
TOMORROW
starts here.
CISCO
Cisco live!

Multi-Hypervisor Networking - Compare and Contrast

BRKVIR-2044

Alejandra Sanchez Garcia

Customer Support Engineer, CCIE DC

#clmel

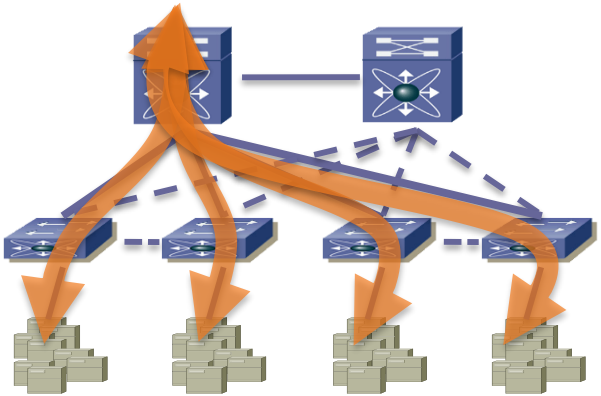
Cisco live!

Agenda

- Evolution of the Workloads in the Data Centre
- Achieving Virtualisation in Multiple Hypervisor Options
- Various Hypervisor Networking Options at the Host
- Normalising the Complexity of Multi-Hypervisor Networking
- Summary / Q&A

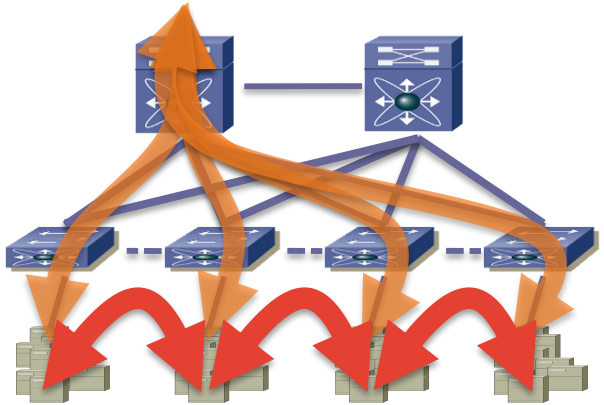
Changing Traffic Patterns:

Siloed Data Centre



Tenant Elasticity

Dynamic Data Centre



- Mostly North-South traffic flows
- Over-subscription acceptable for client-server type of applications
- Poor link utilisation. Spanning Tree blocks ports

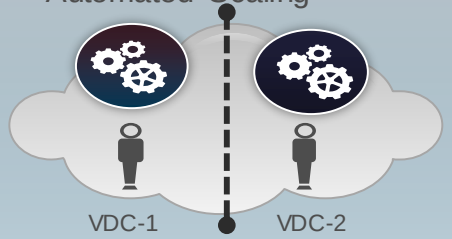
- Mix of North-South and East-West traffic flows
- Virtualisation increases L2 Domains
- Spanning Tree blocking affects scalability

Cisco live!

Physical → Virtual → Cloud Journey

Consistency reduces operational risk and complexity

PHYSICAL WORKLOAD	VIRTUAL WORKLOAD	CLOUD WORKLOAD
• One app per Server • Static • Manual provisioning	• Many apps per Server • Mobile • Dynamic provisioning	• Multi-tenant per Server • Elastic • Automated Scaling



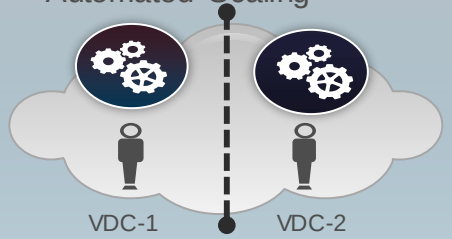
CONSISTENCY: Policy, Features, Security, Management, Separation of Duties

Switching	**Nexus 7K/5K/3K/2K**	**Nexus 1000V, VM-FEX**
Routing	**ASR, ISR**	**Cloud Services Router (CSR 1000V)**
Services	**WAAS, ASA, NAM**	**vWAAS, VSG, ASA 1000V, vNAM, NS 1000V**

Physical → Virtual → Cloud Journey

Consistency reduces operational risk and complexity

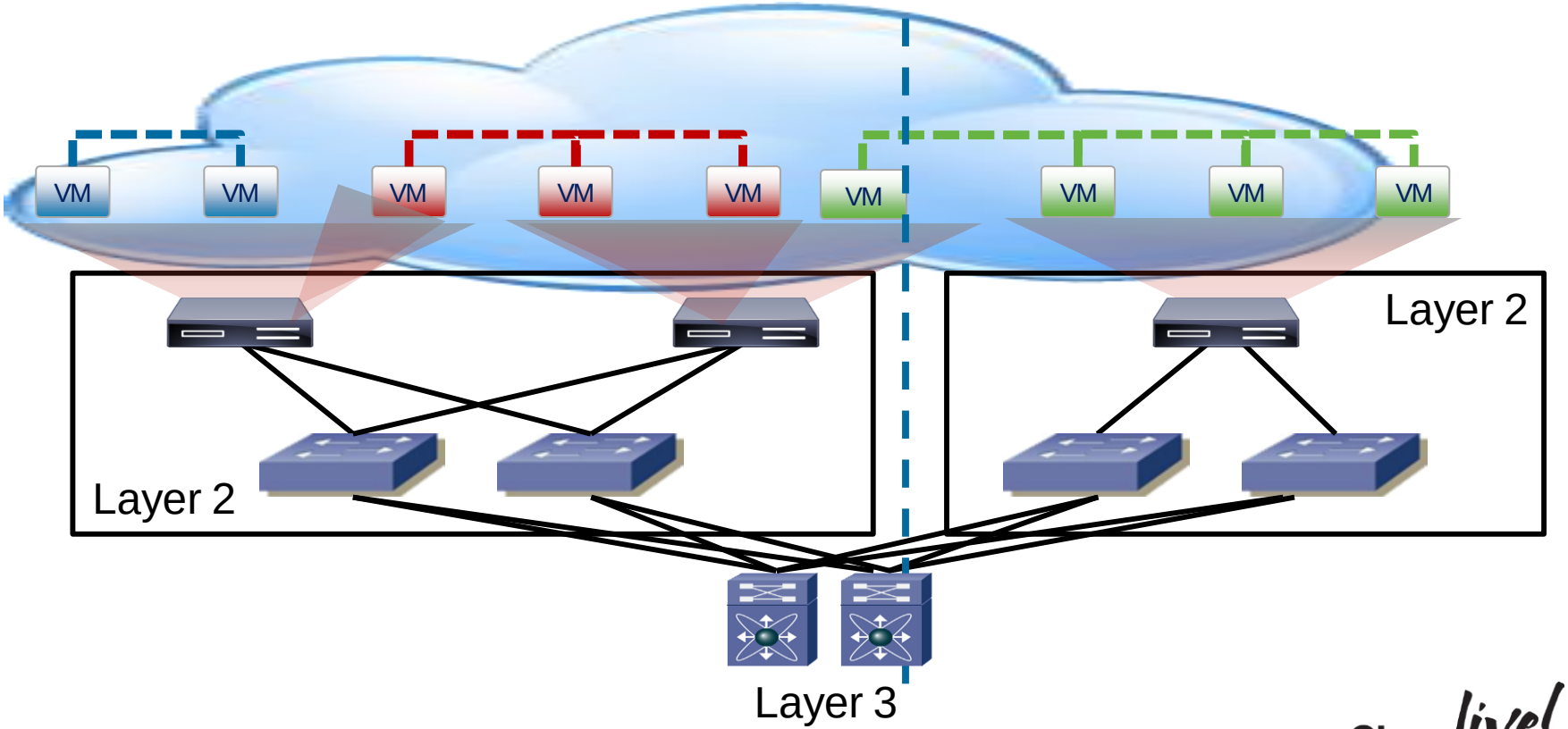
PHYSICAL WORKLOAD	VIRTUAL WORKLOAD	CLOUD WORKLOAD
• One app per Server • Static • Manual provisioning	HYPERVISOR Hyper-V vSphere OpenStack(KVM)	• Multi-tenant per Server • Elastic • Automated Scaling



CONSISTENCY: Policy, Features, Security, Management, Separation of Duties

Switching	Nexus 7K/5K/3K/2K	Nexus 1000V, VM-FEX
Routing	ASR, ISR	Cloud Services Router (CSR 1000V)
Services	WAAS, ASA, NAM	vWAAS, VSG, ASA 1000V, vNAM, NS 1000V

Virtual Workload on Physical Data Centre

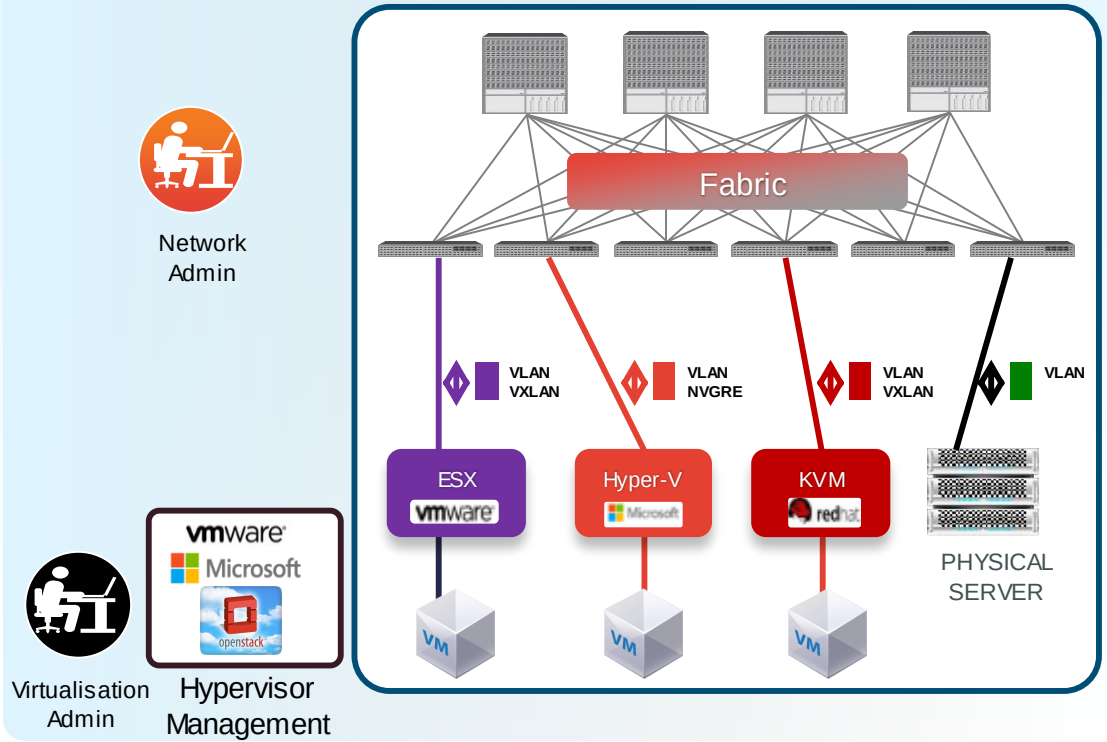


Agenda

- Evolution of the Workloads in the Data Centre
- Achieving Virtualisation in Multiple Hypervisor Options
- Various Hypervisor Networking Options at the Host
- Normalising the Complexity of Multi-Hypervisor Networking
- Summary / Q&A

Multi-Hypervisor Encapsulations

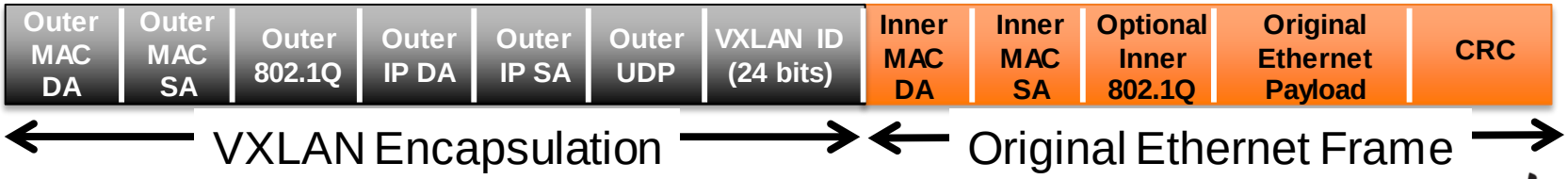
- Encapsulations:
  - VLAN for Bare-Metal
  - VLAN/VXLAN for ESXi
  - VLAN/VXLAN for KVM
  - VLAN/NVGRE for Hyper-V



Virtual Extensible Local Area Network (VXLAN)

- Ethernet in IP overlay network
  - Entire L2 frame encapsulated in UDP
  - 50 bytes of overhead
- Include 24 bit VXLAN Identifier
  - 16 M logical networks
  - Mapped into local bridge domains
- VXLAN can cross Layer 3

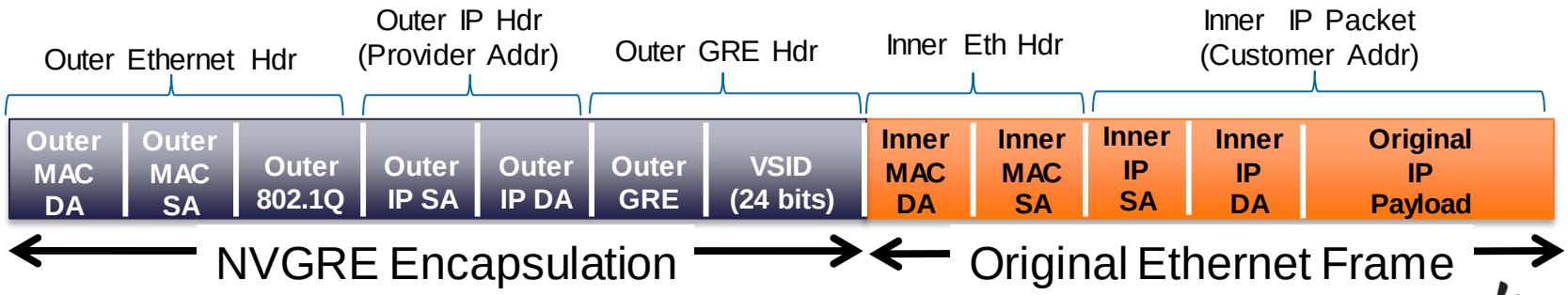
- Tunnel between VEMs
  - VMs do NOT see VXLAN ID
- IP multicast used for L2 broadcast/multicast, unknown unicast
- Technology submitted to IETF for standardisation
  - With VMware, Citrix, Red Hat and Others



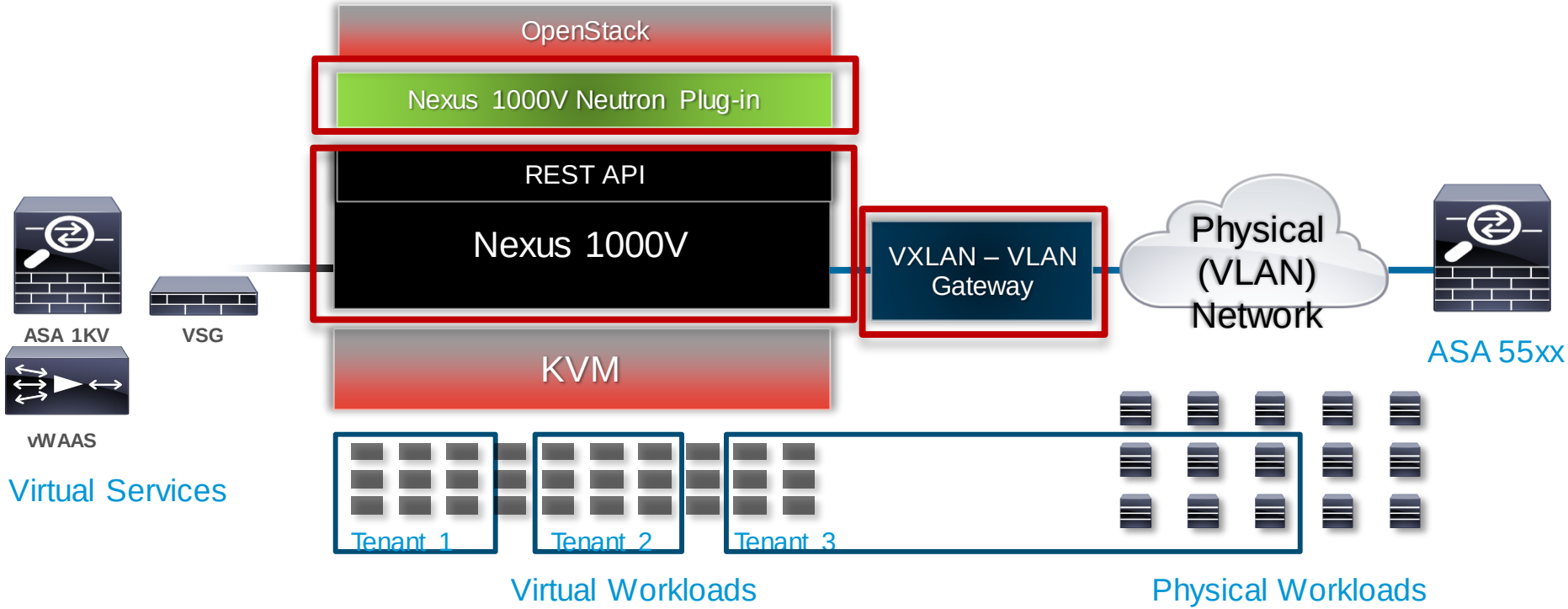
Network Virtualisation over GRE (NVGRE)

- MAC over GRE Tunnelling
  - Entire L2 frame encapsulated in GRE
  - 50 bytes of overhead
- Include 24 bit VSID Identifier
  - 16 M logical networks
- NVGRE can cross Layer 3

- GRE Tunnel between endpoints
  - VMs do NOT see VSID
- Technology submitted to IETF for standardisation
  - With Microsoft, Arista, Intel, Dell, HP, Broadcom and Emulex

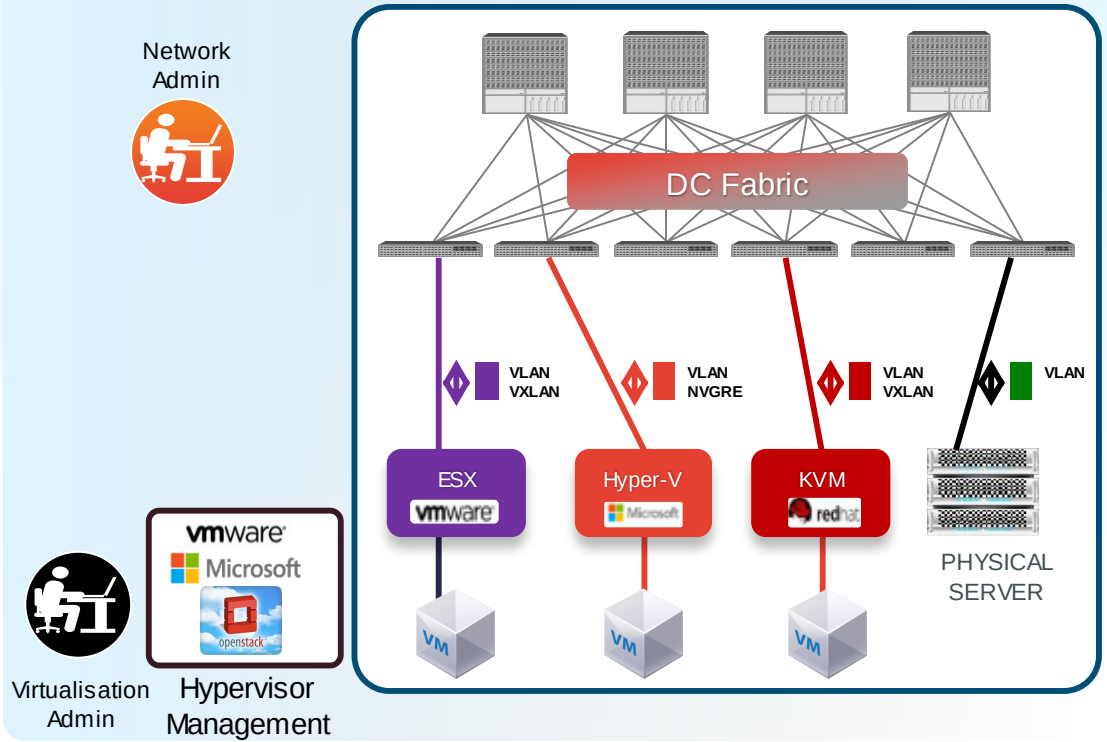


VXLAN Gateway Nexus 1000V with OpenStack



Multi-Hypervisor Managers

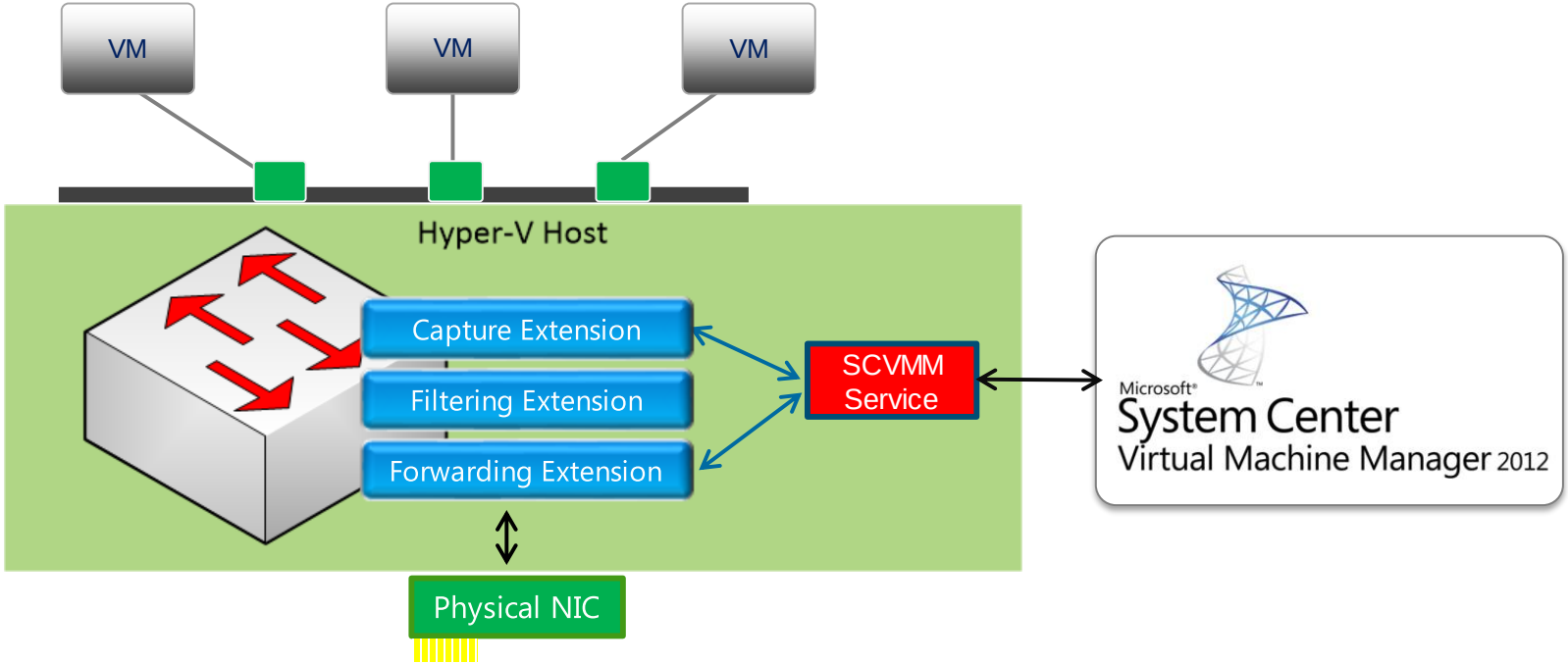
- Each Hypervisor within the Data centre use different points of Management:
  - System Centre Virtual Machine Manager (SCVMM) for Hyper-V
  - vCenter for ESXi
  - Horizon for OpenStack



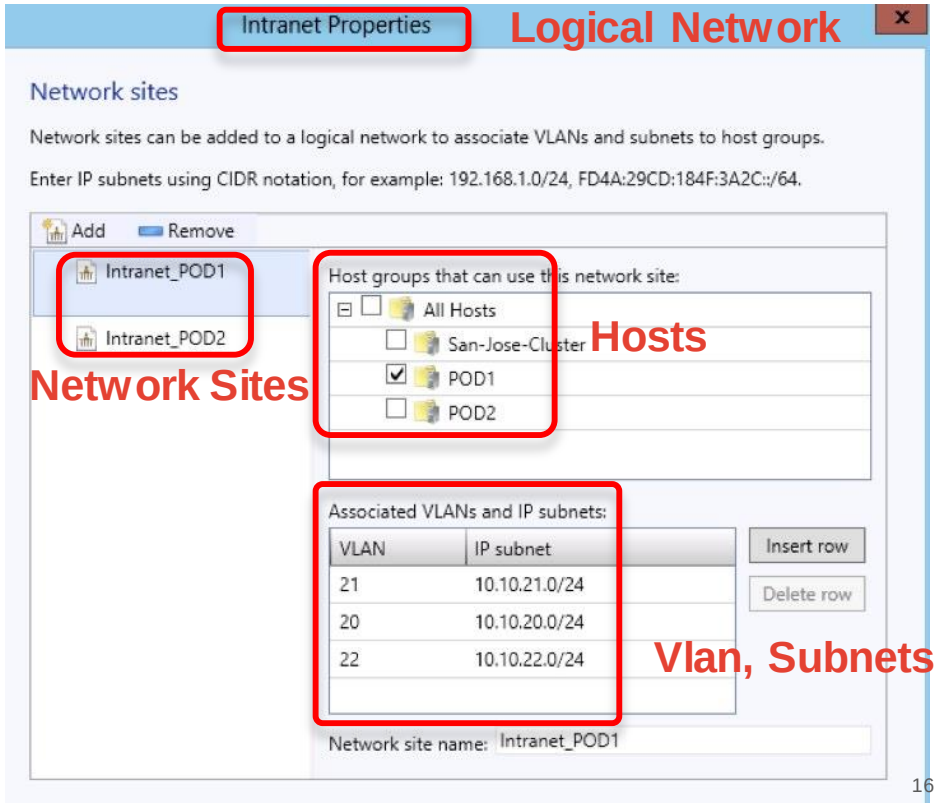
System Centre Virtual Machine Manager

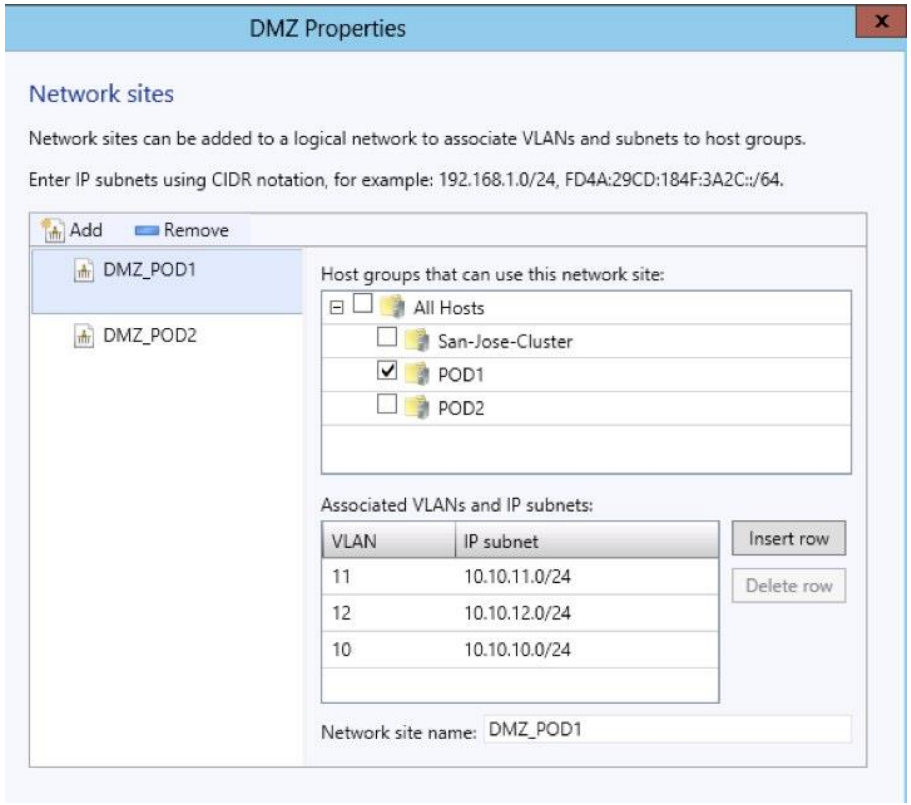
- What SCVMM Manages
  - Hyper-V hosts
  - Virtual Machines
  - Logical Switches
  - Logical Networks and Network Sites
  - VM Networks and Subnets
  - IP Addressing
  - Port Profiles and Classifications

SCVMM Management of Switch Extensions



Hyper-V Networking in SCVMM

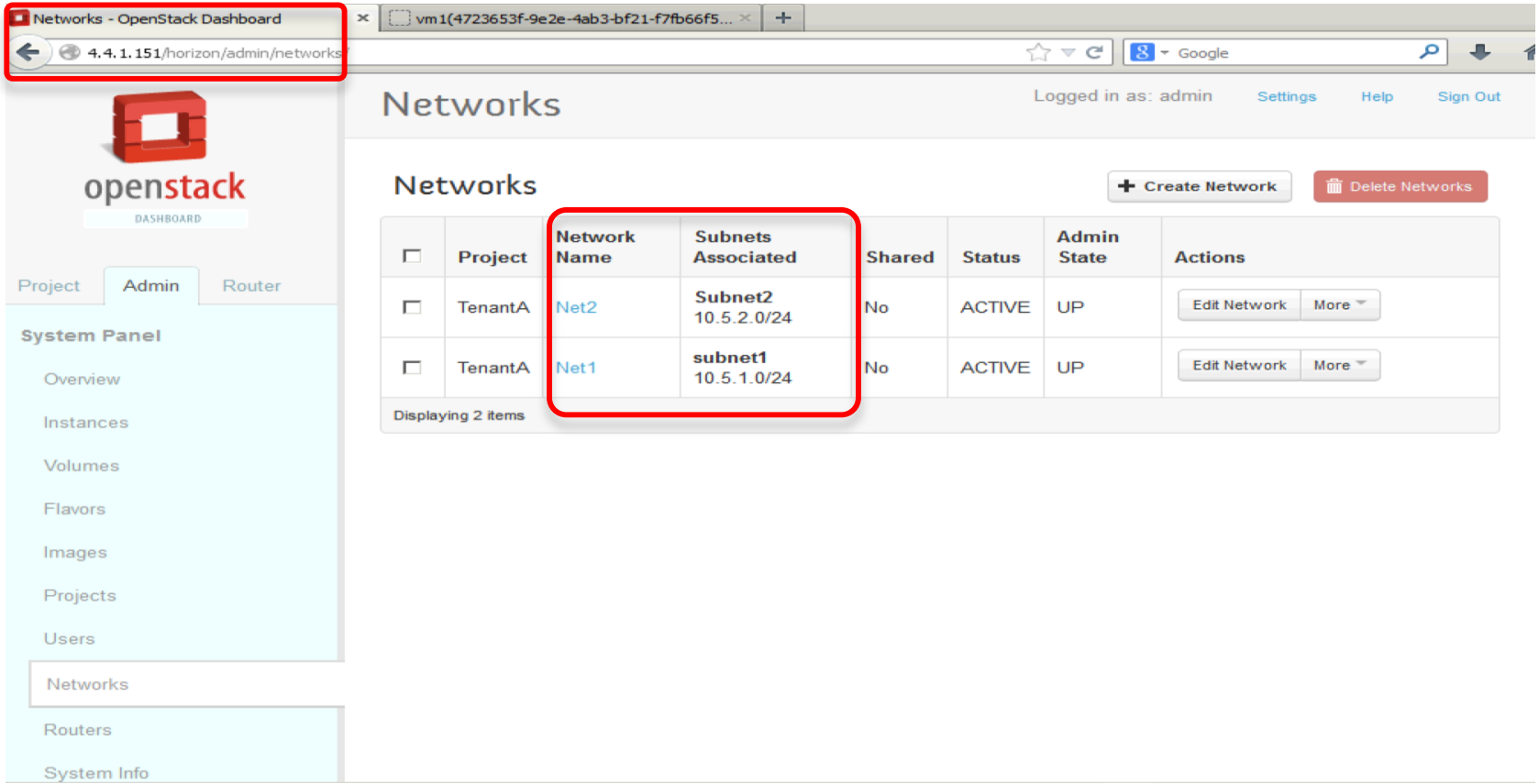




OpenStack Horizon

- Manages OpenStack Virtualisation environment
- Highly customisable based on different plug-in offerings/capabilities
- Easily Integrated based on published API's
- What OpenStack Controller Manages
  - OpenStack hosts
  - Virtual Machines
  - Logical Switches
  - VM Networks and Subnets
  - Virtual Routers
  - IP Addressing
  - Port Profiles and Classifications

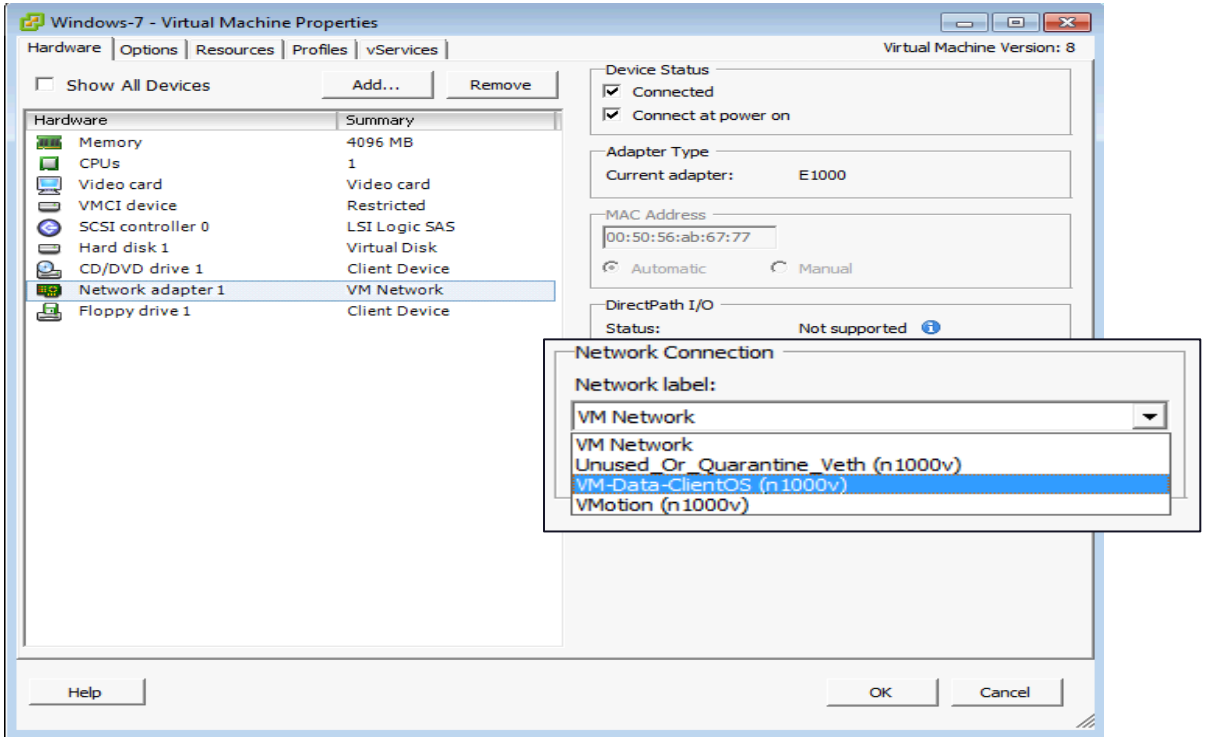
Networking in Horizon



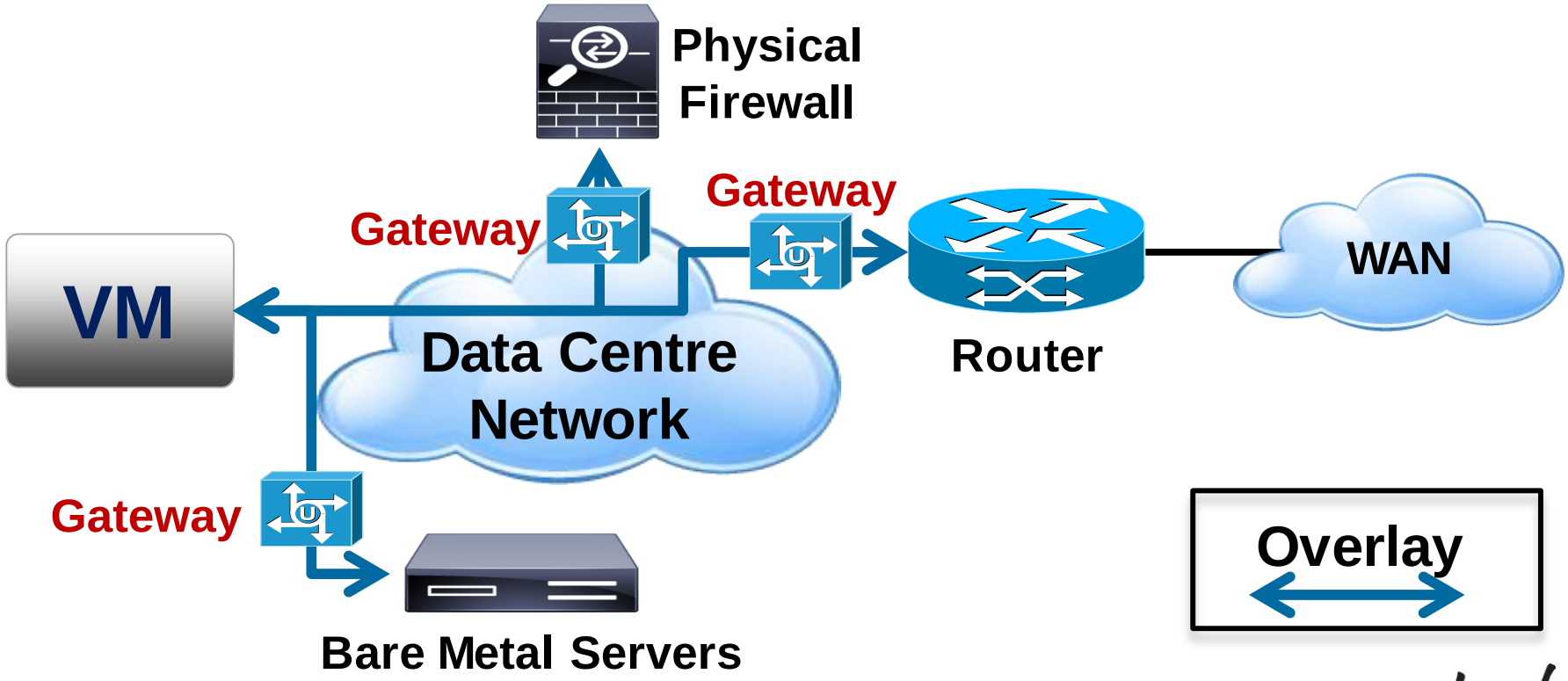
Virtual Centre

- What vCenter Manages
  - ESXi hosts
  - Virtual Machines
  - Standard Switches (Host-based)
  - Distributed Virtual Switch (Multi-Host)
  - VM Networks and Subnets
  - Port Profiles

vCenter Networking for ESXi



Virtual Overlay Network



What Does All This Mean?

- Complexity in Networking
  - Which encapsulations to use for mixed Hypervisor environment?
    - VLAN scalability
    - No VXLAN for Hyper-V or Bare-Metal
    - VXLAN-VLAN Gateways
- Complexity in Management
  - How do I configure networks in Hyper-V, KVM/OpenStack and ESXi?
    - Different tools
    - Different uplinks
    - Who does what?

Hypervisor Technology Comparison

VMware ESX	Microsoft Hyper-V	Openstack
Virtual Distributed Switch (VDS)	Logical Switch	Open vSwitch
Port Group	Virtual Port Profiles + VM networks	Logical Networks (Internal/External)
vmknic	Host VNIC	Virtual Adapter
Folder/Data Centre	Host Group	Tenant
vMotion	Live Migration	Live Migration
Distributed Resource Scheduling (DRS)	Dynamic Optimisation	Nova Scheduler
Distributed Power Mgmt (DPM)	Power Management	Nova Scheduler
vCenter, vCloud Director	SCVMM, SCO	Dashboard Horizon
Site Recovery Manager	Hyper-V Replica	Gluster
Virtual Machine Disk (VMDK)	Virtual Hard Disk (VHDX)	QuickEMUlator Copy on Write (QCOW2) or VMDK

Agenda

- Evolution of the Workloads in the Data Centre
- Achieving Virtualisation in Multiple Hypervisor Options
- Various Hypervisor Networking Options at the Host
  - Hyper-V, KVM/OpenStack, ESXi
- Normalising the Complexity of Multi-Hypervisor Networking
- Summary / Q&A

SCVMM Networking Concepts

- Logical Networks
- Network Sites
- VM Networks
- VM Subnets
- Port Classifications
- IP Pools

Logical Networks and Network Sites

Logical Networks

- Helps model different types of networks in an Enterprise. e.g. Internal, DMZ, Branch etc.
- Provisioned by VMM Admin during initial Fabric Provisioning
- Named Networks hide details from the users of the Network – Server Admin, Tenant Admin, Self Service User.
- Is a group of one or more “Network Sites”

Network Sites

- Is a collection of (IP Subnet, VLAN) pairs.
- Flexibility with usage
  - All IP Subnets in a DC can be in one Site
  - Each Subnet/POD/RACK can be a site

Avatar Corp

The Network team supports two types of Networks –
Internal – for VMs/Hosts behind the DMZ
DMZ – for VMs/Hosts in the DMZ

Madrid

WAN

Barcelona

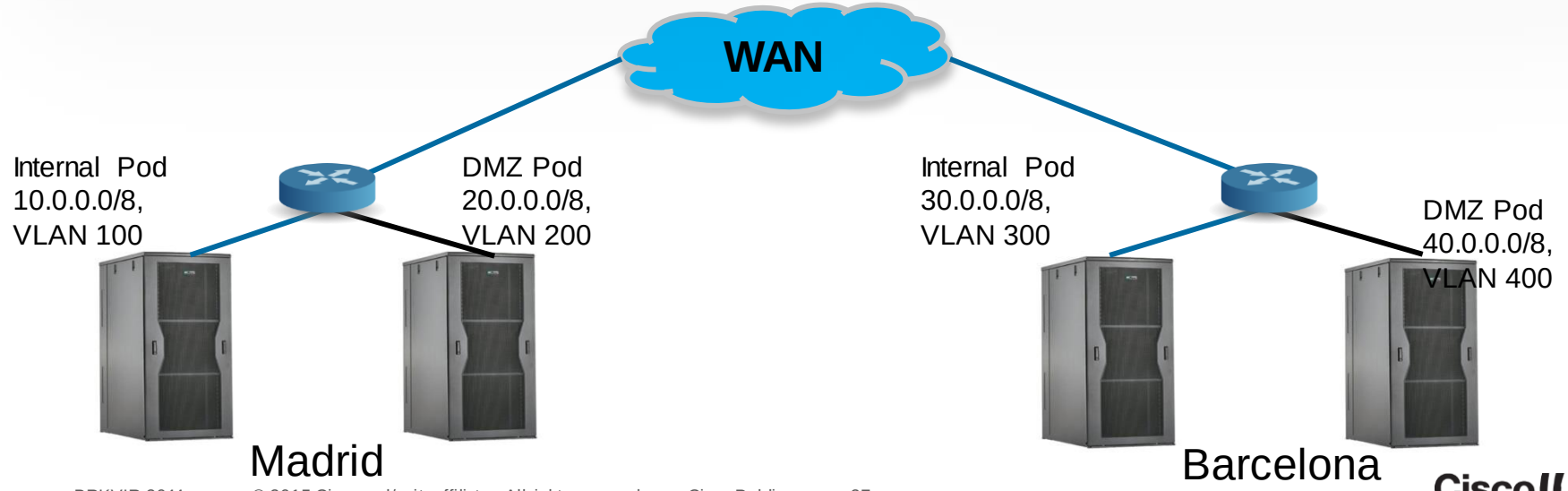
Logical Networks and Network Sites

Logical Network – "Internal"

- Network Site "Internal-Madrid"
  - 10.0.0.0/8, VLAN 100
- Network Site "Internal-Barcelona"
  - 30.0.0.0/8, VLAN 300

Logical Network – "DMZ"

- Network Site "DMZ-Madrid"
  - 20.0.0.0/8, VLAN 200
- Network Site "DMZ-Barcelona"
  - 40.0.0.0/8, VLAN 400



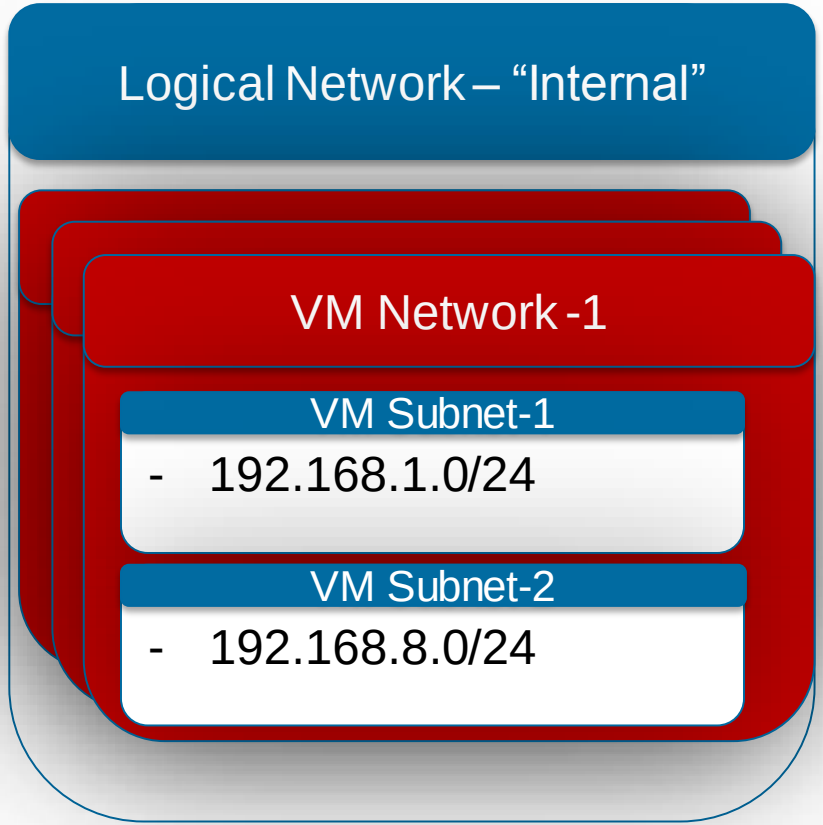
Hyper-V VM Networks and VM Subnets

VM Network

- Defines a Layer 3 domain identified by a Routing Domain ID
- Contains one or more VM Subnets.
- Tenant Admin uses provisioned Logical Networks to define VM Networks.

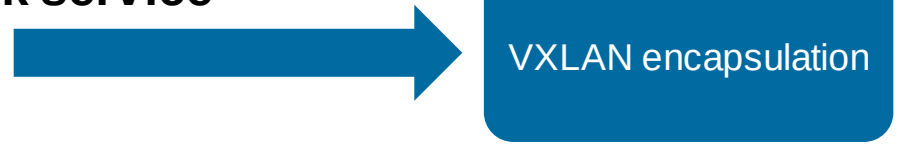
VM Subnet

- Defines a Layer 2 / broadcast domain.
- VMs connect to a VM Subnet in a VM Network in SCVMM
- VM Subnet ID is unique across VM Subnets

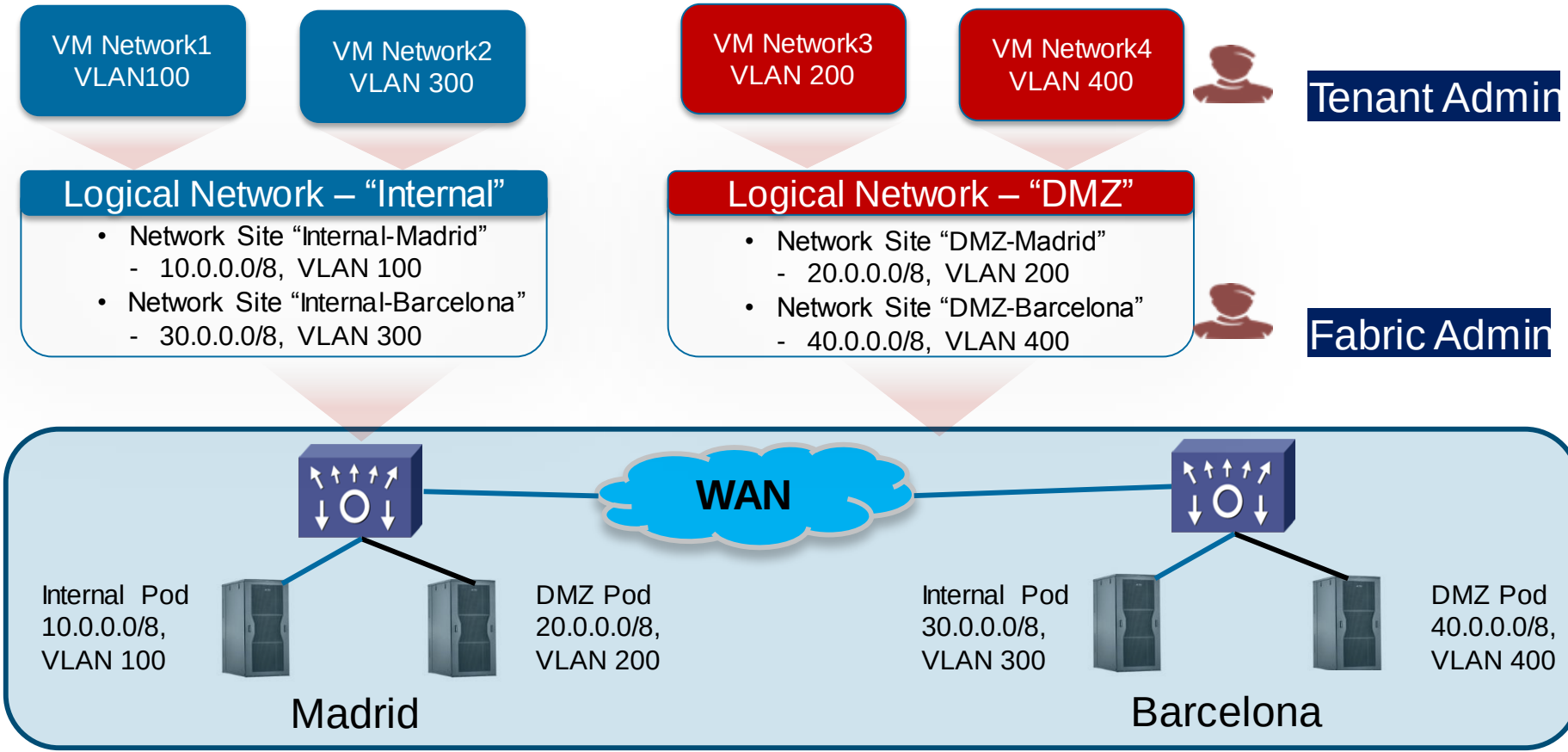


Hyper-V VM Network Options

- **Network virtualisation**
  - NVGRE encapsulation
- **VLAN-based configuration**
  - VM network for each network site and VLAN
- **No isolation**
  - VM network is the same as the logical network
- **External network service**
  - Nexus 1000v

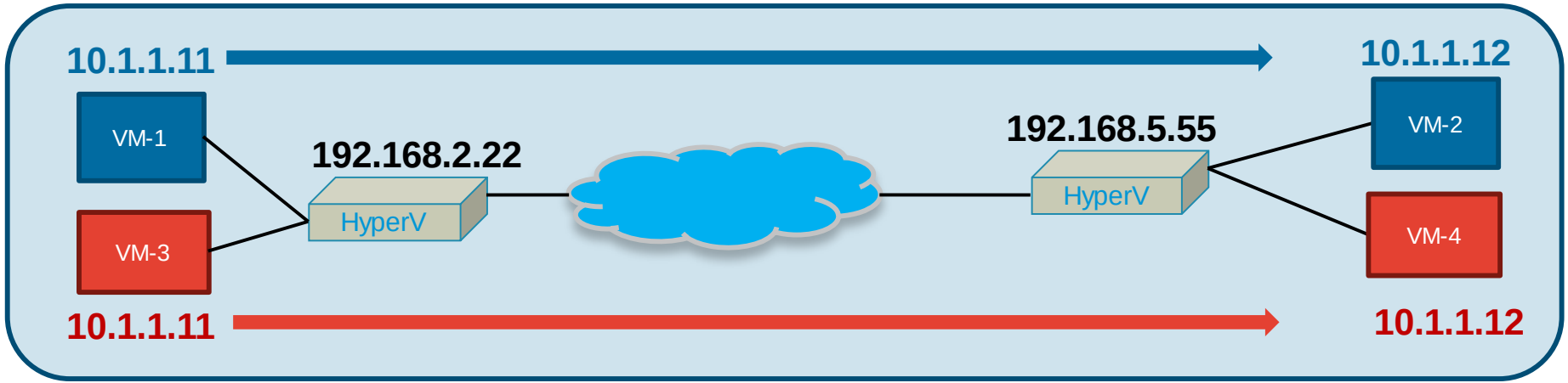


VLAN based VM Networks



NVGRE Based VM Networks

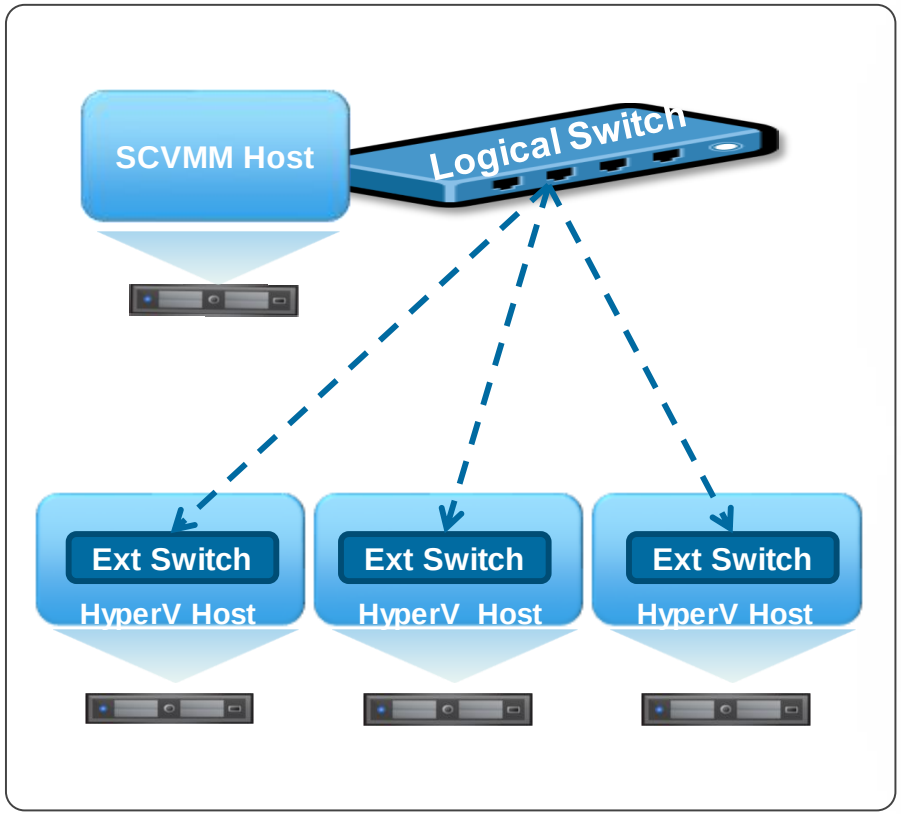
Logical Network – "Internal"



NVGRE Encapsulation ← → Original Ethernet Frame

192.168.2.22->192.168.5.55	GRE Key=5001	10.1.1.11->10.1.1.12
192.168.2.22->192.168.5.55	GRE Key=6001	10.1.1.11->10.1.1.12

SCVMM Logical Switch



Overview

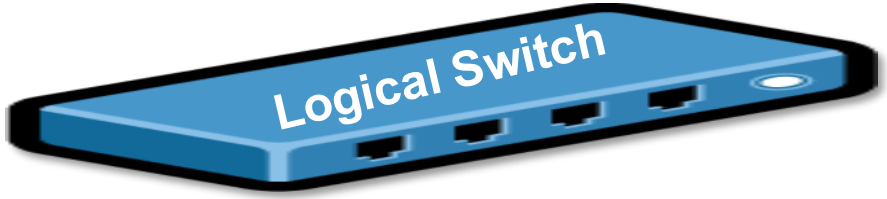
- **Switch Template** created on SCVMM
- Allows VMM Admin to define Network Policy on Virtual Ethernet and Uplink Interfaces
- Allows consistent configuration on all HyperV Hosts where Logical Switch is instantiated.

Limitations

- Not a Distributed Virtual Switch
- Many HyperV Switch Features can't be defined on the Switch template. (e.g. ACL, SPAN) leading to **Host Level Management**.

SCVMM Logical Switch

1. Select Switch Extensions
   - Capture
   - Monitor
   - Forwarding
2. Define Uplink Profiles
   - Mode – Team / No Team
   - Uplink Profile 1
   - Uplink Profile n
3. Define Port Classifications
   - Port Classification 1
   - Port Classification n



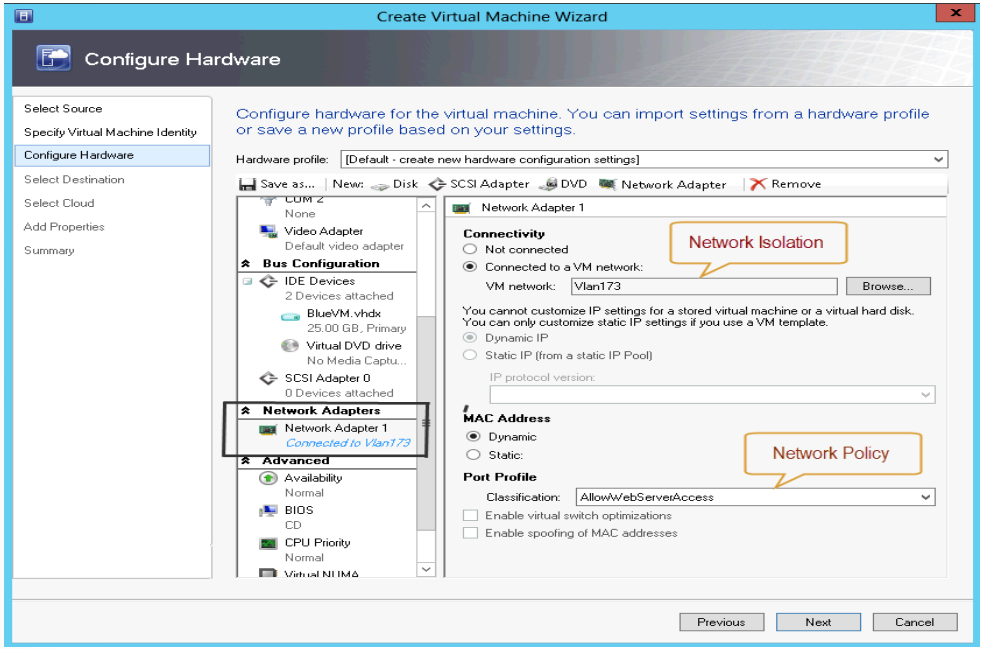
Network and Policy Decoupled in HyperV

VMWare ESX

- Port Group
  - Network connectivity (e.g. vlan)
  - Policy (e.g. SPAN, ACLs)

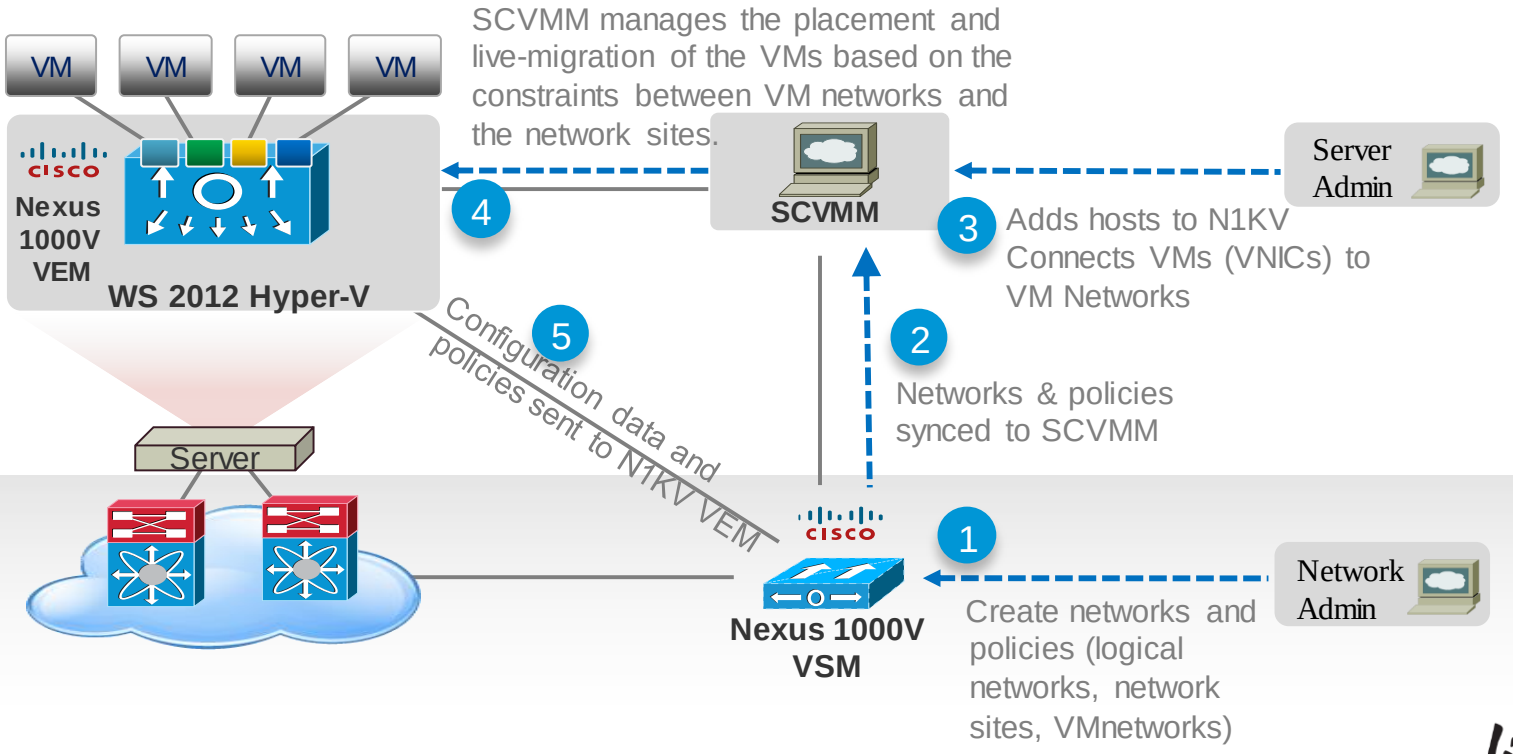
Microsoft HyperV

- Port Classification
  - Veth policy (e.g. QoS)
- VM Network and VM Subnet
  - Determine VM isolation



Cisco Nexus 1000V for Hyper-V

Operational Model with SCVMM



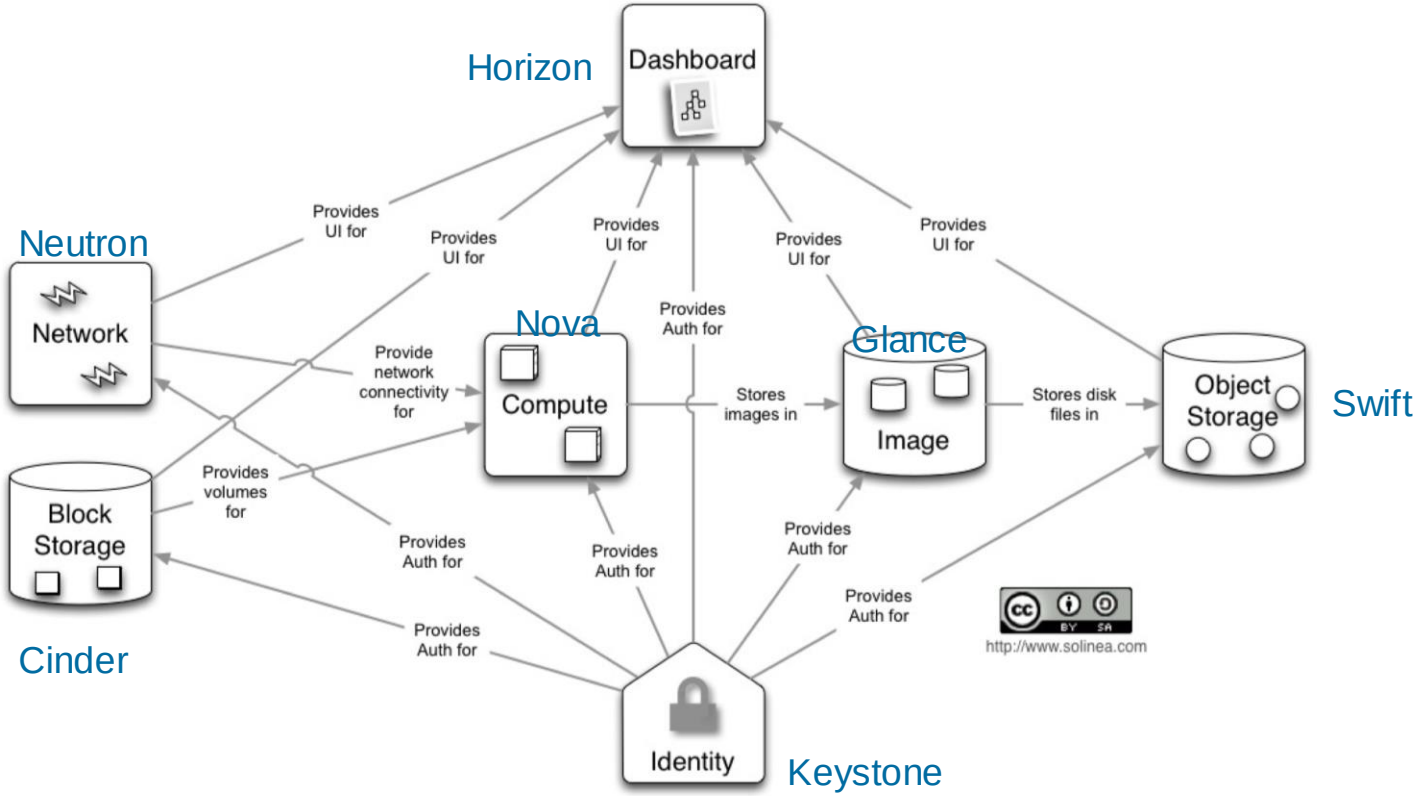
Agenda

- Evolution of the Workloads in the Data Centre
- Achieving Virtualisation in Multiple Hypervisor Options
- Various Hypervisor Networking Options at the Host
  - Hyper-V, KVM/OpenStack, ESXi
- Normalising the Complexity of Multi-Hypervisor Networking

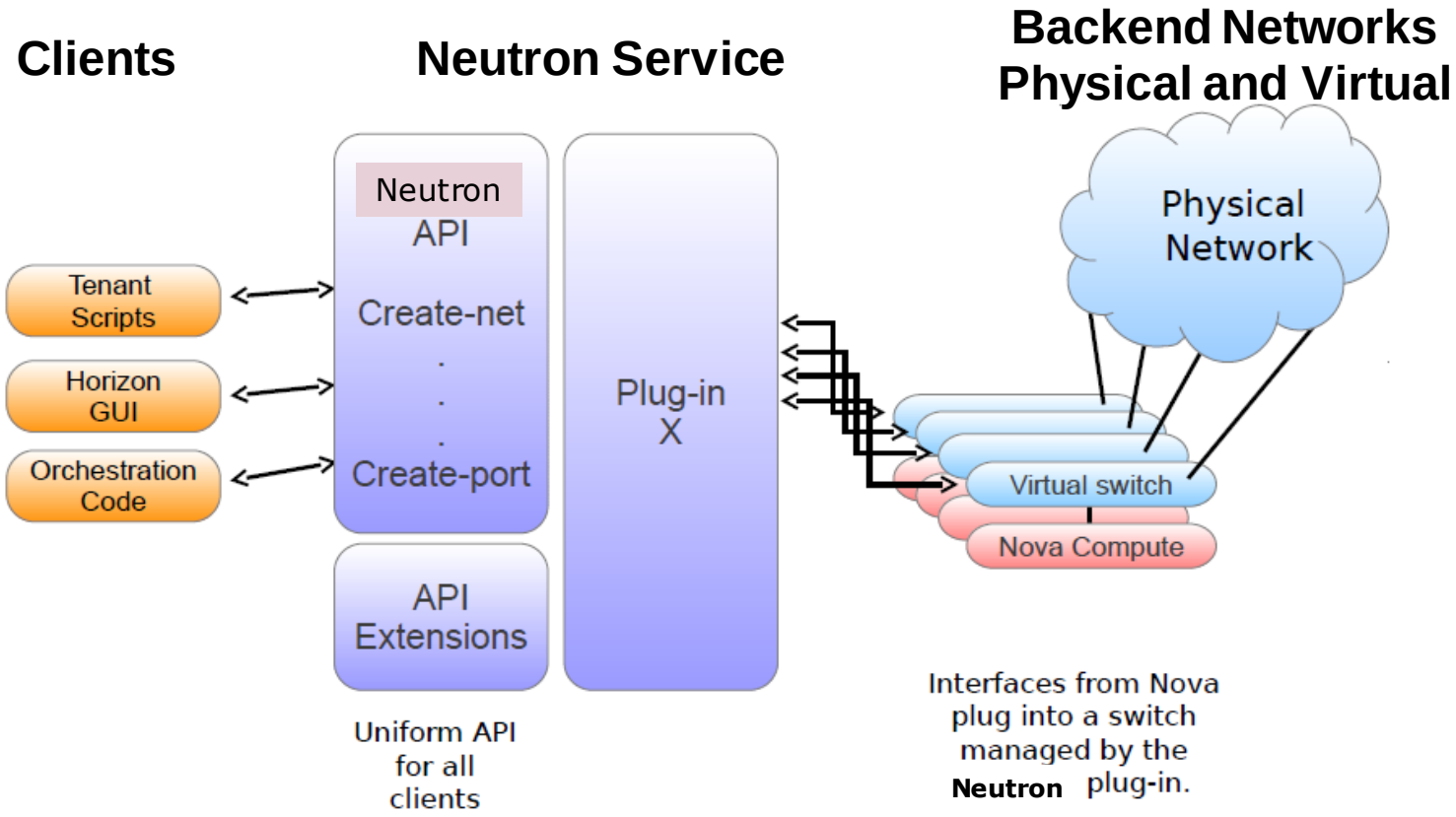
OpenStack Core Projects

OpenStack Compute (Nova)	• Software to provision virtual machines on commodity hardware at massive scale
OpenStack Image Service (Glance)	• Services for discovering, registering, and retrieving virtual machine images
OpenStack Object Storage (Swift)	• Software to reliably store billions of objects distributed across commodity hardware
OpenStack Dashboard (Horizon)	• A self-service web portal to allow administrators and users to manage OpenStack resources
OpenStack Network Service (Quantum/Neutron)	• Provides “network connectivity as a service” between devices managed by other OpenStack services
OpenStack Identity (Keystone)	• Provides “unified authentication” across all OpenStack projects and integrates with 3rd party authentication systems

OpenStack Element Dependencies



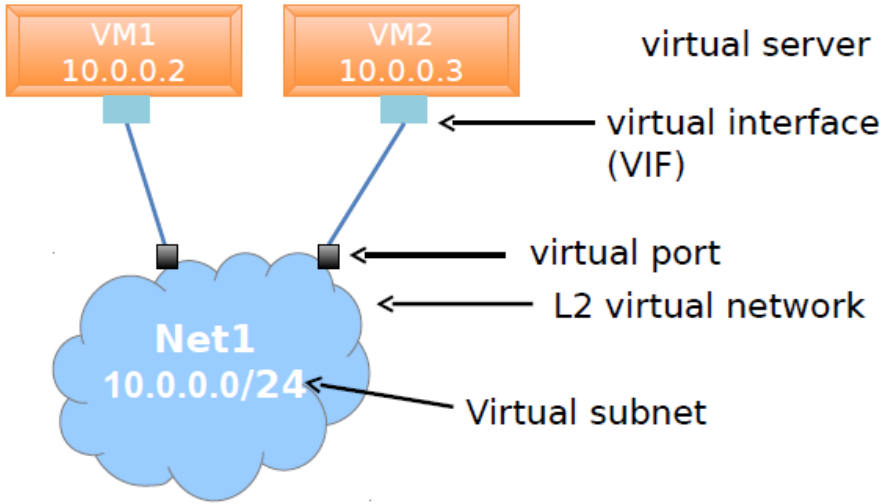
Neutron Architecture



Basic Neutron Abstractions & APIs

Nova

Neutron



"virtual networks" and virtual subnets are fundamentally multi-tenant, just like virtual servers (e.g., overlapping IP's can be used on different networks)

Networks

- Create, Delete, Update
- List, Show

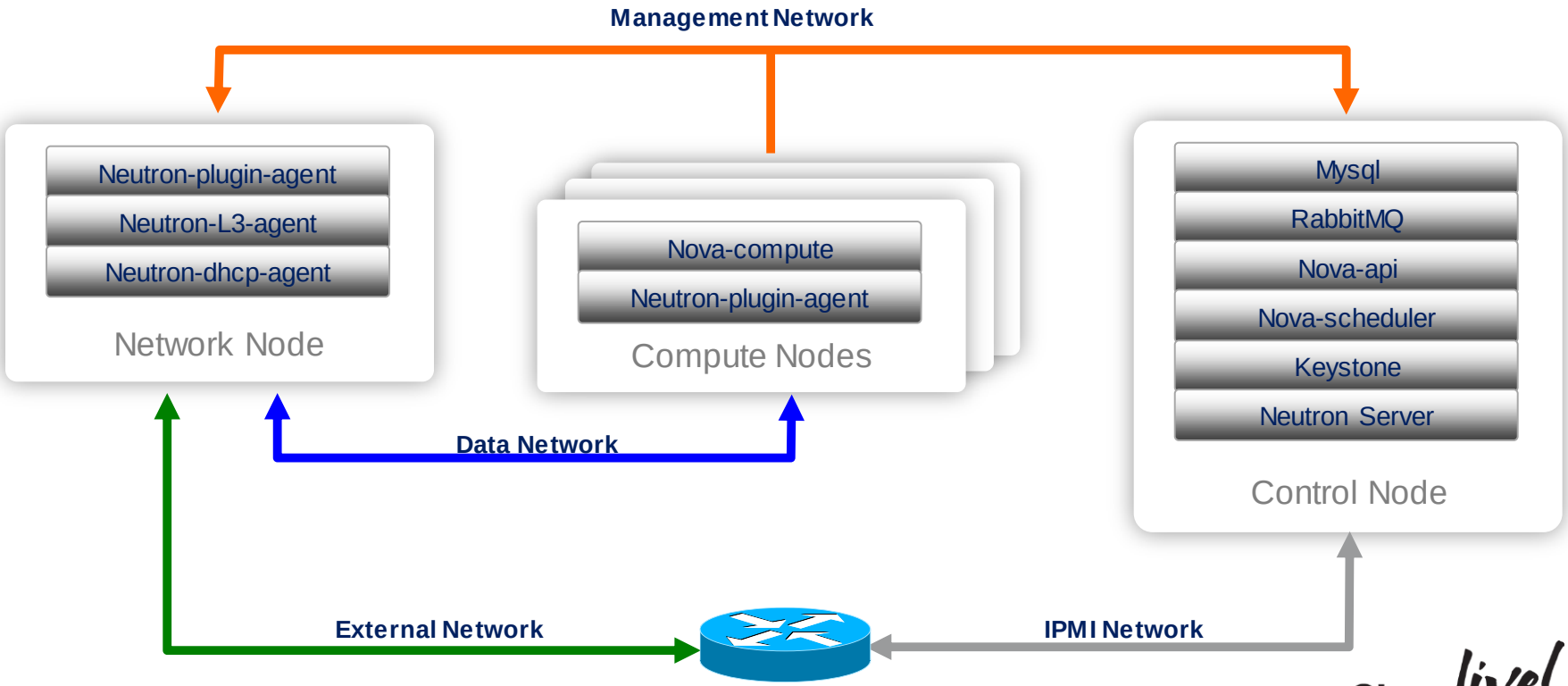
Subnets

- Create, Delete, Update
- List, Show

Ports

- Create, Delete, Update
- List, Show

A Simple OpenStack Deployment



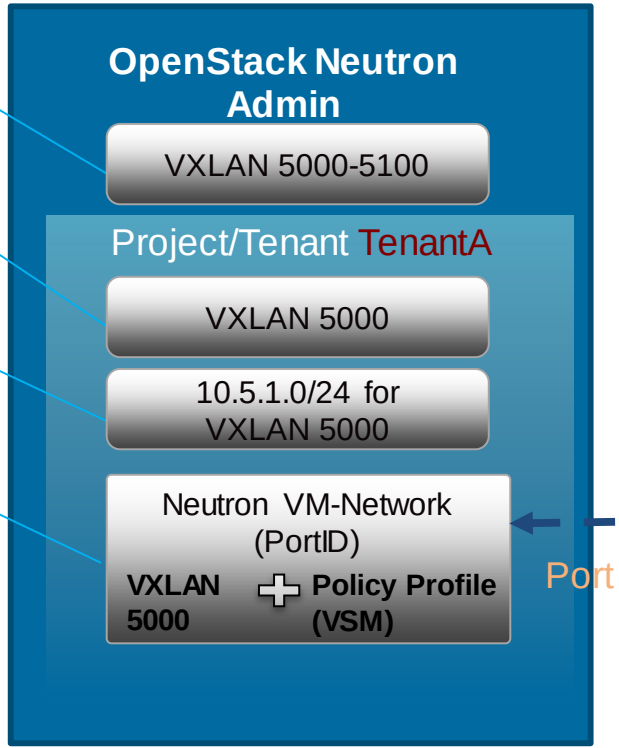
Neutron Work Flow with Cisco Nexus1000V

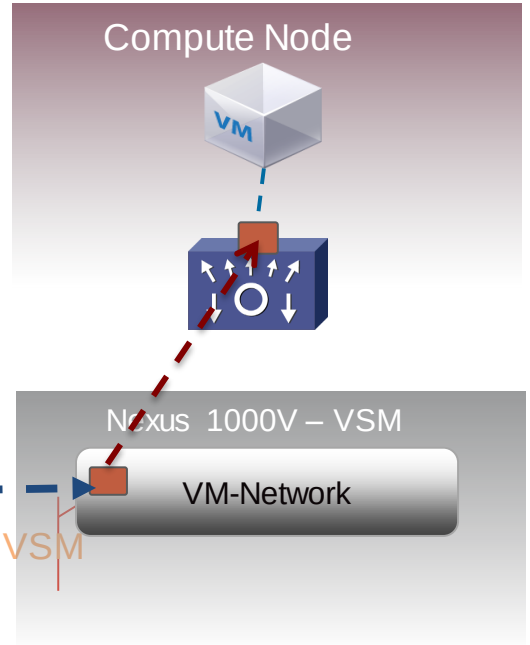
Create Network Profile Type VXLAN (TenantA)
(Pool created and assigned to tenant)

Create Network (net1)
(Tenant Self Create)

Create Subnet (subnet1)
(Assign IP Pool)

Create Port using network and policy
(Created when VM is instantiated)





Port is created in VSM

Port Profile Configuration in KVM/OpenStack

Configuration Templates

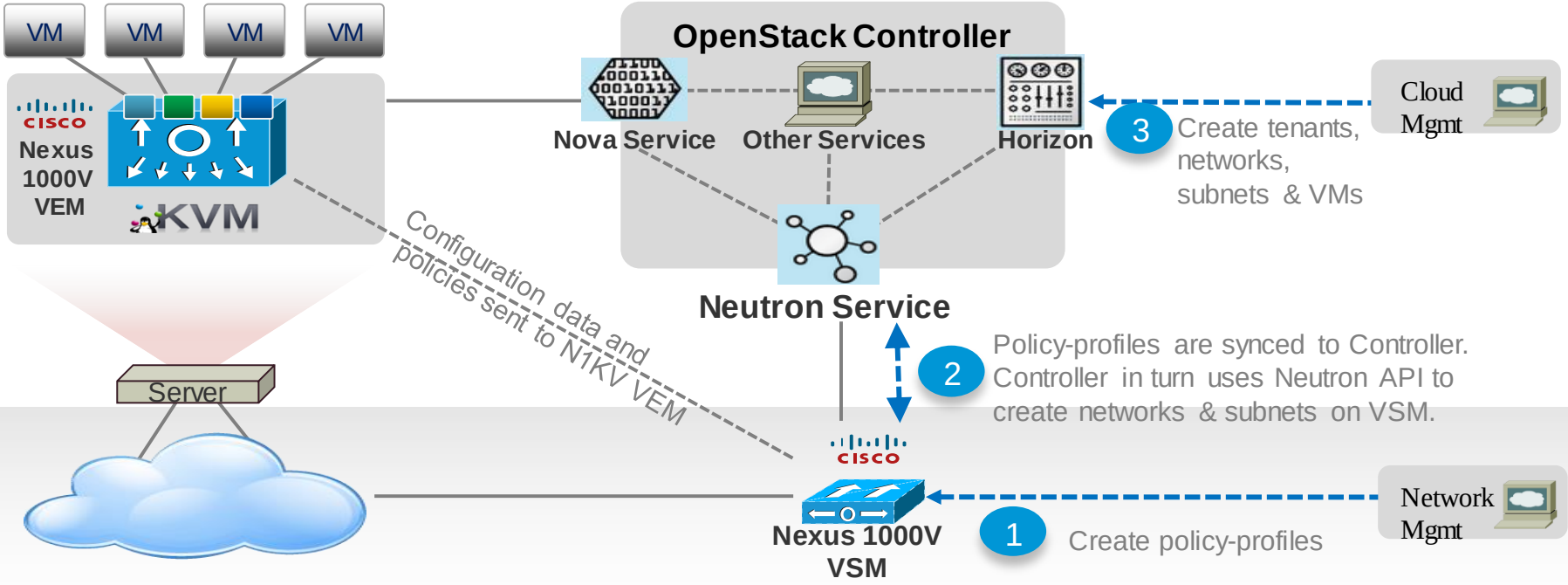
```
n1000v# show port-profile name VM-Data-ClientOS
port-profile VM-Data-ClientOS
      type: Vethernet
      description:
      status: enabled
      max-ports: 32
      min-ports: 1
      inherit:
      config attributes:
       switchport mode access
       switchport access vlan 110
       no shutdown
      evaluated config attributes:
       switchport mode access
       switchport access vlan 110
       no shutdown
      assigned interfaces:
       Vethernet10
```

Supported Commands Include:

- ✓ Port management
- ✓ VLAN
- ✓ PVLAN
- ✓ Port-Channel
- ✓ ACL
- ✓ Netflow
- ✓ Port security
- ✓ QoS

Cisco Nexus 1000V for KVM

Integration with KVM & OpenStack

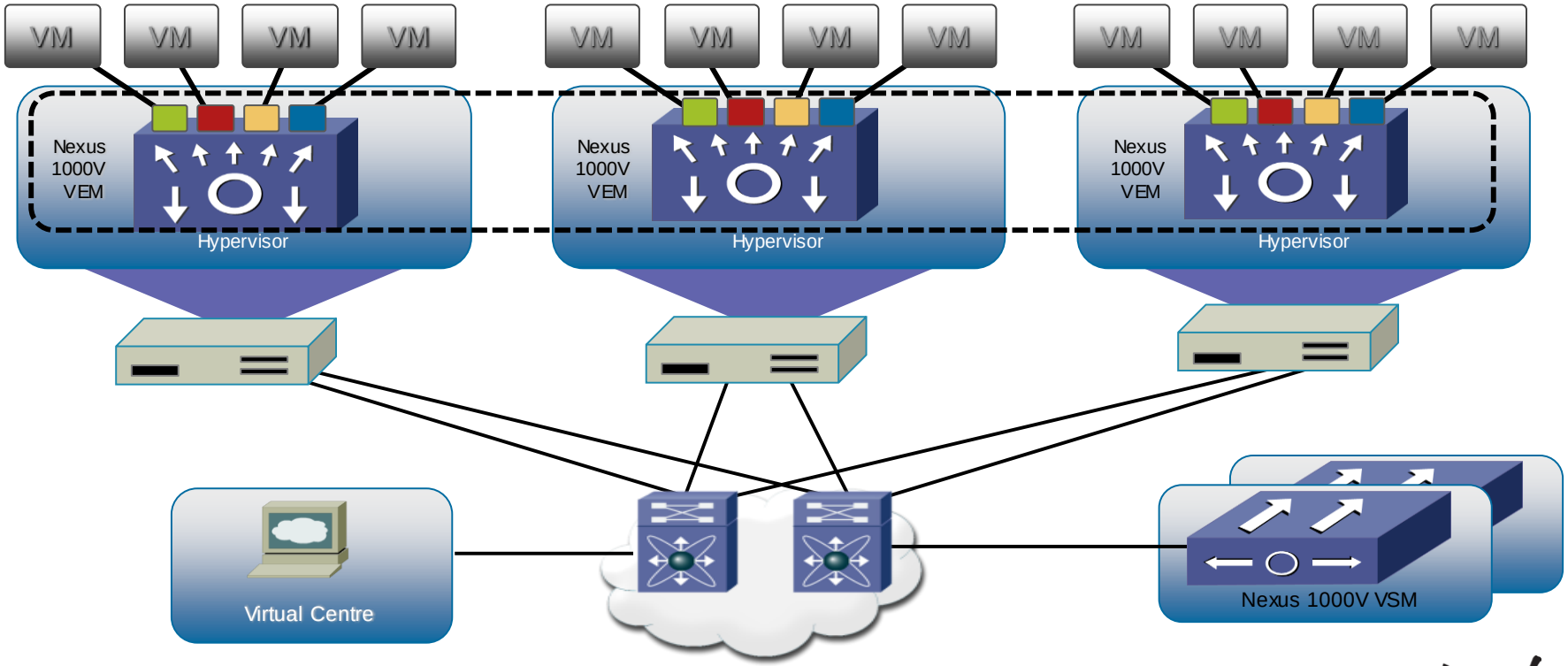


Cisco live!

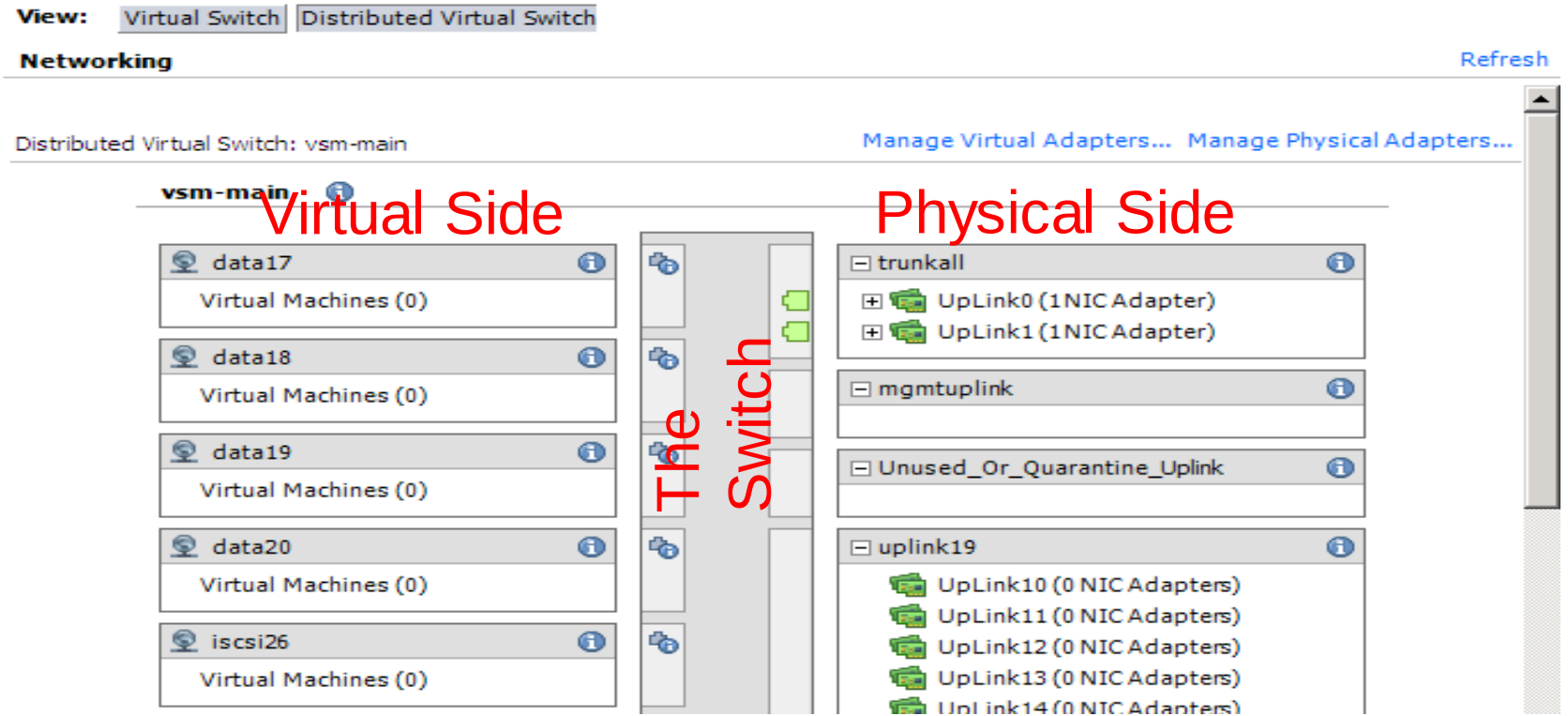
Agenda

- Evolution of the Workloads in the Data Centre
- Achieving Virtualisation in Multiple Hypervisor Options
- Various Hypervisor Networking Options at the Host
  - Hyper-V, KVM/OpenStack, ESXi
- Normalising the Complexity of Multi-Hypervisor Networking

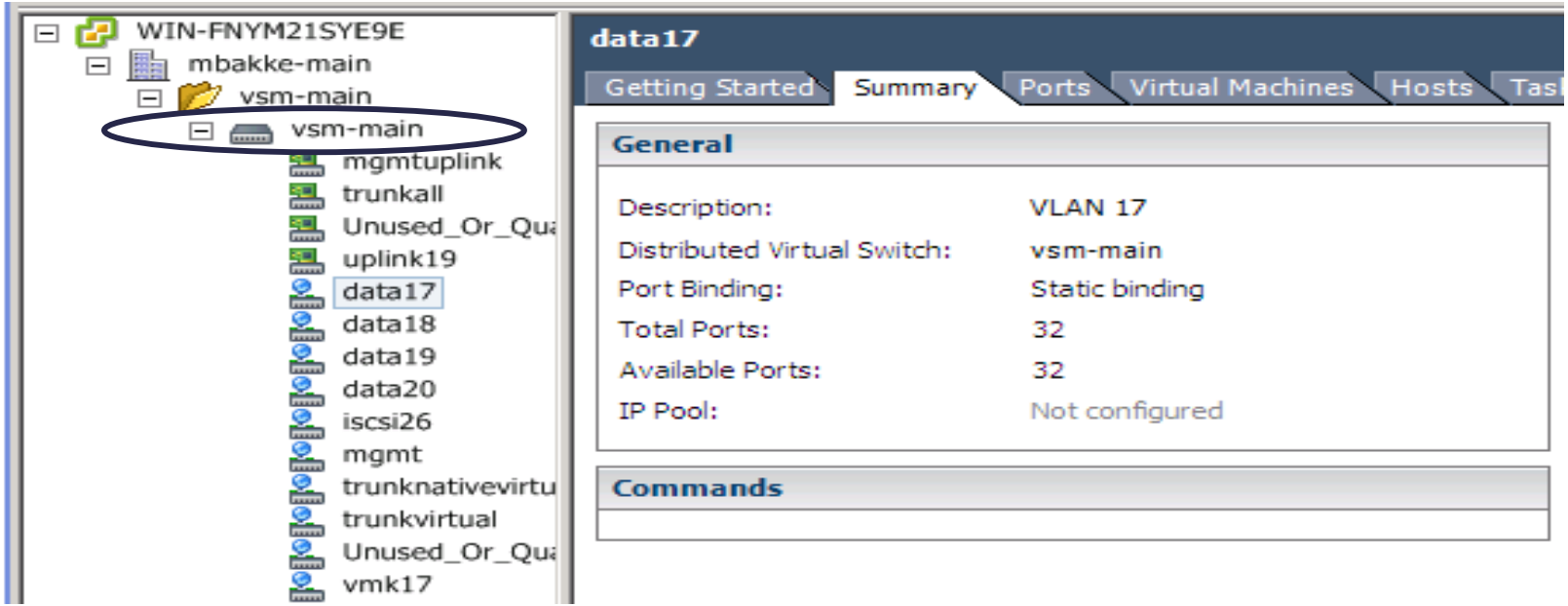
Cisco Nexus 1000V Architecture for ESXi



Nexus 1000V on vCenter

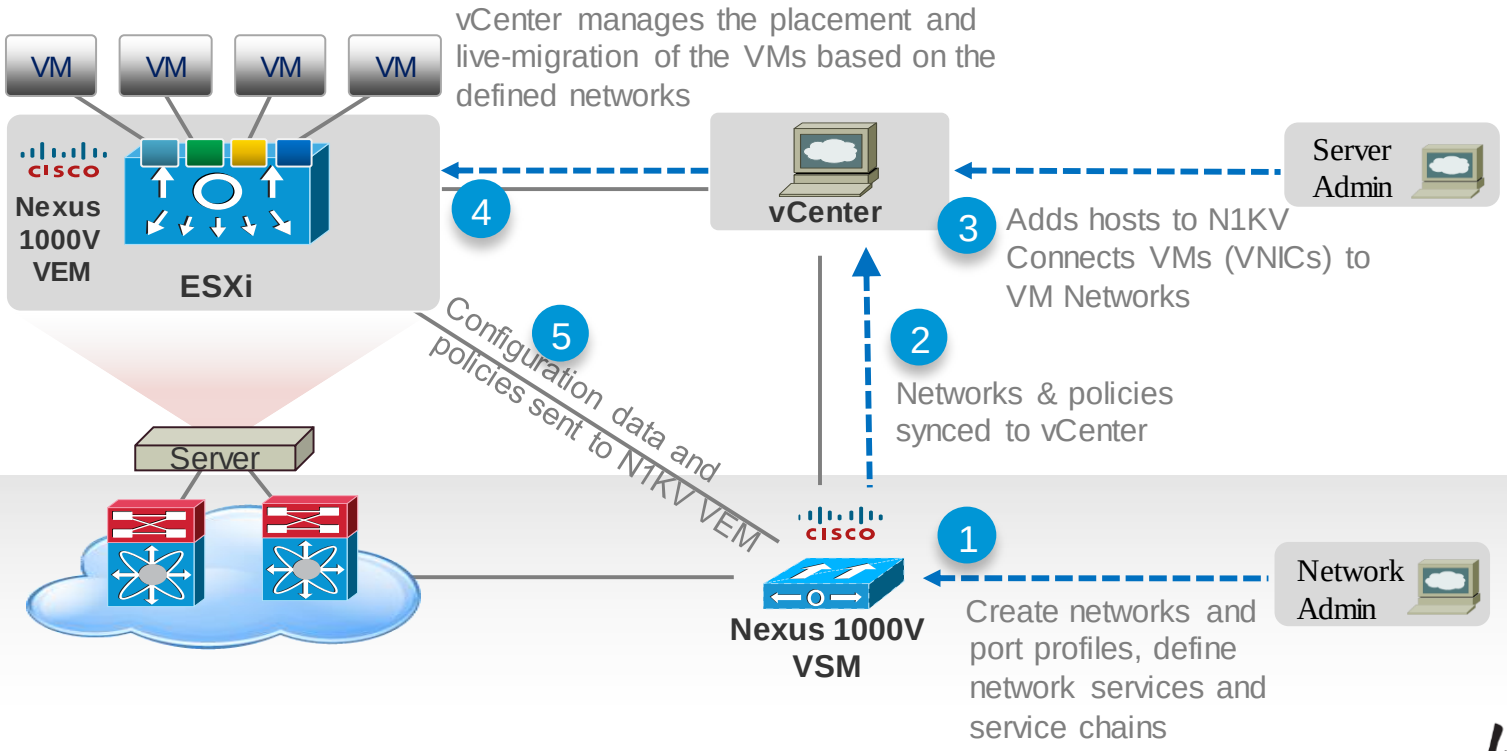


Nexus 1000V on vCenter



Cisco Nexus 1000V for ESXi

Operational Model with vCenter



Agenda

- Evolution of the Workloads in the Data Centre
- Achieving Virtualisation in Multiple Hypervisor Options
- Various Hypervisor Networking Options at the Host
- Normalising the Complexity of Multi-Hypervisor Networking
  - Nexus 1000V (configuration samples)
- Summary / Q&A

Unified Management Interface Across Hypervisors

- NTP
- TACACS+
- RADIUS
- Netflow
- SPAN & ERSPAN

- NX-OS CLI
- SNMP Support
- NetConf/XML
- CDP
- Syslog

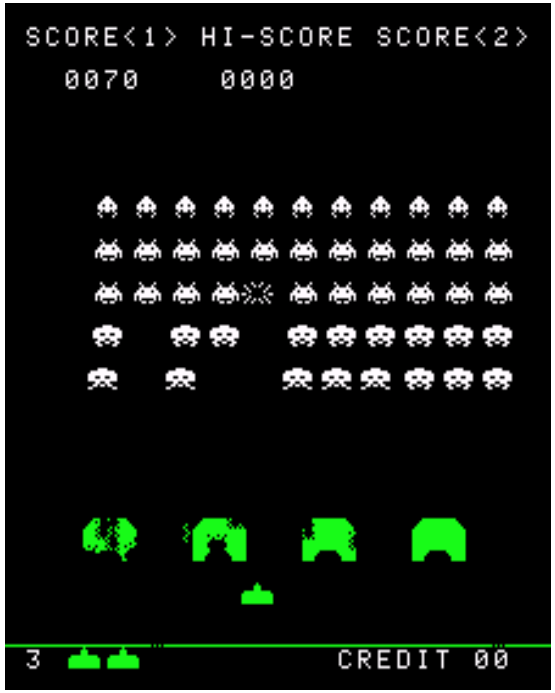
Cisco Nexus 1000V

vm-network-definition (id, vlan, ip-pool) – for network segments
logical-network-definition (name, id, connected-ports) – fabric n/w
virtual-port-profile (type, id, maxports, switch-id) – for vEth
uplink-port-profile (state, type, id, maxports, switch-id) – for PNIC
ip-address-pool (name, dhcp-server, range etc.) – for ip-pools

REST-APIs for manageability

Why Not Configure Virtual Ports?

- Too many ports, and they move too fast
- Network admin needs **sanity**
- Server admin needs **freedom**
  - To deploy and move virtual machines
  - To deploy and move physical hosts



Source: http://images.webmagic.com/klov.com/screens/S/wSpace_Invaders.png

Port Profiles – Current Nexus 1000V

- Instead of configuring individual Ports, create a Port Profile
- Set up ahead of time:
  - VLANs
  - ACLs
  - NetFlow
  - QoS
  - Private VLANs

And all other port config!

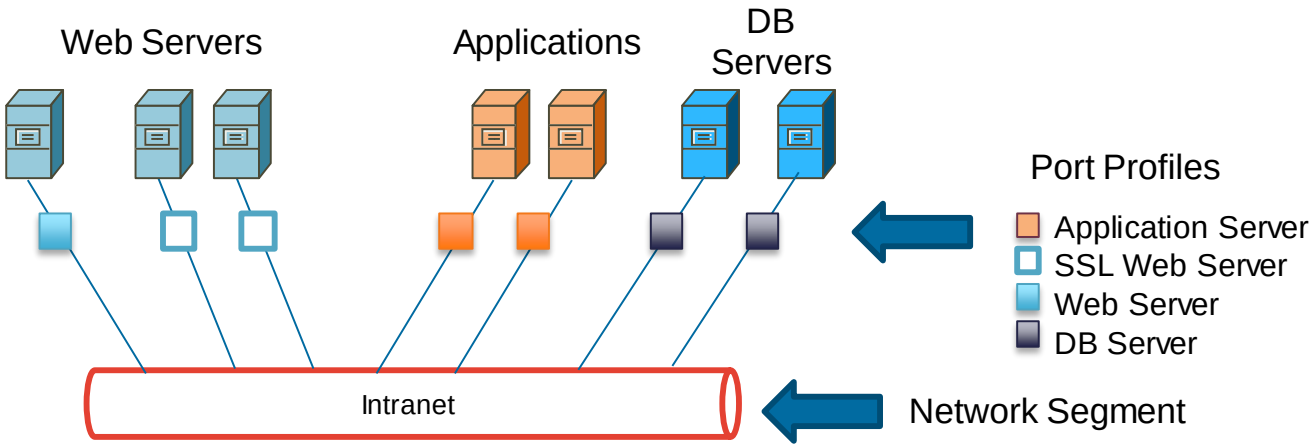
```
# port-profile database
switchport mode access
switchport access vlan 10
ip port access-group myacl in
no shut
state enabled
```

Re-use it multiple times!

Network Segments and Port Profiles

Networks and Profiles are Two Different Things

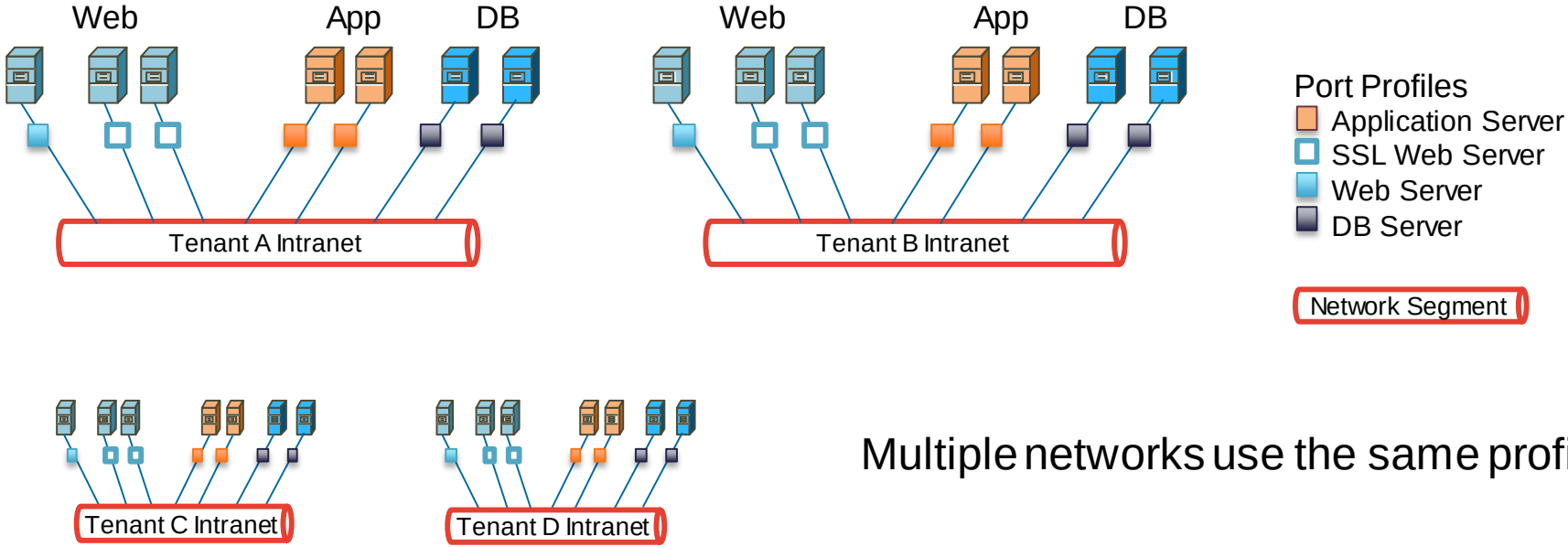
Different ports need different protection on the same network



One network, multiple profiles for access

Network Segments and Port Profiles

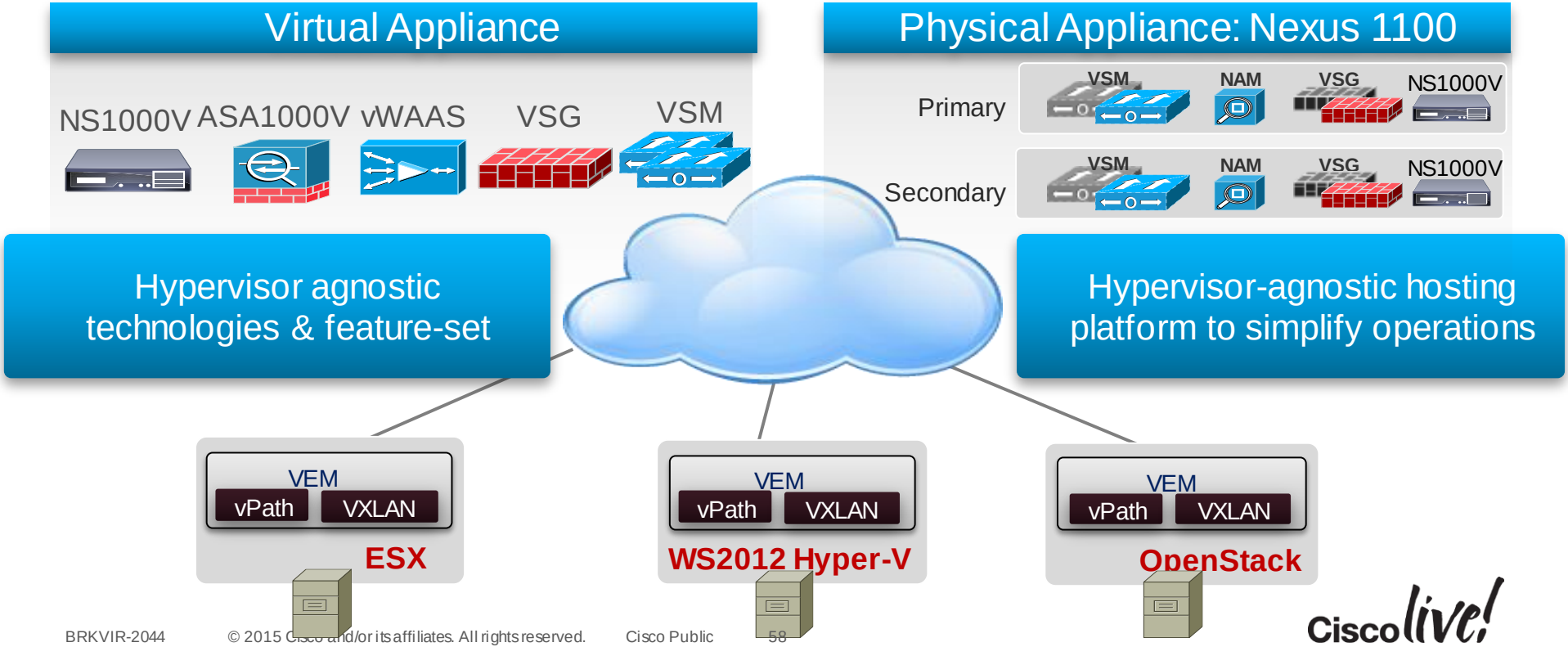
And many networks can share the same protection requirements



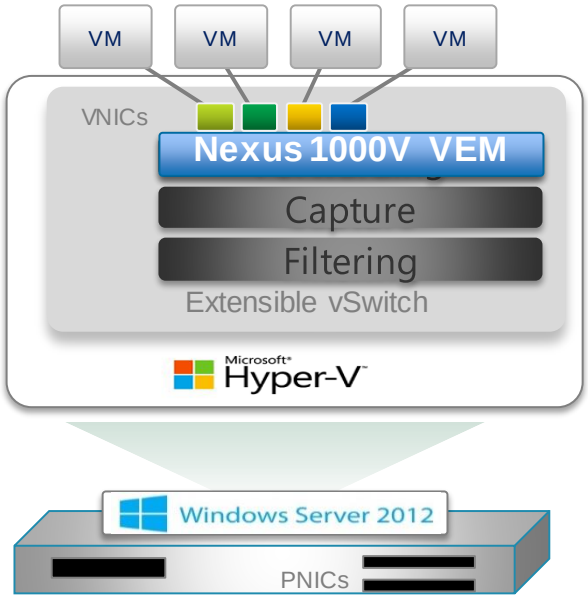
Multiple networks use the same profiles

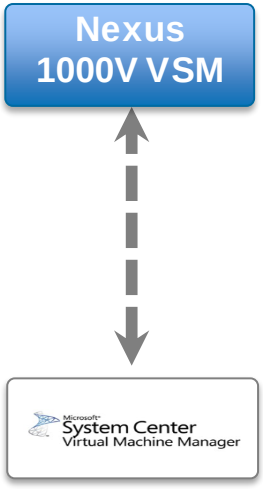
Cisco Nexus 1000V Overview

Consistency across multiple hypervisors



Cisco Nexus 1000V for Hyper-V





- Advanced NX-OS feature-set
- Innovative Services architecture (vPath)
- Consistent operational model
- SCVMM Integration

Nexus 1000V for Hyper-V VSM Configuration

1

```
N1KV(config)#  logical-network  Intranet
```

2

```
N1KV(config)#  network-segment-pool  IntranetSFO
Nexus1000V(config-net-seg-pool)#   logical-network  Intranet
```

```
N1KV(config)#  network-segment-pool  IntranetNY
Nexus1000V(config-net-seg-pool)#   logical-network  Intranet
```

3

```
N1KV(config)#   network-segment  vlan173
Nexus1000V(config-net-seg)#   switchport  mode  access
Nexus1000V(config-net-seg)#   switchport  access  vlan  173
Nexus1000V(config-net-seg)#   network-segment-pool  IntranetSFO
Nexus1000V(config-net-seg)#   publish  network-segment
```

4

```
N1KV(config)#   port-profile  type  ethernet  PortChannelProfile
Nexus1000V(config-port-prof)#   channel-group  auto  mode  on  mac-pinning
Nexus1000V(config-port-prof)#  no  shutdown
Nexus1000V(config-port-prof)#   state  enabled
```


Cisco live!

Nexus 1000V for Hyper-V VSM Configuration

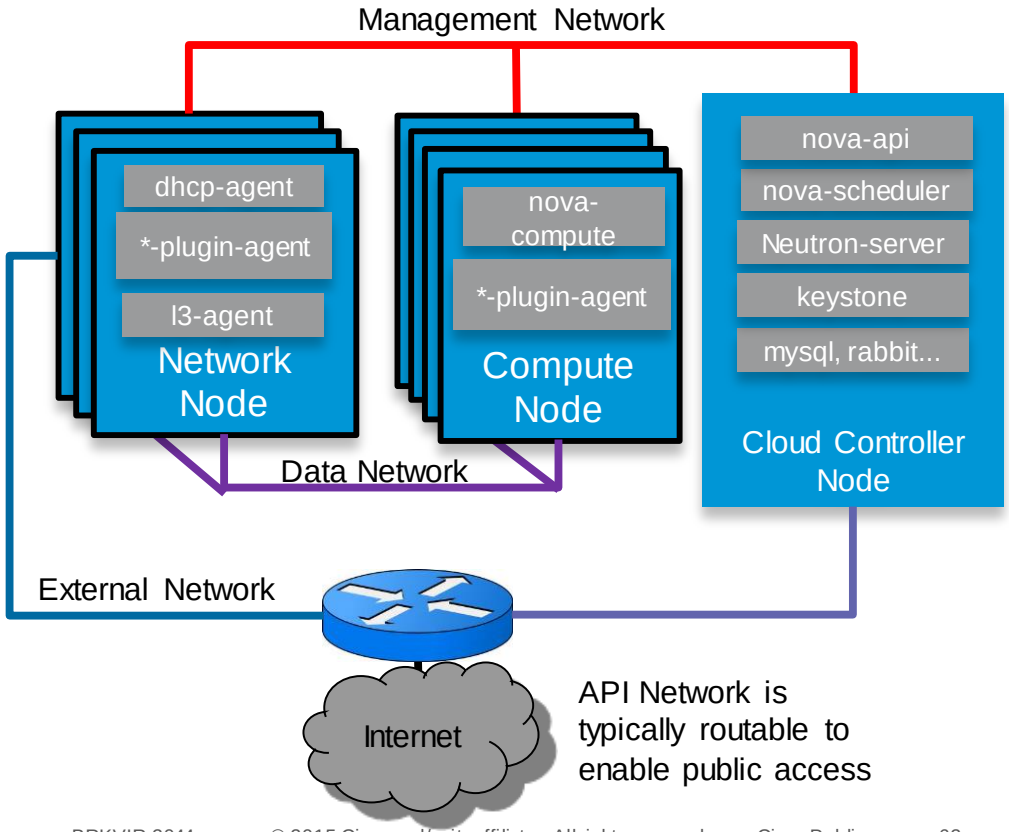
5

```
N1KV(config)#  port-profile type vethernet WebServerProfile
Nexus1000V(config-port-prof)#  publish port-profile
Nexus1000V(config-port-prof)# no shutdown
Nexus1000V(config-port-prof)#  state enabled
```

6

```
N1KV(config)#  uplink-network Nexus1000VUplinkProfile
Nexus1000V(config-uplink-net)#  import port-profile PortChannelProfile
Nexus1000V(config-uplink-net)# network-segment-pool IntranetSFO
Nexus1000V(config-uplink-net)# network-segment-pool IntranetNY
Nexus1000V(config-uplink-net)# publish uplink-network
```

KVM/OpenStack with Nexus 1000V



- vPath Service Insertion/Chaining
  - CSR, VPN, Firewall, etc.
- Consistent operational model
- Leverage Nexus 1000V REST API

Nexus 1000V for KVM/OpenStack VSM Config

1

```
switch(config)# network segment manager switch
Nexus1000V(config-net-seg-pool)#  dvs name vsm-kvm-440
```

2

```
vsm-kvm-440(config)#  port-profile type vethernet NSM_Template_vlan
vsm-kvm-440(config-port-prof)#  guid 16c55294-91a8-41e6-906a-a1b84f1db881
vsm-kvm-440(config-port-prof)#  state enabled
```

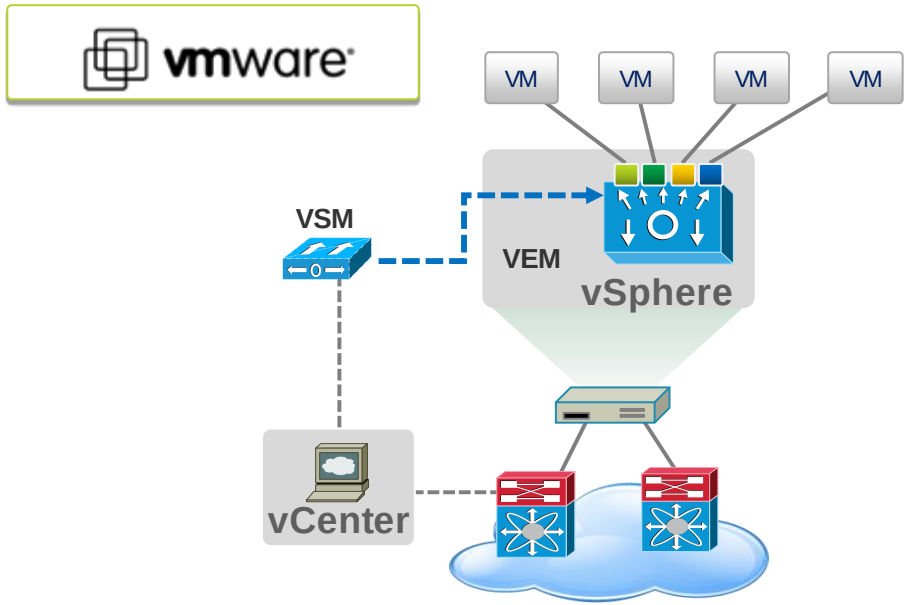
3

```
vsm-kvm-440(config)# network segment policy default_vlan_template
vsm-kvm-440(config-network-segment-policy)type vlan
vsm-kvm-440(config-network-segment-policy)import port-profile
NSM_Template_vlan
```

4

```
vsm-kvm-440(config)#  port-profile type ethernet sys-uplink
vsm-kvm-440(config-port-prof)#  switchport mode trunk
vsm-kvm-440(config-port-prof)# switchport trunk allowed vlan 1-700
vsm-kvm-440(config-port-prof)# mtu 1550
vsm-kvm-440(config-port-prof)#  state enabled
vsm-kvm-440(config-port-prof)# publish port-profile
```

ESXi with Nexus 1000V



- Advanced NX-OS feature-set
- Innovative Services architecture (vPath)
- VXLAN Overlay Networking
- VSUM

Nexus 1000V for ESXi VSM Configuration

1

```
switch(config)# hostname vsm-esx
vsm-esx(config)#
```

2

```
vsm-esx(config)#  port-profile type vethernet Test
vsm-esx(config-port-prof)#  vmware port-group
vsm-esx(config-port-prof)#  switchport mode access
vsm-esx(config-port-prof)#  switchport access vlan 351
vsm-esx(config-port-prof)#  no shutdown
vsm-esx(config-port-prof)#  state enabled
```

3

```
vsm-esx(config)#  port-profile type ethernet uplink
vsm-esx(config-port-prof)#  vmware port-group
vsm-esx(config-port-prof)#  switchport trunk allowed vlan 1-700
vsm-esx(config-port-prof)#  channel-group auto mode on mac-pinning
vsm-esx(config-port-prof)#  system vlan 351-353
vsm-esx(config-port-prof)#  state enable
```

Consistency of Network Segments and Port Profiles

Splitting the port-profile into “Network Connectivity” and “Policy”

ESXi Version

```
# port-profile app-server
switchport mode access
switchport access vlan 10
ip port access-group app_server in
no shut
state enabled
```

```
# port-profile db-server
switchport mode access
switchport access vlan 10
ip port access-group dbserver in
no shut
state enabled
```

Hyper-V & KVM Version

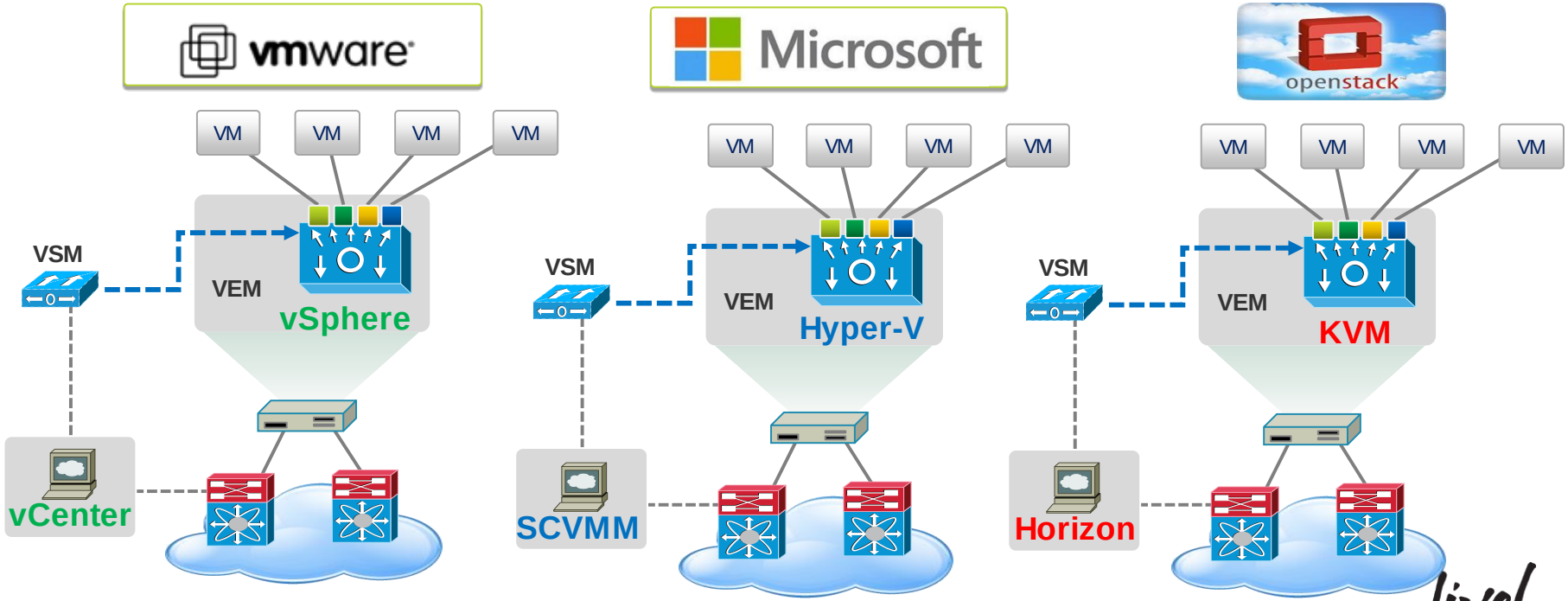
```
#nsm network segment db-network
switchport mode access
switchport access vlan 10
```

```
# port-profile app-server
ip port access-group app_server in
no shut
state enabled
```

```
# port-profile db-server
ip port access-group dbserver in
no shut
state enabled
```

Cisco Nexus 1000V for Multi-Hypervisor

Consistent Architecture across hypervisors



Agenda

- Evolution of the Workloads in the Data Centre
- Achieving Virtualisation in Multiple Hypervisor Options
- Various Hypervisor Networking Options at the Host
- Normalising the Complexity of Multi-Hypervisor Networking
- Summary / Q&A

Key Takeaways

- Understand networking in the 3 most popular Hypervisors
- Grasp the complexity and differences between various Hypervisor networking operations
- Understand how the Nexus1000V provides consistency to different Hypervisor switching mechanisms


Q & A
Cisco live!

Complete Your Online Session Evaluation

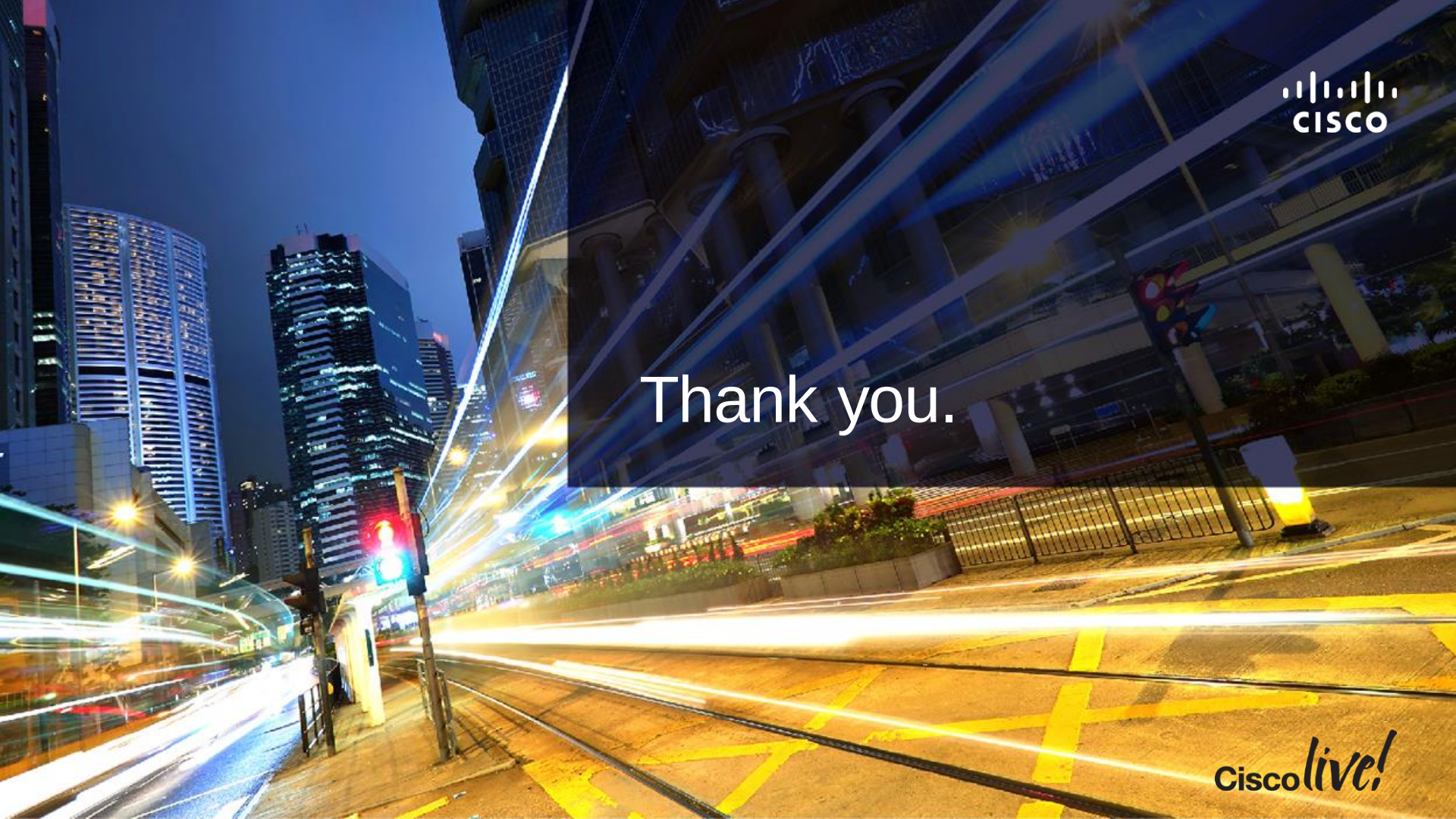
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com


Thank you.


CISCO