Nuage Networks

Virtualised

Services Platform

Packet Pushers White Paper

About the Author

Greg Ferro is a Network Engineer/Architect, mostly focussed on Data Centre, Security Infrastructure, and recently Virtualisation. He has over 20 years in IT, in a wide range of employers working as a freelance consultant including Finance, Service Providers and Online Companies. He is CCIE#6920 (Emeritus) and has a few ideas about the world, but not enough to really count. Also a host of the Packet Pushers Podcast and writes on his well known blog at http://etherealmind.com.

Packet Pushers Profile

Packet Pushers is a podcast and community website where real engineers get together to talk about their experiences. It's deliberately nerdy, passionately technical and led by experienced network engineers. Some of the best and brightest technical people share their knowledge and experience talking about the latest topics. We strive to engage across all areas of Networking.

Packet Pushers Perspective

Packet Pushers is focussed on technology and engineers. We provide independent views and opinions. There were very few independent voices telling their stories and experiences in 2009; Packet Pushers was started to discuss data networking and form a community. Today, Packet Pushers is a thriving group of independent voices sharing knowledge, experiences and insight into Network Engineering with over 100 contributors, widespread recognition and growing vendor & industry support.

The Packet Pushers Podcast is deliberately technical, nerdy and lighthearted. There is no technical pandering to the audience. We discuss industry, products, technology, heavy on tech and find humour where we can. The podcast has over 12,000 listeners per show.

About White Papers

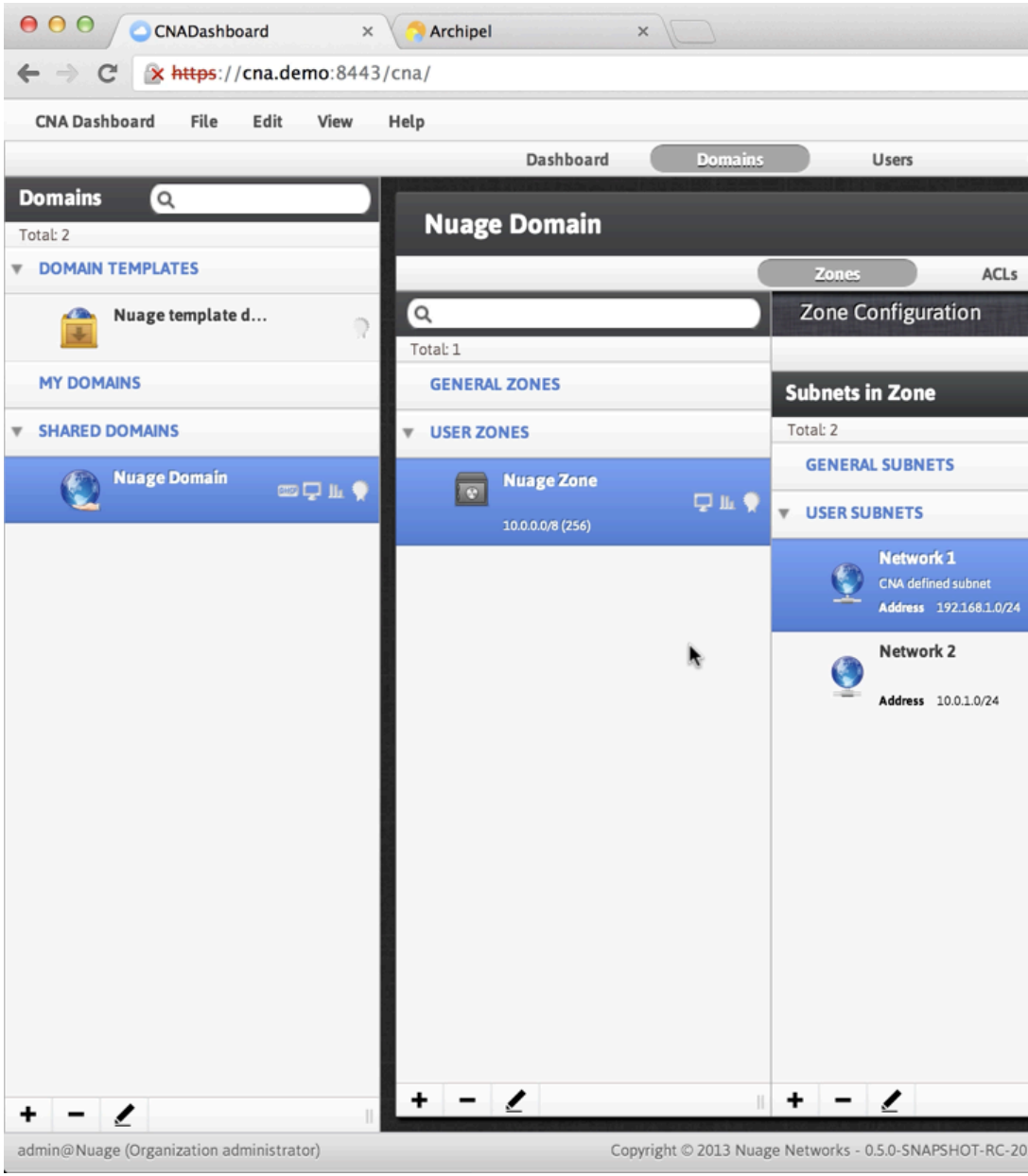
Most vendor white papers are aimed at the CIO and other managers, tending to be heavy on marketing and long on business value. However, a senior engineer will only consider these aspects once the technology has a viable purpose or use case. Packet Pushers delivers content that focusses on the technology.

NUAGE NETWORKS

Today's virtual networking is about multiple logical devices from a single physical network device, but the future of networking is software network devices that are hosted on generic hypervisors. The Nuage Networks strategy delivers a Software Defined Networking (SDN) product that controls & manages the virtual access networks at three tiers: in the WAN, throughout the data centre, and between data centres.

The Nuage Networks Virtualised Service Platform (VSP) can be described in three parts. The Virtualised Services Directory VSD) policy management and analytics application drives the Virtualised Services Controller (VSC) which configures distributed virtual routing & switching (dVRS) software agents in the server hypervisor.

First, we look at how the data and control planes merge into your existing network with the dVRS flow forwarding agent. Then, we look at how the Nuage Networks VSP management plane uses a policy engine, derived from service provider networking, that not only manages & configures the dVRS devices but also provides deep visibility for operations & control of configuration.



Introduction

In networking, the physical Ethernet connection to the server has been the edge of the network. The growing use of hypervisors means that networking now happens inside the server platform in software as well as extending the network reach beyond the physical uplink. How can you engineer a reliable and trustworthy network unless you can manage the true network edge ?

One of the most common network design principles of the last decade is to move complexity to the network edge and simplify the network core. For example, in the mid 2000s, MPLS changed the WAN with label forwarding in the core while performing traffic classification at the edge. In virtual networking, we are seeing the same sort of transformation, where the software switching in the hypervisor can perform complex traffic manipulation, and then forward across a simple network core. To properly manage this functionality, software networking in the server hypervisor must become part of the overall network.

Consider how your network will change if the software network inside the server becomes the new network edge and moves the physical network devices to the network core. Moving the access layer into the hypervisor gives control and visibility to the operator and the security team.

This whitepaper is a sponsored introduction to Nuage Networks and their unique approach to Software Defined Networking that bring together a complex software edge and simple core into a unified network infrastructure for both Enterprise and Service Provider environments.

The Server as the Network

Nuage Networks is integrating software networking with the physical network by extending the network edge inside the hypervisor. Existing virtual switches allow programming of the network connectivity by creating connections between the physical NIC and virtual NIC. In effect, today's virtual switches are virtual patch panels that simply connect virtual NICs to the physical NIC installed into the server. Networking needs to move away from static placement like that. Today's so-called "virtual networks" are still dependent on physical devices in the network – the physical appliance has a virtual instance of itself, but the network services are still delivered from the hardware appliance.

If we upgrade the software switch from a simple physical network connection that is shared among virtual machines to a highly functional network device, and then add path forwarding to the software so that the server can switch frames and route packets in the server kernel, we end up with an active network device in the server that can make complex forwarding decisions.

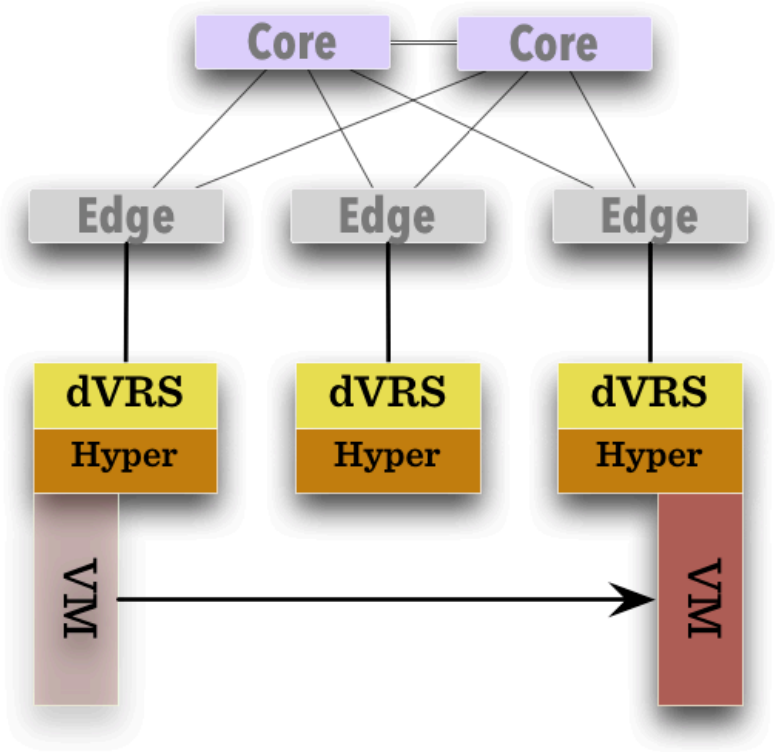
For example, deploying firewalls in virtual contexts does not place the firewall service close to the application itself. Designers still have to build secure LAN and WAN connections to and from the virtual firewall. Nuage Networks has designed a solution that can extend the network services INSIDE the server.

Controller Based Networking

We need a new approach to operation and control of networking. Today, it is possible for an engineer to manage a few hundred network devices with an SSH client, a good diagram, an SNMP monitoring tool and experience. But what about tomorrow? Consider an Ethernet switch of today connecting as many as 48 servers - one network device to man-

age. But what if each of those servers houses a network service for routing, switching and firewalling that must be managed? Adding a network device to the server operating system results in an explosion of network devices to be managed, meaning that CLI administration of those devices becomes unrealistic.

To add to operational complexity, virtual machines can move between hypervisors at any time. The Network team cannot easily identify the sources and destination point of servers within the network when those points are moving targets.



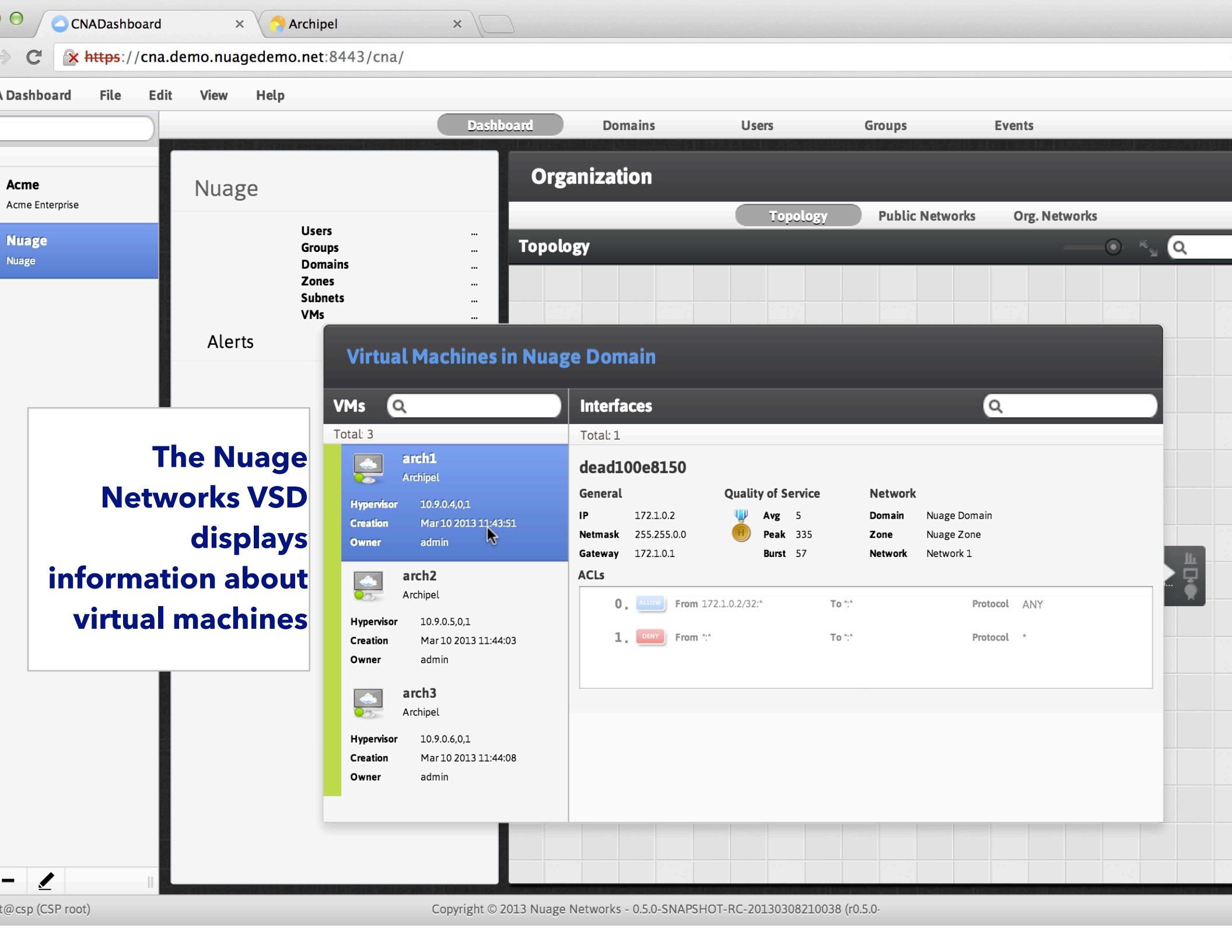
Virtual Machines Move Between Hypervisors Change Network Dynamic

While Network Management Systems (NMS) help with complexity, today's tools area based on aging protocols that lack feature richness and flexibility. Certainly SNMP has been a successful tool over time, but the protocol has serious limitations. The data is not well defined, and SNMP MIBs are too frequently poorly designed and badly documented, making their use non-trivial. For these reasons, SNMP is often deployed as a "read only" tool, its usefulness limited to statistics gathering and status monitoring.

To overcome these management challenges, the central component of the Nuage Networks SDN solution is the VSD application. VSD is a web-based, graphical console that connects to all of the dVRS nodes in the network to manage their deployment and configuration. The VSD module distributes the policies through a number of Nuage Virtual Services Controllers (more on this later) to all of the dVRS nodes in the network to manage their deployment and configuration.

For an example of VSD's management interface, let's examine the screenshot on the next page. First, the Nuage Networks VSD Dashboard shows the network adapter of the server as part of the overall network configuration. Second, the domain is separated into policy zones that each server is assigned to. Finally, because the controller performed the configuration on all the dVRS agents and is notified when changes occur, VSD can display the actual network configuration of the virtual machine.

There's more power to dVRS than just the tight integration with VSD, though. Let's take a look.


CNADashboard
Archipel
https://cna.demo.nuagedemo.net:8443/cna/
Dashboard File Edit View Help
Dashboard Domains Users Groups Events
Acme
Acme Enterprise
Nuage
Nuage
Nuage
Users ...
Groups ...
Domains ...
Zones ...
Subnets ...
VMs ...
Alerts
Organization
Topology Public Networks Org. Networks
Topology
Virtual Machines in Nuage Domain
VMs
Total: 3
arch1
Archipel
Hypervisor 10.9.0.4,0,1
Creation Mar 10 2013 11:43:51
Owner admin
arch2
Archipel
Hypervisor 10.9.0.5,0,1
Creation Mar 10 2013 11:44:03
Owner admin
arch3
Archipel
Hypervisor 10.9.0.6,0,1
Creation Mar 10 2013 11:44:08
Owner admin
Interfaces
Total: 1
dead100e8150
General
IP 172.1.0.2
Netmask 255.255.0.0
Gateway 172.1.0.1
Quality of Service
Avg 5
Peak 335
Burst 57
Network
Domain Nuage Domain
Zone Nuage Zone
Network Network 1
ACLs
0. ALLOW From 172.1.0.2/32:* To *:* Protocol ANY
1. DENY From *:* To *:* Protocol *
The Nuage Networks VSD displays information about virtual machines
t@csp (CSP root)
Copyright © 2013 Nuage Networks - 0.5.0-SNAPSHOT-RC-20130308210038 (r0.5.0-

The Value of dVRS

The dVRS approach offers a range of network services.

- Uses standards-based protocols such as OpenFlow between the VSC controller and dVRS agents.
- Uses flow routing to manage traffic flows in the server.
- Can perform traffic load balancing through flow path management.
- Based on popular & proven Open vSwitch software.
- Performs routing locally in the hypervisor.
- Performs packet filtering in the server.

While development of dVRS continues, with features such as stateful firewalling & load balancing on the roadmap, the highlight feature is **Distributed Virtualised Routing.** This concept allows network data to be routed at the edge of the network instead of being routed via the core through large hardware switches. To demonstrate how this works, we need to introduce the concept of a **Tunnel Fabric.**

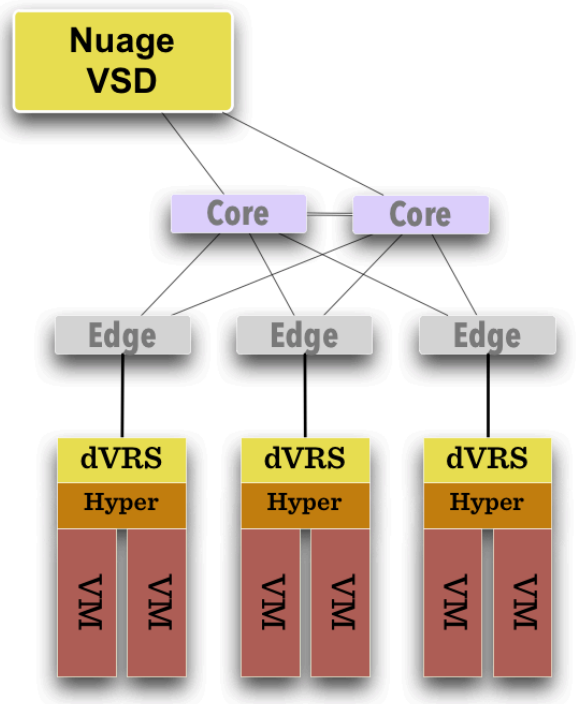
The Tunnel Fabric

In a traditional network design that connects virtual machines to the physical LAN, the network edge (usually a top-of-rack L2 switch) is connected to each of the hypervisors; hypervisors then connect to virtual machines using virtual NICs. This approach is in common use today and shown in the diagram below.

SIMPLE CORE, SMART EDGE

The data centre network has always focused on using L2 Switching at the edge and L3 routing in the core because high speed routing was expensive & complex. But around the mid-2000's, service providers network deployed MPLS to perform edge routing on PE routers & perform label switching in the Core. The advantages were to distribute complexity and simplify the core network so that stability and performance was improved.

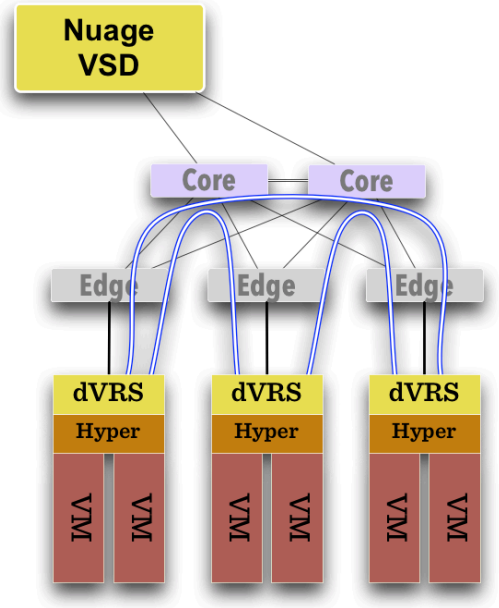
So why do Data Centre Networks have smart cores & dumb edges ?



Basic Physical Network Connectivity

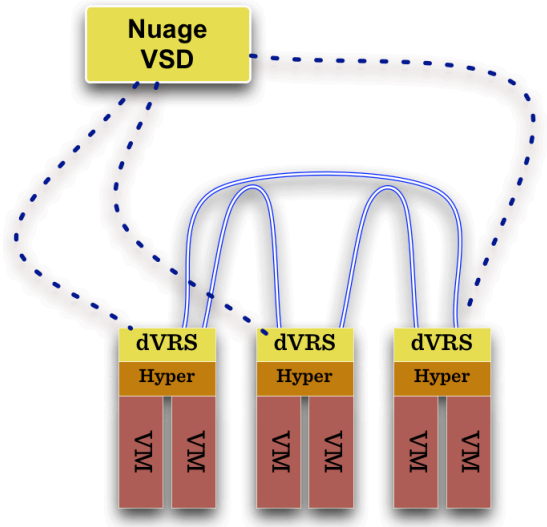
While satisfactory for simple installations, there are a number of technical limitations with this approach. Multi-tenant traffic flows require complex technologies to maintain separation, e.g. MPLS, VRF-Lite or PVLAN. Another issue is that security gaps in the virtual switch require expensive audits to ensure policy is being enforced. And of course, there's no visibility of virtual machine traffic that is switched inside the hypervisor.

We can update the traditional model and overcome these limitations by using a tunnelling protocol to connect the dVRS switches together. Thus, both L2 and L3 flows moving through the dVRS device can be encapsulated from one dVRS device to another or sent directly to the physical network if required. In this way, virtual machine traffic follows the most efficient path between two hypervisors while maintaining secure multi-tenant separation and eliminating the requirement for a complex separation protocol.



Distributed Routing with a Tunnel Fabric from dVRS

dVRS endpoints can map directly to each other in this way because the VSC models a complete network topology, including knowledge about all endpoints in the network. An algorithm determines the outbound paths for each dVRS in the network and encapsulate the flows into a tunnelling protocol such as the industry-standard VXLAN which is optimised for high performance in multipath LANs. MPLS over GRE is used for connections to WAN edge devices.



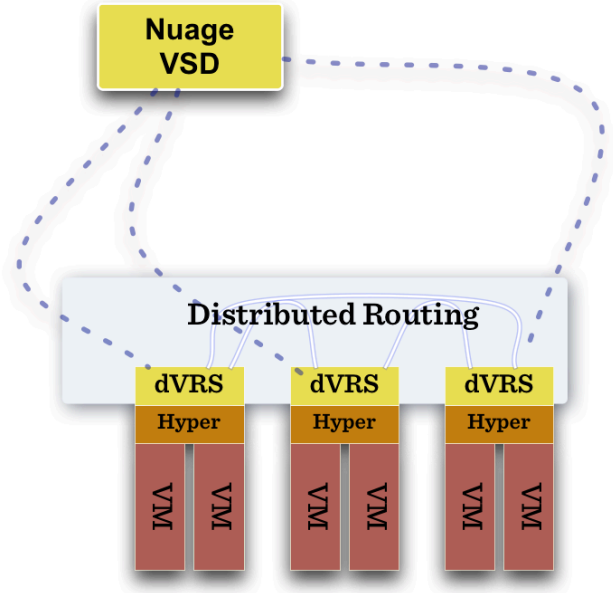
The Tunnel Fabric

Replacing an existing physical network is enormously challenging for most organisations, due to the capital costs and business risk of a network refresh. Using tunnels between the dVRS means that the existing IP/Ethernet Fabric in your data centre needs no upgrades or changes. In the modern ITIL compliant organisation, network change remains enormously difficult since existing network protocols are not designed for rapid change or capable of reliable reconfiguration.

It should also be noted that tunnelling protocols use minimal resources in the Data Centre LAN. To the physical network, tunnel packets are simply UDP streams that consume a handful of TCAM entries in core switches. The dVRS implementation of VXLAN does not require an IP Multicast PIM-BiDir or PIM-SM configuration like VMware's vCloud. Features like anycast replication and local acknowledgement to cope with broadcast, unknown unicast, and multicast (BUM) traffic handle the issues addressed by multicast in other VXLAN implementations.

Distributed Routing

Each dVRS routes traffic into the network according to its flow table. Therefore, the entire dVRS system performs *routing at the **edge** of the network*. Distributed routing is like an ultimate "traffic engineering" setup where routing CPU load is distributed to a large number of devices, the routing complexity is managed by a single controller, and the entire data plane routes the shortest path across the underlay network.



Distributed Virtual Routing

A dVRS can't make a forwarding decision in a vacuum, as events in the underlying physical network must be considered. Nuage Networks has extensively considered how to provide the VSC controller with all the information required to have a complete model of the network. The VSC implements an OSPF, IS-IS or BGP listener to monitor the state of the physical network. Therefore, if routes starts flapping, the VSC is able to incorporate those events into the decision tree.

Multiple Controllers, Multiple Data Centers and Multivendor

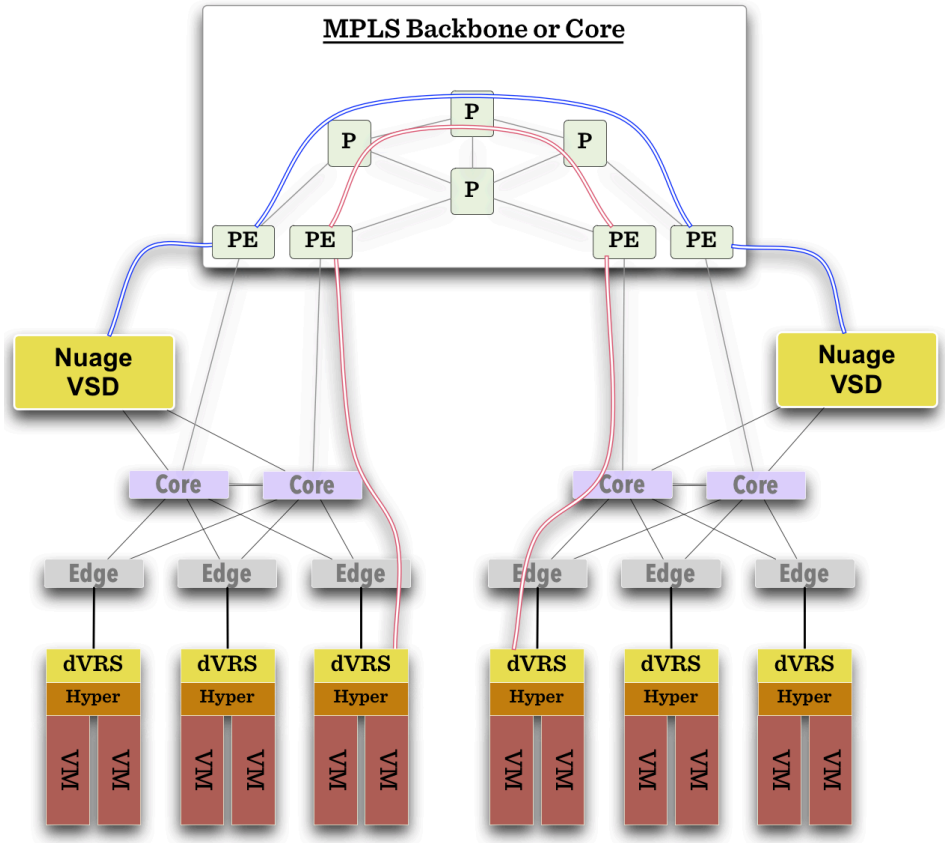
One of SDN's fundamental questions is that of scale. In how large of a network can a unified SDN environment function? The Nuage Networks solution is designed with the capability of growing to the massive scale required by cloud providers and service providers.

Within a single data centre, scale is handled by multiple VSC controllers, each handling a group of dVRS devices. To scale between multiple data centres, VSC controllers build on the single data centre scale model by horizontally connecting controllers at the top of the hierarchy.

As shown in the diagram on the left, VSC controllers are synchronised using MP-BGP. A BGP connection peers with PE routers at the WAN edge, and then the VSC controller uses MP-BGP to synchronise controller state & configuration with VSCs in other data centres. This is vital for end-to-end network stability. The VSC controllers must run at the same critical level as BGP routing updates to ensure coherence between the data centres - controller synchronisation is as vital as BGP peering updates. BGP is well-designed to transfer a large volume of structured data - that's what Internet routing tables are.

When dVRS devices are communicating to non-local dVRS devices, data is tunnelled in MPLS-over-GRE to the PE router. Modern routers from most vendors support GRE termination in hardware, and this ensures low latency and immediate compatibility with existing network equipment in the WAN. The VSC controller will be communicating with the PE using BGP to establish the MPLS path and monitor the circuit establishment.

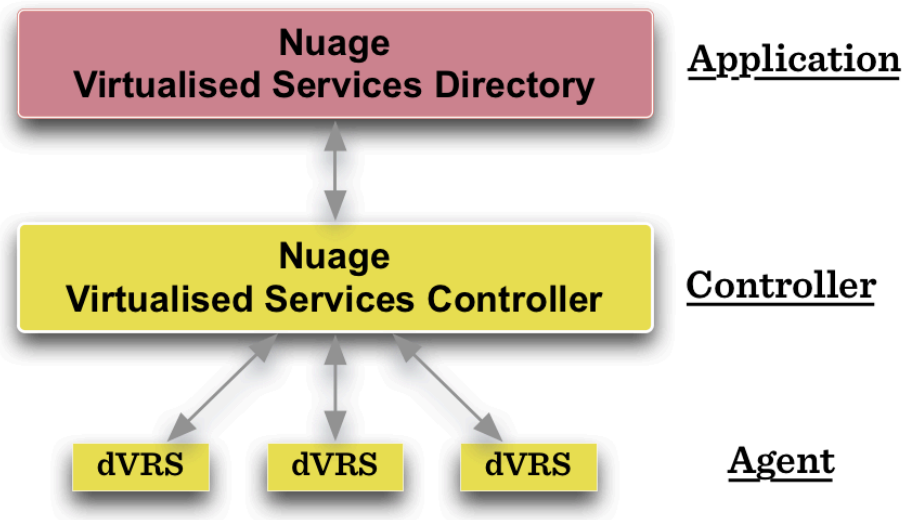
Nuage Networks delivers an site to site SDN strategy by integrating with the existing equipment in your network and utilises existing MPLS WAN services with little change to your existing network.



The VSD Policy Controller

We have covered the data and control plane of the Nuage Network VSP platform where the dVRS agent creates a network edge that delivers new services in the hypervisor and the VSD controller provides operational control of the elements. But there is more to uncover in the VSD Controller.

The "VSD Controller" consists of the Virtualised Services Directory (VSD) application and Virtualised Service Controller (VSC) SDN controller.



The Virtualised Services Directory is a policy engine; configuration of the dVRS is derived from a series of templates. For example, the virtual port is a policy element with a unique identifier that applies to the server template AND the dVRS template. When the virtual port moves from one dVRS to another dVRS as part of the server move, the policy template is inherited at the new location with attributes like MAC Address, QoS, VLAN membership, monitoring data, etc. This design is derived from existing software handling large 3G and DSL networks for a proven approach to scaling and flexibility.

A second benefit of a policy driven configuration is that the local node only contains configuration that is directly relevant. A BGP-enabled Internet-facing router must house enough compute resources be able to hold 400K route entries in memory and in the TCAM table, even if only forwarding traffic for 1,000 routes. In a VSD system, the exact flow rules to handle the traffic that will reach the dVRS are calculated and distributed. As a result, the CPU / Memory consummating is much reduced. There are less mature vSwitch solutions that require up to 2 Gigabytes of memory to hold a very large and mostly unused flow table.

The policy derived configuration allows for mobility, reduced resource consumption and improved application control. It's a key differentiator from other SDN applications.

POLICY SERVERS

In 3G & DSL networks, an endpoint connects to a central server for login, authentication, authorisation and network parameters. A customer inherits the final configuration after the server has analysed policies such as physical location, account standing, device type, network status. These policies combine to build the final configuration in a completely flexible way.

Seven Pillars of Cloud Network Automation

The premise of cloud networking is to achieve a network that is programmable, flexible and valuable. Nuage Networks promotes this vision with "Seven Pillars of Network Automation" that are instantly recognisable as key elements that solve challenges in Software Defined Networking. The seven pillars are:

- L3 Scalability
- L2 Isolation
- L2-L4 services
- VPN Compatibility
- SDN Programmability
- Policy Management
- Performance Monitoring

L3 Scalability

L3 Scalability refers to the state held in the physical network of the Data Centre and the WAN. Each IP Route and MAC Address consumes CPU & Memory resources in physical routers and switches. Creating a Tunnel Fabric means that only the IP and MAC Address of tunnel endpoints are visible to the physical network. Because the forwarding occurs at the edge of the network, network paths are optimal from the edge, through the core, and even over the WAN.

The physical network does not hold state regarding the endpoints. Thus, additional tenants do not consume MPLS VRFs, BGP routes or TCAM resources across the backbone.

The software network also scales since the state/configuration in the dVRS is minimised by the VSD controller using policy templates to localise the flow tables.

L2 Isolation

Securing a Layer 2 network is complex. Extending multiple VLANs across an Ethernet trunk to a virtual host is an unmanaged security risk with loss of control and possible VLAN bypass attacks. With dVRS agents installed to the hypervisor, traffic flows are managed end to end - right up to the server network adapter. This complete isolation of Layer 2 is inherent in a flow managed network and dramatically reduces the operational cost of the network.

L2-L4 Services

We described flow forwarding at the network edge using a extended definition. Today, network forwarding uses only the destination address. The VSD will define flows on source *and* destination IP address, source/destination TCP port, VLAN tags and more. The result is application aware forwarding. This is further enhanced with the VSD end to end view of the network and the servers within its own ecosystem.

VSD has the ability to "know more" about payloads and application intention and allow the operator to build new network services. The policy derived configuration provides granular control and configuration of L4 services that move with the VM.

VPN Compatibility

A VSD can operates directly with MPLS VPN and allows interoperability with existing WAN services. This provides for Data Centre Interconnection at Layer 2 and Layer 3 between customer owned facilities,

but also provides for Hybrid Cloud connectivity to external cloud services. Nuage dVRS agents in an external cloud can be integrated into single coherent network that spans an MPLS backbone. Consider an MPLS path between multiple data centres that can support VM migration and recovery from a single application platform. When the server team relocates a VM, the network operator will have a visual display of the network configuration from the VSD web interface.

Combined with the flow monitoring capabilities, you can gain real visibility of end-to-end performance because the dVRS has visibility of the entire flow at the server ingress.

SDN Programmability

Nuage Networks has developed an extensive set of the REST APIs for the VSC controller to support SDN programmability to external resources. An SDN platform is not self contained and must connect to other orchestration platforms and services. The VSC controller is architected to add new APIs as SDN Networking develops interoperability standards over the coming years. OpenStack is already supported.

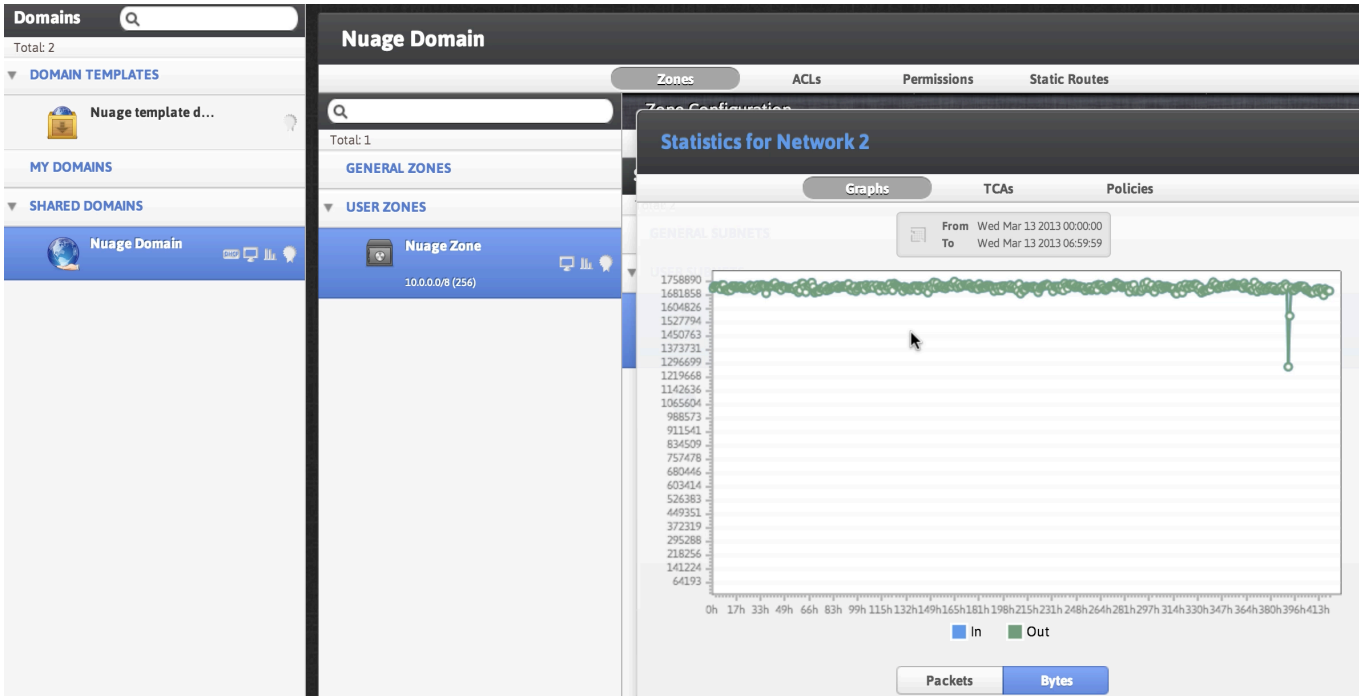
Policy Management

A VSD uses a number of administrative abstractions to, perhaps for the first time, apply policy to network in virtualised platforms. This VSD policy engine allows for flexible configuration tools in the web configuration. For example, master templates allow for baseline tenant setup and then creation of per-tenant policies. Constructs like Domains, Shared Domains and Zones allows for flexible configuration options that are vital in meeting the diverse requirements of a multi-tenant data centre. Deriving profit from a cloud often means reliable support for a diverse of range of different requirements.

Performance Monitoring

The VSC Controller will poll performance and status information from the dVRS agent and show the statistics and graphs of the current status that is roughly equivalent to physical switch port monitoring. The diagram below show the utilisation of an entire subnet. In a traditional network, this would require a significant investment in sFlow collectors and analysers to crunch this type of data.

Remember that the performance data is collected by a unique object in the VSD architecture. Even though a server or VLAN moves within a single data centre, or between data centres, the data is still presented from a single interface.



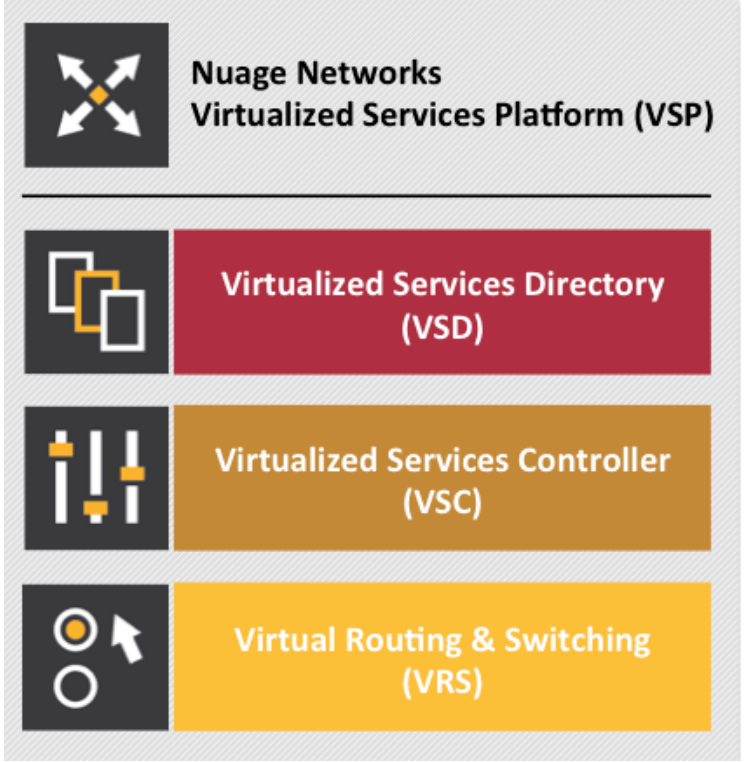
SDN is arriving

The Packet Pushers have been discussing the possibilities of SDN for the last two years. We've speculated, discussed, wondered and dreamed about what we would need in an SDN solution while knowing what programmatic networking *could* do. When you run down the capabilities of the Nuage Network VSP product, it's hard to find anything missing. Let's start at the top.

The VSD policy & analytics engine presents a unified web interface where configuration and monitoring data is presented. The VSD is API-enabled for integration with other orchestration tools. Alternatively, you can develop your apps. Either way, the VSD is based on tools from the service provider world, and therefore scaling potential looks very good. It integrates multiple data centre networks by linking VSDs together and exchanging policy data (not configuration data).

The VSC also addresses scaling - you can have multiple VSC controllers per data centre to meet your performance requirements and uses the same operating system used in Alcatel-Lucent Service Routers today. Nuage Networks has chosen to use standards-based protocols like OpenFlow and MP-BGP where practical, and gave us a verbal commitment to use open standards where possible and practical in the future.

The dVRS network agent addresses many of the "known issues" when using software switching and tunnels. Unique configuration per agent means better performance while consuming less CPU/Memory in the hypervisor. dVRS avoids the IP Multicast requirement in the network core with smart features (that will certainly need some proving). Finally, the dVRS agent uses the VSD policy configuration to deliver real network services to applications - security through edge filtering, flow balancing, Layer 3 routing at network ingress and even plain L2 Switching by simple path selection.



Finally, you can get started on your existing network by simply installing three virtual machines for the Nuage Networks VSP and few more to be "hypervisors". Your existing network needs zero configuration changes to get started in a single data centre.

This whitepaper is sponsored by Nuage Networks, but we still say that they have delivered on much of SDN's promise. It's hard not to be excited about the positive changes in networking that SDN is making. Nuage Networks has a product that you should add to the very short SDN list of solutions available today for your network strategy in the years to come.

Packet Pushers

Too Much Networking Would Never Be Enough

Packet Pushers Interactive LLC (US)
Thropos Ltd (UK)

http://packetpushers.net