



vCloud Director, Nexus 1000V, and VXLAN Technical Deep Dive

Simon Momber, VMware Cloud Architect

Sean Gilbert, VMware Senior Alliance Manager

Francesca Gutierrez, VMware Director of Global Alliances

Syed Ghayur, Cisco Nexus 1000V Technical Marketing Engineer

Gunnar Anderson, Cisco Nexus 1000V Product Manager

Public Webcasts Series, Spring 2012

Date	Technical Track Topics	Webinar
2/14/12	Virtual Security Gateway (VSG) v1.3 Technical Deep Dive	Play
2/22/12	Nexus 1000V v1.5 Technical Deep Dive	Play
2/29/12	Nexus 1010-X v1.4 Technical Deep Dive	Play
3/7/12	vWAAS and Nexus 1000V Technical Deep Dive	Play
3/14/12	FlexPod & Nexus 1000V/1010	Play
3/21/12	QoS for multimedia traffic in the Virtualized DC (w/ Nexus 1000V)	Play
3/28/12	Vblock & Nexus 1000V / VSG / vWAAS	Play
4/4/12	vCloud Director, Nexus 1000V, and VXLAN Technical Deep Dive	Register
4/11/12	Cisco's CloudLab Deep Dive: Hands-on labs for N1KV, VSG & VXLAN	Register

Above table and presentations: www.cisco.com/go/1000vcommunity

Agenda

- VMware vCloud Director Integration Options
- VMware vCloud Director Technical Deep Dive
- Understanding VXLAN
- Nexus 1000V with VXLAN
- FAQ
- Resources
- Q&A as we go...



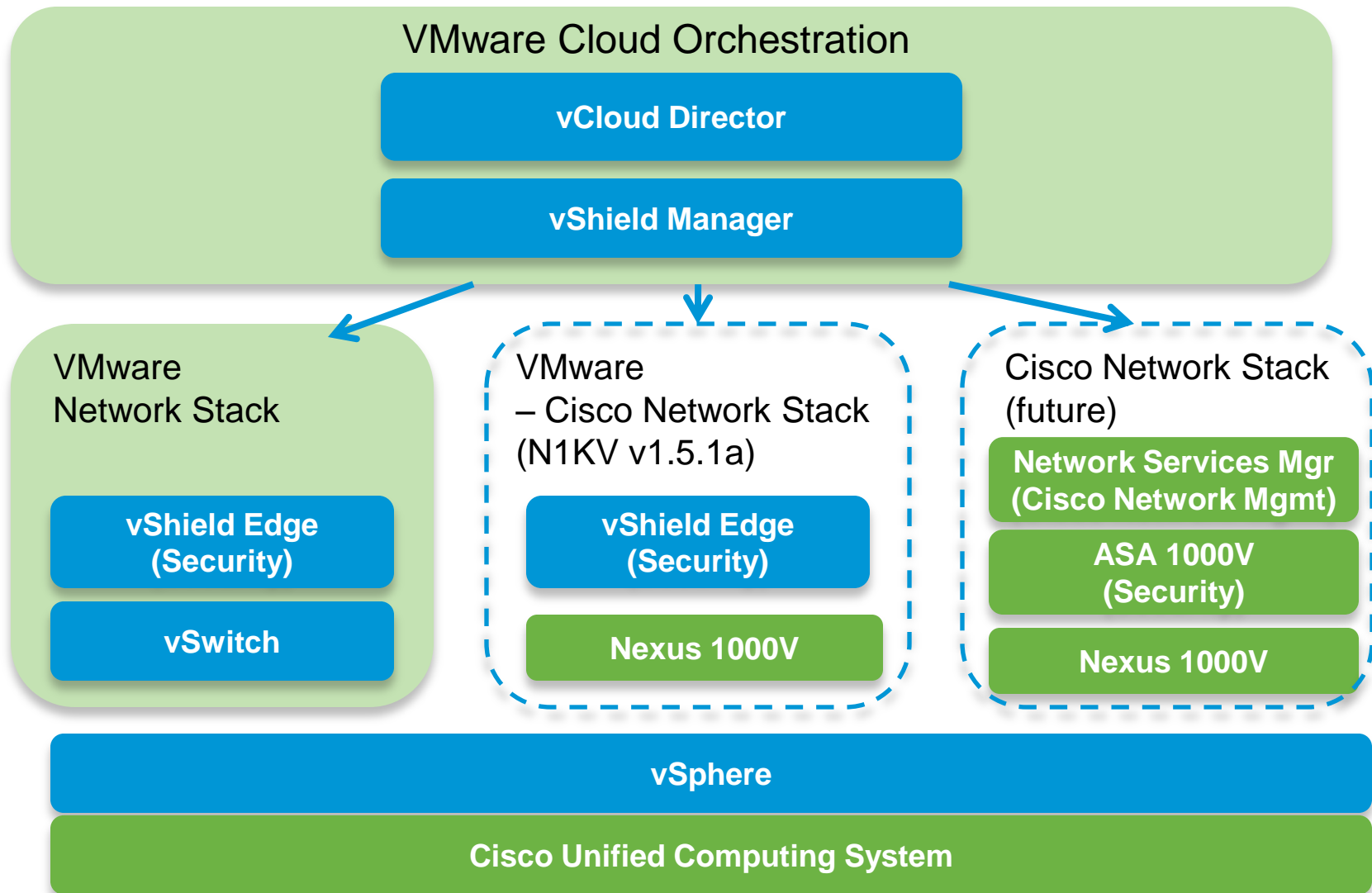
VMware vCloud Director Integration Options



Disclaimer

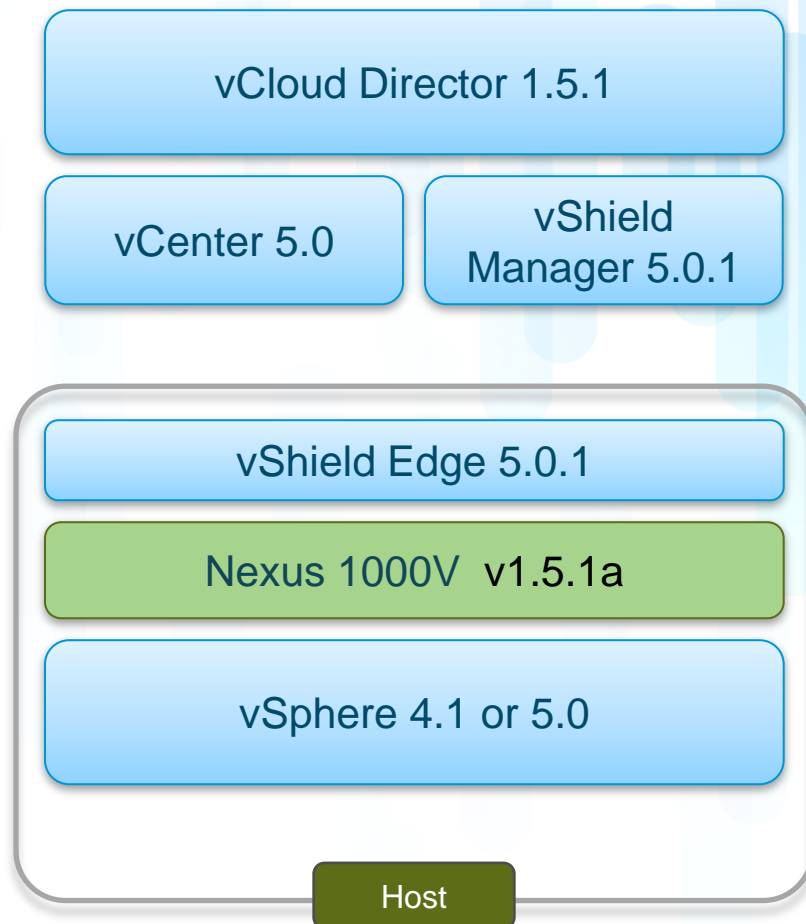
- This session may contain product features that are currently under development.
- This session/overview of the new technology represents no commitment from VMware to deliver these features in any generally available product.
- Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.
- Technical feasibility and market demand will affect final delivery.
- Pricing and packaging for any new technologies or features discussed or presented have not been determined.

vCloud Director Integration



Nexus 1000V: vCloud Director Integration

- Cisco Nexus 1000V Series 1.5 Release 4.2(1)SV1(5.1a) is fully integrated into VMware vCloud Director.
(Shipping late April)
- Support dynamic network provisioning
 - Port-group backed pools
 - VLAN-backed pools
 - Network isolation backed pools (via VXLAN)
- Choice of vSphere 4.1 or 5.0



Fully functional stack w/ VXLAN once Nexus 1000V Release 4.2(1)SV1(5.1a) ships late this month

Nexus 1000V (v1.5.1a) Supporting vCloud Director Network Pools

vCloud Director Network Pools	vCloud Director 1.0	vCloud Director 1.5
Port Group Network Pool	Yes	Yes
VLAN Backed Network Pool	No	Yes
Network Isolation Network Pool	No	Yes (VXLAN)



VMware vCloud Director Technical Deep Dive



VMware vCloud Director (vCD)

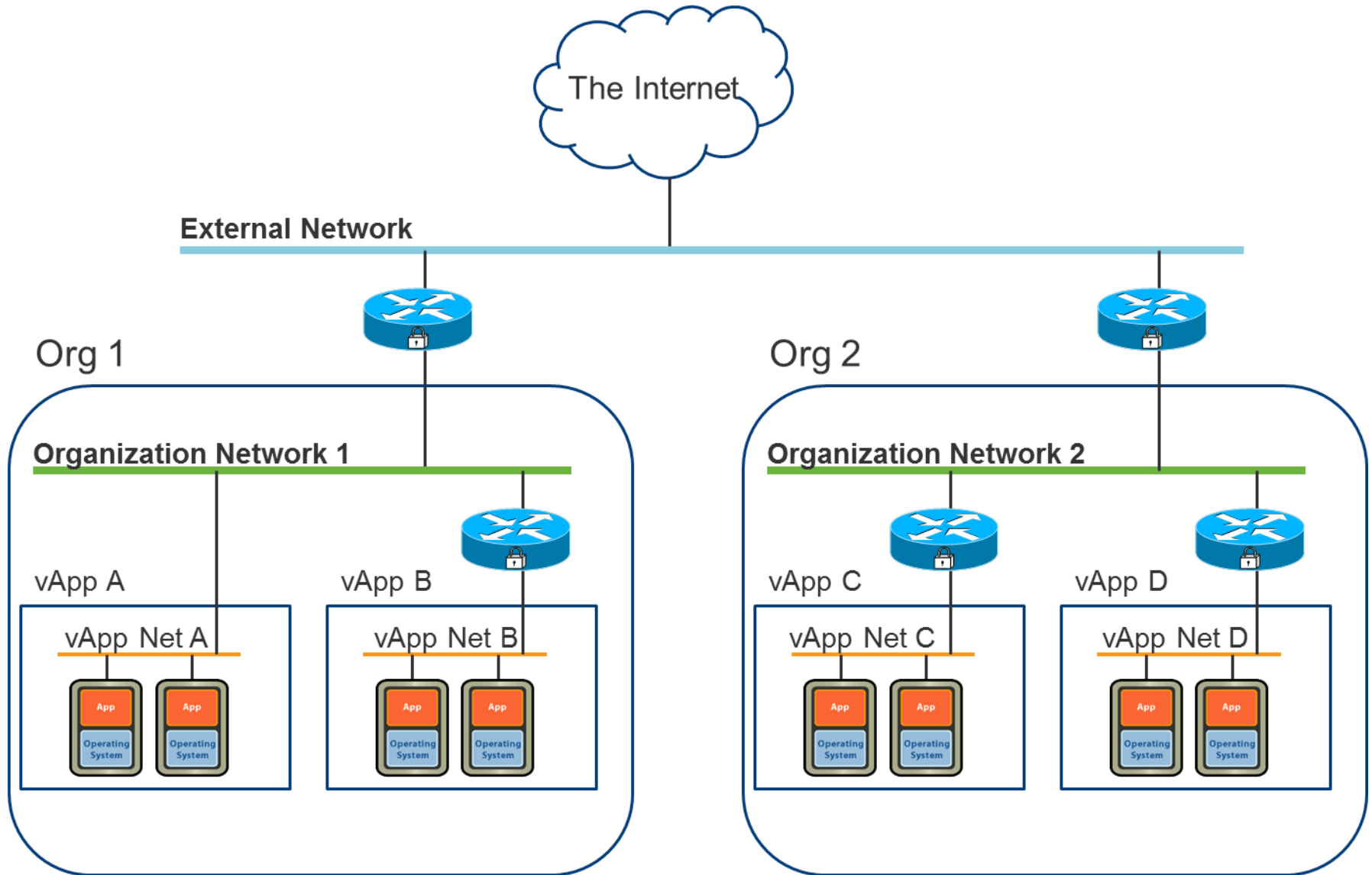
- Define standard infrastructure tiers called Virtual Datacenters
 - Pool virtualized infrastructure resources across multiple vCenter Servers
- Define standard collections of VMs called vApps
- Create Organizations and manage users with RBAC
- Provide UI for users to self provision vApps into Virtual Datacenters
- Provide secure multi-tenancy using vShield Edge



VMware vShield Edge for vCD

- vShield Edge provides end point security
 - Available for download with vSphere Enterprise and Enterprise Plus.
- One vShield Manager required per vCenter Server
 - Provides network edge security
 - Provides firewall, NAT, port forwarding, IP masquerading and DHCP functionality (enforces multi-tenancy)
 - Edge appliances deployed and managed by VMware vCloud Director on vSphere.
 - Does not require separate database
- Licensing
 - Upgradable to vShield Edge 1.0 (full version which includes site-to-site VPN and load balancer)

vCD Networking Option - The Big Picture



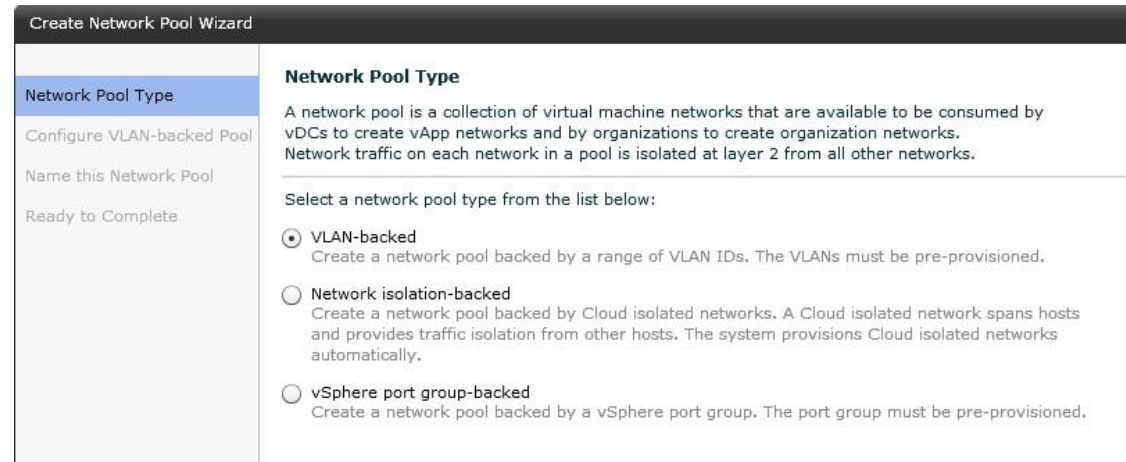
vCD Networking Options – Network Types

- External Networks:
 - Network that is external to VCD
 - Created in vSphere/vCenter environment and consumed by VCD to provide external connectivity to Organizations
- Organization Networks:
 - Contained wholly within an organization
 - Provides connectivity for vApps
 - Backed by Network Pools
- vApp Networks:
 - Contained wholly within a vApp
 - Can be attached to an Organization Network
 - Backed by Network Pools

vCD Network Pools: Overview

- A set of pre-configured network resources that can be used for Organization and vApp Networks

- Picture these as a collection of preconfigured switches that can be assigned to organizations or vApps



- Three Types of Network Pools in VMware vCloud Director

- Portgroup-backed

- Have to be created in vSphere manually or through orchestration
- Do not have to be VLAN isolated (but should for L2 isolated)
- Assign a collection of them to VMware vCloud Director

- VLAN-backed

- Like portgroup-backed with VMware vCloud Director orchestrating the creation of the portgroups as needed using assigned VLANs to isolate the portgroups.

- vCloud Network Isolation-backed (vCD-NI)

- VMware proprietary network isolation technology

Networking Isolation Options - Current Shortfalls

- Failover would require re-IP or stretched VLANs
 - No VM portability between L2 zones
- Scaling limited and dependent on pool type
 - VLANs in short supply
 - vCD-NI shared broadcast
 - Portgroup backed pools require work up front and not as flexible



Understanding VXLAN



VXLAN – Virtual eXtensible LAN

Functionalities

- Fast, on-demand provisioning of large number of isolated (layer 2) networks
- On demand networks without physical network re-configuration
- Massive scale for multi-tenant environments.
- Allows virtual layer 2 network to stretch across physical layer 2 boundaries
- VM mobility across physical network boundaries and datacenters

VXLAN IETF draft

<http://tools.ietf.org/html/draft-mahalingam-dutt-dcops-vxlan-00>

Why VXLAN?

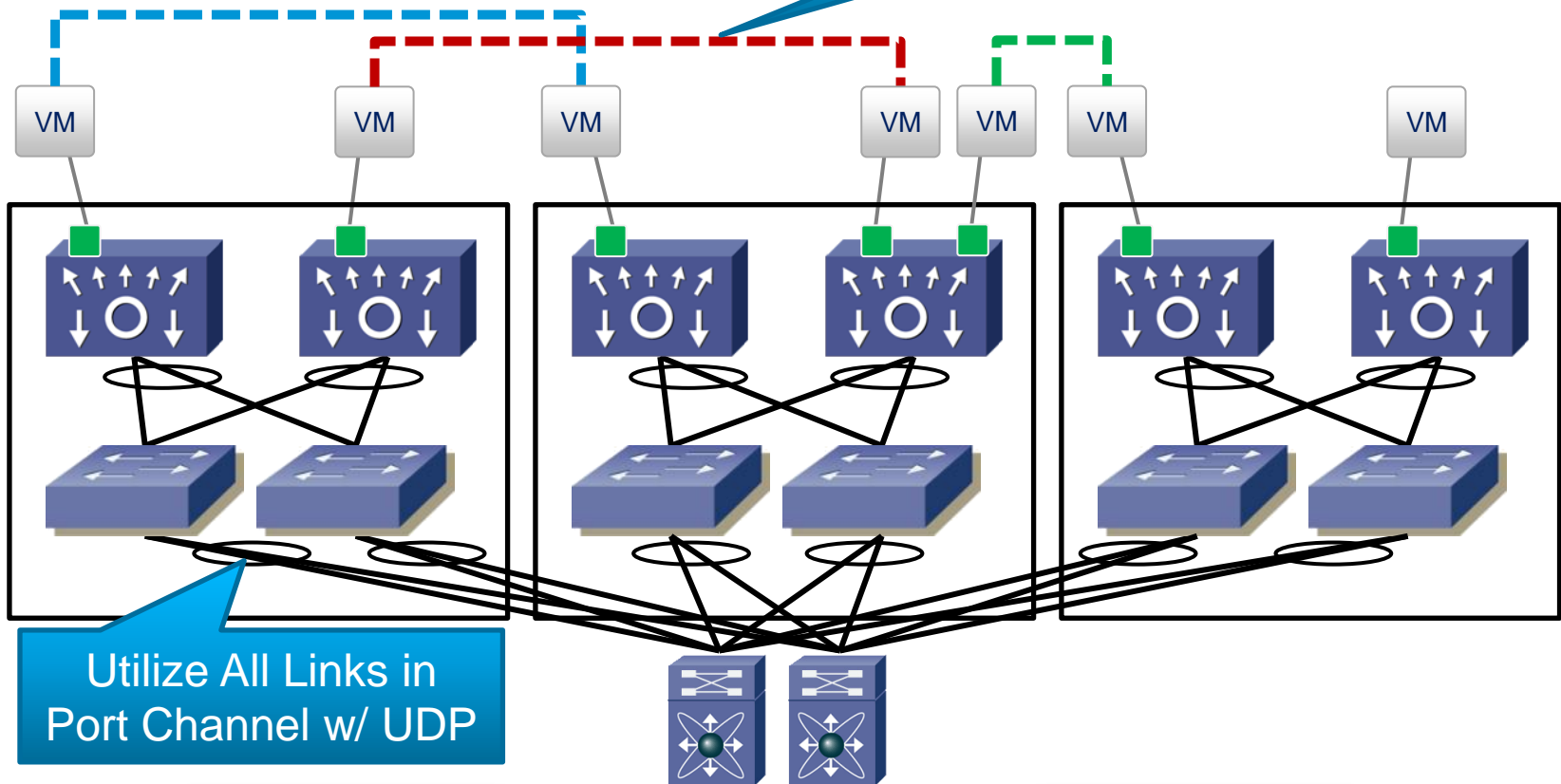


Drivers

- Need cross cluster mobility
- Enable provisioning workload where compute is available. Avoid operational heaviness of VLAN's
- Enable network snapshot on same Layer 2 (dev/test)
- Provision large number of tenants (>4K limits of VLAN's, avoid STP)
- Enable stateful movement of workloads

Scalable Pod Deployment with VXLAN within a Data Center

Logical Network Spanning Across Layer 3



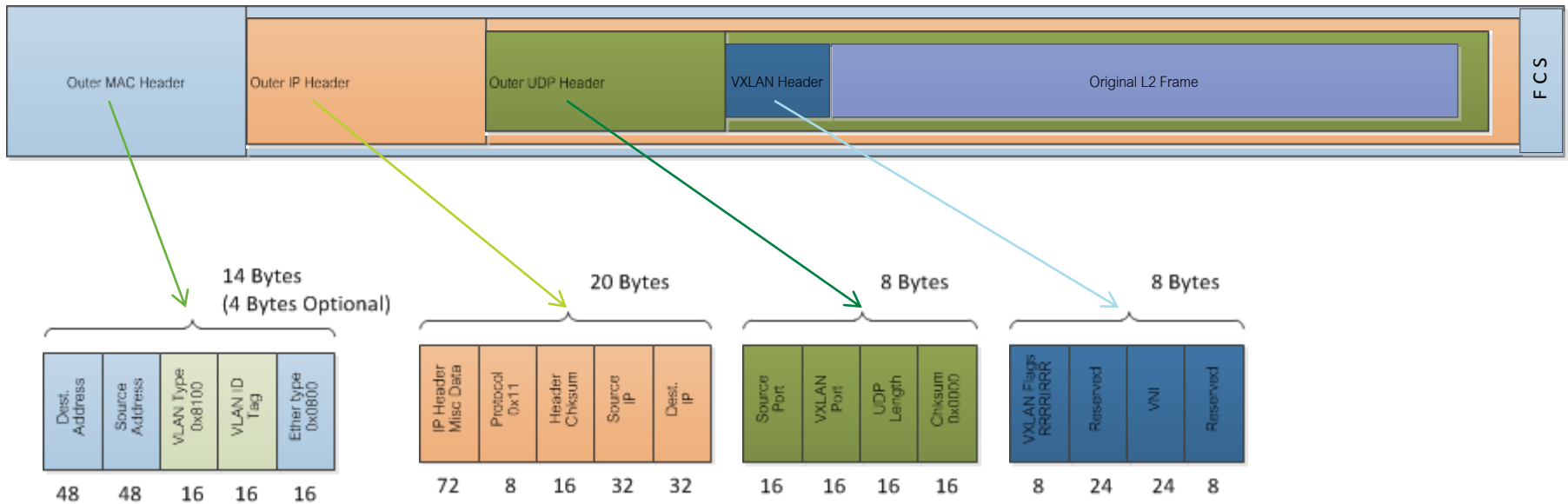
Utilize All Links in Port Channel w/ UDP

Add More Pods to Scale

VXLAN Overview

- Each overlay network is known as a VXLAN Segment
- Each VXLAN Segment identified by a 24-bit segment ID (VNI)
- VXLAN traffic carried between VXLAN Tunnel Endpoints (VTEP)
- The ESXi hosts or N1KV act as the VTEPs
- VM traffic carried over point to point tunnels between VTEPs
- VM to VM traffic is encapsulated in a VXLAN header
- VM to VM traffic on same portgroup and host is not encapsulated
- VTEP uses multicast to discover unknown destination VTEP for VM
- VM MAC to VTEP mapping gleaned from VTEP multicast traffic

VXLAN – Packet Structure



Original L2 frame given a VXLAN header with VNI

UDP header has a UDP destination port reserved for VXLAN

Frame check set 0x0, if not destination VTEP should calculate the FCS to verify

IP header has destination and source addresses of the VTEPs

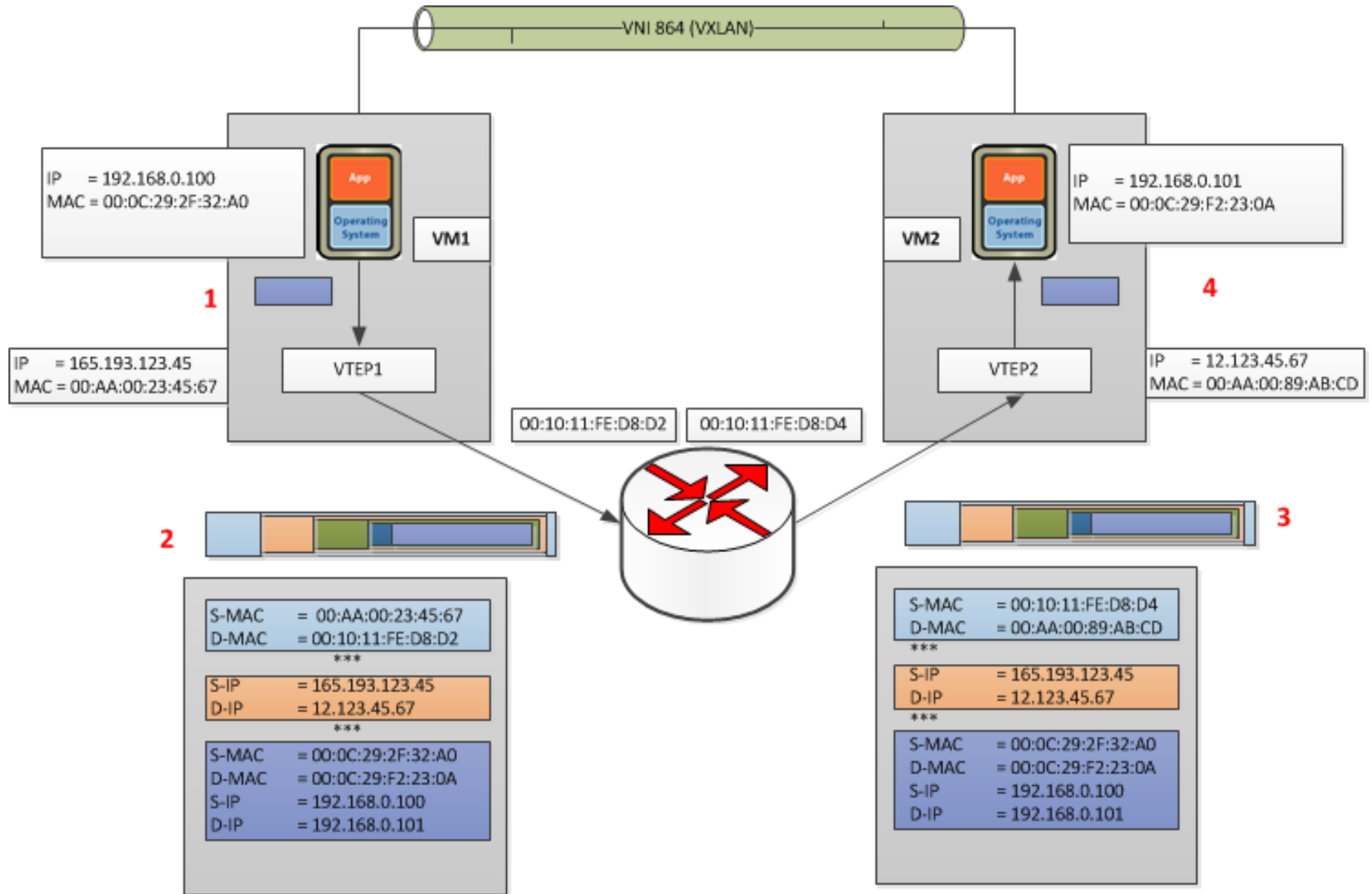
Outer MAC header has source VTEP MAC and next hop MAC as destination

Outer MAC packet can have optional VLAN information if needed

VXLAN – How to Works

- Requires
 - A distributed switch
 - vmk NIC and IP address per switch
 - Multicast addresses
- How it works
 - Multicast address is mapped to a VXLAN segment ID for isolation
 - VM to VM traffic is tunneled over a layer three by a VTEP
 - Node learning done via multicast not broadcast
- Advantages
 - Does not rely on VLAN IDs for isolation
 - Works over any layer three multicast enabled network
 - No “distance” restrictions, managed by multicast radius
- Disadvantages
 - Multicast required end to end

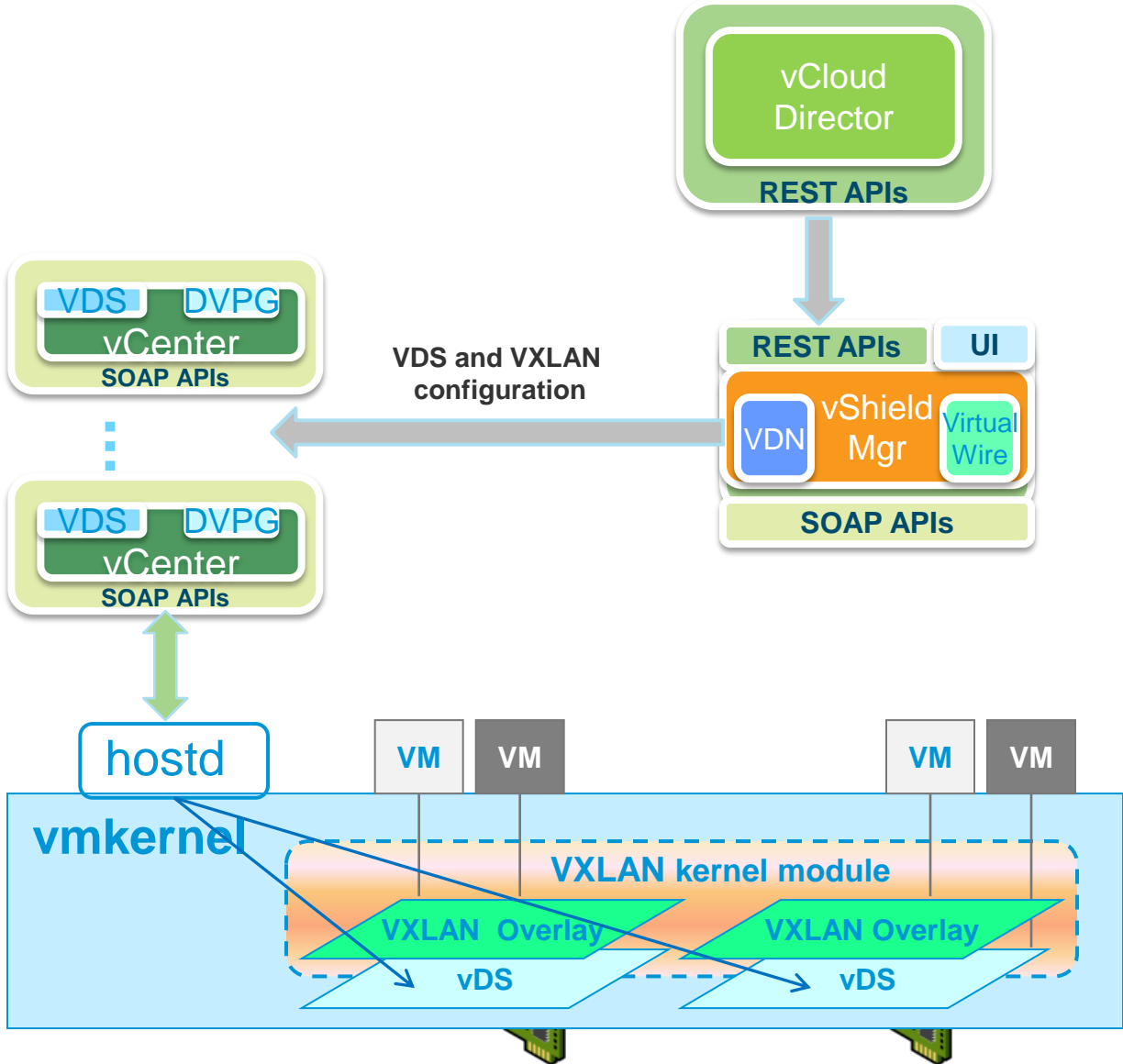
VXLAN: VM to VM communication



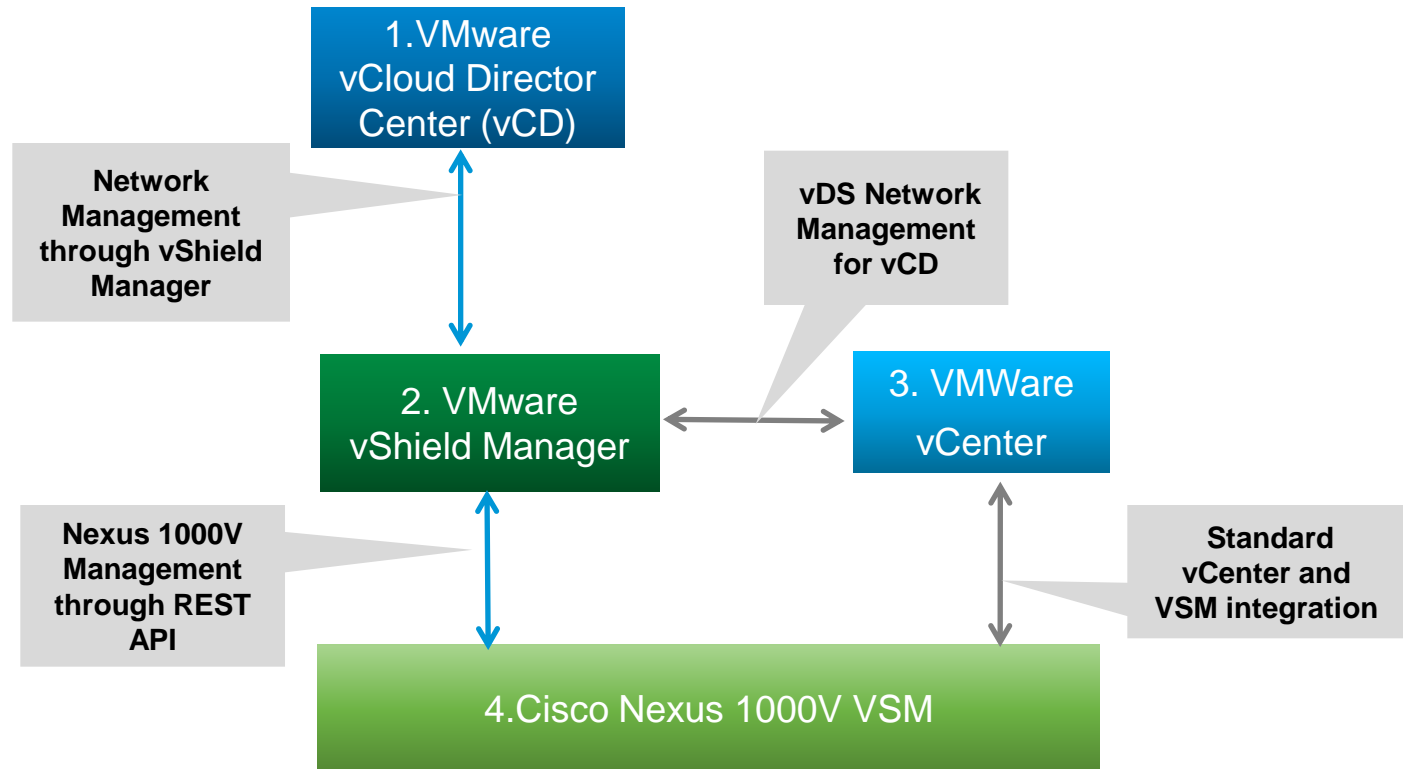
VXLAN Configuration

- Configurations
 - Handled by vShield Manager as part of VXLAN provisioning work flow
 - MTU needs to be increased to 1550 Bytes (minimum 1500 + 50 VXLAN bytes)
 - Leverage vmkernel TCP/IP stack for IGMP
- Turn on 5 tuple hash distribution for uplink LACP
 - Encapsulation will generate a source UDP port based on a hash of inner packet 5-tuple
- Physical Switch Configuration
 - MTU increase to match vDS changes, Jumbo frame O.K.
 - IGMP snooping on physical switches
 - PIM for multicast routing
 - Use Bidirectional Mode (Bidir/SDM) instead of PIM Sparse Mode (PIM-SM)

End-to-End Architecture



Nexus 1000V vCloud Director Integration



VXLAN in vCloud Director 1.5 today

Create Network Pool Wizard

Network Pool Type

A network pool is a collection of virtual machine networks that are available to be consumed by vDCs to create vApp networks and by organizations to create organization networks. Network traffic on each network in a pool is isolated at layer 2 from all other networks.

Select a network pool type from the list below:

- VLAN-backed**
Create a network pool backed by a range of VLAN IDs. The VLANs must be pre-provisioned.
- Network isolation-backed**
Create a network pool backed by Cloud isolated networks. A Cloud isolated network spans hosts and provides traffic isolation from other hosts. The system provisions Cloud isolated networks automatically.
- vSphere port group-backed**
Create a network pool backed by a vSphere port group. The port group must be pre-provisioned.

Network Pool Type
Configure VLAN-backed Pool
Name this Network Pool
Ready to Complete

Create Network Pool Wizard

Configure Isolation-backed Pool

Enter the settings for the new network pool below:

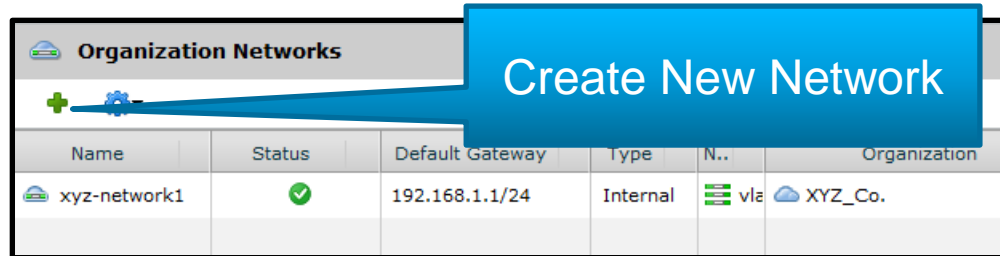
Number of VCD isolated networks:
 *

VLAN ID:

Select vNetwork Distributed Switch

Network Pool Type
Configure Isolation-backed Pool
Name this Network Pool
Ready to Complete

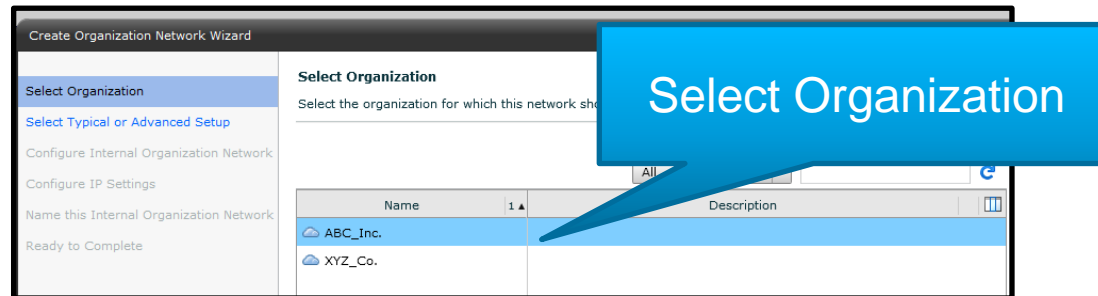
vCloud Tenant Network Creation (1/2)



Organization Networks

Create New Network

Name	Status	Default Gateway	Type	N..	Organization
xyz-network1	✓	192.168.1.1/24	Internal	vla	XYZ_Co.



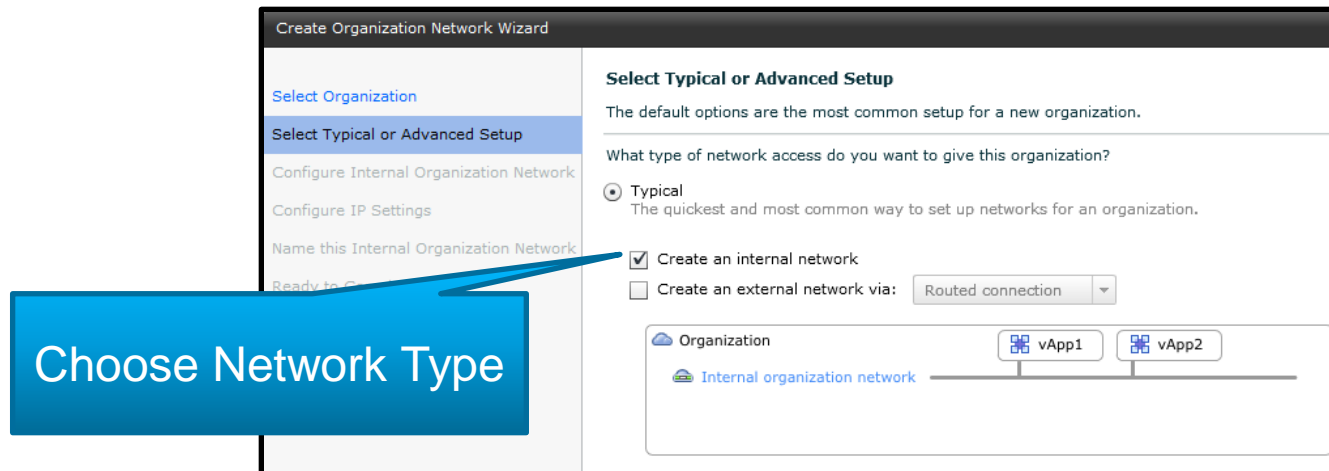
Create Organization Network Wizard

Select Organization

Select the organization for which this network should be created.

Name	Description
ABC_Inc.	
XYZ_Co.	

Select Organization



Create Organization Network Wizard

Select Typical or Advanced Setup

The default options are the most common setup for a new organization.

What type of network access do you want to give this organization?

Typical
The quickest and most common way to set up networks for an organization.

Create an internal network

Create an external network via: Routed connection

Organization: vApp1, vApp2

Internal organization network

Choose Network Type

vCloud Tenant Network Creation (2/2)

Create Organization Network Wizard

Select Organization
Select Typical or Advanced Setup
Configure Internal Organization Network
Configure IP Settings
Name this Internal Organization Network
Ready to Complete

Configure Internal Organization Network

Select the network pool that allocates the internal network.

If you don't see the network pool you need:
[create a new network pool](#)

Only use networks that are accessible by this organization

Select Network Pool

Name	vCenter	Type	Network (Used/T...
segmentation	VC1	Cloud Network Isolation	0 / 500 0%
vlan	VC1	VLAN	1 / 101 1%

Choose Network Pool

Create Organization Network Wizard

Select Organization
Select Typical or Advanced Setup
Configure Internal Organization Network
Configure IP Settings
Name this Internal Organization Network
Ready to Complete

Configure IP Settings

Enter the network settings of the new organization network below:

Network mask: *

Default gateway: *

Primary DNS:

Secondary DNS:

DNS suffix:

Set Network Details

Configuration: Integrating N1KV and vShield Manager

1. Turn on Network Segmentation Manager feature on N1KV

```
N1KV(config)# feature feature network-segmentation-manager
```

2. Add N1KV in vShield Manager as a Managed switch with VXLAN and Multicast address pool range

Add Switch Provider

Provide the base URL to the provider's service API and credentials to login.

Name: * Nexus1KV-NSM-1

Service API base URL: * https://172.25.180.128/n1k/services/NSM

Username: * admin

Password: * *****

Provide a segmentID pool and multicast range unique to this vShield manager.

Segment ID pool: * 4400-4410

Multicast addresses: * 225.0.0.1-225.0.0.2

Ok Cancel

Cisco Nexus 1000V VXLAN Benefits

- Extends physical server/network operational model into the cloud
- Troubleshooting within a VXLAN
 - Port statistics
- Quality of Service
 - IEEE 802.1p
 - Differentiated Service Code Point Marking (DSCP)
 - Rate Limiting
 - Class Based Weighted Fair Queuing
- Security
 - Port Security
 - Access Control List
- Network Customization
 - Tenant-specific network policy including DSCP for VXLAN
- XML API for Customization & Integration
- Supports vSphere 4.1 or 5.0



FAQ



Are VXLANs secure ?

- With proper precautions they can be just as secure as regular networks. It is true however, that there is a greater risk of attacks and users must understand this and take measures to guard against it. In the worst case, an attacker can inject himself into a VXLAN by sending IP-encapsulated packets from anywhere. Of course this requires access to the IP network. A first line of defense is to have a perimeter firewall that denies IP traffic with the VXLAN encapsulation from the outside.
- This does not prevent attacks from the inside. For that users would need to control access at internal routers to ensure that only authorized tunnel endpoints can inject packets into VXLAN tunnels. This can be done statically (knowing the physical topology of the network) or by employing additional IP security mechanisms that guarantee encryption and/or authentication.
- Rather than re-invent this particular wheel, the VXLAN draft lets users make use of existing methods to secure VXLAN tunneled traffic, while pointing out where the risks lie.

VXLAN encapsulation will also take some CPU cycles (thus impacting your VM performance)

- While VXLAN encapsulation will not impact VM performance per se, it will eat CPU cycles that could be used by VMs. If your hypervisor host has spare CPU cycles, VXLAN overhead shouldn't matter, if you're pushing it to the limits, you might experience performance impact.
- However, the elephant in the room is the TCP offload. It can drastically improve I/O performance (and reduce CPU overhead) of network-intensive VMs. The moment you start using VXLAN, TCP offload is gone (most physical NICs can't insert the VXLAN header during TCP fragmentation), and the overhead of the TCP stack increases dramatically.
- If your VMs are CPU-bound you might not notice; if they generate lots of user-facing data, lack of TCP offload might be a killer.

But VXLAN has its limitations – for example, only VXLAN-enabled VMs will be able to speak to each other

- Almost correct. VMs are not aware of VXLAN (they are thus not VXLAN-enabled). From VM NIC perspective the VM is connected to an Ethernet segment, which could be (within the vSwitch) implemented with VLANs, VXLAN, vCDNI, NVGRE, STT or something else.
- At the moment, the only implemented VXLAN termination point is Nexus 1000V, which means that only VMs residing within ESX hosts with Nexus 1000V can communicate over VXLAN-implemented Ethernet segments.

vSphere Multicast Support

- There is a good white paper on the topic on the VMware site called Multicast Performance on vSphere 5.0 that deals with performance changes that have been made to enhance multicast support in vSphere 5.
- The recurring question I get is how multicast is handled in vSphere. The short answer is the vSwitch does not play a role in the IGMP join and leave messages that the VMs send in order to start and stop receiving multicast groups respectively.
- When a VM is vMotioned, its vNIC configuration goes with it. The destination hosts sees this vNIC configuration and updates its forwarding tables to forward the necessary multicast traffic it receives to the VM. To prevent any transient multicast packet loss after a vMotion, the vSwitch also injects an IGMP query into the VM, using its unicast MAC address, so that multicast receiver presence is known to the pSwitches immediately. This avoids the VM missing multicast traffic by having to wait for next IGMP query to come from a IGMP querier on the network.

What about network services ?

- Since VXLANs are expected to be deployed in hosted environments people naturally want to know how to enable network services (firewalls, IPS, load balancing, WAN optimization) for VXLANs. The answer to this is pretty much the same as for routers. Either the services need to be enabled in endpoints that can be attached to VXLANs (i.e. virtual in the immediate future), or these services need to become VXLAN aware or someone needs to perform a bridging function between VXLANs and whatever it is that the services understand (physical interfaces, VLANs etc.)

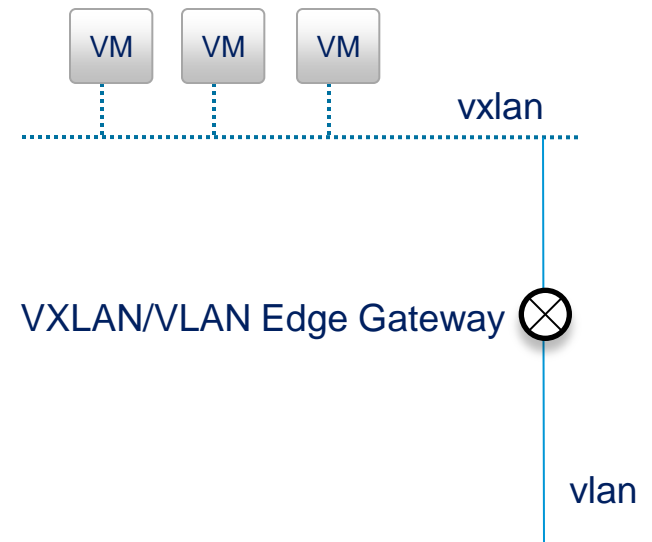
Communication Outside VXLAN

- VXLAN-to-VLAN L2 Edge Gateway with physical network services on VLAN

vShield Edge

ASA 1000V (June 2012)

Hardware based edge gateway (TBD)



MAC-in-GRE

- Why did VXLANs use a MAC-in-UDP encapsulation instead of MAC-in-GRE? The easy answer is to say, for the same reasons OTV and LISP use UDP instead of GRE. The reality of the world is that the vast majority (if not all) switches and routers do not parse deeply into GRE packets for applying policies related to load distribution (Port Channel and ECMP load spreading) and security (ACLs).

MAC-in-MAC

- Cisco and VMware, along with others in the hypervisor and networking industry have worked together on a common industry standard to replace vCDNI -- namely VXLAN. VXLAN has been designed to overcome the shortcomings of the vCDNI MAC-in-MAC encapsulation -- namely load distribution, and limited span of a layer 2 segment.
- VMware has not communicated anything to this regard, although the future of this technological direction is VXLAN.

So now we can migrate VMs across subnets ?

- We want to make clear that VMs connected to VXLANs do not need to change their own IP addresses as a consequence of this technology. Essentially, VMs connected to a VXLAN remain unaware that they are on a VXLAN -- just as they are usually unaware of running on VLANs. It is up to the underlying network to ensure connectivity between such VMs and provide layer-2 semantics such as mac-layer broadcast and unicast traffic. As a consequence, any mobility event -- live or otherwise -- has no effect on the internals of the VM.

What about routing across VXLANs ?

- The answer to this will evolve over time just as it did with VLAN technology. If a router is ignorant of 802.1Q tagging it cannot route across VLANs unless someone else terminates VLAN tagging on its behalf. For instance an 802.1Q-capable L2 switch can strip the tag and forward native Ethernet frames to/from the router. The router would then only support one “VLAN interface” on each physical interface.

I personally see VXLAN as a end to end solution where we can't interact on the network infrastructure anymore. For example, how would these VMs be able to connect to the first-hop gateway?

- Today you can use VXLAN to implement “closed” virtual segments that can interact with the outside world only through VMs with multiple NICs (a VXLAN-backed NIC and a VLAN-backed NIC), which makes it perfect for environments where firewalls and load balancers are implemented with VMs (example: VMware’s vCloud with vShield Edge and vShield App). As said above, VXLAN termination points might appear in physical switches.

Resources



Whitepapers, Deployment Guides, other

- [Deploying the VXLAN Feature in Cisco Nexus 1000V Series Switches](#) **New**
- [Solution Brief: VMware vCloud Director and Cisco Nexus 1000V](#)
- [Cisco Nexus 1000V Integration with VMware vCloud Director](#)
- [Cisco Nexus 1000V Series Switches Deployment Guide Version 3](#) **New**
- [Scalable Cloud Networking with Cisco Nexus 1000V Series Switches and VXLAN](#)
- [Virtual Networking Features of VMware vSphere Distributed Switch and Cisco Nexus 1000V Series Switches](#)
- vCD with VXLAN & Nexus 1000V forthcoming with Nexus 1000V Release 4.2(1)SV1(5.1a)

Reference Solutions

Solution	Nexus 1000V	Nexus 1010	Virtual Security Gateway	Virtual WAAS	NAM (N1010)
Vblock	✓		✓	✓	
FlexPOD	✓	✓			
Virtual Desktop	✓	Implicit Support	✓	✓ *	Implicit Support
Virtual Multi-tenant DC (VMDC)	✓	Implicit support	✓	In Planning	Implicit support
DC-to-DC vMotion	✓	Implicit support	✓	✓	Implicit support
PCI 2.0	✓	Implicit support	✓		Implicit support
Hosted Collaboration	✓	Implicit support			Implicit support

CCO Links

Software, Documentation & Screencasts

Product	CCO Links
Nexus 1000V (v1.5.1) www.cisco.com/go/1000v	<ul style="list-style-type: none">• SW Download• Documentation• Screencasts
Nexus 1010 & 1010-X (v1.4) www.cisco.com/go/1010	<ul style="list-style-type: none">• SW Download• Documentation
Virtual Security Gateway (v 1.3.1) www.cisco.com/go/vsg	<ul style="list-style-type: none">• SW Download• Documentation• Screencasts
Virtual Network Management Center (v1.3.1a) www.cisco.com/go/vnmc	<ul style="list-style-type: none">• SW Download• Documentation• Screencasts
Data Center Network Manager [v5.2(2a)] www.cisco.com/go/dcnm	<ul style="list-style-type: none">• SW Download• Documentation

Reference Solutions

With Nexus 1000V, Nexus 1010, VSG & vWAAS

- [Vblock with Nexus 1000V](#)
- [Vblock with VSG and vWAAS](#)
- [FlexPOD with Nexus 1000V and Nexus 1010](#)
- [Virtual Multi-tenant Data Center with Nexus 1000V](#)
- Virtual Desktop
 - [1000V and VMware View](#)
 - [1000V and Citrix XenDesktop](#)
 - [1000V and VSG in VXI Reference Architecture](#)
- Virtual Workload Mobility (aka DC-to-DC vMotion)
 - [Cisco, VMware and EMC \(with 1000V and VSG\)](#)
 - [Cisco, VMware and NetApp \(with 1000V and VSG\)](#)
- [PCI 2.0 with Nexus 1000V and VSG](#)

N1K Public Webcasts, Fall 2011

Date	Technical Track Topics	Webinar	Prezo
7/27	Long Distance vMotion with Nexus 1000V and VSG	Play	PDF
8/10	PCI Reference Architecture with Nexus 1000V and Virtual Security Gateway	Play	PDF
10/05	Nexus 1000V, VXLAN, and vCloud Director	Play	PDF
10/12	Virtualized Multi-Tenant Data Center (VMDC)	Play	PDF
10/19	Nexus 1010 v1.3 - What's New?	Play	PDF
10/26	Virtualized Workload Mobility - Latest Design Guidance	Play	PDF
11/02	UCS and Nexus 1000V - Best Practices	Play	PDF
11/09	Virtual Security Gateway (VSG) v1.2 - what's new? v1.3 - what's coming?	Play	PDF

Webinar Link: www.cisco.com/go/1000vcommunity

N1K Public Webcasts – Spring 2011

Date	Business Track Topics	Webinar	Preso	Q&A
3/22	Nexus 1000V/1010 Overview and Update	Play	PDF	PDF
4/05	Virtual Network Services: Virtual Service Datapath (vPath), Network Analysis Module (NAM), Virtual Application Acceleration (vWAAS)	Play	PDF	PDF
4/19	Virtual Security Gateway (VSG) Overview (Installation Videos: Link)	Play	PDF	PDF
5/03	Journey to the Cloud w/ N1KV: vCloud Director & Long Distance vMotion	Play	PDF	PDF
5/17	Secure Virtual Desktop with Nexus 1000V & VSG	Play	PDF	PDF

Date	Technical Track Topics	Webinar	Preso	Q&A
3/29	Nexus 1000V v1.4 Features & Install Overview (Installation Screencasts Link)	Play	PDF	PDF
4/12	Nexus 1010 Overview & Best Practices	Play	PDF	PDF
4/26	Virtual Security Gateway (VSG) Technical Overview	Play	PDF	PDF
5/10	Nexus 1000V Key Features Overview	Play	PDF	PDF
5/24	Nexus 1000V Troubleshooting	Play	PDF	PDF

Webinar Link: www.cisco.com/go/1000vcommunity

N1K Public Resources

- CCO Links

1000V: www.cisco.com/go/1000v

1010: www.cisco.com/go/1010

VSG: www.cisco.com/go/vsg

VNMC: www.cisco.com/go/vnmc

vWAAS: www.cisco.com/go/waas

NAM on 1010: <http://www.cisco.com/en/US/products/ps10846/index.html> (or www.cisco.com/go/nam)

- Deployment Guides

[Nexus 1000V Deployment Guide](#)

[Nexus 1000V on UCS – Best Practices](#)

[Nexus 1010 Deployment Guide](#)

[VSG Deployment Guide](#)

- White papers:

[Nexus 1000V and vCloud Director](#)

[N1K on UCS Best Practices](#)

[Nexus 1000V QoS White paper \(draft\)](#)

[VSG and vCloud Director \(draft\)](#)

[vWAAS Technical Overview, vWAAS for Cloud-ready WAN Optimization](#)

- Cheat Sheets

Nexus 1010 Configuration Cheat Sheet v.2.0
<https://communities.cisco.com/docs/DOC-28188>

Nexus 1000V w/ UCS Configuration Cheat Sheet v.1.1
<https://communities.cisco.com/docs/DOC-28187>

More on the way....

Cisco Cloud Lab

Hands On Training & Demos

- Hands on labs available for Nexus 1000V and VSG in Cloud Lab
- <https://cloudlab.cisco.com>
- Open to all Cisco employees
 - Customers/Partners require sponsorship from account team for access via CCO LoginID
 - Extended duration lab licenses for 1000V and VSG are available upon request



Welcome to Cisco CloudLab

Please select one of the available labs, by clicking on its name. Hover over the lab name content.

Available labs:

- Cisco Nexus 1000V - Basic Introduction (N1K-000111)
- Cisco Nexus 1000V - Installation (N1K-000211)
- Cisco Nexus 1000V - Upgrade to 1.4 (N1K-000310)
- Cisco Virtual Security Gateway (VSG) - Introduction (VSG-000110)
- Cisco Nexus 7000 - Introduction to NX-OS (N7K-000110)
- Cisco Overlay Transport Virtualization (OTV) (N7K-000210)
- Demo: Cisco Nexus 1000V (Pre-Configured) (N1K-100111)
- Demo: Cisco Virtual Security Gateway (VSG)(Pre-Configured) (VSG-100110)

VXLAN Basic Introduction too

Additional N1K Public Links

- N1K Download and 60-day Eval: www.cisco.com/go/1000vdownload
- N1K Product Page: www.cisco.com/go/1000v
- N1K Community: www.cisco.com/go/1000vcommunity
- N1K Twitter www.twitter.com/official_1000V
- N1K Webinars: www.cisco.com/go/1000vcommunity
- N1K Case Studies: www.tinyurl.com/n1k-casestudy
- N1K Whitepapers www.tinyurl.com/n1k-whitepaper
- N1K Deployment Guide: www.tinyurl.com/N1k-Deploy-Guide
- VXI Reference Implementation: www.tinyurl.com/vxiconfigguide
- N1K on UCS Best Practices: www.tinyurl.com/N1k-On-UCS-Deploy-Guide

Thank you.

