LEVERAGING SDN TO CREATE CONSUMABLE, PROGRAMMABLE AND SCALABLE CLOUD NETWORKS

STRATEGIC WHITE PAPER

Software-Defined Networking (SDN) is an approach to networking that allows networks to be consumed in a way that is similar to how compute and storage resources can be consumed – through virtualization. The promise of SDN is to drive service velocity and efficiency by decoupling how network services are conceived and consumed from the manner in which they are instantiated and activated and to achieve this through IT-friendly abstraction.

The key principles of SDN are:

- Decoupling of the network forwarding plane from the network control plane
- Centralized programmability of network resources
- Abstraction of network functionality to enable seamless consumption of network resources

This white paper describes how SDN simplifies networking. It then explores how the Nuage Networks Virtual Services Platform leverages SDN to make data centers and networks consumable, programmable and scalable.

TABLE OF CONTENTS

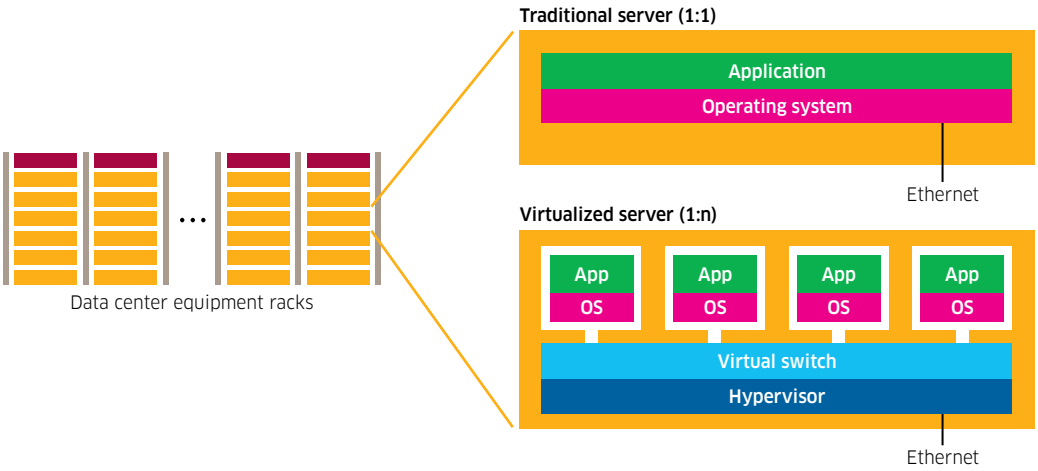
THE IMPACT OF VIRTUALIZATION

Historically, a single server/system was only able to run one operating system (OS) on which applications could be instantiated. For instance, the ability to run a Windows® OS next to a Linux™ OS was not possible on the same physical server.

With the evolution of virtualization, which allows the separation of OSs from the hardware on which they run, multiple operating systems and applications can run on a single server hardware platform. The key advantage of the move to server virtualization is that it enables more efficient use of the server's hardware resources (CPU/memory) by allowing it to be used by multiple OSs/applications.

Virtualization introduces the concept of a hypervisor layer, which allows the base OS to host multiple virtual machines (VMs), each having its own client OS (for example, Windows, Apple® OS X, Linux) for hosting various applications. The hypervisor hosts a virtual switch, which provides each VM with appropriate networking constructs and capabilities (for example, Virtual Private LANs (VLANs)) to provide network virtualization.

Figure 1. Server deployments – dedicated (1:1) and virtualized (1:many)



The leading hypervisors in the market today are:

- ESXi: provided by VMware®
- KVM: Linux-based supported by Red Hat® through Linux distribution
- XEN: provided by Citrix®
- Hyper-V®: provided by Microsoft®

While virtualization in the compute world has evolved over the last few years, the networking components have not developed to keep pace. As a result, networking is not nearly as easy to consume as compute and storage, which are delivered by the leading Cloud Management Systems, including: Openstack™, Apache CloudStack™, CloudBand™, VCloud®-Director/VSphere®.

A number of important impacts on networking have been introduced as a result of the compute virtualization evolution as highlighted in Table 1.

Table 1. Network impact with virtualization

	Tradition compute environment	Virtualized compute environment
Number of network endpoints	1	40-100 VMs/server
Nature of network endpoints	Static	Very dynamic
Duration as configured	Months/years	Hours/days/weeks
Network service requirements	Simple	Variable

Traditionally, data center networking has been primarily delivered through the use of VLANs. While VLANs provide the base functions of network virtualization, they represent a primitive model that is closely coupled with the physical network and doesn't scale to meet the requirements of the cloud environment. As a result, when limited to using VLANs:

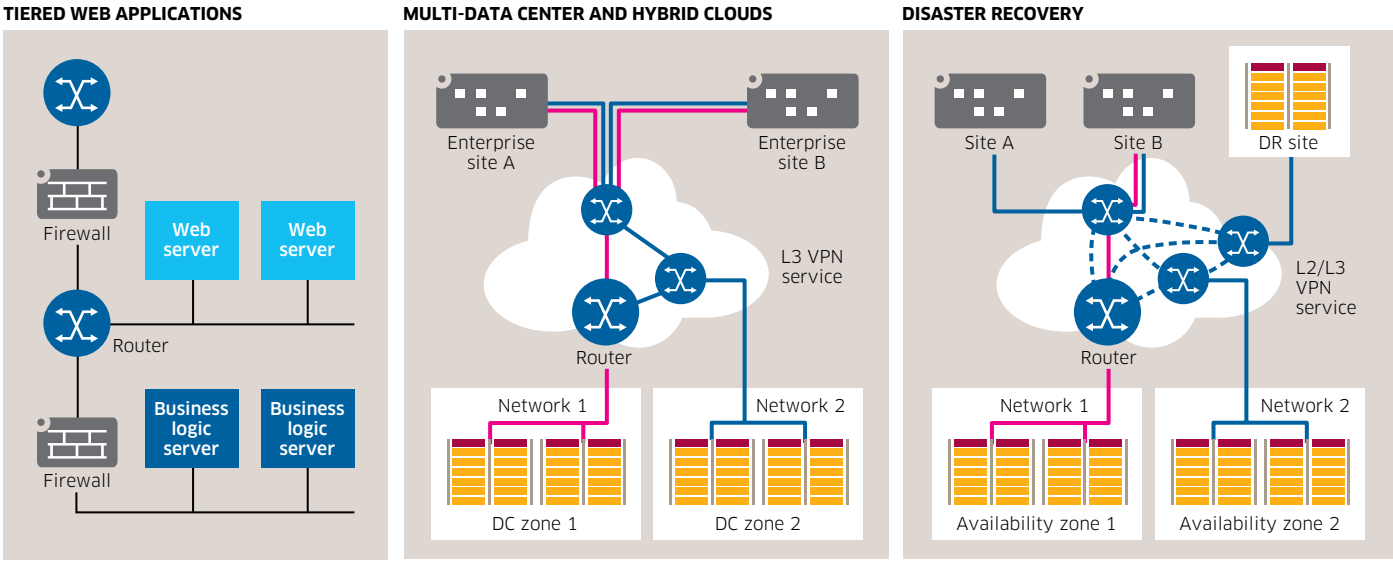
- Networking needs to scale 1:1 with the virtual environment. Since traditional switches were not built with this in mind, a VLAN-based network in a virtualized environment reduces the maximum scale to a few 100 servers, assuming 40 VMs per server. Going beyond this number will introduce networking complexities and increase OPEX.
- VM mobility is very cumbersome since VLANs are globally assigned or assigned per server/interface. If a VLAN is in use on a server it cannot be re-used. As a result, an application with a certain VLAN cannot be moved to a different server that has the VLAN id assigned to another application that is running. VM mobility is an essential function in the virtualization world to optimize resource utilization in the network.
- Traditional switches were built for a static LAN model, where network connections were expected to remain unchanged for months or years. Meanwhile, in the virtualized environment frequent changes are required to cope with application demands, customer demands and efficiency improvements. Dynamic re-programming of networking functions becomes an important consideration to cope with moving forward. These changes arise from new demands that applications and customers place on virtualized networking systems, or from Cloud Management Systems. The latter strive to optimize the efficiency with which the server infrastructure supports cloud applications and workloads.
- A tenant for an enterprise requires not just Layer 2 (switched) connectivity, but also Layer 3 (routed) connectivity between its application subsystems/tiers, and also depends on higher level (Layer 4) security and load-balancing functions. A traditional Layer 2 virtualization approach is not enough to support cloud applications running in a virtualized environment. While customers can instantiate routers, firewalls and load-balancers, the orchestration of all these functions is very complex and difficult to change due to the manual management of this connectivity. The operational costs of coping with the demands and changing requirements of customers are too high. Businesses cannot afford the delays associated with meeting these demands using traditional network operating models. Also, due to the highly manual operational techniques that are the norm today, human errors are prevalent and these lead to outages and service downtime.

As shown in the examples in Figure 2, there need to be different ways to optimize networking in the new virtualized environment for the cloud. SDN has been proposed to address the problems discussed above, and it does so by:

- Decoupling the data-plane from the control-plane
- Providing a high degree of programmability
- Providing an application-friendly abstraction of network capabilities

The next sections introduce the Nuage Networks Virtualized Services Platform (VSP) and explain how it enhances the operation of the networking layer. These enhancements make it possible to support customer demands to turn up cloud applications instantaneously, according to policy, and without restrictions or boundaries.

Figure 2. Typical enterprise cloud networking examples



NUAGE NETWORKS VIRTUALIZED SERVICES PLATFORM

The Nuage Networks VSP is an innovative SDN solution made up of three key building blocks: Virtual Routing and Switching (VRS), Virtualized Services Controller (VSC) and Virtualized Services Directory (VSD).

Virtual Routing and Switching: The VRS participates in the data-plane of the SDN environment, and is offered in several variants depending on customer deployment scenarios.

- A hypervisor-resident version acts as a virtual switch interacting with VMs and the hypervisor on each server:
  - ¬ VRS-V: VMware version running on ESXi
  - ¬ VRS-K: KVM version running on Linux
  - ¬ VRS-X: XEN version in a Citrix hypervisor
  - ¬ VRS-H: Hyper-V version running on Microsoft

All of the above are software versions running on the hypervisor. In this way, each physical server implements a VRS instance and becomes part of a distributed virtual routing and switching framework. This makes it a seamless part of a controlled but extensive cloud networking infrastructure.

- A VRS-G (Gateway) runs as a VM on virtualized servers, or as a module on bare metal servers. The VRS-G provides interworking with non-virtualized data center assets (servers and appliances). Nuage Networks also provides a high-performance gateway platform, the Nuage Networks 7850 Virtualized Services Gateway (VSG), which is a 1 Tb/s gateway for integrating bare metal assets at scale in large cloud data centers.

The VRS leverages IP connectivity to provide virtualized Layer 2 and Layer 3 networking capabilities. IP has been proven to scale, providing global connectivity in a broad-based way through the Internet. On top, IP decouples the virtualization from the physical infrastructure, which is crucial for mobility and scalability since no VM/tenant information is visible in the IP layer.

Virtualized Services Controller: The VSC is an SDN controller that programs the data center network forwarding plane elements (VRS) with all of the appropriate networking parameters required for customer slices of the virtualized network.

The VSC auto-discovers the various networking parameters of the VMs attached to the server and programs those parameters (such as, Layer 2 switching, Layer 3 routing, QoS, and security rules) transparently and automatically into the VRS. This in turn programs them instantaneously into the network fabric.

The VSC leverages OpenFlow™ and the Open vSwitch Database (OVSDB) Management Protocol to communicate with the distributed network endpoints (VRS). This allows the Nuage Networks solution to interwork with other vendors' Open vSwitch functions.

The VSC is a software module, based on the proven Alcatel-Lucent Service Router Operating System (SR OS), which carries over a decade of live large-scale network experience.

The Nuage Networks VSP is built for scale, and seamlessly federates controller instances through the use of a proven Internet protocol (MP-BGP). This approach also allows Nuage Networks endpoints to interwork automatically with MPLS VPN devices in the WAN in a scalable and flexible way. MP-BGP is the base-line protocol that has been used in MPLS VPNs for years, and is already fully standardized.

Virtualized Services Directory: The VSD is a policy and analytics module within the Nuage Networks VSP platform.

The VSD gathers and programs the application networking policy information (such as Layer 2, Layer 3, security, and QoS) per tenant, per network slice, and per user group level, and interacts with Cloud Management Systems through open RESTful APIs.

The VSD provides an application/network template function, which helps network designers implement networking templates. These easy-to-use templates can in turn be used multiple times by IT administrators of the customer's network slices. In addition, the VSD provides a full degree of IT-friendly and application-centric network service abstraction in order to make the networks readily consumable by IT applications and their users.

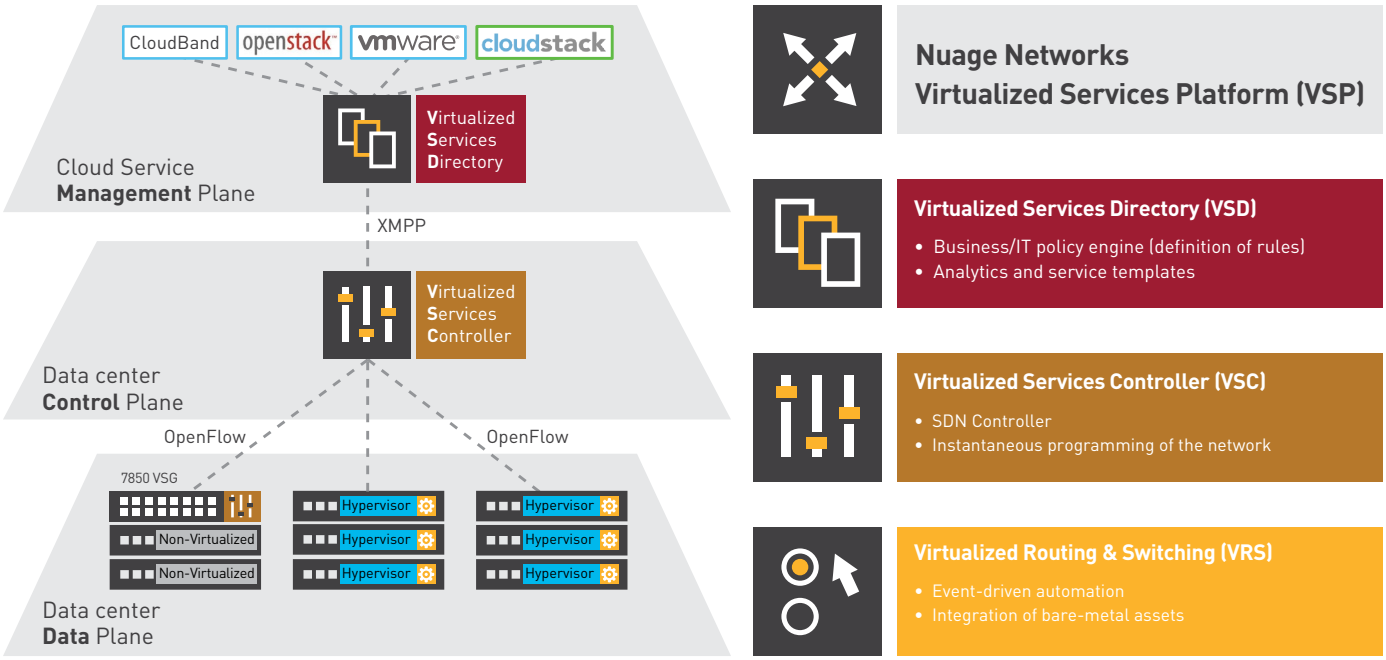
The VSD includes a Hadoop®-based analytics engine. It leverages big data analytics techniques to provide full visibility of all networking aspects on a per-customer basis, which can be used for billing, historical analysis and debugging.

The Nuage Networks VSP is an SDN solution built on a fully open foundation, leveraging standard protocols to ease integration and interoperability. Nuage Networks VSP is agnostic to the choices that have already been made in the data center. Nuage Networks VSP integrates and interworks with the hypervisor environment of choice, any network

switching equipment installed in the data center, and any Cloud Management System (including VCloud-Director, VSphere, Cloudstack, Openstack, HP™ Matrix Operating Environment (MoE), and CloudBand) that is preferred by the customer, including hybrid environments of any combination.

The importance here is that Nuage Networks VSP operates with the existing installed base and does not impose interworking constraints or introduce lock-in issues that are the hallmark of competitive offerings. Nuage Networks VSP makes network resources consumable as demanded by cloud service environments, including enabling Network Functions Virtualization (NFV) environments and seamless data center-to-VPN service delivery.

Figure 3. The Nuage Networks Virtualized Services Platform

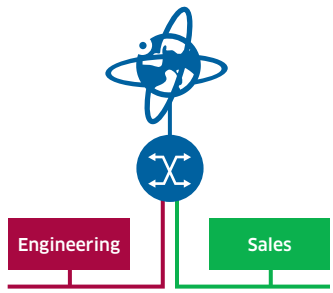


DATA CENTER NETWORKING

Traditional data center networking has imposed end-to-end service boundaries through the use of Layer 2 and Layer 3 networking constructs including switching domains and network subnets. These have hindered the flexibility and adaptability of the network to instantly react to changes at the application later.

To illustrate the benefit of SDN delivery with the Nuage Networks VSP solution, a common network service example has been identified which will be used to compare the traditional and SDN network deployment models.

Figure 4. Tenant networking example



Network service example

The example assumes a customer tenant configuration with two networks: one to be used by the engineering group, and the other by sales. The engineering department can only communicate with the sales department through web traffic; all other communication should be blocked. Both the engineering and sales teams are allowed to communicate with the Internet.

The traditional approach

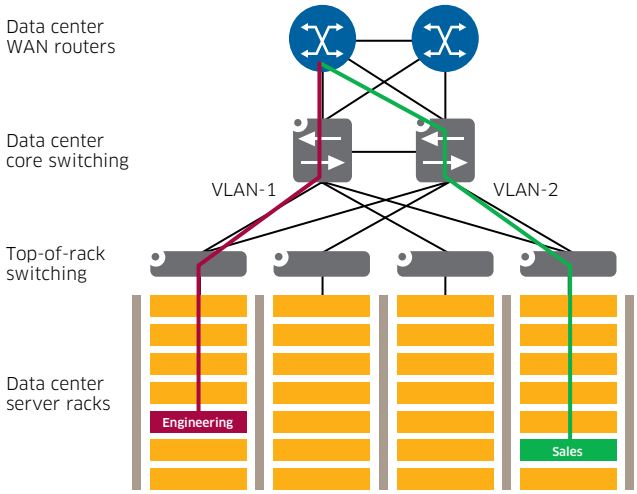
To deploy this scenario with traditional networking technologies, the following applies:

- Each network is assigned a VLAN; VLAN-1 for engineering and VLAN-2 for marketing and sales.
  - ¬ To initiate the networking, each VLAN needs to be assigned by the Cloud Management System in the v-switch on the hypervisor, and needs to be provisioned in the data center network across all switches and up to the switch on which the router is connected. When certain VLANs are already in use, this is not possible and the networking cannot be established, so the network operations team must continually administer which VLANs are already assigned in the network. This is done in a tedious, highly manual fashion today.
- Each network is connected to a router: VLAN-1 with subnet-1 for engineering and VLAN-2 with subnet-2 for sales.
  - ¬ A router instance needs to be configured and connected to the assigned VLANs and the relevant subnets need to be configured in the router. When this is done, traffic will always have to be forwarded back and forth to the router location, which is not very efficient. The router becomes a bottleneck since all traffic needs to go through the router when communication happens between the departments.
- A DHCP server needs to be assigned to provide IP addressing for the different departments depending on the subnet they are assigned to.
  - ¬ The network operations team needs to set up a DHCP server that assigns the IP information to the respective DHCP request for the applications in each network (engineering or sales), matching the subnets configured on the router.
- The router implements a security rule to allow only business application traffic between the engineering department and sales and allow traffic to and from the Internet.
  - ¬ The network security teams needs to apply a security policy on the router interface that allows the proper traffic to be forwarded between the engineering department and sales department, out towards the Internet and to validate the configuration for correct operation.

This example clearly illustrates the operational complexity when configuring the network to support an application. A high degree of manual intervention is required, as separate teams need to configure specific functions, and do so on various network domains and elements. This process is complex and creates an opportunity for several problems:

- Due to capacity or maintenance actions in the data center, or arising from server hardware issues, an application may require relocation on another server on which the VLAN was not configured. To accommodate this requirement the network needs to be reconfigured to provide reachability to the new location including any intermediate switching elements. The new configuration needs to be fully retested to ensure information security and performance.
- If the engineering subnet needs to be extended, network operation team input is required to configure this in the router for the respective VLAN. The DHCP server configuration requires modification and the security rules need to be changed in-line with the new subnets, and fully tested.
- In high availability scenarios (which are commonplace), these actions become even more difficult to administer, since various elements are involved simultaneously with in-depth testing of normal and failure scenarios before the solution can be released to production.
- When a tenant configuration changes, various components need to be reconfigured to accommodate the new demands for the tenant.

Figure 5. Traditional data center tenant networking



Clearly, should the situation described above be required for multiple customers simultaneously, there will be a delay in responsiveness. It can and does take an unacceptably long time (days or even weeks) to accommodate networking demands when customers request that applications be turned up or workloads move around the data center.

Some data center operators have begun to address these issues with modifications to orchestrator/OSS systems to improve response times. However, these systems are very complex and hard to maintain as software changes happen regularly. This approach is not successful when dealing with changes in hardware vendors.

The Nuage Networks approach

With the Nuage Networks solution, changes are handled by a fully automated process that can react instantaneously. This makes network operations much simpler across an open cloud environment.

The following describes in more detail how the Nuage Networks VSP solution with its key SDN functionality addresses the engineering and sales environment described above:

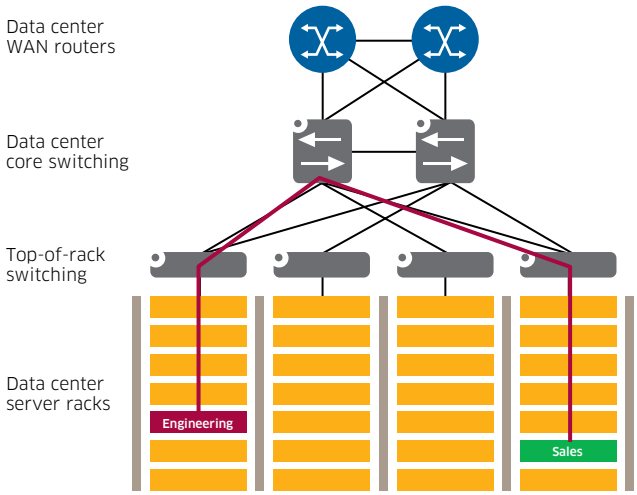
- A network designer implements a template, which corresponds with the design for the desired customer network. This is a straightforward 5-click operation through a simple, IT-friendly GUI.
- Network operations will instantiate the template for the customer; this will instantaneously set up the complete network according to policies defined for the customer.
- When the engineering or sales applications are instantiated, the corresponding networking configuration is derived from the template instance and all networking aspects are implemented automatically through the VSD/VSC, which programs the forwarding/security tables accordingly in the VRS where the customer applications are initiated.
  - ¬ The operations team doesn't need to touch the configuration of the data center switches, and no VLANs or routers need to be configured, since the networking is provided through virtualization overlays at the IP layer. The VSC programs all forwarding/security entries automatically in the corresponding VRSs where the applications are attached, and a full tenant network is automatically established.

- ¬ There is no need to set up separate DHCP servers, since Nuage Networks VSP has this capability built into the solution. Adding subnets to the engineering and sales departments automatically instantiates the corresponding forwarding entries in the various VRS(s) where the applications for this tenant are attached.
- ¬ All security rules are automatically derived from templates that the network designer has previously set up — even if the deployment team chooses to add additional subnets to the engineering or sales department.
- ¬ Also, the VRS provides full routing and switching so no extra routers need to be configured. This provides very efficient routing between applications in the customer tenant slice without bottlenecks.

The Nuage Networks VSP automates the full instantiation of the tenant networking requirements through SDN programmability and abstraction.

The template can be used as many times as required, should this operation need to be repeated multiple times. The Nuage Networks VSP solution instantiates the necessary networking and provides full isolation between tenants and through the robust implementation of SDN technology pillars, which simplifies the operation of the data center network substantially.

Figure 6. Tenant networking with Nuage Networks Virtualized Services Platform



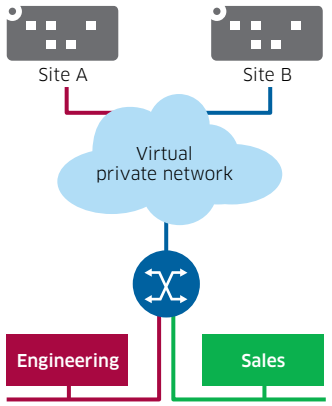
The Nuage Networks VSP benefits are:

- Faster response time to customer demands, which results in much higher customer satisfaction
- Simplified business operations through templates that are created once and used many times
- Operational simplification through automation, with SDN programmability and abstraction
- Elimination of tedious manual operations, which in turn eliminates the potential for human errors associated with implementation and modification of customer tenant configurations
- Higher data center network and server efficiency through elimination of bottlenecks, ultimately resulting in lower CAPEX and higher profitability

Data center connectivity to the WAN

This section builds on the example in the previous section. It highlights how the Nuage Networks VSP compares with traditional networking approaches when it comes to connecting the tenant configuration to a VPN outside of the data center.

Figure 7. Tenant networking example – VPN connectivity



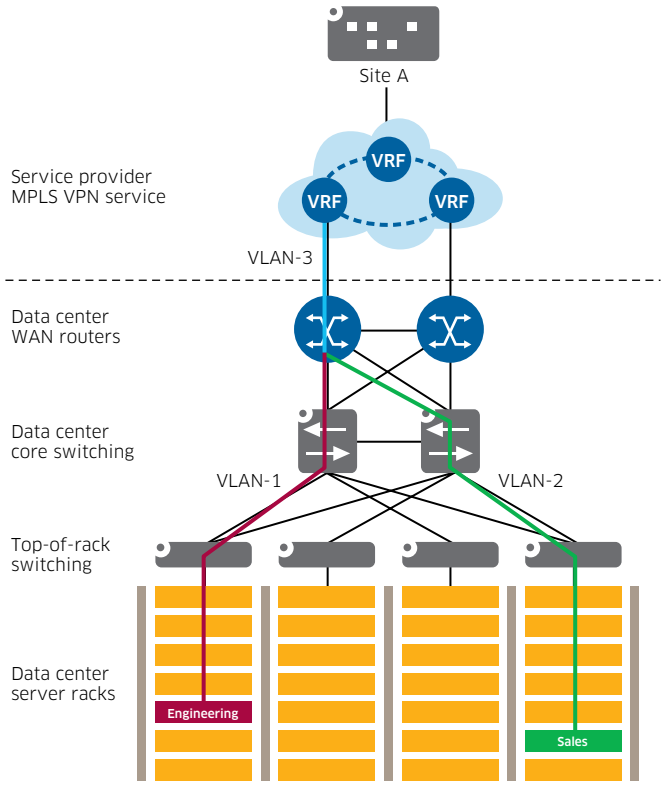
The traditional approach

To deploy this solution using the traditional data center networking approach, the following steps need to be undertaken:

- A VLAN needs to be configured between the data center router and the WAN router.
- A routing protocol needs to be set up to provide resiliency in case of failures. The configuration needs to be applied on both the data center router and the WAN router. However, to offer Layer 2 and Layer 3 VPNs in the WAN, different resiliency mechanisms for Layer 2 and Layer 3 VPN stitching must be deployed and configured which further complicates the network operation.

Traditionally, ownership of data center network operations and WAN operations is maintained by different network teams. Coordination between the data center networking people and WAN networking people is required, most likely via a formal project structure and manual processes. Moreover, with multiple tenants needing to be provisioned, this segmented operational model introduces delay as well as scalability issues as each tenant requires dedicated VLAN/routing protocols.

Figure 8. Traditional data center to VPN connectivity



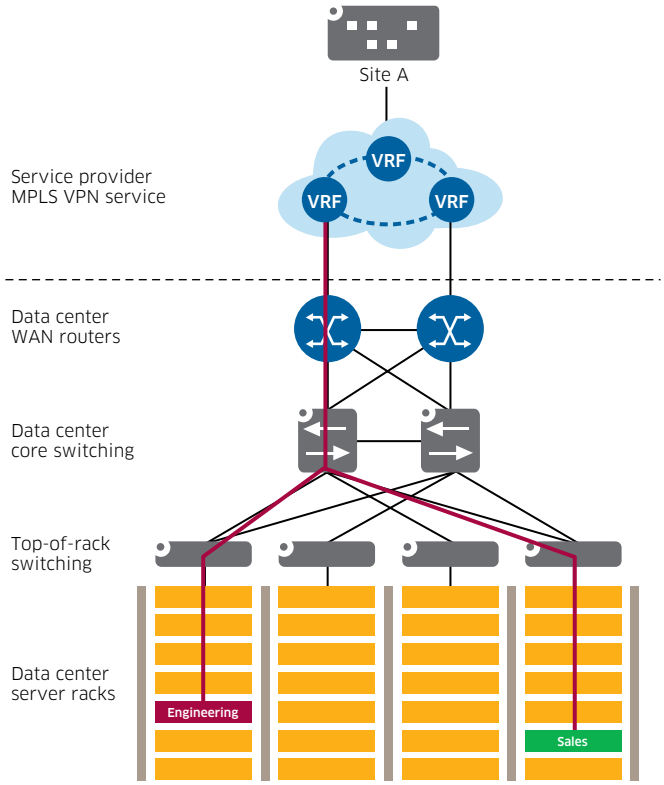
The Nuage Networks approach

To address the needs of this environment, the Nuage Networks VSP solution leverages MP-BGP, which is inherently a multi-tenant protocol. This means that only a single protocol instance is required regardless of the number of tenants that need to be

instantiated. Further, MP-BGP is a scalable, policy-controlled protocol. The WAN networking team and data center networking team only need to agree on which Route-Target/Route-Distinguisher needs to be used per tenant.

With that in place, connectivity between the data center and the WAN network gets instantiated automatically and without the need for provisioning additional VLANs. Given that MP-BGP is universal between Layer 2 and Layer 3 VPNs, the complexity of disparate resilience mechanisms is avoided when providing Layer 2 (Carrier Ethernet) or Layer 3 (IP VPN) based VPNs. Moreover, Nuage Networks VSP provides the option for the data center operator to remove the data center WAN routers from the connectivity, which reduces CAPEX.

Figure 9. Data center to VPN stitching with Nuage Networks Virtualized Services Platform



Benefits of the Nuage Networks VSP solution include:

- Timely business response to customer demands, which results in much higher customer satisfaction
- Leverages MP-BGP, which leads to higher network utilization and ultimately to lower CAPEX; enhances scalability
- Reduction of CAPEX through elimination of need for the data center gateway (WAN) routers.
- Simplification of protocols: no differences between Layer 2 (Carrier Ethernet) and Layer 3 (IP VPN) service constructs, leading to simplified WAN connections and reduced OPEX
- Simplification of business operations through template-based create-once, use-many times network policies, reducing OPEX

- Operational simplification through automation, with SDN programmability and abstraction, reducing OPEX
- Eliminates tedious manual operations, thereby eliminating human errors associated with implementation and modification of customer tenant configurations
- Higher data center network efficiency through elimination of bottlenecks, ultimately resulting in lower CAPEX and higher profitability

SOFTWARE-DEFINED VIRTUAL PRIVATE NETWORKS

This section describes how Nuage Networks VSP uses SDN principles to enhance VPN services to the WAN (creating Software-Defined VPNs (SD-VPNs)), and compares this to a traditional VPN approach.

The example assumes there are two VPNs, one Layer 3 and one Layer 2. In the diagrams, blue is used for the Layer 3 VPN and red for the Layer 2 VPN.

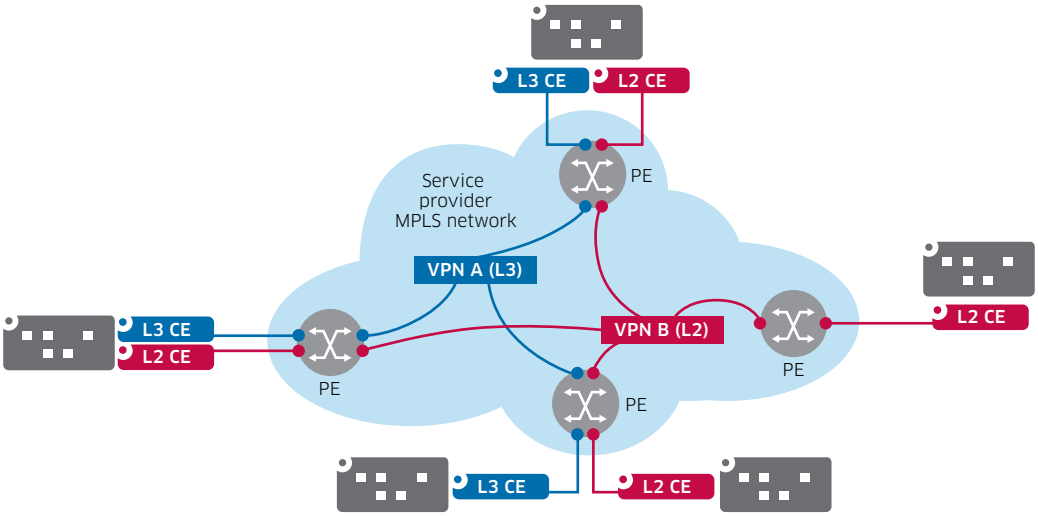
Traditional wide area VPN service

In a traditional VPN approach, Layer 2 or Layer 3 VPNs are deployed on the service provider's edge (PE) routers using VPLS for Layer 2 VPNs or IP VPN for Layer 3 VPN services. The service is terminated at the enterprise site with dedicated CPEs connected in a peer-to-peer configuration as a customer edge (CE).

To deploy this scenario with traditional networking technologies, the following happens:

- Each VPN site gets a dedicated CPE per service, which is configured with the LAN configuration as well as the WAN configuration to the service provider's PE.
  - ¬ The WAN connectivity is provided through a dedicated link or through a VLAN when a shared access network is used. WAN connectivity is provided with an IP address for IP VPN and a Layer 2 connection (VLAN) when Layer 2 VPNs are deployed.
  - ¬ When IP VPNs are provided, a routing protocol might be deployed to learn the routes between the Layer 3 sites.
  - ¬ The WAN PE and CPE are configured with the appropriate QoS parameters in order to provide the proper SLA for the customer.
- A DHCP server is set up in the WAN to provide address assignment to the LAN equipment, or a Network Address Translation (NAT) function is set up to hide the addressing from the WAN and a local DHCP server on the CPE is set up.
- Security policies are configured on the CPE(s) and WAN PE(s) to ensure proper security for the communication. For instance, it can be established that certain sites can only communicate with other sites with specified application types (for instance block HTTP but allow e-mail).
- Each VPN needs a dedicated configuration on the CPE sites and WAN PE(s) on which the VPNs are connected. A dedicated system provides the configuration on the CPE, and another system provides connectivity on the WAN PE(s).
  - ¬ Consistency between the WAN PE and CPE needs to be assured with respect to connectivity, QoS, IP addresses and security policies.

Figure 10. Traditional WAN VPN approach



When network acquisitions are made, the WAN PE routers need to be integrated in order to provide global VPN service. This typically adds complexity and compounds delays since different service providers use different rules for QoS, IP addressing, security and routing policies. Also, when global VPNs are targeted, this leads to additional complexities in representing the acquired networks with a single autonomous system, and long lead-times to make this integration happen.

On top of that, dedicated CPE(s) are provided for Layer 2 services and Layer 3 services. Also, depending on the functionality required by the customer (such as WAN acceleration and firewalls), additional CPE(s) may be required at customer locations.

Wide area VPN services using SD-VPNs

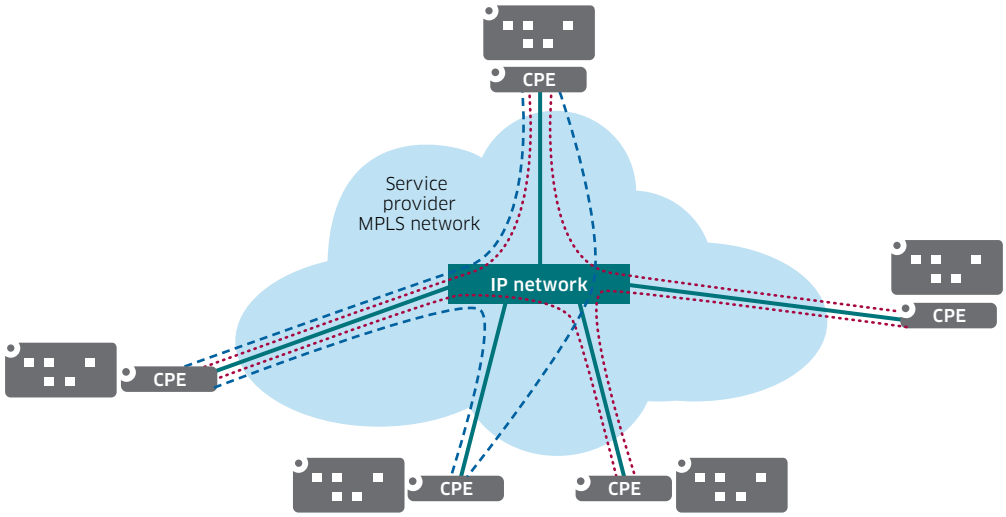
Applying SDN principles to the VPN service construct significantly simplifies the service creation and deployment process.

- With SD-VPNs, a VPN overlay provides connectivity from the CPE, rather than separate VPNs from both the WAN PE and CPE. The CPE is controlled from the Nuage Networks VSP, which programs all forwarding rules (Layer 2/Layer 3 connectivity, security, QoS) based on the policy that is provided for the VPN on the VSD.
  - ¬ Given that VPNs are based on IP connectivity, the SD-VPN solution requires global IP connectivity through an IP VPN or the Internet. When networks are acquired, the enterprise simply needs to request global IP connectivity rather than undertaking a full integration and interworking of multiple service provider VPN networks. In this way, the SD-VPN model can provide a much faster time to market.
  - ¬ The underlying WAN service can evolve from MPLS to IP, which no longer needs to be provisioned with a per-customer VPN; this avoids complexities. As IP networks inherently provide QoS-based traffic forwarding, these can be utilized to offer the required SLA conditions contracted to the enterprise.
- Because the Nuage Networks VSP integrates full network policies for Layer 2/Layer 3 connectivity with security and QoS, the same template constructs that benefit the data center can be implemented for the WAN services (SD-VPNs). When the CPE boots up, the related forwarding rules and policies are downloaded and programmed in the

CPE from the centralized VSC, making installation and provisioning much simpler. No additional DHCP servers or NAT policies need to be assigned since they are all assigned and programmed from the VSC.

- Because it supports a federation of SDN controllers, the Nuage Networks VSP provides a very scalable solution to thousands of CPE(s). The solution leverages the same protocols deployed in the WAN, so easy interworking with the WAN PE(s) is seamlessly provided via the widely supported and open standard MP-BGP.

Figure 11. The SD-VPN approach



A key additional benefit is that the SD-VPN solution provided by Nuage Networks leverages an open CPE model, which is controlled through software.

The VRS integrates all Layer 2, Layer 3, QoS, and security policies and forwarding rules and is fully programmable through the SDN controller (VSC). This allows for a unified CPE model, which reduces the number of CPE types that the service provider needs to maintain.

Additionally, VM-based software applications can be installed directly on the CPE so service providers can deploy their own applications depending on the customer's requirements. This approach reduces the required inventory and applications can be deployed either on the CPE or in a data center. With the advanced service chaining built into Nuage Networks VSP, service providers can now use an NFV approach when deploying network applications (including firewalls, load balancers, and NAT). This allows them to select the best possible location (CPE or data center) depending on the enterprise's VPN configuration requirements. In essence, the CPE becomes a "mini data center" in the SD-VPN model.

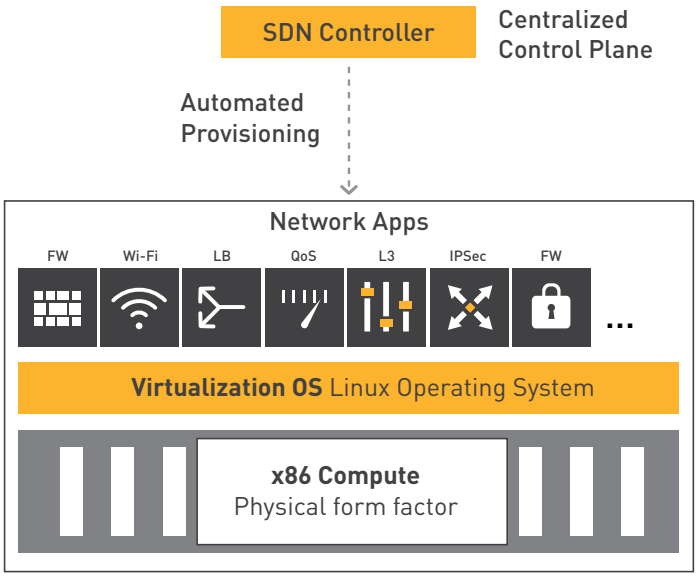
With the SD-VPN open approach, the solution can be leveraged to provide enhanced services inside the customer LAN environment. This approach enables the service provider to develop more effectively integrated and fully managed service offerings.

The SD-VPN approach also enables the deployment of a complete self-service model. The SD-VPN service provider can give the enterprise full visibility of and access to all configuration options via a self-service portal that provides options for service

functions and deployment control from a central location. This makes it possible for each enterprise customer to manage its own services, which in turn improves customer satisfaction and provides dramatically faster time to market.

For example, an enterprise using an SD-VPN based service could initiate per-link encryption for a number of sites. To do so, they would simply request the addition of the encryption via the centralized portal by highlighting which of their sites requires the functionality. Using the centralized SDN controller (VSC), the SD-VPN would automatically reconfigure to provide the service change.

Figure 12. The SD-VPN CPE model



Benefits of the Nuage Networks VSP SD-VPN solution include:

- Open CPE model based on common, off-the-shelf x86-based hardware, which reduces CAPEX since the CPE models are driven by the open compute market and not via vendor specific proprietary hardware implementations
- Lower CPE inventory and installation times leading to reduced OPEX; easy upsell from customer VPN service without the need to change CPE
- Simplification of business operations through template-based create-once, use-many times network policies, reducing OPEX
  - ¬ Eliminating tedious manual operations and reducing the opportunity for human errors associated with implementation and modification of customer SD-VPN configurations
  - ¬ Operational simplification through automation, with SDN programmability and abstraction, reducing OPEX
- Full customer driven self-service VPN solution with high degree of visibility and configuration flexibility, leading to increased customer satisfaction
- Enables service providers to expeditiously and efficiently leverage global IP network footprints, by simplifying network operations/integration when deploying international VPN services

CONCLUSION

The key to profitable delivery of cloud services is agility in application delivery, with an application-friendly user experience and superior economics. This is what enterprises expect when they move to the cloud.

Data centers are the engine room of the cloud, where compute and storage facilities are concentrated. Applications that run in the cloud run in these data centers. Economies of scale combine with the realities of user experience and corporate compliance to dictate the level to which data center facilities need to be consolidated or distributed. As expected, a mix of scenarios emerges depending on needs. Some highly consolidated mega-data centers are optimized for unit cost and homogeneous applications; others are more distributed to leverage micro- and nano-data center facilities that optimize performance through proximity to users.

In either case, by definition, the cloud is a distributed system in which applications run remotely from their users. And the more distributed a system is, the more important it is for its constituent parts to be effectively, efficiently and reliably interconnected.

The network is the connective tissue of the cloud. In the background, it is the networks across server and storage clusters that ensure the performance of applications. It is the network within and across data centers that makes the storage and compute resources elastic and enables graceful disaster recovery. And it is the network between users and the data center that provides open or secure access to the applications and content depending on the nature of the application.

Nuage Networks believes that a better network drives a better cloud. In the cloud mindset, applications are deployed quickly, with compute and storage resources spun up dynamically and instantly as required. But the network infrastructure has lagged. Today, it is nowhere near as responsive as it needs to be. It takes weeks of elapsed time and numerous iterations of work orders between manual processes in order to establish the network connectivity required by virtual machines that come up in seconds in support of application requirements. That is simply not good enough for the cloud era. What's needed is reflexive and instantaneous network establishment, in tune with the needs of applications in the cloud.

Further, broad-based migration of business-critical applications to the cloud requires more than what has been seen to date for consumer cloud offerings and early public clouds. Those certainly have shown what is possible, and proven that the technology and business models are ripe to transform the delivery of business applications. But business applications demand more from the cloud. The Internet is a great infrastructure, but not the ideal infrastructure for mission-critical business applications. Again, that's because responsiveness is key and because control and visibility are paramount to IT departments who are committed to ensuring application performance for their workgroups.

Today, the largest enterprises depend on IP-based private network infrastructures. The cloud infrastructure can evolve to provide the same kind of security, control and reliability these private infrastructures offer, with the addition of agility and economies that are implicit in the cloud proposition. The Nuage Networks VSP solution with its robust implementation of SDN principles and key pillars of programmability through abstraction and efficiency through automation stands to change the game. Nuage Networks VSP will deliver business-grade hybrid cloud services that pave the way for the post-Internet era.

Cloud technologies hold so much promise for enterprises, helping them achieve unprecedented application deployment velocity and resource efficiency. Clearly there is a fantastic opportunity for service providers to leverage cloud technology to evolve their service delivery models as well. In addition to offering cloud-based services, telecom service providers are in their own right very large enterprises that deliver value proportional to the capital and operational efficiency of their network assets.

Of course it would make sense for them to leverage cloud technologies to virtualize key network functions, enabling them to be distributed in a more open and dynamic environment. That is the fundamental driver of the NFV movement.

ALCATEL-LUCENT AND NUAGE NETWORKS LEAD THE WAY

Alcatel-Lucent is among the first global suppliers of networking equipment to appreciate the full scope and value of the cloud as a transformative technology. Over the past three years Alcatel-Lucent has invested in key technologies that are at the heart of making better cloud networks a reality.

Better means more open, more agile, more programmable, more automated, and more cost-effective. It means providing not only the technology and platforms, but also the expertise and know-how to help service providers build clouds, prepare their existing networks for the cloud, leverage the cloud, and monetize their cloud assets.

Service providers today are looking to:

"network the cloud" – and ensure that cloud networks are instantaneously responsive to user application needs and drive new cloud-based business models (thus, the move to SDN)

or to:

"cloudify the network" – and deliver telecommunications services much more efficiently while enabling new capabilities in an open environment (thus, the move to NFV)

Alcatel-Lucent believes that the ideal cloud network infrastructure MUST provide three key attributes in order to be viable:

- **Automation and customization:** to provide a network that responds immediately to application needs, and evolves over time with a close fit to application lifecycle
- **Flexibility and reach:** to eliminate networking boundaries that restrict placement of workloads and applications
- **Control and performance:** to ensure visibility and deterministic service behavior; a best-effort cloud is insufficient for broad business adoption

Alcatel-Lucent is uniquely positioned to guide telecom and cloud service providers through this transition with platforms and products that allow them to adopt and adapt cloud technologies to meet their needs.

This paper has illustrated several of the deployment modes that are possible with the Alcatel-Lucent venture Nuage Networks and the Virtualized Services Platform. It demonstrates how Nuage Networks VSP provides a robust SDN solution to address common data center networking scenarios and data center connectivity to the WAN. It also illustrates innovative models for VPN service delivery with SD-VPNs.

The Nuage Networks approach makes data centers and networks consumable, programmable and scalable. It virtualizes and automates the data center network infrastructure, and extends the reach of cloud services to enterprise locations and private data centers. While eliminating unnecessary network boundaries, the Nuage Networks solution has been designed to operate seamlessly across operational and organizational boundaries as well.

The network is not the end-game in the cloud environment, application delivery is. But the network is a key means by which cloud reach, performance and user experience are delivered and ensured. Alcatel-Lucent raises the bar on this critical part of the cloud infrastructure equation.

ABBREVIATIONS

API	Application Programming Interface
BGP	Border Gateway Protocol
CAPEX	Capital Expenses
CE	Customer edge router
CPE	Customer premises equipment
DC	Data center
DHCP	Dynamic Host Configuration Protocol
HQ	Headquarters
L2, L3, L4	Layer 2, Layer 3, Layer 4
MP-BGP	Multiprotocol Border Gateway Protocol
MPLS	Multi-Protocol Label Switching
NAT	Network Address Translation
NFV	Network Functions Virtualization
OPEX	Operational Expenses
OS	Operating System
OSS	Operation Support System
PE	Provider Edge router
QoS	Quality of Service
SDN	Software-Defined Network
SD-VPN	Software-Defined VPN
SLA	Service Level Agreement
SR OS	Alcatel-Lucent Service Router Operating System
VLAN	Virtual Private LAN
VM	Virtual Machine
VPN	Virtual Private Network
VRS	(Nuage Networks) Virtual Routing and Switching
VRS-G	(Nuage Networks) Virtual Routing and Switching Gateway
VSC	(Nuage Networks) Virtualized Services Controller
VSD	(Nuage Networks) Virtualized Services Directory
VSP	Nuage Networks Virtualized Services Platform

Alcatel·Lucent