Understanding the Total Cost of Acquisition of Cisco ACI vs. VMware NSX for vSphere Environments

June 2015

Prepared by:

Zeus Kerravala

Understanding the Total Cost of Acquisition of Cisco ACI vs. VMware NSX for vSphere Environments

by Zeus Kerravala

June 2015

ZK Research
A Division of Kerravala Consulting

Executive Summary

Software-defined networking (SDN) is reinventing the networking industry and enabling organizations to embrace the cloud computing era. With SDN, networking equipment becomes more programmable and enables automation that increases business velocity, while simultaneously delivering capital and operational savings.

Vendors have differed in their approach to delivering on the promise of SDN. In this paper, we compare two such SDN platforms: Cisco's Application-Centric Infrastructure (ACI) and VMware's NSX platform.

Cisco's ACI is an integrated overlay model that addresses both physical and virtual networks as one network, in a consistent application-centric policy-driven framework. VMware's NSX is a hypervisor overlay-based model that is VMware centric and requires network gateways to talk to bare-metal applications and other network endpoints.

Cisco's ACI provides a single pane of glass for managing all application components including physical and virtual networks, Layer 4-7 (L4-7) services, and, in the future, compute and storage. ACI correlates the health of the network to that of the application, and it provides deep visibility and troubleshooting capabilities.

NSX introduces a pure overlay network and has no direct visibility into the underlying physical network, delegating the correlation between overlay and underlay to other tools. NSX provides automation only for virtual networks, and currently it does not provide any management of underlay physical devices.

Cisco ACI offers open interfaces and application programming interfaces (APIs), and it supports multi-hypervisor environments. The open Northbound and Southbound APIs of the ACI controller, APIC, provide seamless integration with existing management, orchestration, L4-7 services, and physical and virtual devices. This provides complete investment protection to customers by enabling them to integrate their existing IT systems into an ACI architecture. NSX limits customers' choices by offering different products and functionality for vSphere and Linux-based hypervisors and providing no Microsoft Hyper-V support.

NSX requires a license for every host that participates in the overlay. In addition, the NSX architecture requires additional compute capacity for implementing gateway functions and running management components with high levels of availability.

zeus@zkresearch.com

Cell: 301-775-7447
Office: 978-252-5314

Influence and insight through social media

Cisco's integrated overlay approach results in a leaner architecture, requiring fewer components and providing automation and visibility benefits across multiple types of workloads. This translates into a significantly lower acquisition cost when compared to NSX. In this paper, we compare the costs of building a private cloud infrastructure using the two design options—NSX and ACI.

Introduction: The Era of Private Clouds Is Here

As IT organizations seek to automate their infrastructure, they often consider implementing and adopting a private cloud. The objective is to enable automated, self-service provisioning of cloud applications. Such applications will likely also need to interact with existing legacy applications or databases, or with newer "big data" applications such as SAP HANA and Hadoop that do not run virtualized.

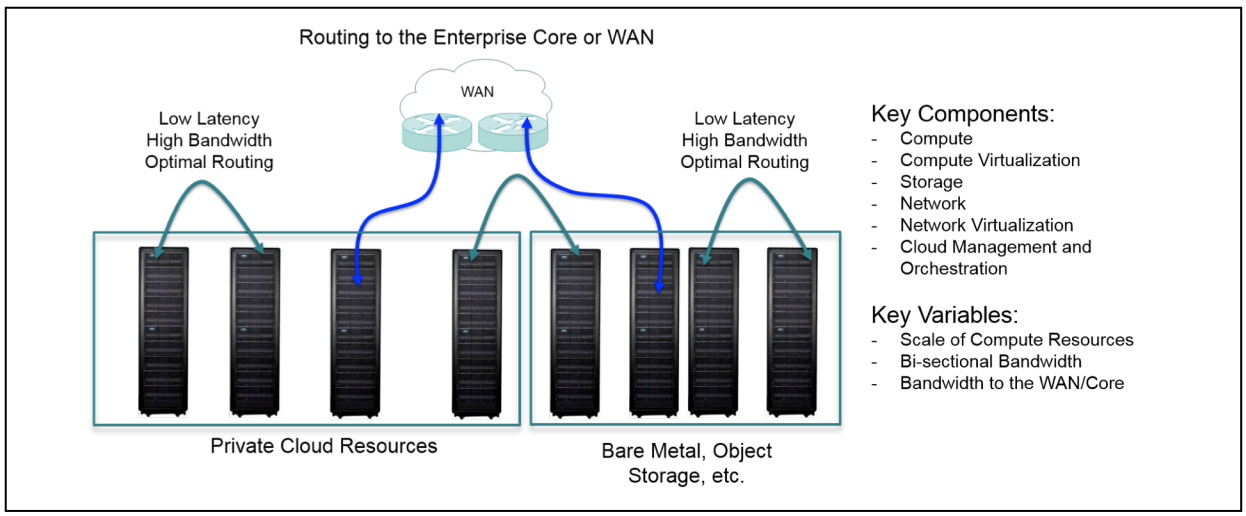
When building a private cloud, its multiple components including compute, storage, networking and virtualization must work seamlessly together, and a robust cloud management platform (CMP) is also required. The CMP enables the abstraction and pooling of physical and virtual resources for consumption on an on-demand, elastic, self-service basis. For this to be done efficiently, the underlying components must offer programmable APIs to the CMP.

Each component of the cloud architecture outlined above should be evaluated on its own merit. In terms of networking, a key asset is network virtualization with programmable APIs that are leveraged by the CMP. Both NSX and ACI provide RESTful APIs (i.e., software frameworks composed of guidelines and best practices for the creation of scalable web services) to the CMP.

To compare NSX and ACI, we use a generic infrastructure design for a private cloud following both vendors' design guidelines, which are publicly available. The performance of the infrastructure will depend on many variables, including the compute and storage choices, which are beyond the scope of this paper. For simplicity, from a networking perspective, our example considers the bi-sectional bandwidth available to the applications running in the private cloud and the bandwidth to the WAN or enterprise core.

Exhibit 1 shows several racks, some which will be part of the new private cloud infrastructure and others that may run legacy or bare-metal applications or perhaps provide additional storage capacity for cloud applications. We expect that the physical network fabric will provide high-bandwidth and low-latency connectivity in all cases.

Exhibit 1: The Building Blocks of a Private Cloud Infrastructure



Source: ZK Research, 2015

Section II: Understanding ACI vs. NSX

VMware NSX is a pure software-based network overlay solution. All NSX components are software elements running in the ESXi hypervisor kernel or as virtual machines (VMs). Because NSX is a software-only solution, the physical network must be acquired from another vendor and considered separately. It is also important to note that NSX does not provision or manage the physical switches as of this writing, so NSX isn't a true "apples to apples" comparison to ACI but provides a subset of capabilities. In fact, in some cases, ACI may be the physical network fabric that NSX runs on.

Cisco ACI, on the other hand, implements a full SDN solution—meaning the RESTful APIs can be used to program the virtual network to support the private cloud, but they also can be used to program the physical network settings, including interface-level settings, port channels, quality of service (QoS) and routing policies.

The difference in the approach to network virtualization and SDN between NSX and ACI has a few important consequences in practical terms, as summarized in Exhibit 2.

Exhibit 2: ACI vs. NSX

	ACI	NSX
Network Automation	Enables full automation of all virtual and physical network parameters through a single API.	Automation is limited to virtual networks for virtual machines. No automation of physical switches is possible.
Connecting to Legacy Networks	Legacy workloads can be directly connected to the fabric, and/or legacy network devices can connect to the fabric using standard multi-chassis LACP, for instance, providing sub-second convergence.	L2 software gateways running on ESXi must be used, which provides limited performance and slow convergence (greater than sub-second) in failure scenarios.
Routing Implementation	Routing is implemented in hardware at line rate for East–West and North–South regardless of workload connected to the fabric (physical or virtual), with sub-second convergence on failure scenarios.	East–West routing can be done at the hypervisor, but it requires an extra distributed logical router control VM per IP domain space.* North–South routing requires deploying ESR VMs per IP domain space. Redundancy and load balancing are possible, albeit with slow convergence.
Network Availability	Sub-second convergence is possible for link and node failures.	Routing and bridging services implemented in servers and/or VMs react slowly to network changes. Sub-second convergence is not attainable.
Advanced Network Service Insertion	ACI L4-7 service insertion is done via an open SDK where partners can develop a device package to represent their services to the APIC controller. It supports both virtual and physical service appliances.	NSX L4-7 service insertion is accomplished through a closed API and is subject to licensing.** It supports only virtual services appliances from certified partners (i.e., no physical appliance support).

*We refer to an IP domain space as an isolated routing and forwarding table, which is commonly referred to as a VRF (virtual routing and forwarding).
**See page 18 of the VMware product guide for details about VMware NSX API licensing (www.vmware.com/files/pdf/vmware-product-guide.pdf).

Source: ZK Research, 2015

NSX requires the use of software gateways whenever a VM that resides inside the network overlay needs to communicate with endpoints outside of the overlay. If the VM and the other endpoints are in the same subnet, they need to communicate through a Layer 2 (L2) gateway service (NSX Distributed Logical Router [DLR] L2 bridge function). If they are in different subnets, they must communicate through an NSX Edge Services Router (ESR) virtual machine. These software gateways require dedicated compute capacity to perform their functions.

Consequently, for a given scale of a private cloud infrastructure, the NSX design option will require more physical servers (with corresponding licenses) when compared to an ACI solution. Of course, having more servers also requires more network ports, transceivers, etc.

A future enhancement to alleviate this problem is through NSX integration with hardware vendors by using Open vSwitch Database (OVSDB) Management Protocol for implementing L2 gateway services in hardware. At the time this paper was published, this option was not yet available on NSX for vSphere. The NSX controller has tremendous visibility into VMware's infrastructure, but it does not have full visibility into or management capabilities for third-party hardware. For example, software upgrades on hardware switches and the provisioning of physical ports must be done outside of NSX.

ACI is network centric, but it supports multiple hypervisor offerings on top of the physical fabric. Because of this, any workload can run on top of ACI—including NSX or other server-based overlay solutions—and companies can realize the benefits it provides in terms of network automation. Further integration enables the Application Policy Infrastructure Controller (APIC) to learn the full state from the Virtual Machine Manager (VMM) and program the virtual switching layer. For vSphere, this integration exists already. For Hyper-V and open source offerings, such integration relies on the open OpFlex protocol. This protocol provides a way for the policy controller (APIC) to provide the necessary network and policy configuration to the virtual switch of the hypervisor using an open declarative approach. Microsoft will natively implement OpFlex as part of its Hyper-V offering. For open source hypervisors such as Xen and KVM, an OpFlex agent can be added to the Open vSwitch (OVS). In the case of OpenStack specifically, an enhancement has been added to Neutron to enable it to express policy in a high-level language that directly maps to ACI constructs: the Group-Based Policy (GBP) Neutron plugin.

Section III: Solution Design Description

Design Premises

As explained in the introduction, our comparison considers a scenario for building a fully automated infrastructure either as a new deployment or as an expansion of an existing data center deploying new pods for a private cloud.

We considered the following customer objectives in our study:

1. The solution must enable the definition of multi-tier application blueprints inclusive of the network connectivity and policy. The application blueprints will map dynamically onto the infrastructure in an elastic and self-service way, including virtual machines and virtual networks as required.
2. All requirements for network connectivity and policy will be provisioned and/or de-provisioned in a programmatic and automated way.
3. All applications must have the option to be visible by external networks if required; therefore, the solution must also automate routing to and from the enterprise core/WAN.
4. Applications running in the private cloud infrastructure must be able to access and/or interface with applications or data running on bare-metal infrastructure.

The network for a private cloud infrastructure must offer API-based programming of secure virtual networks, with multi-tenancy and dynamic service insertion where required. By "secure virtual networks," we are referring to policy-based networking, where essentially communication is enabled between applications only as defined by the administrators. Both ACI and NSX comply with these objectives.

The goal of the comparison is to evaluate the total cost of acquisition of the chosen SDN solution. We also must consider the impact the architecture may have from a cost perspective on other components of the solution, such as the number of servers and licenses required as a consequence of the SDN choice. Also, the cost of licenses and hardware required to run the solution as well as the required service subscription cost are included.

The cost of storage is not included in the comparison because any storage option should work regardless of the SDN chosen, and the cost will be the same across both solutions. This includes using traditional storage arrays from EMC, NetApp or other established companies; converged storage solutions such as VMware VSAN; or newer scale-out storage solutions such as Ceph. The scale of the storage solution should not impact the cost of one SDN offering versus another because the hypervisors will access storage directly and not through the NSX overlay. However, it is worth noting that ACI brings an additional operational benefit because the access to IP storage resources from the hypervisor also benefits from the programmability and telemetry provided by ACI.

Compute, Virtualization and Cloud Management Design Choices

Because our focus is on comparing the NSX and ACI SDN offerings, the choice of compute, virtualization and cloud management software are the same for both design scenarios. The scenarios normalize on the following:

- Cisco UCS C-Series configurations for compute
- Cisco ONE Enterprise Cloud Suite
- VMware vSphere Enterprise Plus for virtualization
- VMware vRealize Suite for cloud management

However, ZK Research recommends that customers review each of these components separately and evaluate them on their own merits as well.

It is important to note that the choice of cloud management solution does impact the cost of NSX. The cost of permanent NSX licenses is lower if the product is acquired as an add-on to the vRealize Suite than if procured for use with another cloud management platform. In addition, it is also important to note that the NSX version we considered works only on vSphere environments, while ACI can work with virtualization offerings from Microsoft, Red Hat and others.

Physical Network Design and SDN Solution

The scenario models a physical network providing redundant top-of-rack (ToR) switches to every rack, with up to 20 physical servers per rack. All servers are connected using redundant 10GE network interface cards (NICs). A potential out-of-band management network could be considered, but we omitted it from this comparison for simplicity.

The network design implements a leaf-and-spine architecture with equal-cost multipath (ECMP) routing to ensure a scale-out approach that can accommodate the growth of the private cloud. Each ToR switch will connect to the spine switches using 40GE interfaces over multimode fiber (MMF).

In the ACI design option, the physical network also implements the SDN solution. In the NSX option, the physical network implements a Layer 3 (L3) ECMP-routed underlay.

Implementing Automated Policy Enforcement

Both ACI and NSX offer the possibility of filtering traffic between application tiers. In ACI, this is done by grouping physical or virtual endpoints into endpoint groups (EPGs) and then applying contracts that define what traffic is allowed between them. In NSX, virtual endpoints can be added into security groups. The policy enforcement in NSX is done using the Distributed Firewall (DFW) feature that runs in the vSphere ESXi Virtual Distributed Switch (VDS), so this is limited to endpoints that exist within vSphere only. The DFW enables stateful tracking of the traffic flows. In ACI, policy is enforced in hardware at the ACI leafs and in software at the optional Application Virtual Switch (AVS), where stateful connection tracking is also implemented.

Both ACI and NSX provide lateral movement protection between tiers and within an application tier, implementing policy as described above. This is what many refer to as micro-segmentation.

Advanced Security and Network Services Insertion

While micro-segmentation offers a level of protection, it does so by implementing packet filtering at the header level. These days, most exploits focus on legitimate application ports and protocols; therefore, advanced security requires inspection at the application level. This requires deeper packet inspection, such as that provided by next-generation firewalls (NGFWs) and/or intrusion prevention system (IPS)/intrusion detection system (IDS) capabilities. These advanced protection mechanisms are not natively provided by ACI and NSX. Both platforms provide the capability to redirect traffic to a partner security solution.

Similar to the considerations for storage, the use of an NGFW between application tiers or at the infrastructure perimeter can be considered orthogonal to our comparison because both would be added on to the SDN solution. The way ACI and NSX handle service insertion is very different. NSX

only supports the use of virtual services appliances, while ACI supports using both virtual and physical appliances. In NSX, the virtual services appliance from the partner must run in every host in a vSphere Distributed Resource Scheduler (DRS) cluster where the service is defined, whether required or not in a particular host. In ACI, however, virtual or physical appliances can be sized independently of the vSphere DRS cluster definition, and they can be shared across many clusters if required. This difference in approach between NSX and ACI has an impact on the total acquisition cost of the solution, and it should be considered if required by the solution.

Also, NSX provides basic load-balancing features as part of NSX Edge when enabled. ACI requires the use of a partner's services, such as Citrix, F5, Avi Networks and open source alternatives including HAProxy. NSX also supports using partner load-balancing services, however, only in the virtual appliance form factor from F5.

The evaluation of the total cost of using the NSX Edge load-balancing feature must consider the compute resources dedicated to this function. An NSX Edge VM configured to do HTTP-based load balancing is not 10GE capable, and several VMs (and relevant vCPUs and vRAM) will be required depending on the performance. The number of VMs needed will increase if Secure Sockets Layer (SSL) offloading is required. These extra compute resources, and the licenses they consume, must be factored into the total cost of the solution.

All these considerations make an apples-to-apples comparison between ACI and NSX complicated, particularly because F5's and Citrix NetScaler's application delivery controllers (ADCs) are significantly more feature rich than the native NSX Edge. Open source HAProxy offers equivalent functionality to NSX Edge's load-balancing capabilities.

When considering ADCs and security, many options are available. Some customers may evaluate ADCs and security technology separately from the rest of the infrastructure. Others may choose to combine F5 with Check Point or use Cisco Adaptive Security Appliance (ASA) and NetScaler. Another scenario is to add a new vendor and/or an open source solution such as HAProxy. Adding a new vendor is possible with ACI's open approach. With NSX, however, this may require extra cost because the API to integrate L4-7 services is licensed as per the VMware product guide. (Note: See page 18 of the VMware product guide for details about VMware NSX API licensing: *www.vmware.com/files/pdf/vmware-product-guide.pdf*.) Because of the complexity of choices, ADCs have been omitted from the TCO comparison.

Routing, IP Address Management and Network Address Translation Services

The applications hosted on the private cloud infrastructure require appropriate addressing and access to the WAN and potentially the Internet. The IP Address Management System (IPAM) is beyond the scope of this design comparison, and we assume it to be equal for both options. Depending on the design, network address translation (NAT) may or may not be required when routing subnets within the private cloud infrastructure.

NSX Edge provides basic NAT capabilities for IPv4. These are not provided in ACI natively. However, ACI does not require extra resources to provide routing for virtual networks within the overlay. Leaf switches can be configured as border leafs and routed in hardware to the WAN.

Depending on the design options, NAT, if required, may be provided in the WAN routing platform. If this is not the case, the proper resources required must be factored into the cost. For the TCO scenarios in this paper, we consider the WAN bandwidth to be optimized for NSX Edge performance at 10 Gbps per ESR VM with the possibility to load balance up to eight ESRs. Adding NAT to the comparison requires changing that scenario because load balancing is eliminated from ESR when NAT is enabled. This would potentially limit routing from the private cloud to the capacity of a single ESR VM (sub-10GE).

For simplicity and for the purpose of trying to keep comparisons fair, we consider a scenario in the comparison where we add the Cisco ONE Enterprise Cloud Suite to the ACI solution instead of the vRealize Suite. This brings the Cisco cloud management stack to the ACI solution as well as licenses for Cisco CSR 1000V, which could be used to implement NAT if required in a similar way as NSX Edge.

Section IV: Solution Descriptions

Exhibit 3 summarizes the components of the two solutions being considered.

NSX-Based Design Details

We have used the NSX for vSphere Design Guide (NSX for vSphere Design Guide 2.1: *www.vmware.com/files/pdf/products/nsx/vmw-nsx-network-virtualization-design-guide.pdf*) as the main

Exhibit 3: ACI vs. NSX Solution Components

SOLUTION COMPONENT	ACI DESIGN	NSX DESIGN
SDN Solution	ACI: ACI licenses for every leaf, API Controller Cluster	NSX: NSX licenses for every server
Network Solution: Leaf and Spine Design	Leaf: Nexus 9300 Spine: Nexus 9500 or 9300	Leaf: Arista 7150S or 7050 Spine: Arista 7500E or 7050
Compute	Cisco UCS C220 M3	Cisco UCS C220 M3
Virtualization Platform*	vSphere Enterprise Plus	vSphere Enterprise Plus
Cloud Management Platform	vRealize Suite Enterprise or Cisco ONE Enterprise Cloud Suite**	vRealize Suite Enterprise

*Virtualization licenses are included in the vRealize Suite Enterprise cost.
**When selecting the Cisco ONE Enterprise Cloud Suite, virtualization licenses for vSphere Enterprise Plus with Operations Management are added as required.

Source: ZK Research, 2015

source of information to determine the design of the NSX-powered solution.

The design guide recommends leaf and spine network architecture with an L3 control plane approach using ECMP to load balance traffic and maximize available bandwidth. We consider redundant top-of-rack switches for each rack, with dual-homed servers in every case.

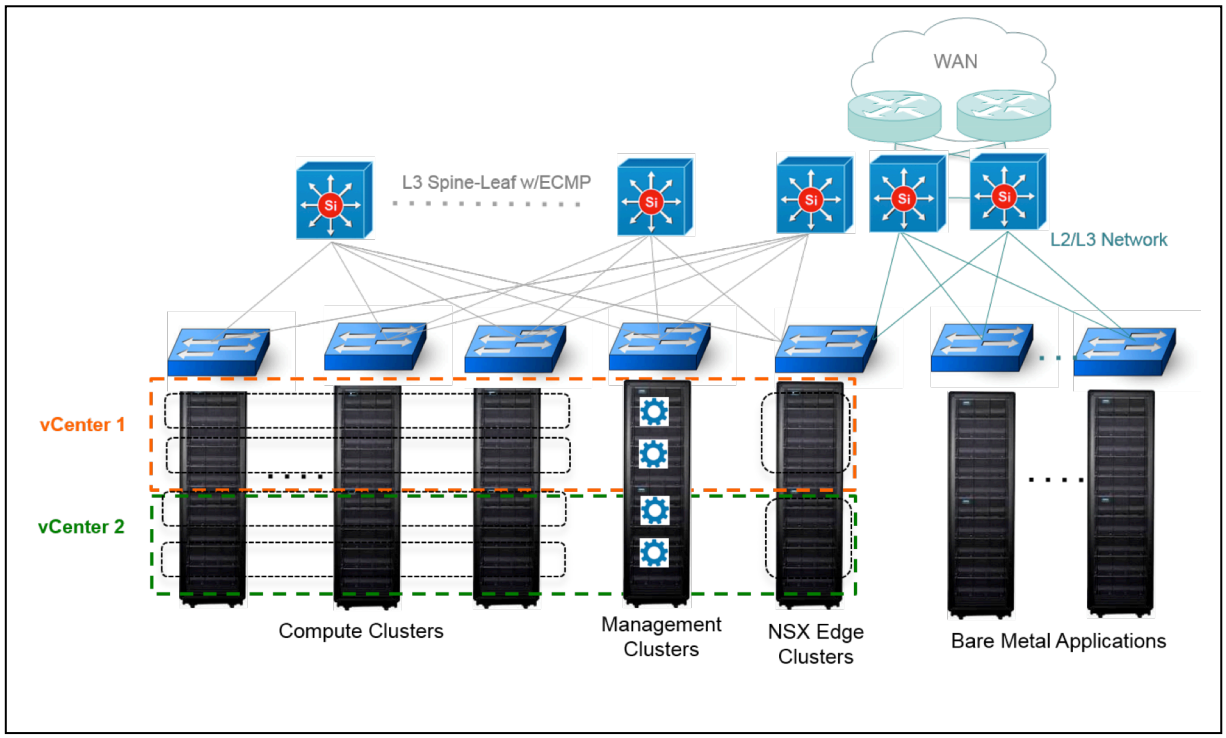
The physical network design involves, as outlined in Exhibit 3, Arista Networks switches, including an advanced license option that features Enhanced L3 (Open Shortest Path First [OSPF], Border Gateway Protocol [BGP], Protocol-Independent Multicast [PIM]) and Advanced Features (Latency Analyzer [LANZ], Zero Touch Provisioning [ZTP], VM Tracer, etc.). In this design, the network underlay has no visibility or integration with the NSX overlay, and vice versa.

NSX and vRealize Suite tools do not perform any physical network automation. This means that the physical switches must be pre-provisioned with the required virtual LAN (VLAN), routing information and access control list and interface settings. For racks with servers running NSX ESR, this imposes an extra operational burden that is significant but beyond the scope of this document. On management clusters, there may also be a need to extend VLANs between racks. The end result is that you have three different types of hosts running ESXi:

- **Hosts that run application workload virtual machines,** where VM networking is handled within the NSX overlay but ESXi infrastructure traffic such as Internet Small Computer System Interface (iSCSI), Network File System (NFS) and vMotion is still handled on standard VLANs that must be manually preconfigured.
- **Hosts that run management systems such as the NSX Manager, NSX Controllers, vCenter, vRealize and their associated databases:** These hosts and networks are not part of the overlay and must also be configured manually.
- **Hosts that run NSX gateway functions, either for L2 or L3 services:** These can be DLR control virtual machines, DLR bridge servers or NSX ESRs.

The diagram in Exhibit 4 describes the overall architecture and represents an existing network

Exhibit 4: Network Configuration Using VMware NSX



Source: ZK Research, 2015

connecting bare-metal applications and providing access and connectivity to the WAN routers. It is a generic design with the following aspects:

- One or more racks will be dedicated to hosting management clusters. (Depending on the scale of the infrastructure and availability requirements, this can be limited to a single rack.)
- One or more racks will be dedicated to NSX Edge and DLR virtual machines. These may serve for routing to the WAN, for bridging to the bare metal applications and also for routing in between vCenter domains if there is a need for multiple vCenters.
- Various racks will have the hosts dedicated to compute capacity of the private cloud. These will typically be split into various vSphere Distributed Resource Scheduler (DRS) clusters, all of them enabled with NSX kernel modules.

The cost of the NSX solution will be impacted by the number of servers that need to be dedicated to gateway and/or management functions. As of NSX version 6.1.3, there is a one-to-one mapping between NSX Manager and vCenter. This means that if the scale of the infrastructure requires multiple vCenter domains, then multiple NSX Managers and accompanying controller clusters will also be required. This affects the infrastructure in various ways:

- **More compute hosts are required for management clusters.** Each domain requires hosts to run vCenter, NSX Manager and three NSX controller VMs in a cluster as a bare minimum. For availability considerations, the NSX controller VMs should be in different physical hosts, as should the NSX Manager and vCenter.
- **Each pair of NSX Managers and vCenters constitutes a separate domain.** This means that logical switches and DLRs do not extend across vCenter domains. For this reason, traffic between applications that are hosted under different vCenter domains must traverse an NSX Edge virtual machine, or in fact two: one under one NSX Manager, another under the other NSX Manager.

In the following sections, we explain the criteria that we have followed to determine how many servers are required to implement management and gateway functions with NSX.

NSX VXLAN to VLAN L2 Gateway

If an application needs to connect to an endpoint outside of the overlay but in the same subnet, an L2 gateway function is required. This is true also if traffic needs to be sent from the overlay to a physical services appliance such as a physical firewall.

The L2 gateway function in NSX for vSphere is implemented through the DLR VM. The NSX DLR virtual machine is very small in size and will typically be deployed in redundant pairs (active/standby), with each running on a different server. This VM is used for the management plane and configuration of the L2 gateway function.

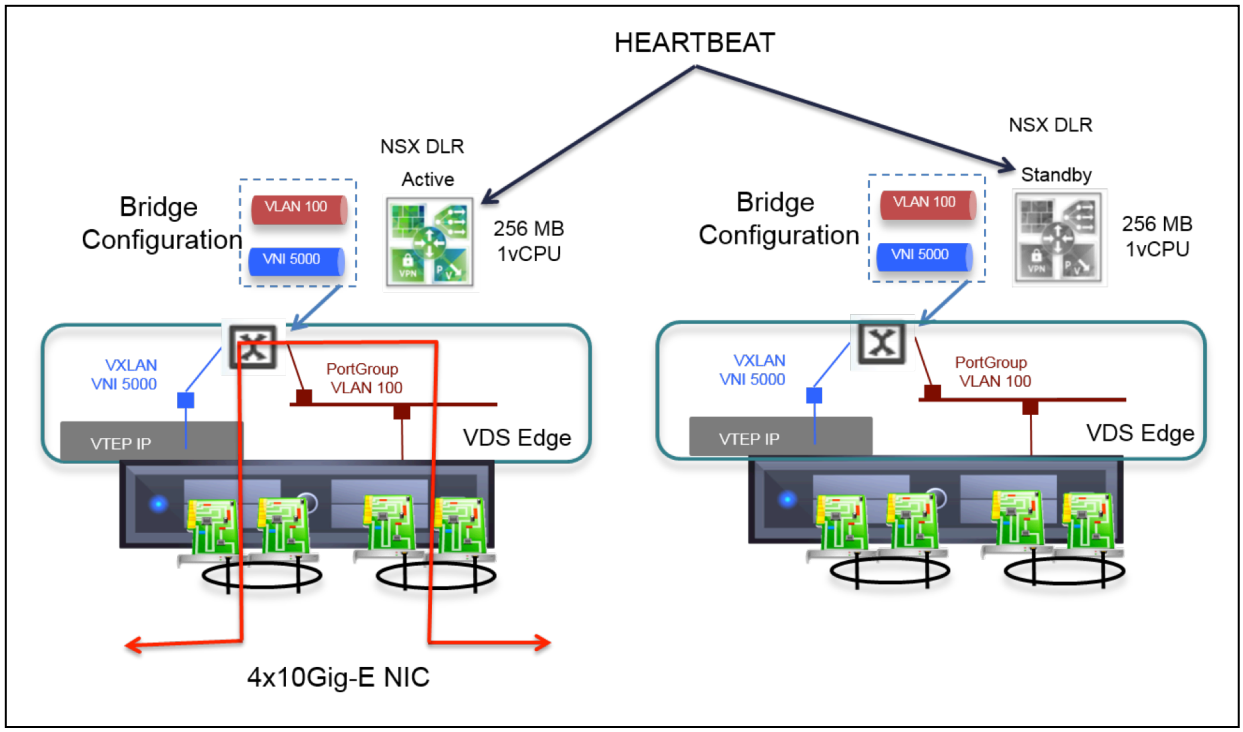
Exhibit 5 shows a typical L2 gateway use case, where a server equipped with 4x10GE NIC configured in redundant Link Aggregation Control Protocol (LACP) uplink groups could in ideal conditions run 20 Gbps of Virtual Extensible LAN (VXLAN) to VLAN traffic. (Note: No public information was available to validate the performance of a DLR bridge function configured to bridge a VXLAN segment and a VLAN. Based on interviews with technical engineers familiar with this configuration, this should be considered the best-case scenario. This model includes a typical server equipped with four 10GE NICs and dual-socket E5-2697s that can run at line rate, or equivalent to 20 Gbps full duplex. This should be considered an optimized solution because that level of throughput requires in excess of 60 Mbps for 64-byte packet sizes.) In this configuration, an additional server is required for standby functionality.

This model considers one dual-socket server with two dual-port 10GE NICs for each 20 Gbps of L2 gateway capacity required, plus another one for redundancy.

NSX Routing

For the routing of North–South traffic, VMware recommends using the NSX ESR virtual machine. Because there are no public benchmarks outlining performance, this study assumes that a single VM with X-Large (VM with 6vCPU and 8 GB of RAM) capacity is capable of routing up to 10 Gbps. The NSX ESR also can work in an active/standby configuration, with a secondary VM provisioned typically in another host in the cluster ready to take over if the primary one fails.

Exhibit 5: Single Server with Two Port Channels Connected with Dual 10 Gig

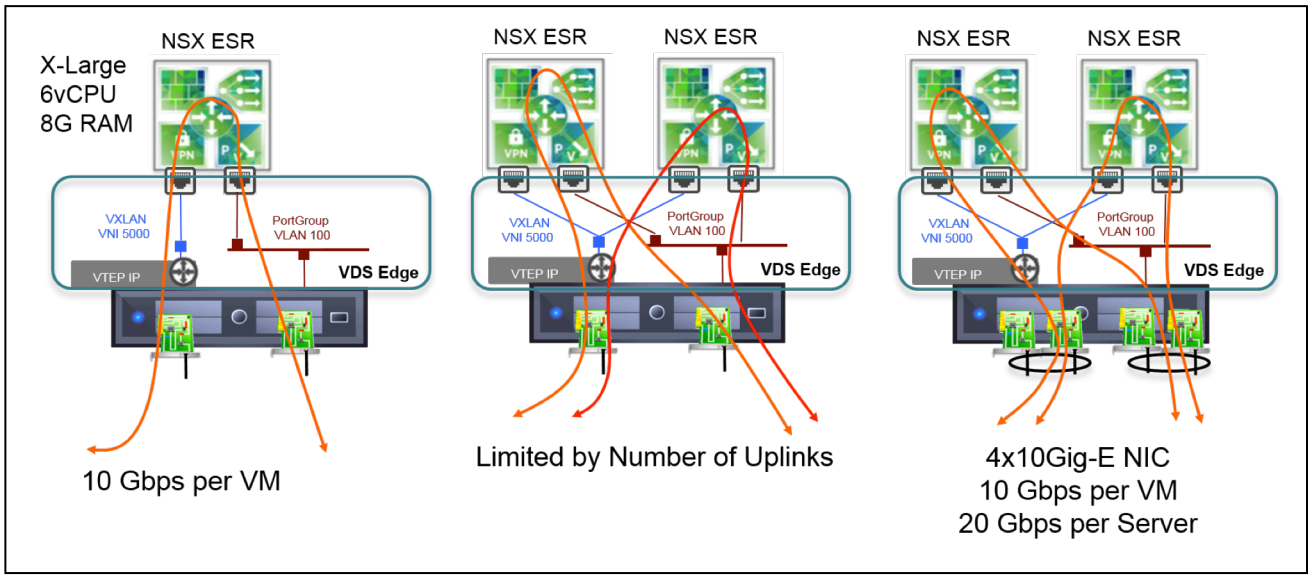


Source: ZK Research, 2015

However, if more than a single VM of throughput is required (i.e., if the traffic exceeds 10 Gbps), the recommended configuration is having multiple ESRs running in parallel leveraging ECMP across them. In such a configuration, routing can exceed 10 Gbps, but no stateful services, such as NAT and firewalls, will be supported.

For two X-Large ESRs to accomplish the routing of more than 10 Gbps, the server must be equipped with the necessary NIC configuration, or multiple servers are required. In practical configurations, customers will need to run multiple ESRs across multiple servers. Exhibit 6 depicts the described scenario with flows load balancing across two X-Large VMs.

Exhibit 6: NSX Edge ESR Configurations



Source: ZK Research, 2015

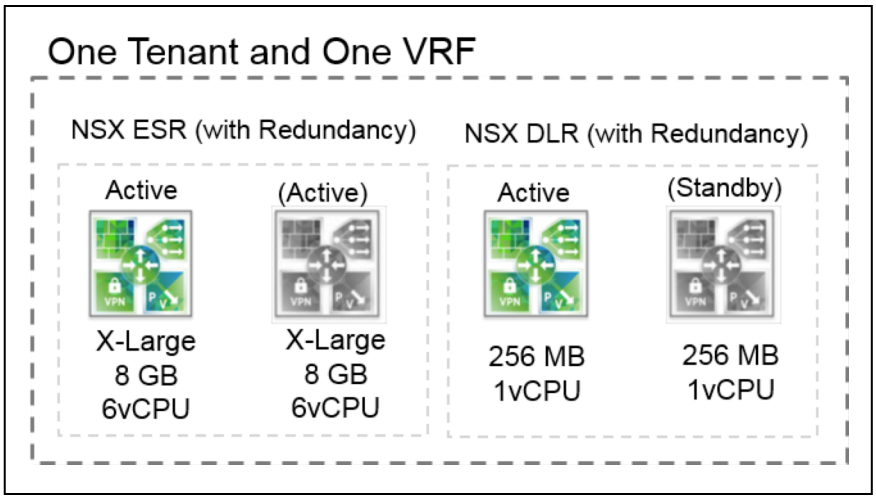
The number of ESR VMs to run per host is therefore limited in terms of performance by the total number of NICs configured on the server. For simplicity in our comparisons, we consider a fixed configuration server with a dual-socket 12-core E5-2697 equipped with four 10GE interfaces. Depending on the requirements of the private cloud for performance, you will need more or fewer servers, as explained above.

However, performance is not the only variable. For example, NSX Edge currently does not support virtual routing and forwarding (VRF) functionality—meaning it works with a single routing and forwarding table. This can pose a problem if there is a need to support overlapping address spaces and/or for multi-tenancy in general (where routing domains must be isolated between tenants even if they have unique address spaces).

The more tenants and/or VRFs required, the more NSX Edge ESRs and DLR VMs are required. As shown in Exhibit 7, if redundancy is required, four VMs are required per VRF. The complexity grows with the number of VRFs or the number of tenants (or both), as shown in Exhibit 8.

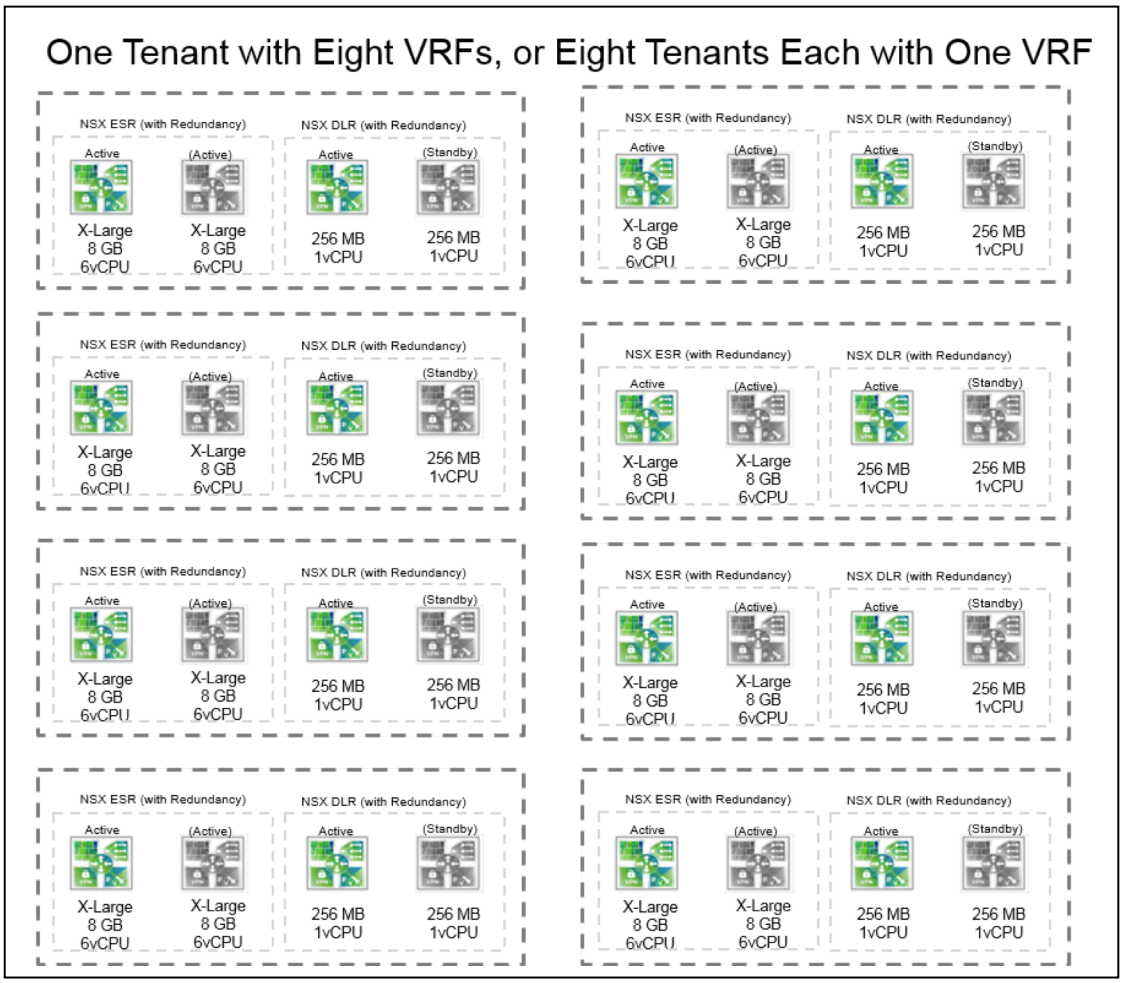
The complexity of designing the NSX Edge Clusters poses a challenge when creating the solution. One concern is limiting the number of ESR VMs per host. If the physical host has 4x10GE interfaces, putting too many VMs on it may not guarantee enough performance. In addition, CPU oversubscription must be considered as well because packet processing is primarily a CPU-bound application. The models in this paper consider no more than eight X-Large NSX Edge ESR VMs per 24-core server with 4x10 Gig-E interfaces, resulting in a two-to-one vCPU oversubscription.

Exhibit 7: One Tenant and One VRF Configuration for NSX ESR



Source: ZK Research, 2015

Exhibit 8: One Tenant with Eight VRFs or Eight Tenants Each with One VRF



Source: ZK Research, 2015

Considerations When Using More than One vCenter

Currently, NSX has one-to-one mapping to a vCenter server. This means that for each vCenter server, it is necessary to deploy a set of NSX Manager and controller clusters. This means that two VMs under different vCenter servers are deployed in different overlays. For the vCenters to communicate, a route between the two overlays must be created—meaning NSX Edge capacity must be provisioned for the information flow. For total cost of ownership (TCO) calculations, one server for each 20 Gbps of bandwidth per NSX domain is factored in.

Summary of NSX Design Considerations

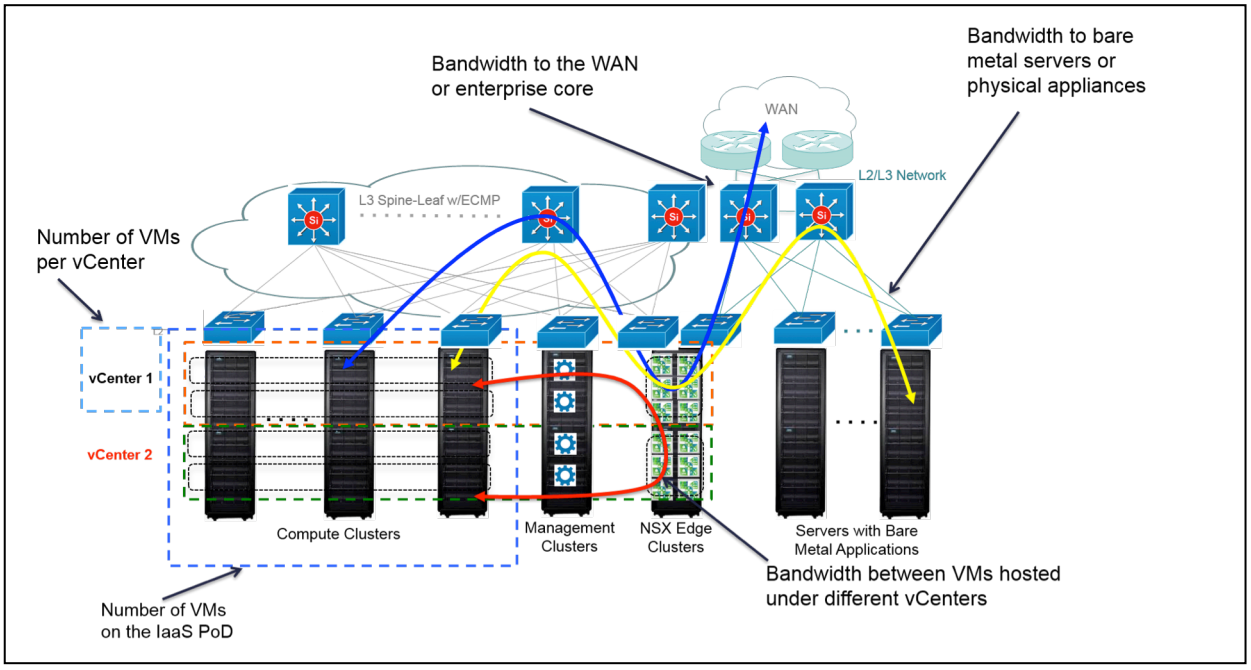
Exhibit 9 provides a high-level representation of an NSX implementation. The exhibit shows the key parameters that should be considered to size the infrastructure and determine the necessary amount of servers, racks, ToR switches and so on. In summary, the maximum number of virtual machines (A) expected in the private cloud infrastructure for the considered operational period will determine the number of physical hosts required (20 virtual machines per host, in this case). In turn, the number of VMs that are considered per vCenter (B) determines the number of NSX domains. (Note: vCenter supports a maximum of 10,000 active virtual machines. However, for availability reasons, to reduce the size of the failure domain, and for other scalability considerations, customers typically choose a smaller value.) In the exhibit, we show two domains just to illustrate that multiple domains may be required depending on size and scale.

The bandwidth configured for the data center connection to the enterprise core or WAN (C) will determine the number of VMs and servers required to run the NSX ESR that will route traffic in and out of the private cloud infrastructure.

Similarly, there may be a need for certain applications to reside on the same subnet as bare-metal workloads, or to access physical load balancing or firewall appliances. This is specified in terms of bandwidth required (D) and will determine the number of hosts running DLR bridge functions.

Finally, if more than one vCenter is required, we must also consider the minimum bandwidth necessary for applications hosted under different vCenters (E). This determines the number of VMs and servers dedicated to running the NSX ESR that will route between NSX domains. We consider this number in addition to the WAN bandwidth (C) because it is very possible that an application needs access to/from the WAN while concurrently another application needs to access data or resources under another vCenter.

Exhibit 9: VMware NSX Implementation



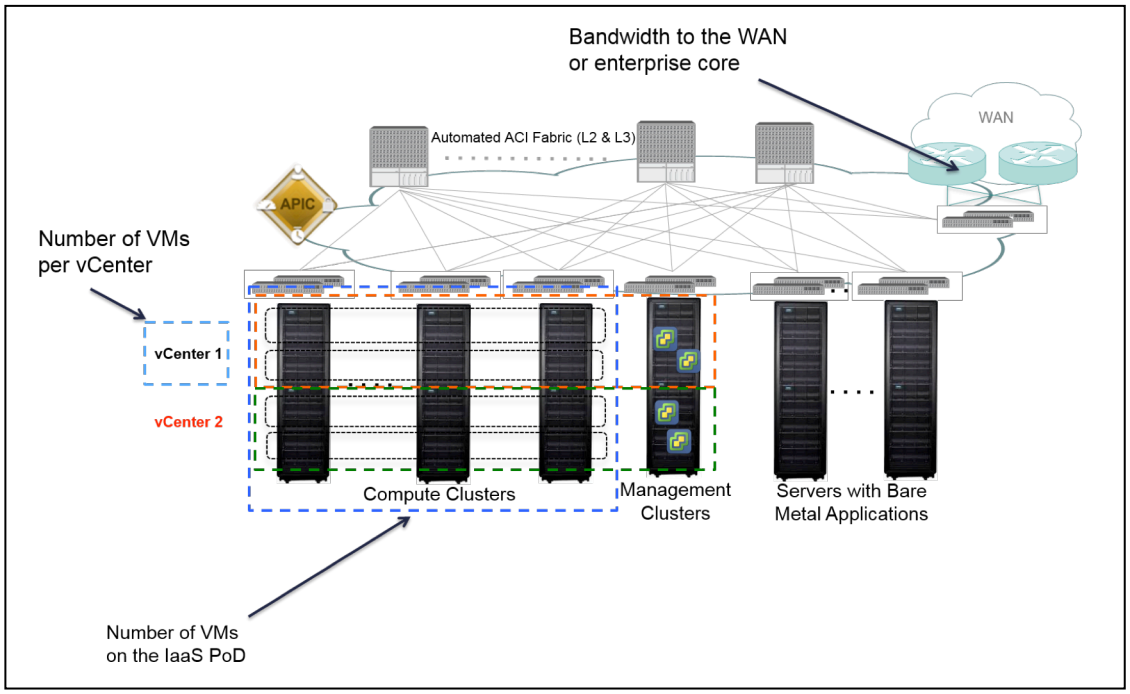
Source: ZK Research, 2015

ACI-Based Design Details

We used the Cisco Application Centric Infrastructure Design Guide (*www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-731960.html*) as the main source of information to determine the design of the ACI-powered option. The premises for scaling the infrastructure are the same as in the NSX scenario (Exhibit 10):

- The number of virtual machines that will run in the private cloud infrastructure (A)
- The number of virtual machines per vCenter (B)
- The bandwidth connecting the DC router to the enterprise core or WAN (C)

Exhibit 10: Cisco ACI Implementation



Source: ZK Research, 2015

ACI does not require using gateway functions because a distributed default gateway is implemented in every leaf switch. In addition, a single APIC cluster can work with multiple vCenter servers (referred to as multiple Virtual Machine Managers in APIC) or even multiple vCenters and other VMMs, such as Microsoft System Center or OpenStack environments. This translates to simpler operations and using fewer servers.

In terms of the physical topologies, we consider the same uplink capacity per ToR (redundant 40GE uplinks on MMF), the same number of spine switches and the same number of access ports as were used with NSX. Similar to the previous design, we consider 20 servers per rack, each server with dual-10GE ports connected on copper to a redundant pair of ToR switches.

The bandwidth available to each server is therefore 20 Gbps, and the bandwidth available to the rack is 160 Gbps. In the case of the ACI configuration, that bandwidth is available for communication between any VMs, regardless of the vCenter, or between any VMs and bare-metal servers. In the case of the NSX design, the bandwidth between vCenter domains and/or to bare-metal applications is specified and NSX Edge configuration is inferred as per the above explanations.

Connections to the WAN are accomplished by using ports off leaf switches in a virtual PortChannel (vPC) over which traffic is routed to the DC routers in hardware.

Section V: Solution Comparison Scenarios

This section represents two design scenarios based on actual customer deployments. One customer is a US-based midsize organization and the other is a large European, enterprise-class company.

Scenario 1: US Midsize Organization Solution for Up to 2,500 Virtual Machines

In this scenario, a fully automated infrastructure that must scale up to 2,500 virtual machines is used. The deployment considers a single vCenter server and 20 Gbps in capacity to the WAN. The details are summarized in Exhibits 11, 12 and 13.

Exhibit 11: Midsize Business Implementation of ACI vs. NSX

REQUIREMENT	ACI DESIGN	NSX DESIGN
Number of VMs	2,500	2,500
Number of VMs per vCenter	2,500	2,500
Number of VMs per ESXi Host	20	20
Bandwidth to the WAN/Core	20 Gbps	20 Gbps
Bandwidth Between vCenter Apps	N/A (single vCenter)	N/A (single vCenter)
Bandwidth Between VMs and Bare Metal/Physical Appliances	160 Gbps per rack (2x40GE uplinks per ToR switch)	80 Gbps
Number of 40GE Uplinks per ToR Switches	2	2
Number of VRFs	1	1

Results, including one-year service cost and list prices:

	ACI DESIGN	NSX DESIGN
Number of Compute Hosts	125	125
Number of Edge and Gateway Hosts	Not required	10
Number of Management Hosts	1	2
Number of ToR Switches	16	18
Number of 40GE Ports	64	72

Source: ZK Research, 2015

Exhibit 12: NSX Design Costs

NSX Design: Physical Arista Network Cost (Including One Year of Service)

ITEM	DESCRIPTION	QUANTITY	LIST PRICE
ToR Switch	Arista DCS-7050TX-64-F with Advanced License option	18	$611,910
Spine Switch	Arista DCS-7150S-64-CL-F with Advanced License option	2	$82,286
40GE Transceiver	40GBASE SR4 QSFP+ transceiver	18	$143,640
Service and Support (One Year)	A-Care Software and NBD hardware replacement/same day ship		$31,176
			Total $869,012

NSX Design: Compute (Servers) Cost (Including One Year of Service)

ITEM	DESCRIPTION	QUANTITY	LIST PRICE
Compute Server	UCS C220 M3 SFF 2xE5-2680v2, 128 GB RAM, Intel x540 dual-port 10GBASE-T adapter	127	$2,761,361
NSX Edge Server	UCS C220 M3 SFF 2xE5 2680v2 , 128GB RAM, Intel x540 dual-port 10GBASE-T adapter	9	$281,412
Service and Support (One Year)	SMARTnet 8X5XN		$41,133
			Total $3,083,906

NSX Design: VMware vCloud/vSphere Licenses

ITEM	DESCRIPTION	QUANTITY	LIST PRICE
Cloud Management Platform	vCloud Suite Enterprise	272	$3,126,640
Virtualization Platform	vSphere Enterprise Plus (included in vRealize Suite)		
Service and Support			$781,728
			Total $3,908,368

NSX Design: NSX Licenses

ITEM	DESCRIPTION	QUANTITY	LIST PRICE
Network Virtualization	NSX for vSphere permanent per socket license (add-on to vRealize Suite)	272	$950,640
Service and Support			$237,660
			Total $1,118,300

Overall Cost of Acquisition for NSX Including One Year of Service Using List Pricing for 2,500 VMs, One vCenter, One Tenant and 140-to-1 Oversubscription to the WAN

ITEM	LIST PRICE
Network (Arista + NSX)	$2,057,312
VMware vCloud/vSphere Licenses	$3,908,368
Compute	$3,083,906
	Total $9,049,586

Source: ZK Research, 2015

Exhibit 13: ACI Design Costs

ACI Design: Physical Network Cost (Including One Year of Service)

ITEM	DESCRIPTION	QUANTITY	LIST PRICE
ToR Switch	Cisco Nexus N9K-C9372TX with ACI license included	16	$568,000
Spine and APIC	Nexus 9336 ACI Spine switch with 36p 40G QSFP (including APIC cluster)	2	$125,664
40GE Transceiver	QSFP 40G BiDi short-reach transceiver	64	$70,080
Service and Support (One Year)	SMARTnet 8X5XNBD		$24,040
			Total $787,784

ACI Design: Compute (Servers) Cost (Including One Year of Service)

ITEM	DESCRIPTION	QUANTITY	LIST PRICE
Compute Server	UCS C220 M3 SFF 2xE5-2680v2, 128 GB RAM, Intel x540 dual-port 10GBASE-T adapter	126	$2,739,618
NSX Edge Server	UCS C220 M3 SFF 2xE5-2680v2, 128 GB RAM, Intel x540 dual-port 10 GBASE-T adapter	Not required	$0
Service and Support (One Year)	SMARTnet 8x8xN		$38,109
			Total $2,777,727

ACI Design: VMware vCloud/vSphere Licenses

ITEM	QUANTITY	LIST PRICE
vCloud Suite Enterprise	252	$2,896,740
Service and Support		$724,248
		Total $3,620,988

Overall Cost of Acquisition for ACI Including One Year of Service Using List Pricing for 2,500 VMs, One vCenter, One Tenant and 140-to-1 Oversubscription to the WAN

ITEM	LIST PRICE
Network Cost (Physical and Virtual)	$787,784
VMware vCloud/vSphere Licenses	$3,620,988
Compute	$2,777,727
	Total $7,186,499

Source: ZK Research, 2015

Comparing Both Designs

Exhibit 14 provides a side-by-side comparison of the costs involved in the first year of acquisition (with one-year service included).

Strictly considering the network components, the ACI solution is 62% less expensive. The network component is small as a percentage of the total investment compared to the investment in vCloud licenses and the cost of compute. However, because using ACI requires using fewer servers and—consequently—fewer vCloud licenses, there are additional savings on those items as well.

The conclusions can be summarized as follows:

- The ACI-based solution is 62% less expensive than an NSX and Arista-based network offering.
- The ACI-based solution enables 7% savings in virtualization and cloud management licenses and 10% savings in compute costs.
- The overall solution is 20% less expensive when using Cisco ACI.

Other operational considerations include the following:

- ACI has 38% fewer servers and 36% fewer network devices to manage.
- The NSX solution takes 12 racks while ACI only takes 9.

Exhibit 14: The Cost of ACI vs. NSX for a Midsize Organization

Midsize Enterprise with 2,500 VMs, One vCenter, One Tenant and 140-to-1 Oversubscription to the WAN (One Year) TCO

OVERALL COST OF ACQUISITION INCLUDING ONE YEAR OF SERVICE USING LIST PRICING	ACI DESIGN	NSX DESIGN	SAVINGS WITH ACI
Network (Switches, Transceivers and Required SDN Licenses)*	$787,784	$2,057,312	62%
VMware vCloud Suite or vSphere Enterprise + Licenses	$3,620,988	$3,908,368	7%
Servers (for VM and NSX Edge, if required)	$2,777,727	$3,083,906	10%
Total Solution Cost (Including One Year of Service)	**$7,186,499**	**$9,049,586**	**20%**

*Includes the cost of physical network and virtualization licenses. For NSX design, this means NSX licenses for all hosts that require it as well as the cost of Arista switches and licenses. For ACI design, this means Nexus 9000 series cost, ACI licenses and an APIC controller cluster.

Source: ZK Research, 2015

Scenario 2: Large European Enterprise Solution for Up to 25,000 Virtual Machines

This scenario is based on a large enterprise in Europe. The deployment is a fully automated infrastructure that must scale up to 25,000 virtual machines. The deployment considers a failure domain of 5,000 VMs per vCenter server. This deployment is implemented across two data centers that operate in active/active configurations and are connected by Dense Wavelength Division Multiplexing (DWDM) links. The customer is scaling up its core connection to using multiple links up to an aggregate of 100 Gbps. The details of this scenario are summarized in Exhibit 15.

Exhibit 16 provides a side-by-side comparison of the costs involved in the large European enterprise implementation scenario in the first year of acquisition (with one-year service included). Considering the network components, the ACI solution is 80% less expensive when comparing list prices.

The conclusions can be summarized as follows:

- The ACI-based solution is 80% less expensive than an NSX and Arista-based network offering, not counting the savings on compute.

Exhibit 15: Large European Enterprise Implementation of ACI vs. NSX

REQUIREMENT	ACI DESIGN	NSX DESIGN
Number of VMs	25,000	25,000
Number of VMs per vCenter	5,000	5,000
Number of VMs per ESXi Host	20	20
Bandwidth to the WAN/Core	100 Gbps	100 Gbps
Bandwidth Between Apps on Different vCenters	160 Gbps per rack (2x40GE uplinks per ToR)	80 Gbps
Bandwidth Between VMs and Bare Metal/Physical Appliances	160 Gbps per rack (2x40GE uplinks per ToR)	80 Gbps
Number of 40GE Uplinks per ToR	2	2
Number of VRFs	15	15

Results, including one-year service cost and list prices:

	ACI DESIGN	NSX DESIGN
Number of Compute Hosts	1,250	1,250
Number of Edge and Gateway Hosts	Not required	110
Number of Management Hosts	5	10
Number of ToR Switches	128	140
Number of 40GE Ports	512	560

Source: ZK Research, 2015

- The ACI-based solution enables 68% savings on virtualization and cloud management licenses and 17% savings on compute costs.
- The overall solution is 47% less expensive when using Cisco ACI.

In addition, the ACI design delivered better performance because no traffic flows were constrained by a gateway function that became underprovisioned as the infrastructure evolved. And although we have not considered operational expenses as part of this exercise, the customer articulated that Cisco ACI provided an advantage there, too. For instance, in this particular example, we calculated that in total, the network in the NSX design has 142 switches to manage, plus eight NSX gateways and as many as 270 NSX Edge VMs (each managed independently)—compared to Cisco ACI, where all infrastructure is managed from a single point: the APIC controller cluster.

Section VI: Conclusions

Both ACI and NSX can respond to an organization's need to automate networking via programmable

Exhibit 16: Simulation with 25,000 VMs, Five vCenters, 15 Tenants and 252-to-1 Oversubscription to the WAN (One Year)

OVERALL COST OF ACQUISITION INCLUDING ONE YEAR OF SERVICE USING LIST PRICING	CISCO ACI DESIGN	NSX WITH ARISTA L3 ECMP UNDERLAY	CISCO ACI SAVINGS
Network (Switches, Transceivers and Required SDN Licenses)	$5,881,508	$29,162,330	80%
VMware vCloud Suite or vSphere Enterprise + Licenses	$13,318,060	$41,095,340	49%
Cisco ONE Enterprise Licenses	$7,530,000	$0	
Servers (for VM and NSX Edge, if required)	$27,667,040	$33,144,244	17%
Total	**$54,396,608**	**$103,401,914**	**47%**

Source: ZK Research, 2015

network virtualization. NSX is not a complete networking solution as it requires a physical network or fabric to run on top. ACI, on the other hand, is a programmable fabric that integrates network virtualization. The integrated approach taken by Cisco ACI translates into significant economic advantage over a solution built using VMware NSX and another network vendor (Arista, in this study). In the case of a design with VMware NSX, the customer must procure the physical network in addition to the licenses that enable it to build a network virtualization solution that only works with vSphere. NSX is licensed per socket, and this quickly adds up in higher costs. In contrast, Cisco ACI delivers its benefits by adding a license per ToR switch.

In addition, the server-based architecture of NSX for vSphere inevitably requires adding additional server capacity to implement various gateway functions, such as bridging between overlay VXLAN and VLANs or routing traffic external to the overlay. These functions are simply not required in the integrated overlay approach with ACI. This translates into extra costs for an NSX design, represented by an increased number of servers and their required licenses (per-socket licenses for vRealize Suite and NSX) and a corresponding increase in the physical network footprint. The servers required to run network functions are also potentially more costly because they require a larger number of NIC interfaces and run best using high-end CPUs (network loads are CPU-bound tasks, in most cases).

This study did not factor in some of the operational risks and associated costs, such as the benefits enabled by simplicity of management and troubleshooting. ACI provides a single interface point for managing physical and virtual networks, whereas the NSX plus Arista solution requires multiple management interfaces for underlay and overlay, which increases management complexity, limits visibility into underlay networks and drives up troubleshooting costs. The cost of space, power and cooling was not factored in, but this will also contribute to ongoing costs being higher in the NSX design. Also, customers must rely on disjointed multivendor solutions when implementing the NSX architecture, which exposes them to product delivery risk and architectural alignment issues among vendors. In comparison, Cisco's integrated overlay approach provides a leaner architecture that drives operational efficiency and significantly lowers operational costs.

Cisco ACI Offers Savings in Compute and Virtualization Licenses

In a design aimed at on-premises private cloud with capacity of up to 2,500 virtual machines, NSX required 10% extra compute capacity and three more racks' worth of equipment. The required capacity would be higher as the bandwidth needs increased for the overlays to communicate with external endpoints.

At a higher scale, in a design for up 25,000 virtual machines, we obtained a similar percentage of overlay networks that translated into six additional racks of equipment.

In terms of cost, this difference means that a private cloud built with Cisco ACI could save between 10% and 17% on server costs and about 7% to 49% in virtualization and cloud management licenses.

Cisco ACI Is Significantly Less Expensive than a VMware NSX Alternative

In our two scenarios, the Cisco ACI network design was between 62% and 80% less expensive than an alternative using VMware NSX and Arista switches. This difference does not include the extra servers and licenses required for running functions such as NSX Edge or NSX gateways because we considered those savings as being part of another budget (i.e., server, virtualization and cloud management licenses).

Once again, this study does not take into consideration operational costs that will also be higher in the NSX design because there are two networks to manage.

Pricing Sources

Pricing information comes from public sources for list prices. For VMware, this includes validation using online resellers. These are the main sources:

- *www.vmware.com/products/vcloud-suite/pricing*
- *www.virtualizationworks.com/NSX.asp*

References

- VMware NSX for vSphere Network Virtualization Design Guide 2.1: *www.vmware.com/files/pdf/products/nsx/vmw-nsx-network-virtualization-design-guide.pdf*
- Cisco ACI Design Guide: *www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-731960.html*