure-4 below), a software and cloud platform that includes single-pane-of-glass management and orchestration (NetCloud Manager), SD-WAN-enabled Linux edge router software (NetCloud OS), and perimeter-secure overlays (NetCloud's SD-Perimeter).

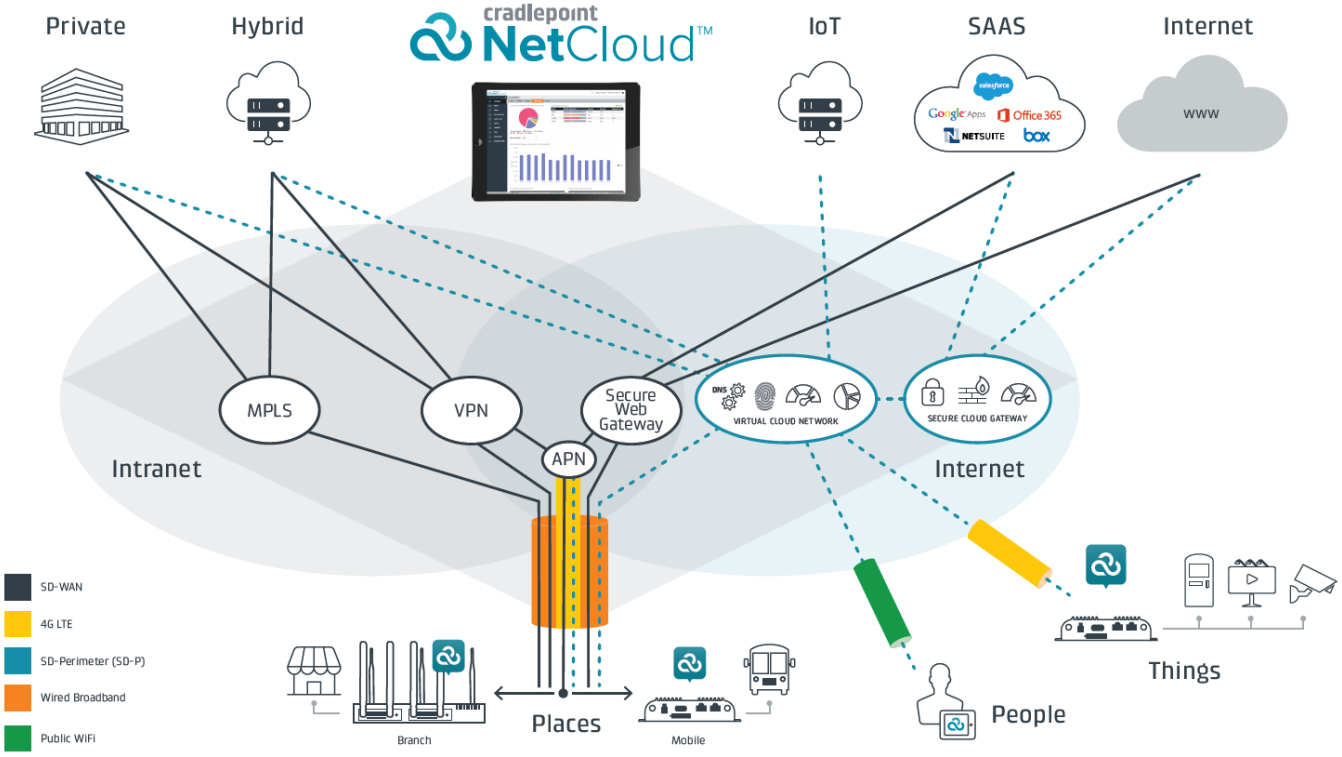

Figure-4: Cradlepoint NetCloud – connecting people, places and things over wired and wireless broadband

Customer Deployments of Cradlepoint NetCloud

The following customer deployment stories illustrate how customers are building NG-WANs today using Cradlepoint NetCloud to securely connect people, places, and things across wired and wireless broadband.

JBT Aerotech (SD-Perimeter)

The Aerotech Division of JBT, a leading global technology solutions provider employing 4,000 people, furnishes airports with ground support equipment, gate equipment, and airport maintenance services. JBT Passenger Boarding Bridges (PBB) and ground equipment contain a variety of IoT devices, including sensors and programmable logic controllers (PLC), used to gathered critical operational data. The company's challenge was to keep these devices connected 24x7 without relying on shared airport network infrastructure, which provide JBT with availability and security challenges, and without significant capital expenditures.

JBT chose Cradlepoint NetCloud and edge routers to connect, secure and manage its IoT devices across the airfield. Instead of using the airport's shared WiFi infrastructure, JBT deployed 4G LTE wireless connectivity that provided higher availability and rapid deployments. Using NetCloud's SD-Perimeter, JBT connects all of the IoT devices on a perimeter-secured and encrypted overlay and microsegments them by airline customer. Now, all remote IoT devices across airports are monitored and managed through a single pane of glass using NetCloud Manager. With Cradlepoint, JBT moved

from manual maintenance to automated alerts and is currently enjoying the benefits of deployment at speed, security, and reduced operating costs.

Ewing Police Department (SD-WAN and SD-Perimeter)

Ewing is a growing community in Central New Jersey. It has 80 patrol officers with 30 vehicles equipped with laptops, tablets, sensors, and body-worn and dash cameras all connected on an in-vehicle WiFi network using 4G LTE as the WAN. One of the department's challenge was keeping its critical applications securely connected even during a temporary loss of cellular connectivity, like when going through an underpass or parking garage. In the past, traditional IPsec VPN tunnels would instantly disconnect at the loss of a connection, causing officers to spend more than 10 minutes re-establishing a tunnel and logging back into each application. This represented both a security and productivity challenge. Additionally, the small IT team needed a way to manage everything centrally and keep remote PCs always connected to its Active Directory domain for security and administrative purposes.

The Ewing Police Department deployed Cradlepoint mobile LTE routers with integrated GPS in their patrol cars for in-vehicle WiFi and NetCloud's SD-Perimeter solution on their PCs to provide a secure, persistent overlay to keep applications connected during disruptions in cellular connection. Additionally, NetCloud's SD-Perimeter solution enables Active Directory domains to be extended across the overlay — keeping patrol car PCs always on domain. NetCloud Manager allows Ewing's IT team to monitor and manage everything remotely. In the future, Ewing Police will be able to add a separate modem to its routers to add Band 14 support — FirstNet private cellular network for first responders — and utilize Cradlepoint's SD-WAN functionality to steer traffic between the commercial and FirstNet LTE connections.

Using Cradlepoint NetCloud, Ewing Police Department has deployed a NG-WAN for its patrol officers and vehicles that provides a secure and resilient connectivity for all devices, enables Automatic Vehicle Location (AVL), and gives its IT team the ability to configure, secure, monitor and manage everything centrally with no additional IT staffing.

Doddle (SD-WAN)

Doddle is at the forefront of making online shopping more safe and convenient with its mobile package lockers. With more than 80 package pick-up and drop-off stores around the UK located in train stations, universities, shopping centers, and business parks, Doddle makes it easy for online shoppers to collect and return their online purchase at a time and place convenient for them. Their customer-centric approach uses innovative technology and a SD-WAN to ensure customers never wait more than three minutes to collect or return a parcel.

Doddle deployed Cradlepoint edge routers at each of its locations to provide in-store WiFi that connects lockers, Point-of-Sale devices and security cameras across wired and wireless broadband links using integrated network security and SD-WAN functionality. Each site utilizes 4G LTE as part of a hybrid WAN connection to ensure non-stop networking and provide optimal performance. Using NetCloud Manager, the small and agile IT team can deploy a new location in minutes and without a truck roll, as well as monitor and manage its rapidly growing WAN from anywhere.

Recommendations for IT Leaders

In the age of DX, delivering a NG-WAN to connect people, places and things is an essential yet challenging task for most IT organizations. As corporations embrace cloud, mobility and IoT in support of DX initiatives, the WAN is at center of application uptime and performance for just about every business function. Using traditional networking, deploying, administering, securing and managing tens of thousands of sites, users and devices — within buildings, vehicles and the field — would be daunting given the cost, complexity and topological and operational constraints. Following are some recommendations for IT leaders to help assess the right next-generation WAN infrastructure for their business.

Take the Long View

Today, the average lifespan for WAN edge infrastructure is 5 to 7 years. IT leaders need to take the long view and look beyond a "branch refresh" to determine the breath of expansion, automation, cloud migration and IoT initiatives that will be rolling out over that period — and the implication to the WAN.

One Size Does Not Fit All

SDN is the biggest paradigm shift in networking since the Internet, but it's not one thing. There are different SDN technologies to address the different demands within NG-WANs; these include SD-WAN and SD-Perimeter. IT leaders should consider which SDN architectures will be required to meet current and future networking requirements as they relate to connecting people, places and things.

Augment or Replace

Bandwidth is one of the biggest WAN costs. IT leaders contemplating a NG-WAN need to consider a migrating part of all of their MPLS connections to Internet broadband. Augmenting MPLS with broadband can alleviative current bandwidth and uptime challenges, but it's adding cost to an already expensive infrastructure. SD-WAN provides an opportunity improve WAN throughput and performance while dramatically reducing costs by replacing MPLS with a hybrid connection that combines wired and wireless broadband.

Time to Cut-the-Wire

4G LTE is a proven network solution for tens of thousands of enterprises that are using it to provide primary connectivity for a plethora of M2M and IoT devices, temporary and fixed branch sites, and in-vehicle networks, and for WAN resiliency at mission-critical branch sites. With the number of WAN endpoint connections exploding, gigabit LTE looming and 5G just around the corner, IT leaders should consider "cutting the wire" and deploying LTE more broadly within NG-WAN infrastructures.

Obscurity Security

By 2020, more than 7.5 million things are forecasted to be connected to enterprise networks over the Internet, creating a potential attack surface of unprecedented proportions. IT leaders will need to develop a new layered security model with a foundation built on obscurity — the ability to create private and secure virtual overlay networks that are "cloaked" from the underlying Internet.

Reduce the Panes

While much of the fascination around SD-WAN has been in its multi-WAN and dynamic path selection capabilities, the real opportunity for reducing human capital costs lies on a new generation of cloud-delivered management and orchestration planes. IT leaders should seek out solutions that can consolidate management functions for connecting people, places and things within a single pane of glass; this includes configuration, deployment, administration, visibility, asset tracking, and policy and security controls.

Meet the Author

Lee Doyle is Principal Analyst at Doyle Research, providing client focused targeted analysis on the Evolution of Intelligent Networks. He has over 25 years' experience analyzing the IT, network, and telecom markets. Lee has written extensively on such topics as SDN, NFV, enterprise adoption of networking technologies, and IT-Telecom convergence. Before founding Doyle Research, Lee was Group VP for Network, Telecom, and Security research at IDC. Lee contributes to such industry periodicals as Network World, Light Reading, and Tech Target. Lee holds a B.A. in Economics from Williams College.