CableLabs®

Technical Brief

Randy Levensalor, Lead Architect, CableLabs, R.Levensalor@cablelabs.com March 2016

CUSTOMER IMPACT FROM VIRTUALIZING NETWORK SERVICES

The impact of Network Function Virtualization (NFV), the technology trend for virtualizing network services and automation on the managed network services of business customers is described in this paper. These network services are traditionally manually deployed on purpose-built physical devices. With the advancement of NFV and automation, network services can be activated and modified without any manual intervention. By taking advantage of these advancements, the customer's experience with a service provider will be seamless, and will align with their expectations from pure-play cloud providers, such as Amazon and Microsoft. This can benefit both the MSO and the customer. The three top MSO and business customer benefits from NFV and automation are highlighted below:

MSO benefits:

- Reduced time to market
- Cost savings
- Rapid innovation for increased revenue

Business customer benefits

- Prompt service activation
- Additional service offerings
- Improved customer service through better end to end visibility

Introduction

This paper discusses the impact of increased automation in conjunction with virtualization for business services customers along with the benefits to service providers who deploy these solutions. These advancements in technology offer potential cost saving and increased revenue opportunities, they also increase the quantity and variety of competitors in this market space. These six examples of business services are a representative set of network-centric services that can be offered to business customers: Ethernet and IP MPLS VPN, SD-WAN, Security services, Bandwidth on Demand, Cloud-managed wireless LAN, and Managed Route. These services have a managed services component where the management of IT tasks is outsourced to the service provider, as many variations on these services and other services

can be delivered. This set provides the context and expectations needed to move forward with most network-centric business services.

Telecommunications providers, OTT providers, and our members have begun deploying Network Function Virtualization (NFV) to serve business customers. NFV is transitioning from proof of concept and evaluation phase to production in either 2016[1] or 2017[2]. In general, service providers are no longer asking, "What NFV services should be deployed?" but "What NFV services to deploy first?" Capital and operations costs will drive many of these decisions but should not be the sole factor when evaluating the virtualization of services. The impact to customers and the types of vendors who are able to offer competing services will also need to be taken into account. This paper evaluates the customer impact of virtualizing and automating a range of network-centric services.

Highest customer impact when deploying NFV:

- Virtualizing services that currently require purpose-built Customer Premise Equipment (CPE).

Highest MSO risk by delaying NFV deployments:

- Customers adopting managed network services from Over The Top (OTT) providers

The six examples of business services listed above are evaluated in this paper. This is a representative list of managed network services of which the findings can be extrapolated and applied to other network services and use cases that are not explicitly covered in this paper.

NFV and Software Defined Networking (SDN) capabilities in the market today could be used to deliver these services, but contemporary solutions often lack the standardization, maturity, operational capabilities, or infrastructure that are needed to rapidly deploy them at scale or 'openness', allowing innovation at the pace demanded by the market. While the customer experience on a per-service basis should remain relatively consistent, many cost savings and operational changes will not be fully realized until the NFV/SDN solutions and operation models mature.

CableLabs is driving advancement in NFV on several fronts, grounded by open dialog with our members. This includes:

- Making contributions to reference platforms developed through collaborative open source projects such as OPNFV, OpenDaylight, and OpenStack.
- Driving requirements into SDOs in the NFV/SDN space including ETSI NFV ISG, the leading body for defining NFV architecture and solutions.
- Ensuring that our members are able to take full advantage of the rapidly growing NFV/SDN space through updates on the work as it evolves and through engagements with NFV/SDN vendors and their products.

Customer needs

The landscape is changing for business customers as they have a much broader array of choices when purchasing managed network services. The range of small and large OTT providers entering the market, telecommunications companies targeting broader market segments, and MSOs targeting larger

[1] http://www.lightreading.com/nfv/nfv-strategies/nfv-will-go-commercial-in-2016/a/d-id/721046
[2] http://inform.tmforum.org/news/2016/01/nfv-pocs-to-continue-in-2016-adoption-to-accelerate-in-2017/

businesses outside their traditional footprint are rapidly expanding the options available to the business customer[3]. NFV is starting a new race for the "First mover advantage" and a smaller barrier to move with reduced customer startup costs for managed network services. It is not only important to be first to market, but managed service providers will need to continue to keep their customers satisfied to stay on their platform.

OTT competitors are able to offer more network and business services over a standard Internet connection. Customer's increased expectations for automation and ease of use can in part be attributed to the adoption of OTT alternatives. Customers are becoming accustomed to more configuration options and fully automated / self-service portals.

Small businesses are expecting more services from their provider and are increasingly looking at pure-play cloud application providers to address these needs. These services must be low cost to fit into the IT budgets of small businesses that often have many of the same security and remote worker requirements as larger companies with limited resources that price high-end solutions out of their reach.

Medium business customers continue to look to offload the bulk of their IT needs to focus on their core business proposition. They are willing to pay more for managed services than small businesses in exchange for increased reliability, available and security; however their resources are still relatively limited.

Enterprises customers typically have their own dedicated IT staff. They want to be able to customize and scale all of their services and often integrate external services through APIs rather than going just to an external portal. Compliance and auditing are also much larger factors for large enterprises.

Benefits of Virtualization

Business customers of all sizes can see substantial improvements in the lifecycle management of the services offered as a side-effect of their service provider virtualizing their offerings and taking advantage of SDN. With reduced activation times, there will be a lower barrier for customer adoption of new services.

MSO Benefits

When delivered properly, virtualization will benefit the MSO through:

- Cost saving
  - Minimize the number of supported hardware platforms
  - Automate tasks that are currently performed manually
  - Reduce capital investment in hardware as well as the expense of managing the inventory
  - Potential reduced energy consumption
- Reduce time to market
  - Minimize turnaround time to activate new services

[3] http://www.lightreading.com/cable/cable-business-services/3-big-hurdles-as-cable-courts-the-enterprise/d/d-id/719721

    - Deliver additional types of services
    - Deliver new capabilities on existing services to existing customers
    - Dynamically deliver and upgrade new services with software updates to services
    - Easily integrate with partner platforms through APIs
- Rapid innovation through frequent releases
- Improve customer satisfaction
    - Accelerated service activation
    - Additional service offerings
    - Improved customer service
    - Self-service
    - High-availability through redundancy and decoupling configuration information from physical devices
    - Horizontal scalability
- Increase volume on higher margin managed services products
- Address vertical markets through personalization and bundling
- Dynamic interconnects and service chaining
- Support for private cloud

The interactions in the service definitions for automated customer interaction can take several forms based on the customer's preference. This can impact the full project lifecycle from service activation, to updates, to deactivation and can be performed via a provider's web portal, mobile application, remote API service, or Customer Service Representative (CSR). Although talking to a live CSR will be eliminated for several customers, CSRs handling the remaining customers' requests will be able to make all of the changes for the customer and will not require the assistance of a technician for any lifecycle changes. With virtualization / automation, all customers will be able to make any lifecycle changes 24/7.

The service provider will store all changes remotely for standard lifecycle operations. Physical access to the vCPE and other hands on work may still be required for troubleshooting. The number of resources troubleshooting issues that are reported by the customer should be reduced.

With many of these services, the provider will have more fine-grained access to analyze the customer's network health and perform proactive maintenance to ensure optimal performance and reliability. Some customers have concerns over access to their confidential information and/or intellectual property. This can be overcome using a model whereby critical data remains on site while non-critical information is hosted or backed up offsite.

Without a CPE

Figure 1 and Figure 2 depict the number of interactions and people that a business customer will be required to interact with to deliver a new service. This assumes that a broadband Internet connection has already been established to all of the customer sites. These two diagrams depict services that do not require additional equipment be delivered to a customer site.

Without a CPE, a customer will still interact with two or three different groups of employees at an MSO. This is not only a cost for the MSO, but it also adds complexity and time to the customers call them to activate a service for the customer. Automating and virtualizing these services can transition the customer to a self-service model or have a single contact that is able take their order and activate it.

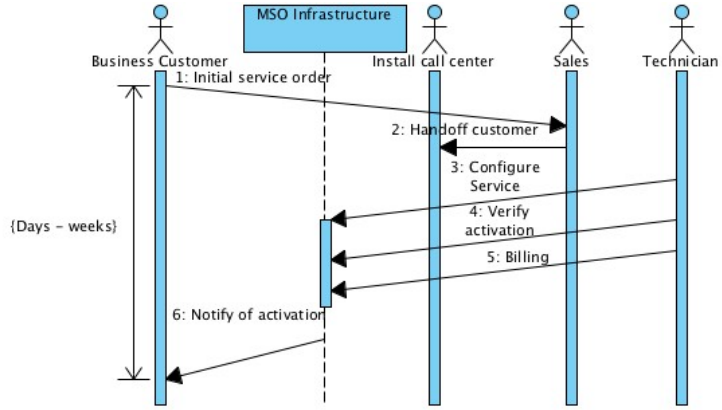

Figure 1 Current Activation

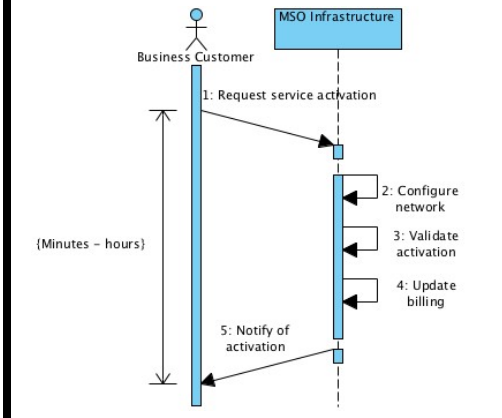

Figure 2 Automated Activation

With a CPE

Figure 3 and Figure 4 depict the number of interactions and people with which a business customer will be required to interact to deliver a new service. Activating the broadband connection is a type of service activation and can benefit from automation. Broadband activation does not have the same NFV benefits with regards to delivering a CPE to a customer site. Since this is the first service, a CPE will still need to be delivered to the customer. Broadband activation is not covered in these use cases due to those differences in the virtualized use case. These two diagrams depict services that require additional equipment be delivered to a customer site.

Delivering and/or configuring the CPE in Figure 3 and Figure 4 at the customer site would need to be repeated for each customer site. The sections highlighted in the red boxes denote additional steps that are unnecessary in cases where service activation does not require CPE installation; these are at least four additional steps that include coordinated access to a customer site and result in increased time (by almost an order of magnitude).

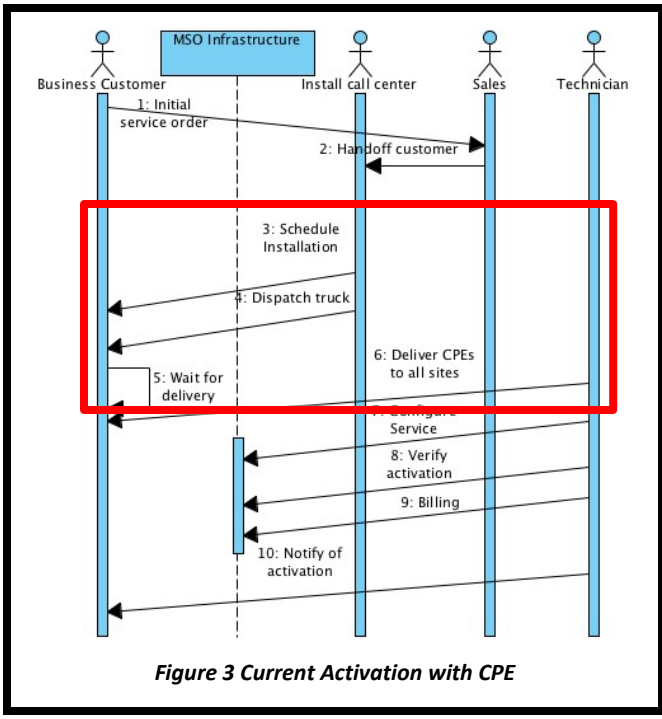

Figure 3 Current Activation with CPE

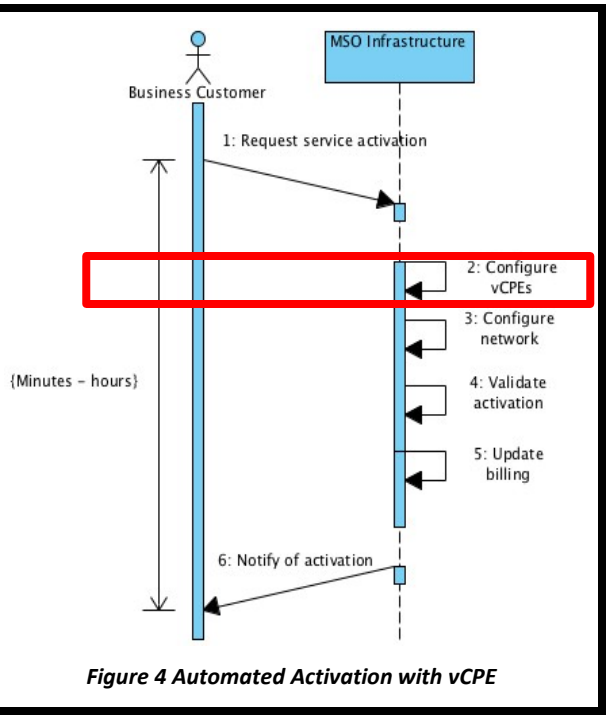

Figure 4 Automated Activation with vCPE

Traditional vs. Virtualized Capabilities

Activation time is one of the more critical customer concerns. There are many additional capabilities that can be considered in the overall customer experience and impact when virtualizing services. An extensive list of customer-impacting capabilities is evaluated in Table 1.

When reading the table, note the following qualifications:

- CPE references only apply to services that traditionally require additional devices on the customer premise.
- Traditional and automated descriptions are representative in nature and not specific to any service provider.
- The experience of the capabilities can vary based on the specific service and the provider's deployment.

The columns provide the following types of information:

- "Capability" – The short name for the capability being evaluated in the given row.
- "Description" – The more detailed description of the capability.
- "Traditional" – The general consensus from the contributors of this paper on how the customer experiences the capabilities of traditional services as they are typically deployed today.
- "Automated" – The generally desired state that can be achieved with automation improvements to deliver these services. Virtualization of at least some portion of the service is often required and the most effective method to automate the service management.

Table 1 Comparison of Traditional and Automated Capabilities

Capability	Description	Traditional	Automated
Activation request	The method a customer uses to initiate an order for a new service.	Contact a call center	Self-service through a portal, app or API
Activation time	The duration of time from the customers' activation request to the service being provisioned and available.	Weeks – months	Minutes – hours
CPE	Equipment that resides on the customer premise and is required to deliver a service.	Purpose built hardware at customer site	General purpose platform supporting multiple services
CPE configuration data repository	The location where the configuration settings for the CPE are typically stored.	On CPE and a backup	On shared cloud storage
Common hardware platform for managed services	With a common platform, all managed services can be delivered using the same type of hardware at the customer site instead of requiring specialized devices be added to the customer's site for each managed service.	Separate platforms (dozens of types of CPEs)	Common platforms (vCPEs)
Snapshot configuration	Archive a known good version of the service configuration. This can be used later to restore a known state.	Not typically done	Yes
Rollback configuration changes	This implies that changes are not only tracked, but the customer or service provider has the ability to revert a change and go back to a previous state.	If EMS system is configured and supports this capability.	Yes
Service configuration change request	The method a customer uses to initiate a change to an existing service.	Call center	Self-service through a portal, app or API. Triggered on a set of pre-defined rules or analytics.
Service configuration change duration	The duration of time from the customers' change request to the service being modified and available.	Hours - days	Second – minutes
Deactivation request	The method a customer to deactivate a service.	Call center	Self-service through a portal, app or API.
Deactivation time	The duration of time from the customers' deactivation request to the service being deactivated and no longer available.	Hours - days	Second – minutes
Trial period	A period of time where a customer can try a service without a commitment.	Cost prohibitive	Easily available
Service assurance dashboard	A portal containing current and historical data related to service assurance.	With newer services	Normalize and view all data
Performance reporting	Providing periodic or on demand reports to customers regarding performance metrics and compliance.	Monthly reports for carriers	Customizable and available to all customers

Capability	Description	Traditional	Automated
Performance alerting	Alerts, such as emails, letting customer administrators know how services are functioning.	Only available with newer services	Customizable and available to all customers
Single front-end for the platforms	The ability for customers to manage all of their services through a single front-end portal with a consistent user experience.	Multiple front-ends (one per service)	Single unified front-end portal
New capability rollout duration	The duration of time for a service provider to roll out a new service or feature to their customers	9+ months	Weeks
On Demand services and IT integration	The ability for customers to integrate changes from their service provider in existing IT processes. For instance, increasing the bandwidth of a MEF connection between two sites while a backup is being performed and restoration to original state once the backup has been completed.	Not available through open APIs	Seamless integration through open APIs that can be called from IT or other applications
Exposed security surfaces	The number of components that are exposed to a malicious security attack. The more exposed surfaces the greater the exposed security surface area.	Well known and relatively hardened platforms	Additional risk with more components. New methods and skills sets required
Ability to roll out security patches	Ability to address security vulnerabilities once they have been identified.	Difficult for firmware updates and require longer test cycles	Quickly roll out security patches over virtual infrastructure
Risk of downtime due to software defect	Risk of a software defect impacting several customers and services.	Lower risk with few software components	Increased risk with more software components shared across several services
Risk of downtime due to hardware failure	Downtime caused by one or more hardware failures.	Multiple devices in series will increase the failure rate at customer premise	Ability to move workloads across multiple hardware devices for redundancy while reducing the number of physical devices

Service Definitions

This section provides details of six network-centric services that are currently offered by MSOs or telecommunications service providers with brief descriptions and a high level set of capabilities. These are used to illustrate services that could be automated through the use of virtualization, and are summarized in Table 2.

The columns in Table 2 provide the following types of information:

- "Service" – The short name for the service being evaluated in the given row.
- "Description" – The more detailed description of the service being evaluated.

- "CPE" – Indicates if a CPE is traditionally required to deliver the service.
  - "Yes" indicates that a service traditionally requires a CPE.
  - "No" indicates that the service traditionally does not require a CPE.
  - "Maybe" indicates that depending on the specific type of service, a CPE may or may not be required.
- "OTT" – Indicates if the service can be provided Over The Top (OTT) meaning there is potentially competition from vendors that do not own the network connection.
- "Market size (Billion) / year" – The projected global market size of the service in billions of US dollars followed by the year that the market is projected to reach the given size. The footnote indicates the source of the projection. These are useful for general sizing and relative scale of the opportunities but are not indicators of the actual market size that is addressable by MSOs.

Table 2 Service Overview

Service	Description	CPE	OTT	Market size (Billion) / year
Ethernet and IP MPLS VPN	Layer 2 & Layer 3 VPNs with bandwidth guarantees	Yes	No	$81 / 2018[4]
SD-WAN	Software Defined Wide Area Network - A layer 3 network over multiple underlay networks.	Yes	Yes	$12.5 / 2020[5]
Security services	Any managed services dedicated to security. (i.e., firewall, DDoS mitigation)	Maybe	Yes	$29.9 / 2020[6]
Bandwidth on demand	On demand adjustments to customer's available bandwidth	No	No	Not available
Cloud-managed wireless LAN	The remote management of the customer's wireless network	Yes	Yes	$2.5 / 2018[7]
Managed Router	Management of the customer's local network and core network services	Yes	Yes	Not available

[4] Infonetics Research Ethernet and IP MPLS VPN Services (September 15, 2015)
[5] http://www.lightreading.com/carrier-sdn/transport-sdn/verizon-taps-viptela-to-beef-up-sd-wans/d/d-id/721152 IDC
[6] https://www.alliedmarketresearch.com/press-release/global-managed-security-services-market-is-expected-to-reach-29-9-billion-by-2020-allied-market-research.html
[7] http://mspmentor.net/managed-services/041214/idc-cloud-managed-wi-fi-market-hit-25b-2018

Ethernet and IP MPLS VPN

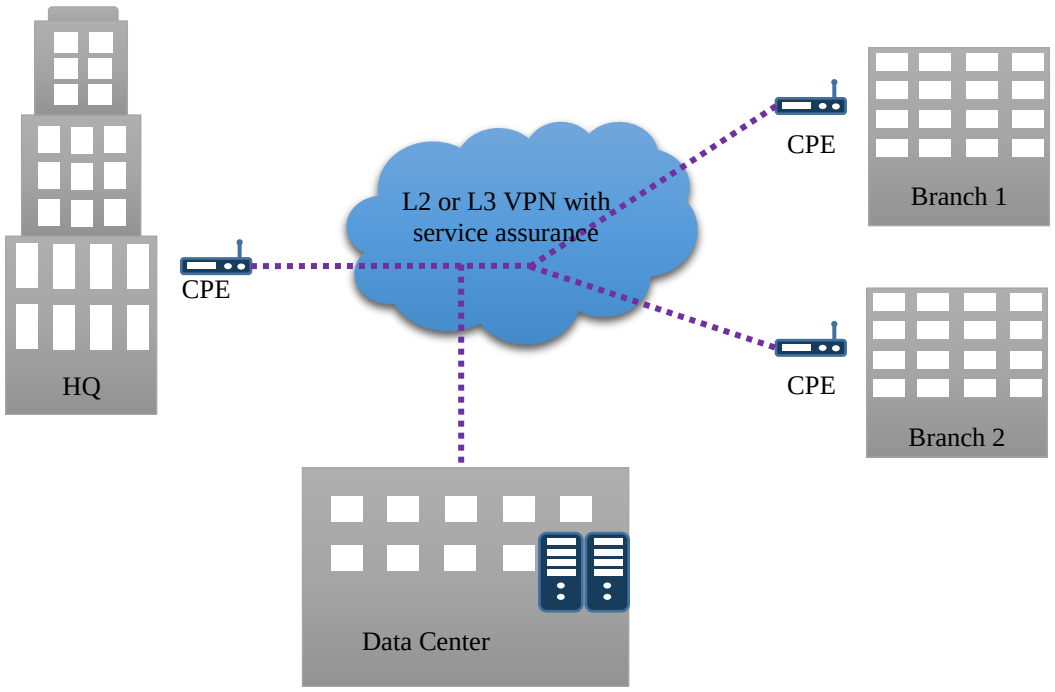

Figure 5 Ethernet and IP MPLS VPN

Ethernet and IP MPLS VPN connections offer guaranteed bandwidth and the ability to prioritize network traffic. These are replacing more TDM and frame relay products. Simple cases are private lines between a customer site and the service provider's network. More complex solutions connect multiple sites, as shown above. Ethernet services provide layer 2 tunnels, while IP MPLS VPNs provide layer 3 tunneling.

Layer 2 VPNs enable the customer to manage their routing. Layer 3 solutions have routing that is managed by the service provider and require less management and expertise be performed by the customer.

Multiple CPEs are traditionally required at each site to manage the physical connection and service assurance. Since multi-site deployments often have locations outside of a service providers footprint, installing these physical deceives can be costly and time consuming. OTT providers are not able to offer a competing solution due to the dependency on the physical connection to the site.

Virtualizing this solution will eliminate the need for several CPEs. By eliminating CPEs and automating the network configuration, it will be possible to provision this solution in minutes instead of months and can allow for offerings of a much wider array of services levels, instead of the two or three that are typically available.

SD-WAN

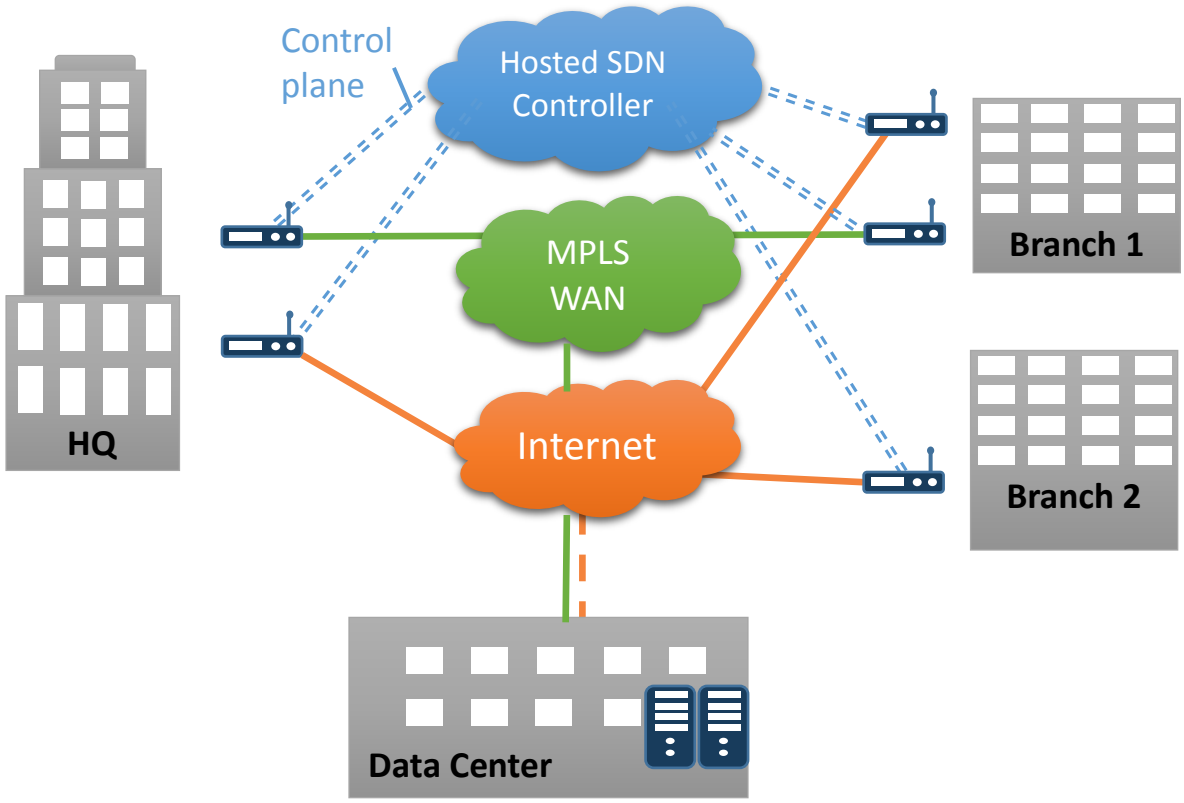

Figure 6 SD-WAN

Software Defined – Wide Area Networks (SD-WAN) services provide many of the same capabilities as IP MPLS VPNs over multiple underlying network types. This includes Ethernet and MPLS VPNs in addition to basic broadband connections. While the bandwidth is not be guaranteed over a basic broadband network, the SD-WAN controller is able to adapt to changing network conditions and prioritize network traffic based on the application needs. Broadband connections typically offer more average throughput than connections with guaranteed bandwidth. This can actually enable a better overall customer experience at a lower cost.

There is typically a central controller that aggregates performance data, authentication and prioritization to optimize the global network. The endpoints on customer sites can either be a dedicated CPE that sits between the customer's local network and the external network(s), or be virtualized with the functionality running on an existing device at the customer premise.

OTT competitors can offer this service since it is independent of the underlying network. Service providers can provide a differentiated solution by integrating this with the access network, assuring bandwidth and QoS, unifying the network management and reducing the number of CPEs needed to deliver the service. This is a way for MSOs to gain a foothold in Enterprise accounts that are dominated by telecommunications companies by supplementing their existing network for their IP-based traffic.

Security Services

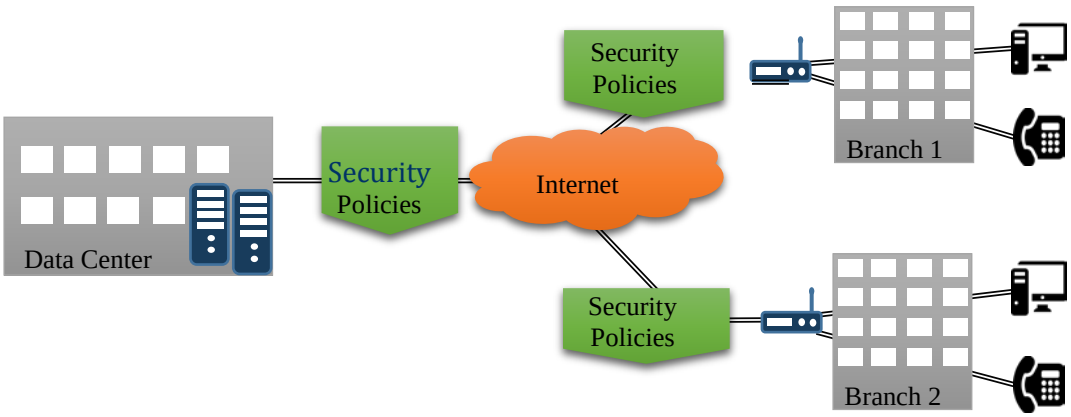

Figure 7 Security Services

Security covers a broad spectrum of services, including firewalls, DDoS mitigation, network isolation, access control, auditing, authentication, authorization and more. This is a growing market, both in terms of revenue and in breadth of offerings. Service providers can offer many of these security services by hosting them in their datacenter or the customer premise. Purpose-built physical devices that are provisioned on a per-customer basis are typically required either on the customer premise or hosted by the service provider, such as a firewall. Capabilities can also be bundled into a single device, such as a managed router. There are also broader varieties of services that can be fine-tuned to meet customer needs and multiple customer segments.

OTT offerings exist for security services. Service providers can offer a more compelling solution through virtualizing these capabilities in their network. Virtualization will reduce the number of both CPE and provider-hosted physical devices allowing for much faster deployment of services and provide the customers with fine-grained control. The IETF has formed the Interface to Network Security Functions (i2nsf) working group to define interfaces for customers to manage network security functions. These interfaces can help expedite customer adoption and ease the rollout of new services.

Bandwidth on Demand

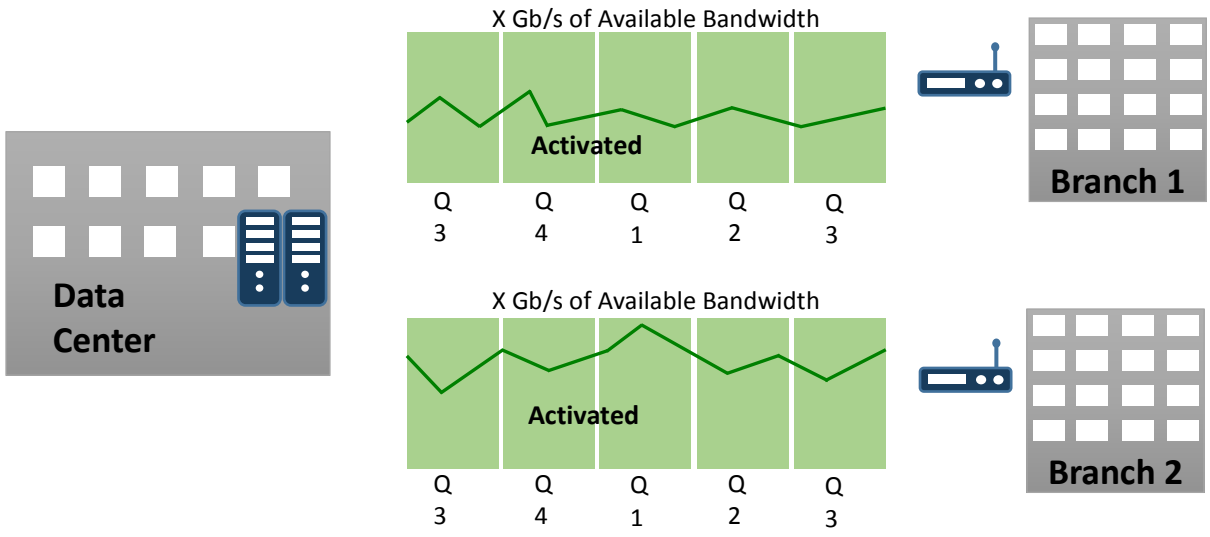

Figure 8 Bandwidth on Demand

On demand adjustments to customer's available bandwidth based on customer requests, time of day or predefined conditions. This service does not require a vCPE and does not have competition from OTT services since it is a core attribute of the connection to the site.

The base service functionality is to increase network capacity as demand grows at the customer's site and can be tied with additional Ethernet connections or capacity needed to fulfill these requests, and more advanced services can enable flexing of capacity based on demand.

An even more sophisticated service is moving to a market-pricing model with capacity costs changes based on the overall network demand. This enables traffic, such as backups, that are less latency sensitive, to be scheduled during off-peak network periods for the provider.

OTT providers are not able to offer a competing solution as this capability lends itself more towards SDN and automation solutions than NFV. Virtualizing policy servers and enabling CPEs to update bandwidth allocations without requiring a restart can simplify the rollout and separate it from requiring firmware or hardware upgrades. OTT providers can offer a similar solution by managing the available bandwidth across multiple connections to a single customer site. The OTT service depends on at least one of the connections being based on variable pricing, such as mobile.

Cloud-managed Wireless LAN

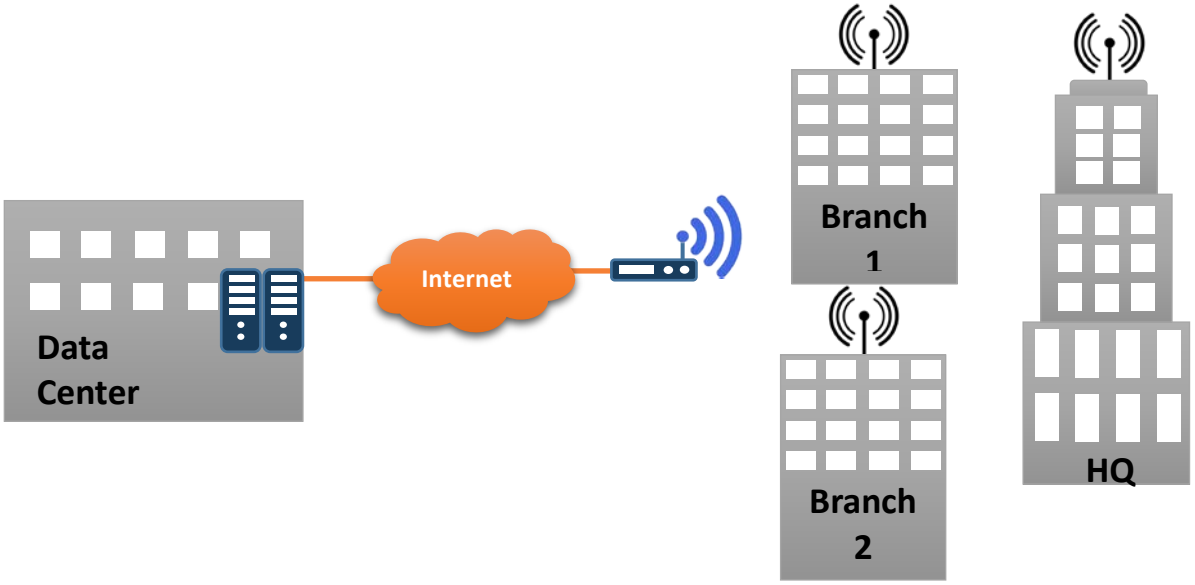

Figure 9 Cloud-managed Wirelesses LAN

The remote management of the customer's wireless network can administer networks across multiple locations via a unified portal; it provides providing management access with a single sign on solutions and simplifies the necessary management functions.

In multi-tenant structures where the service provider has multiple sites, such as office buildings, the service provider can optimize and share access points between multiple customers for an optimal experience, thus reducing resulting in a reduction of the noise caused by oversaturating a small area with too many independent access points.

OTT providers can deliver this managed service; however, many of these capabilities can be achieved through SDN and automation. NFV can still be used to distribute the location of the management functions and chaining together multiple services together would allow for a richer set of capabilities. Virtualizing this solution can decouple the need for physical access to devices to perform routine management, such as resetting SSID, network keys, and passwords as well as allowing for a broad set of other capabilities hosted by the service provider such as expanding this to manage multiple sites and eventually enabling device management outside of the customer's footprint.

Managed Router

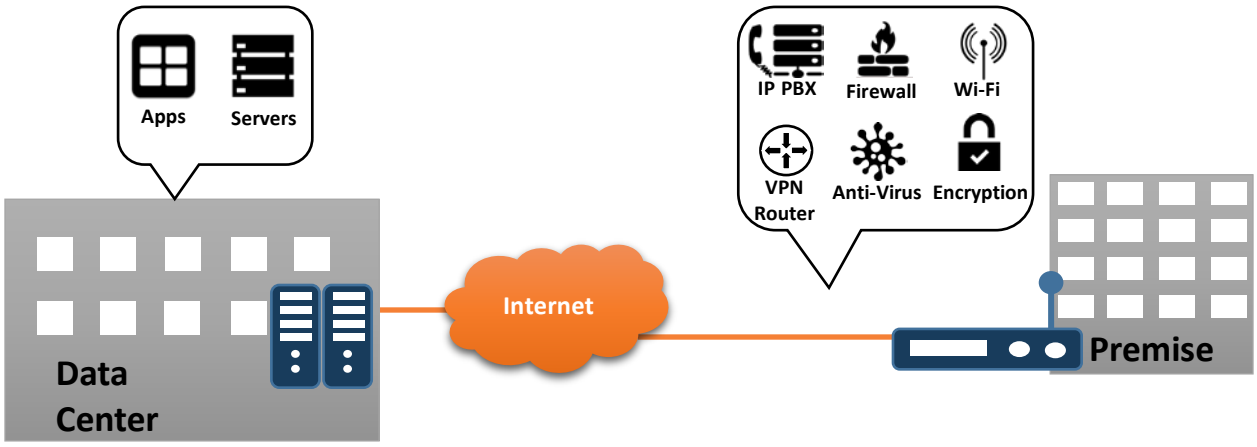

Figure 10 Managed Router

The managed router service outsources the management of the customer's local network and core network services. This service can be very broadly defined as capabilities vary greatly between vendors, service providers, and tiers of service.

Common capabilities include:

- IP Address Management (IPAM)
- DNS
- DHCP
- CDN
- Proxies
- Application optimization
- Print services

OTT competitors can offer this service, but virtualizing this service can allow for a much faster deployment and the reduction of additional CPEs. Integrating this with SDN at the customer site could enable a Bring Your Own Device (BYOD) capability and allow for deeper management of the customer's site.

Conclusion

Automation combined with network virtualization will dramatically improve business customers' experience by adding capabilities, reducing wait times, and expanding the scope of managed services at their disposal. Automation without virtualization can yield some of these benefits; however without virtualization and the ability to run multiple workloads on general-purpose hardware, several of largest time savings and flexibility gains will not be possible. A failure on a service provider not implementing these solutions could remove them from consideration for many managed services.

Increased competition of OTT providers for many managed network services can lead to missing opportunities if MSOs cannot compete with customer satisfaction and capabilities offered by these other providers. The increased bandwidth brought by SD-WAN solutions could be an alternative for some customers to Ethernet and MPLS IP VPN solutions, reducing the likelihood that which could relegate MSOs are merely supplying a network connection.

These challenges also open new opportunities for MSOs to differentiate their service beyond connectivity and into large, managed services markets where they are currently have little or no market share. SD-WAN solutions and the additional bandwidth they bring can provide MSOs with an opportunity to co-exist in Enterprise accounts where they are not the incumbents.

Automation and flexibility in addition to cost and operations considerations when rolling out virtualization across the MSOs networks are crucial to continuing growth in the managed services space for business customers.

Acknowledgements

I would like to thank the following people for providing valuable content and feedback on this document.

Gunnar Peters and John Cowperthwaite, Charter Communications

Guy Meador and Bill Coward, Cox

Richard Nijhoff, Liberty Global

Lance Hassan, Time Warner Cable

Suresh Soundararajan, Comcast

Joel Fini, Mediacom

Steven Pisarski, Carmela Stuart, Paul Fonte, Don Clarke, Kevin Luehrs, and Joan Branham, CableLabs