The role of MPLS in evolving networks.

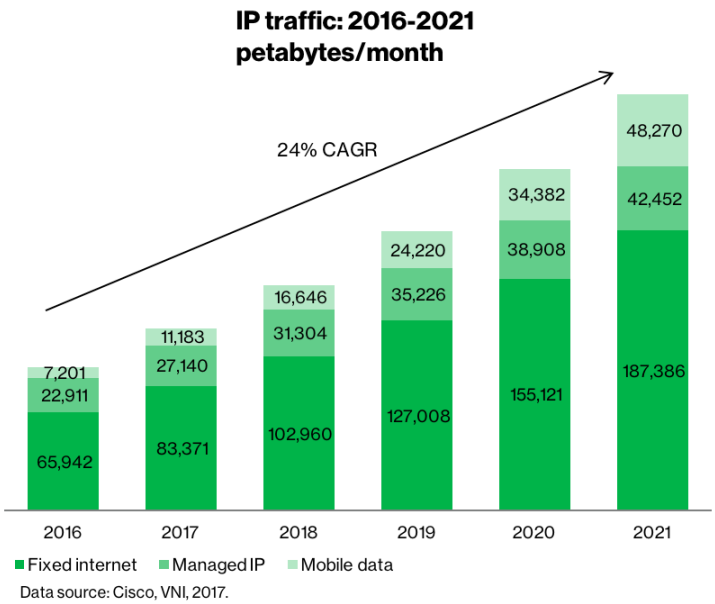
verizon

The network is the lifeline of business–the invisible hand–next to only employees and cash. Small and large enterprises alike are playing a catch-up game in managing networks with innovations in how customers buy, consume and manage products and services. Additionally, cloud adoption, data center utilization and the virtualization of compute and storage elements all contribute to data growth of exponential order. Technology advancements in the way enterprise applications are consumed, such as mobility and Internet of Things (IoT), introduced a myriad of new devices into the network and changed the traffic patterns in Wide Area Networks (WAN).

The data growth is real.

A simple Google search shows that 2.5 exabytes of data is generated in a day, i.e. equivalent to 90 years of HD video. According to Cisco, data is growing at 24% CAGR through 2021 while global IP traffic is estimated to increase nearly threefold over the next 5 years, and will increase 127-fold from 2005 to 2021. Furthermore, Cisco forecasts IP video traffic to be 82 percent of all consumer internet traffic by 2021, up from 73 percent in 2016. It's not a stretch to imagine mission critical application traffic competing with dog and cat videos for network bandwidth on the internet.

Together with exponential growth of data and associated cybersecurity issues, the business risk increases. In addition, the adoption of cloud and datacenter services further contribute to enterprise data growth. The WAN infrastructure needs to adapt to this new environment.



Data source: Cisco, VNI, 2017.

Change in traffic patterns.

Applications that generate, facilitate and store data can now be anywhere in the world. Hundreds of new devices (cell phones, tablets, servers, etc.) are added to enterprise networks each day. This means that enterprise applications are now consumed from a variety of new end-points and geographic locations–disrupting traditional bandwidth requirements, security policies, performance criteria and routing requirements. According to Cisco, the number of devices connected to IP networks will be three times as high as the global population by 2021.

What is the Problem?

The inevitability of the continued growth in data and the change in traffic patterns poses serious challenges to the scalability, security and performance of the enterprise network. Moreover, this problem is amplified for enterprises that use multiple vendors for handling various aspects of complex networks.

Scalability: The network must scale on demand.

As more and more applications move into data centers and hybrid public/private cloud platforms, the need for bandwidth increases. The bandwidth requirement at the source, destination and all the hops in between can vary for a given application due to fluctuating inbound connections. For example, the source could be an application in the cloud or a data center, and the destination could be one or more customer sites. This bandwidth surge can be unpredictable, making it much more difficult to pre-provision. As a result, many enterprises over-provision the bandwidth at the source, as well as at customer sites, thereby overpaying for bandwidth to overcompensate for the inherent unpredictability.

Over-the-Top (OTP) network providers claim to solve this problem by adding redundant paths at the source and destination, and adding more bandwidth as the demand increases. The actual network congestion could be at any hop on the internet. And since they do not own or control the underlying internet, the bandwidth at each of the hops in between remains 'Best Effort' and is not publicly revealed. Meaning, the "scale" happening at the source and destination sites may not meet the application bandwidth requirements end-to-end.

Security: Network and data security must be intelligent and consistent.

Enterprises, to be successful, need to serve customers with integrity and are also obligated to protect customer data–both at rest and in transit. The challenges increase as customers access data from multiple devices with varying (or lack of) security policies. In the midst of all the data breaches, leaks, service interruptions, security violations, Malware, Spyware and DDOS Attacks–no CIO wants their company to be the next breaking news story.

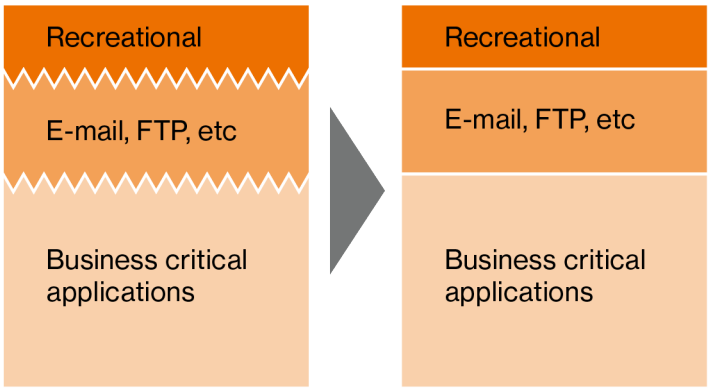
Securing the data at rest is generally not a problem, but securing the data in motion has become more of a challenge. The root of the issue is that the data traverses multiple, unsecure paths via many hops over the internet. Many Over-the-Top (OTP) nontraditional service providers, that promise security, do not own or control the underlying network or routers in the data path. These underlying network elements are owned and managed by multiple service providers that do not communicate or collaborate with each other. The security solution designed by OTP providers is typically at the application layer and the data eventually must traverse the internet, making it vulnerable to a myriad of attacks.

On the other hand, a network service provider who owns the underlying network infrastructure is capable of designing a secure network to meet enterprise business needs. Wherein the enterprise, not the service provider, will choose the end points that need internet access. This type of closed network is intrinsically secure and offers protection against DDOS attacks, Malware, Spyware and the like, that can cause severe network interruptions.

Performance: Network performance must help improve application performance.

Today, whether it's a popular content generating social media application or Point-of-Sale (POS) transaction–it generates, consumes, stores and transfers data over a network directly or indirectly. In a race to learn everything about the customer, to serve customers better and to out-innovate the competition–enterprises generate, live and breathe tons of information. Data generated by customers, employees, vendors, network elements (circuits, routers, firewalls etc.) and applications (logs, configs) is immense and growing. This data is routed through a myriad of network elements, often across the globe, with varying bandwidths.

Networks must be smarter to detect the application riding on them and allocate the bandwidth required and the priority needed. Networks must have the ability to prioritize traffic and offer better than the 'best effort' service that the internet provides. Enterprises must be able prioritize applications at the point of entry (ingress), through the backbone network and when exiting the network (egress). While this is not possible using public-only network infrastructure (internet), it is possible with an MPLS-based network. As an example, enterprise voice and video applications require a higher priority than just casual internet browsing.



Connect to cloud and data centers securely and reliably.

Cloud and data center services have become an essential part of the enterprise network. More importantly, they are here to stay. Some of the most clichéd advantages include cost savings, CAPEX to OPEX spending models, business agility, "Just in Time" resources and more. The list goes on and rightly so.

However, enterprises need to make a conscious decision about 'how to consume' these services. They need to understand the hidden and unintended costs of putting corporate intellectual property on the internet. The ideal way, would be to connect via a private network where the traffic never touches the internet. Once the traffic hits the internet, the priority of a mission critical cloud application that's vital for the enterprise business is given the same priority as the latest viral video of the day. More importantly, the security aspects are much more alarming. Some providers of cloud-based security products (firewalls) recommend the traffic be funneled to their cloud location in order to "sanctify" the traffic. In addition to the inherent risks of handing over enterprise traffic to a 3rd party over the internet, it also adds multiple hops in the data traversal path. Every additional hop that data makes on the internet poses a security risk, in addition to obvious latency issues.

Verizon Integrated Solutions.

The answer to today's network challenges is in finding a provider who can offer integrated network solutions to meet continuously evolving business needs, while diligently managing the scale, security and performance of your network and applications, 24x7x365.

Irrespective of where the applications reside, whether in hybrid public/private clouds or in remote data centers, connecting users to applications over a secure, private, scalable network that provides end-to-end performance is critical to business. Verizon provides a range of network solutions for enterprises of all sizes, including:

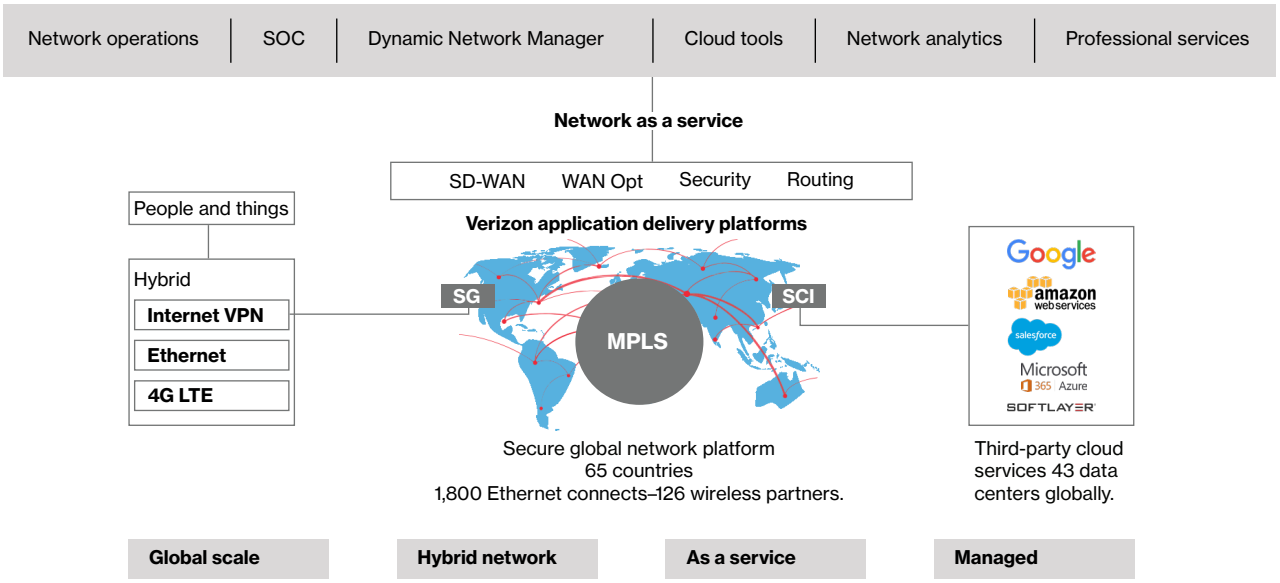
- Private IP, an MPLS based network, enables local, national and global customers, to effectively communicate over a secure, efficient and flexible private network infrastructure.
- Private IP provides the foundation for automating and streamlining business processes, including e-commerce, shared intranets and extranets.
- Unlike public networks, Private IP supports traffic prioritization based on the application profile.
- Verizon's Dynamic Network Manager, a component of our Software Defined Networking (SDN) product, enables customers to virtually control bandwidth speed, schedule port changes, receive alerts and access reports.
- Secure Cloud Interconnect provides easy access to applications and data hosted by leading Cloud Service Providers using secure MPLS.
- Software Defined Networking (SDN) enables software-based control of network functions using cost-effective, general-purpose hardware.
- Virtual Network Services provides a platform that enables application delivery in a fully managed software-based platform.
- Managed Network Services helps improve application performance and availability, and protect business processes.

Conclusion.

The growing number and type of enterprise applications and devices is creating a never-ending sequence of data generation, storage, management, consumption and transfer. The increase in data centers, storage and cloud services is just another indication of the intrinsic value that data offers to enterprises. As the number and variety of devices in the path of the data increases, the network complexity also increases. Enterprises of all sizes face the same conundrum-solving for the scale, security and performance of their network-while managing costs. There's absolutely no magic bullet that can address all network parameters. Enterprise networks need to be diligently managed by experienced professionals to keep applications performing as designed, enhance the customer experience and protect and grow stakeholder equity.

While enterprises are busy handling their business, it's sensible to select a network provider who offers an integrated solution for constantly evolving requirements. Providers must have experience in tackling the enterprise grade network, maintaining performance for every network element in the path of the data and backing the reliability of the network with stringent Service Level Agreements (SLAs). Network service providers, unlike the Internet-based OTP providers, have the ability to prioritize customer traffic as required by the application and above all, have proven experience in 24x7x365 management capabilities of critical networks. A Verizon solution that includes Private IP, Secure Cloud Interconnect, Software Defined Networking (SDN) and Virtual Network Services (VNS), is an integrated, managed solution that meets all these critical network and application requirements.

Verizon Network



References:

White paper: Cisco VNI Forecast and Methodology, 2016-2021.
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html

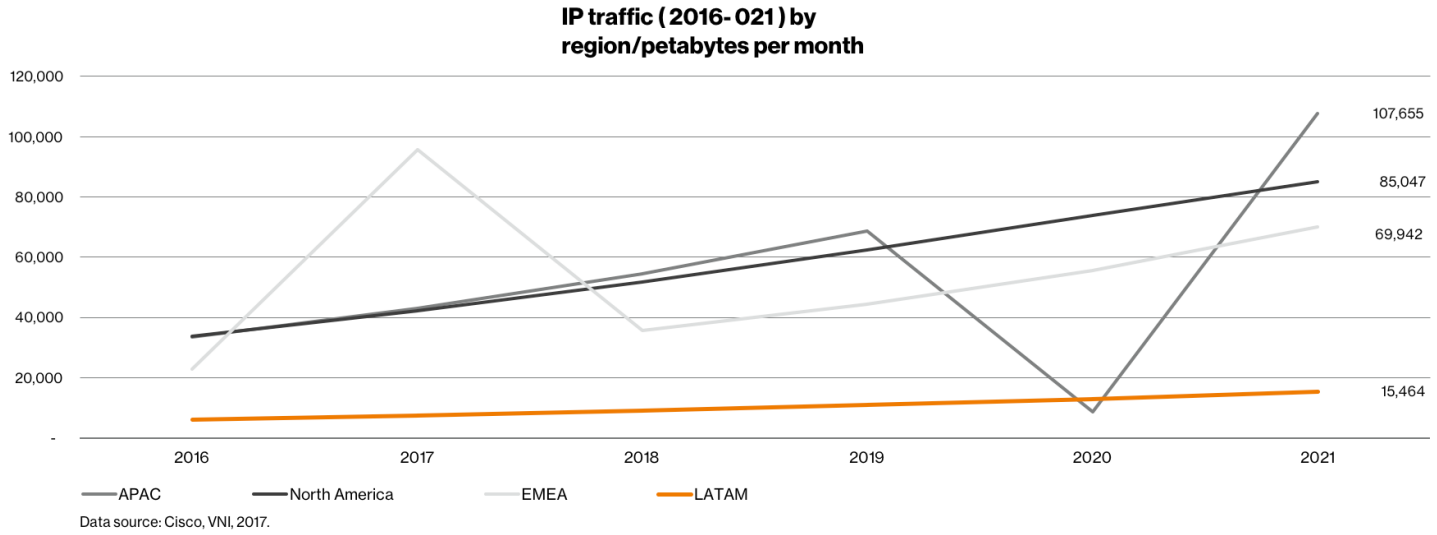
White paper: Making the case for MPLS

Learn more:

Contact your Verizon Enterprise account manager to learn how our network solutions can help transform your business or visit:

www.verizonenterprise.com/products/networking/private-ip/

Appendix:



Data source: Cisco, VNI, 2017.

verizon