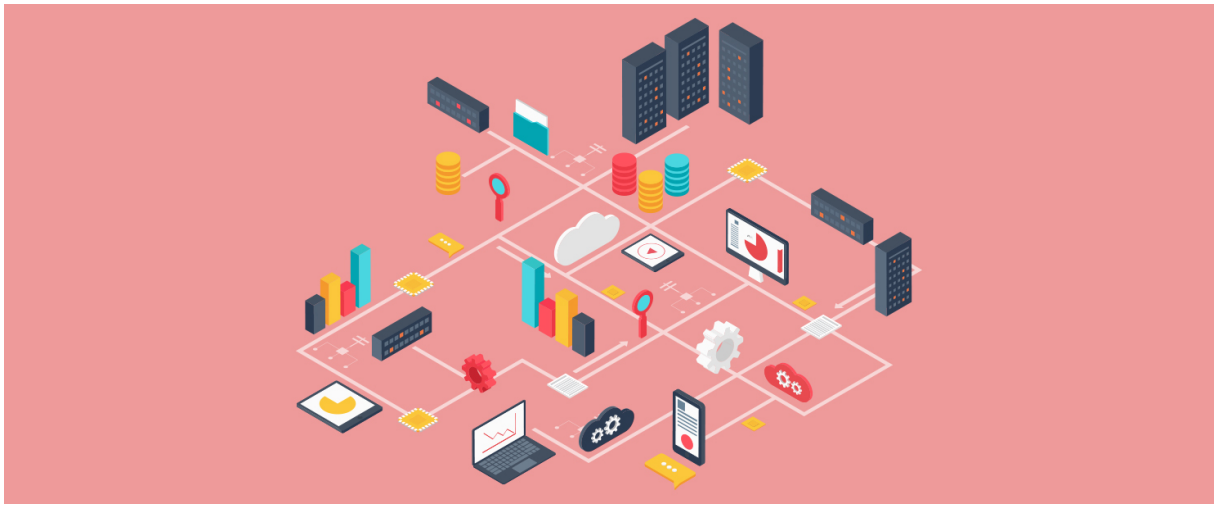

# Software-Defined Wide Area Networking (SD-WAN)

2015-12-11

## Software-Defined Wide Area Network: Does it hold the potential to disrupt MPLS VPNs?

In brief… Yes.

### But let's go back a bit…

In the 90s, we had a surge in label switched shared wide-area technologies such as Multi Protocol Label Switching (MPLS). MPLS rocked the boat and actually succeeded over the existing wide-area-networking (WAN) technologies such as frame-relay and ATM. There is no doubt that the emergence of MPLS disrupted the WAN landscape, which begs the question *'Why did we need MPLS VPNs, when we had a perfectly good Internet which worked rather well?'* Well, the Internet, although phenomenal and groundbreaking, was indeed riddled with challenges. These challenges impacted massive businesses that were dependent on effective communication methods between sites, offices and enterprises. The main issues for these critical communications came down to two flaws; speed and security. The Internet, in all its glory, was unable to offer true security and speed to business critical low latency applications. It didn't take long for some very clever folk at the Internet Engineering Task Force (IETF), and other leading network vendors, to recognise that innovation in this sphere was required. They decided to address these obvious shortcomings by allowing routing equipment to seamlessly separate traffic across a shared Wide Area Network (WAN) into Classes of Service (CoS). Routers would now have the correct queuing algorithms to cope with congestion. If congestion occurred, they would have the ability to prioritise certain traffic types over others. This effectively reduced latency, jitter and packet loss for high priority services. As a result, businesses and operators could make the best use out of their limited bandwidth resources. This did come at a price though! To

help the problem of security limitation, these clever folk put together frameworks and protocols which allowed for the creation of logical routing instances over the same hardware used to route traffic over the Internet. For the first time ever, it was now possible to separate traffic at a software level.

## What did this mean for the industry?

Operators around the world were now able to leverage common infrastructure (routers and backbone links) and provide customers with their own private WANs across an operator's shared packet switched network. This is when MPLS, VPN, VRF, QoS and CoS became the buzzwords in boardrooms and IT conferences around the globe. **20 years on, what are the key factors that led us to a precipice of MPLS VPN disruption?**

- As the Internet grows, so the capacity of links has too. The price of bandwidth has conversely plummeted.
- The processing power of edge routing devices has increased. Because of this, processing encryption tax (which was previously a hindrance to offering large bandwidth encryption at scale) has become less of a bottleneck.
- Software Defined Networking (SDN) and evolving associated standards are maturing, allowing for an even clearer separation of the control and process plane on network infrastructure.
- Enter the 'cloud' revolution. This was driven by a need for workers to be mobile. This has led to a mass migration of enterprise software services moving out of the enterprises' private networks and straight onto the Internet (referred to as the 'Cloud') – such as Amazon Web Services, Drop Box, SalesForce.com, Google Drive, Saicom Cloud PBX to name a few. Because of this, it's not critical for organisations to host any of their applications on their own network. The services are all on the Internet, so a user simply needs an Internet connection to access their applications and data in the cloud.

From what we've discussed until now, it's obvious that this development wasn't good news for MPLS VPN's providers. But if one wanted to communicate securely with other sites and data centres, surely we still need an MPLS VPN to access this securely? Well, no. Several hardware and software vendors were hot on this and saw the potential gap in the market.

# Enter Software Defined - Wide Area networking (SD-WAN)

A new breed of disruptive companies are beginning to emerge into the Software Defined – Wide Area Networking (SD-WAN) technology space. Naturally, the large incumbents, vendors and operators are mostly resisting this change and trying to grasp onto existing revenue streams.

## So what's the big deal about SD-WAN, and what has differentiated it in the market?

So by now, I'm sure you're asking yourself: what's new about SD-WAN? Isn't this just lipstick on a pig, a new buzzword to sell more equipment? Have companies like Cisco, Alcatel and Juniper not allowed organisations to string IPSEC tunnels over the Internet for years anyway? Well, yes, they have. The back-end components and protocols have been in play for some time plus standards have been in existence, which enabled organizations to create secure VPNs over the Internet for quite a while. But, the difference in this new SD-WAN technology, is that they've made it so easy, almost seamless. You don't have to employ heavy lifting network and security experts to get your WAN running over the Internet, with SD-WAN it really is child's play.

## What has SD-WAN done, exactly, to improve the Quality of Experience (QoE)?

Well SD-WAN vendors (such as VeloCloud) have created an easy to use dashboard (or orchestrator) which allows the administrators to quickly set up a meshed (point-to-multipoint) WAN over the Internet in mere minutes. Plus, some of these vendors have even employed **smart algorithms and features**.  In VeloClouds case, these include:

- Flexible Connectivity Choices (The ability to mix inexpensive broadband and MPLS circuits into the same edge device).
- Transport Agnostic - Dynamic Multi-Path Optimisation
    - Continuous Monitoring
    - Dynamic App Steering
    - On Demand Remediation
- Ease of Network Services Insertion - business policy framework which enables one-click services insertion, eliminating complex configurations.

- Business Policy Driven Branch WAN - An approach to SD-WAN management which is business policy driven. Automatic application recognition and categorisation. This removes the task of identifying apps by protocols, ports and IP addresses.

- Deep application recognition, VPN, Next-gen Firewall.

Whilst features are key, one also needs to find a significant reduction in Total Cost of Ownership (TCO). In Veloclouds case we've seen a Triple Benefit TCO Savings (Services, IT Resource or Outsourcing, Network Infrastructure.

## Does this mean the end for MPLS VPNs?

So does this mean you should ditch your MPLS VPN provider and leverage off the Internet for your WAN? Well, not just yet. Some SD-WAN technology will allow you to operate it in parallel to any existing WAN allowing you to use both technologies where you feel it makes sense… meaning you can ***operate in parallel***.

## Making the move to Software Defined - Wide Area Networking

If you are contemplating making the move to SD-WAN, you need to consider the following next steps:

- Ensure that your current Managed Service Provider (MSP) or Internet Service Provider (ISP) is offering a managed SD-WAN as an alternative to your MPLS VPN service.

- Decide whether you will do this yourself or use a partner to manage this for you. This really comes down to your ability to run your own WAN. ISP's and MSP's will generally have the technical ability and infrastructure to ensure that your network remains up. From a commercial perspective it will also make sense to leverage off the ISP's bulk device and licensing power with vendors.

- Check that your provider can offer you both MPLS and SD-WAN as you still might want to run both these technologies in parallel.

- When it comes to Internet bandwidth, you'll need to get the most reliable bandwidth possible. Stay away from unlicensed wireless. Opt for licensed spectrum wireless links and fibre optic connection where possible.

- Many ISPs offer different contention ratios on their Internet infrastructure - try and procure the lowest contention ratio at the best price.

- In most multisite MPLS VPN deployments it makes sense to centralise your Internet breakout in the cloud. Whilst this made business and technical sense in the past when your applications were hosted in your WAN, as applications start moving to the cloud, it makes perfect sense to offload this Internet bandwidth at the edge of your network onto higher capacity Internet links at a fraction of the cost of backhauling this traffic over your expensive MPLS WAN links.

- Whilst the SD-WAN vendors' Customer Premises Equipment (CPE) or Edge device is important, it is as important to get a view into the portal or orchestrator interface. This is really where the magic happens; you need to be comfortable that it can offer you real-time analytics and insights into your SD-WAN, this needs to be easy to use, provide you with quick easy information and must support One Click Provisioning of your Edge devices.

## So, where to from here?

As organisations increase their use of public cloud services, which are forecast to grow 20% CAGR thru 2018[1], they will look at more technically and commercially efficient ways of supporting their Internet and WAN requirements. The commercial and operational benefits will almost certainly sway enterprises to migrate off expensive MPLS VPN networks and onto cheaper Internet circuits managed by SD-WAN. By year-end 2018, 10% of enterprises will have replaced their WAN routing with SD-WAN-based path forwarding, up from less than 1%[1]. SD-WAN completely negate the need for an MPLS VPN, and like all disruption it will create some interesting competition amid vendors and operators around the globe. [1] *Andrew Lerner, Neil Rickard (2 July 2015): Technology Overview for SD-WAN (ID:G00279026).* ***Post written by Greg de Chasteauneuf Chief Technology Officer (CTO) – Saicom Voice Services***