AGILITY REDEFINED: Flexible and Secure Networking Solutions
Secure connections to one another, to information and experiences—wherever, whenever—have changed the way we live and how we do business. No longer limited to physical infrastructure or geography, nor defined by a simple phone call, today’s networks are fluid and complex ecosystems of endpoints. They serve as connections that provide real-time insights for today’s agile businesses, helping them thrive.

Tapping into the power of these connections means re-thinking the way we architect the wide area networks (WAN) that make up the foundation of business connectivity needs. We are seeing organizations move away from static, fixed capacity infrastructures and limited connectivity options to dynamic, secure solutions that are more readily responsive to their needs. They need not only a smart strategy that can address their diverse networking needs but also a full spectrum of visibility and control across multiple functions and connections.

Agility Redefined is a research-led series focused on how companies are leveraging technology to build agility for their business in new ways. In our 2016 Future of Business Agility survey, we spoke to 1,000 IT and business executives, who shared their perspectives on the initiatives they are undertaking to build agility across their infrastructure, operations, workforce and customer experiences. This report offers insights into building a flexible and reliable infrastructure, specifically options available today and on the horizon for the WAN.
THE DRIVE TOWARD FLEXIBLE AND RELIABLE INFRASTRUCTURE

Ten years ago, a typical enterprise may have had 30 critical sites, with critical IT workloads running at each site. Today, due to the desire to get closer to end customers and vendors, that same organization looks very different, with perhaps 10 critical sites and an additional 60 small branches. To accommodate this more flexible structure, this business has also now moved its IT workloads into multiple cloud providers.

As a result of the changing nature of business, as well as the growing availability of good, less costly broadband internet connections, many companies are re-examining their WAN architectures, looking for more security, and the flexibility to address their diverse and growing bandwidth demands and business needs.

In fact, over half of the respondents to our Future of Business Agility survey said improving the flexibility of their infrastructure will be critical in the next three years, and just 20 percent are “very satisfied” with the current flexibility of their technology infrastructure today.

“The speed of change is pushing down on retail to be more agile… the retail industry is sticking to legacy infrastructure with little ability to respond rapidly to the new digital platforms.”

— COO (AT&T Future of Business Agility Survey)

Bandwidth needs for today’s organizations are growing rapidly. Users expect to access corporate applications via high-bandwidth wireless and broadband internet connections. At corporate branch offices, large email attachments and web conferencing are an essential part of the everyday routine. In order to serve these needs, corporate data centers commonly require 1Gbps bandwidth, and often 10Gbps and above. Businesses are also using video to interact with employees, partners and customers, which consumes more bandwidth and requires a higher class of service (CoS) to maintain voice synchronization and prevent choppy images or frozen frames.

Moreover, bandwidth demands aren’t static. Companies see significant fluctuations in data traffic on their networks, seeing peaks as high as 220 percent of average and valleys of 70 percent of average month-to-month, according to respondents to the Future of Business Agility survey.

Growing Demands for Wi-Fi and Internet offload

Public Wi-Fi has become standard in many industries, with an expectation that it will be available at retail locations, restaurants and hotels, for example. Businesses in these verticals are also interested in better understanding consumer behavior via location and other data analytics. The high adoption of smartphones can make the insights gleaned from Wi-Fi highly representative of general consumer behavior.

Some businesses route public Wi-Fi traffic over the MPLS VPN connection at each site and connect to the Internet through a network gateway, while others route...
directly to internet access at the site. This is commonly referred to as internet offload. Internet offload does not require service quality guarantees, and the highly competitive retail vertical (often with low margins) may utilize lower-priced broadband internet connections for local Internet offload.

Optimizing Performance and Costs

In today’s business environment, every cost is scrutinized. In retail, for instance, seasonality and margin pressures leave no room for over-booked network capacity. Where, in the past, a business might prefer private high bandwidth Ethernet connections (5 Mbps-10 Mbps) for its sites, the higher price tag that accompanies these upgrades could now be both unaffordable and unnecessary.

Organizations are increasingly looking for more cost-effective ways of building a WAN that incorporates more than just private, company-owned infrastructure. Broadband internet has become more universal, and businesses can now often find one or more service providers serving their locations. The growing availability of these high speed broadband based connectivity options, coupled with IPsec, now offer high bandwidth at lower prices but without service quality (latency, throughput, repair time) guarantees.

Now that there is a more robust set of both private and public connectivity options, IT departments have the ability balance performance and costs at a site-by-site, or even an application level.

Simplifying Network Management and Enhancing Self-Service Control

A diverse set of connection types, dispersed locations with different bandwidth needs, and the need to access applications both within the network and through the cloud can make managing today’s networks a challenge.

As a result, companies are increasingly looking for new ways to simplify network management and enhance visibility and control. New technologies, such as software-defined WANs (SD-WAN) and multi-function customer premises equipment (CPE) are enabling enterprises to utilize a mix of private (MPLS) and public (broadband Internet) connectivity options to optimize application performance and cost on a per site basis.

Multi-function CPE vendors are offering self-service portals that allow enterprises to deploy, configure and manage all of the devices. VPN access routers may now come with additional functions, such as Wi-Fi access points, firewalls, data patterns, analytics and more. Businesses have started to utilize these multi-function CPE services and are moving away from the old model of deploying multiple devices that specialize in a single function.
VPN TECHNOLOGIES THAT POWER THE WAN

MPLS

Multiprotocol Label Switching (MPLS) is a standards-based technology used to speed up the delivery of network packets over multiple protocols, such as the Internet Protocol (IP). With an MPLS VPN, connectivity is delivered over a single carrier’s private network.

MPLS networks have several defining characteristics. They typically offer higher-speed bandwidth and they offer enhanced Class of Service (CoS) routing, meaning improved quality and speed in transmitting information. MPLS also offers any-to-any routing or efficient connections to any site—avoiding the latency associated with legacy hub-and-spoke WAN architectures. MPLS is particularly useful for data center replication or for large sites that need very high-capacity connections, as MPLS VPNs that scale to 10 Gbps and higher.

Service-level agreements (SLAs) back up performance promises with guarantees for detection and resolution intervals. These guarantees are important for those with mission-critical and time-sensitive applications.

MPLS also offers multicasting and end-to-end security. Multicasting enables video, voice and data streaming to multiple locations at the same time. Examples include a corporate communications team broadcasting important executive announcements to employees around the globe simultaneously via video to distributed locations, or an educational institution better meeting the needs of students by providing live remote lectures to satellite campuses.

End-to-end security is built into this technology because MPLS operates on a private network, which lowers the risk of Distributed Denial of Service (DDoS) attacks and unauthorized network access. This is especially critical for companies with regulatory compliance mandates, such as the healthcare and payment card industries, because it avoids transmitting sensitive data on the public Internet.

IPsec

With an IPsec VPN, a “tunnel” encrypted by Internet Protocol Security (IPsec) algorithms is created between points on the public Internet. IPsec authenticates and encrypts each IP packet of a communication session. Each site in an IPsec VPN often requires IPsec-capable CPE, usually with central tunnel aggregation CPE in a datacenter that all VPN tunnels connect to (often referred to as the “head-end”).

IPsec solutions typically have lower costs, and are useful in reaching sites where
MPLS may not be available, but are exposed to more risk and service quality variability than MPLS networks because they use the public Internet.

For example, using IPsec, retailers, clothing stores and restaurants in a shopping mall can more cost-effectively transmit encrypted, low-bandwidth credit card transactions, inventory requests, and orders. IPsec is also a good option for global expansion to sites that were previously considered too remote or small to support, or for providing access for a single user working remotely. Finally, locations using IPsec can offload Internet traffic locally rather than transmitting it back through the corporate network to a remote internet gateway.

**Security:**

### IPsec VPN vs. MPLS VPN

Both IPsec VPN and MPLS VPN claim to provide highly-secure connectivity as a key feature, but they achieve it in different ways. An IPsec VPN uses the shared public Internet to transport data and uses industry-standard encryption to provide protection against data theft. Because data traverses the public Internet, which is run by multiple operators, these connections are prone to distributed denial of service (DDoS) attacks.

An MPLS VPN, in turn, offers data protection by transporting data over a private network, so only authorized entities have access to the data. Each location’s traffic is segmented from others using an industry-standard customer identification tagging technology known as “label switching.” The data itself may or may not be encrypted within the pipe. Encrypting the data in an MPLS VPN environment provides an additional layer of security, but that may come at the expense of CoS. For instance, if video is encrypted, the network management system may not be able to identify the data as video and assign it a higher priority.

In addition to protecting data against unauthorized eyes, MPLS VPLNs offer protection against service outages caused by a DDoS attack since the data never traverses the public Internet. For example, when a user reaches a third-party cloud service using an Internet/IPsec connection, the session is susceptible not only to intrusions or stolen data, but to the downtime caused by a direct attack on a public address space on the Internet. Those attacks don’t affect connections reaching the cloud via an MPLS VPN, because the MPLS VPN uses a private IP address space.

### Hybrid Networks

Hybrid networks combine two or more technologies in a single WAN. For example, businesses can deploy MPLS VPN at larger or mission-critical sites and IPsec VPN at smaller or less critical sites, and link them together. Or, they might choose to deploy both MPLS and IPsec at the same site—with the MPLS VPN carrying critical or latency-sensitive traffic such as video and the IPsec VPN carrying latency-tolerant traffic such as Email. For example, a business with MPLS VPN connection at a site may choose to augment bandwidth at that site with a broadband Internet connection with IPsec security. Using a combination of these approaches can improve outcomes for a business. Organizations can implement different approaches in different locations, or for different applications to better optimize bandwidth, performance, reliability, and cost on a location-by-location basis, enabling VPNs to drive improved business value.

### Performance Requirements

Because MPLS technology supports traffic policy enforcement, you’ll get better quality for features such as streaming video or audio, and live voice-over-IP calls. For more transactional traffic, such as e-mail and non-critical applications, IPsec may be a practical option.

### How Much Bandwidth You Need

Since IPsec VPNs use the public internet, the amount of bandwidth available at a given time may be variable. An MPLS VPN enables class of service controls to prioritize designated traffic.

### Your Budget

IPsec VPNs are less expensive than MPLS services, but they also generally don’t provide the same levels of network performance as an MPLS VPN.

### Degree of Direct Connectivity Needed

If your organization consists of lots of small sites that need to communicate mainly with a data center, you might run IPsec VPNs only. If these sites need connectivity to other corporate sites, you could connect them to a corporate MPLS VPN service.

Highly Secure Transmission of Mission-Critical Data (MPLS)

Data was transmitted to the datacenter in large batched loads on a schedule of 3 times a week at night so that it didn’t bog down the network during business hours. The data comes from a variety of sources: its franchised retail outlets, plants, and from satellite offices. This mission-critical information includes customer information and information on their customers, so security is of the utmost importance. With the addition of IoT sensors to its network ecosystem, the data volume has increased ten-fold and has caused a need for real-time transmission and redundancy. With MPLS, they get the highest levels of security, performance and Quality of Service (QoS).

Collaborative Work Force (IPsec)

Launching and promoting vehicle inventory is a continuous cycle. The use of collaborative marketing support tools such as web conferencing, and the exchange of marketing materials between dealerships and marketing teams occurs on a daily basis. Typically the transmissions are large due to the high-res nature of the files. Although the information is not as security sensitive as some other data, the continuity and predictability of the network performance at a reasonable cost is important. IPsec enables encrypted transmission of data with medium to high performance at a reasonable cost.

Company Wide Live Broadcasts (MPLS/IPsec Hybrid)

At the launch of every new vehicle, executives hold a live, company-wide broadcast. The broadcast is watched real-time by thousands of employees from headquarters to remote workers around the globe, many of whom are watching the broadcast while continuing with their work. The company has to have the network performance to handle the broadcast without interrupting daily business. MPLS is used in combination with IPsec for internet offload of non-critical data. With QoS, the broadcasts are optimized and virtually latency free.

Corporate Resources On-The-Go (Wireless – Mobility)

Often traveling from dealership to dealership, the direct sales force needs mobile access to sales force automation tools and applications while on-the-go. By enhancing connectivity with mobility solutions, the sales teams have quick access to the resources they need to seamlessly do their job, from virtually anywhere.

Enabling a Robust Customer Experience (Wireless – Wi-Fi)

To improve customer experience, the company has now added Wi-Fi services at retail locations. They can now offer complimentary Wi-Fi to improve their customer’s in-store experience but also push product information and promotions based on their interests.
EMERGING ALTERNATIVES TO ENHANCE VPN FUNCTIONALITY

A variety of newer software-based solutions have emerged to reshape how organizations provision and manage their WANs. For example, with a generic, or universal CPE, an on-demand platform can offer connectivity like a cloud-provisioned solution. Here, all network functions act like apps and are consumed as needed. With this model, companies can still choose from the network function vendors they prefer, deploy exactly the functions they want, and buy the connectivity they need all through a single provider. This is all managed through a centralized self-service portal with robust visibility, management and control.

Another option is to utilize Multi-function CPE options that combine multiple commonly used functions onto a single platform. SD-WAN solutions enable application optimization via dynamic policy routing across multiple network connectivity links. All of these new solutions enable customers to define policies via a portal that are then configured across CPE deployed globally.

These newer solutions provide the enterprise more ways to construct their WANs to make them more agile, more flexible, and better able to meet the current and future needs of the business at lower cost and with greater resilience.

Multi-function CPE

Equipment vendors have designed multi-function CPE systems that can do much more than VPN. While these devices are proprietary equipment from a single vendor, and may not offer all network functions needed, they are more flexible than a single-function device. Additional CPE functions include firewall, LAN switch, Wi-Fi access point, LTE modem, data patterns and venue analytics. Furthermore, these vendors can provide a portal to deploy, configure and manage these devices via cloud-based software control. These functions offer value for verticals such as retail, restaurant, and hospitality with Wi-Fi enabling the retailer to offer public Wi-Fi in the stores and security functions allowing local internet offload.

SD-WAN Solutions

A number of new players have come to market with equipment and software designed for greater flexibility. These Software Defined WAN (SD-WAN) providers have focused on enhancing the performance of VPNs via features such as dynamic policy or performance based routing across multiple network links. Dynamic routing enables real-time selection of the best link over which to send data for a particular application, based on pre-selected policies and performance objectives for latency, jitter, and packet loss. This design can work over any form of network connectivity including MPLS, broadband internet and wireless.

The administrative portals of SD-WAN vendors typically focus on e-controls that enable businesses to build performance...
routing rules or policies and easily change them if needed. This makes deployment, configuration and ongoing management of these devices easier.

**AT&T Solutions**

At AT&T, we’ve extended these concepts further to create differentiated solutions designed to meet the needs of our customers. We have created a multi-function device called AT&T FlexWare that is based on the concept of Network Function Virtualization. CPE functions such as routing, firewall, WAN acceleration etc. are deployed as Virtual Network Functions (VNFs) on the AT&T Flexware device. These virtual functions can be configured and managed via cloud-based orchestrator. More importantly, AT&T provides these virtualized functions from a variety of vendors – making it not just a multi-function device but also a multi-vendor platform for our customers so they can choose and deploy functions that best meet their needs.

For SD-WAN solutions, AT&T is the first provider in the industry to announce both an Over-the-top solution as well as a network-based SD-WAN solution which couples smart SD-WAN CPE with a smart MPLS network. A typical SD-WAN solution is deployed in Over-the-top manner, i.e., SD-WAN CPE is deployed at every customer site and tunnels established over the network transport links among sites. With AT&T’s network-based solution, customers have the flexibility to deploy MPLS only sites, IPsec only sites, and SD-WAN sites – all part of a single, cohesive VPN. This design enables existing customers with MPLS or IPsec VPNs to easily evolve to SD-WAN without undergoing a complete network re-design. Furthermore, in this design, SD-WAN gateways are deployed in the AT&T cloud throughout the world and provide a high level of redundancy. In over-the-top design, the burden to provide resiliency falls on the customer and they have to deploy multiple SD-WAN CPEs at critical sites. Depending on the customer need, AT&T is the only provider that can offer SD-WAN in either Over-the-top design or a network-based design.

AT&T is also integrating SD-WAN solutions with the AT&T Flexware platform. SD-WAN functionality can be deployed as a VNF on an AT&T Flexware device and service chained with other VNFs such as routing and firewall. Coupled with AT&T’s industry leading network connectivity options – MPLS, Broadband Internet, Wireless – AT&T can create a comprehensive high-performance and high-availability network design for customers.
MEETING THE NEEDS OF BUSINESS TODAY… AND TOMORROW

Company demands for communications services are more dynamic now than ever before.

- When a new work-from-home initiative starts, many more employees need remote access.
- When company vehicles are equipped with locating devices supported by a cloud tracking application, traffic between the devices and the cloud application must be accommodated.
- When an application moves from being hosted in a corporate data center to running on a third-party cloud, data center traffic is reduced, and cloud traffic increases.
- When a popular new mobile app for customers rolls out and meets with explosive customer usage, traffic to the data center increases dramatically overnight.

Organizations expect a wide area network that can respond to their dynamic needs. This includes access to a diverse set of connectivity types that offer private connection options like MPLS-based VPNs, public internet-based connections delivered via IPsec, or a combination through a hybrid network solution. And they need the visibility and control to help simplify management of what are often thousands of endpoints.

While there are a number of feature-rich alternatives available today, AT&T has built a robust software-based platform that is transforming the WAN landscape. We are helping our customers integrate disparate networks into a single network of networks. One that offers end-to-end visibility from their connected endpoints through the network and to the cloud. One that brings best-of-breed functions together with a full complement of connectivity options. And is delivered through a single, easy to use interface that puts the control in their hands. So they can optimize every part of the network, and therefore, every part of their business.
For more information contact an AT&T Representative or visit www.att.com/vpn