NetBox as the Source of Truth for Cisco NSO Configurations

Hank Preston, Principal Engineer
Sandbox Architecture and Automation
Twitter: @hfpreston

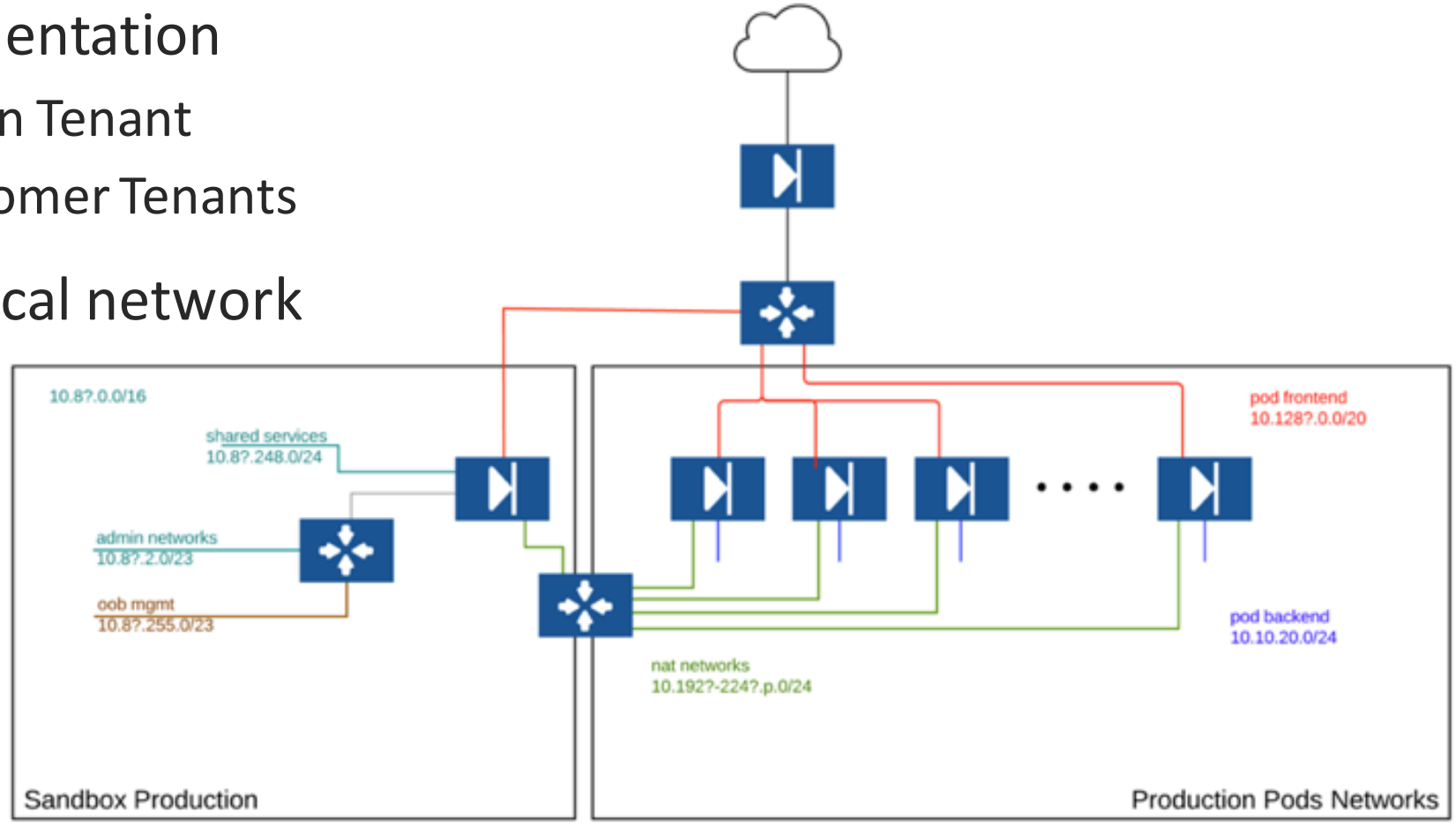
May 19, 2020

- Configuration Management with Cisco NSO
- NetBox as Source of Truth for Cisco NSO

Twitter: @hfpreston | Email: hapresto@cisco.com

Basic Logical Network Topology

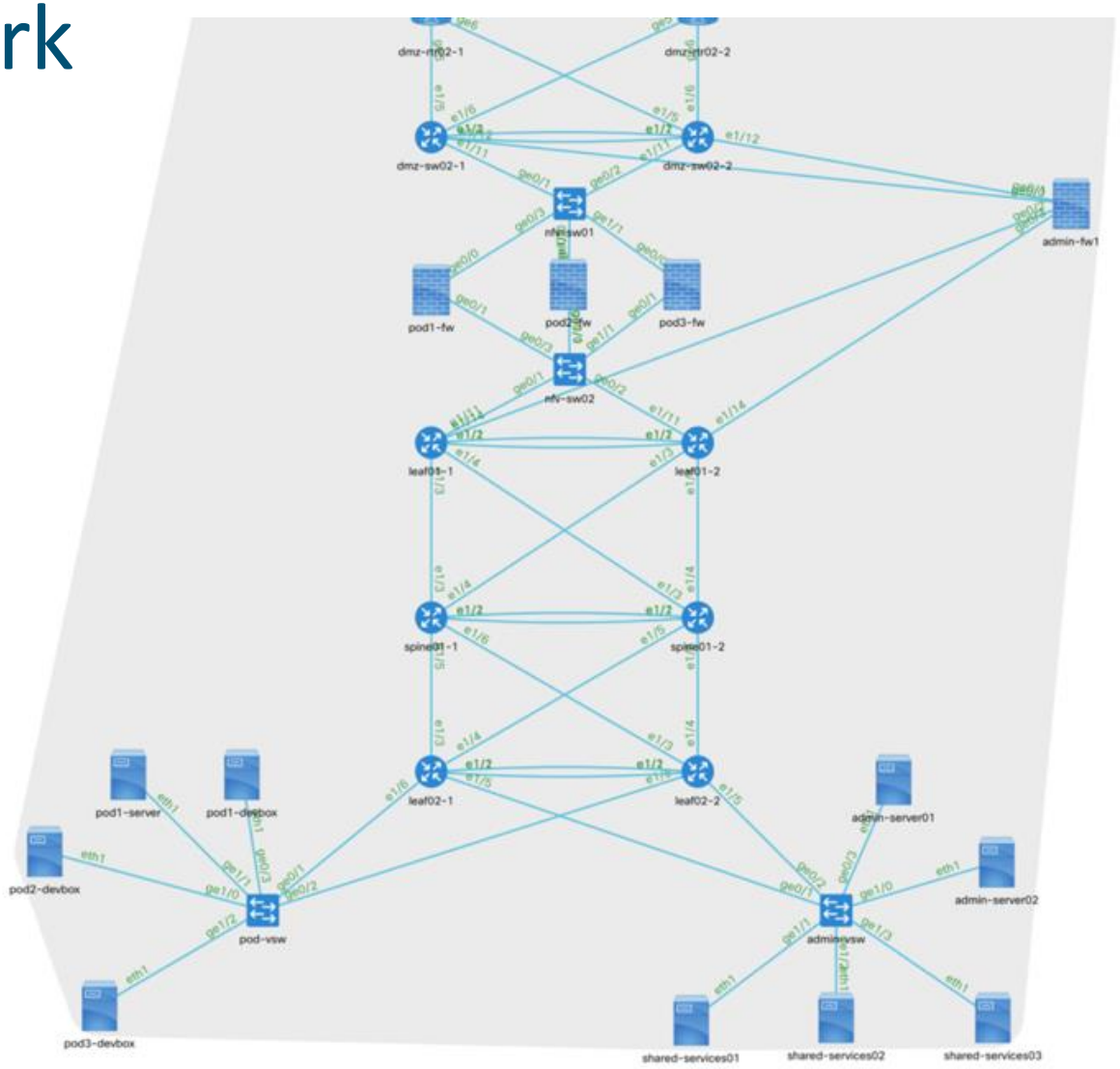
- "Multi-Tenant" segmentation
  - Internal Trusted Admin Tenant
  - Many Untrusted Customer Tenants
- Built on shared physical network



Twitter: @hfpreston | Email: hapresto@cisco.com

Moving to Physical Network

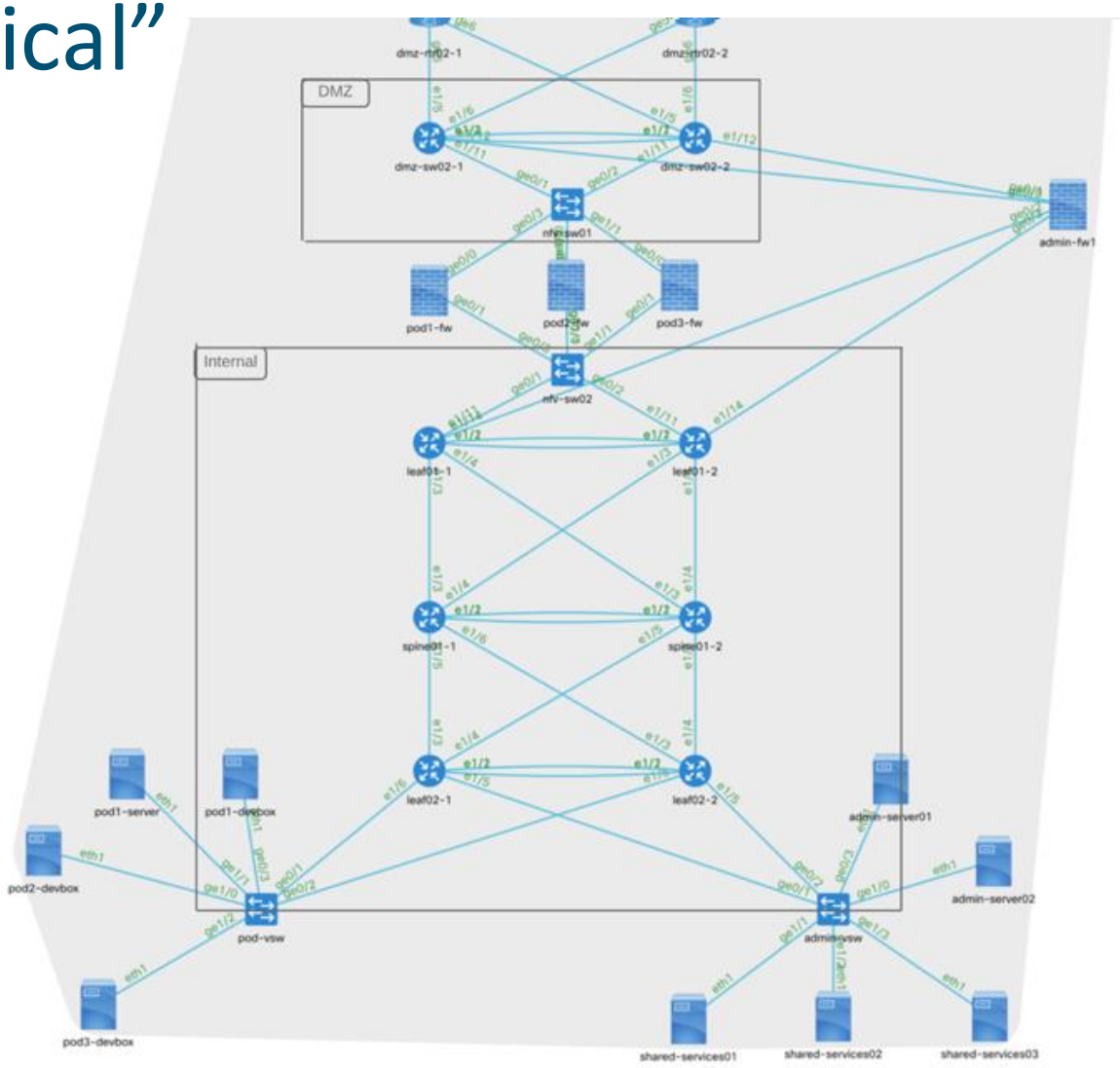
- ”Typical” data center network
- Layer 2 segmentation with VLANs
- Layer 3 segmentation with VRF and firewalls



Twitter: @hfpreston | Email: hapresto@cisco.com

Putting “Logical” on ”Physical”

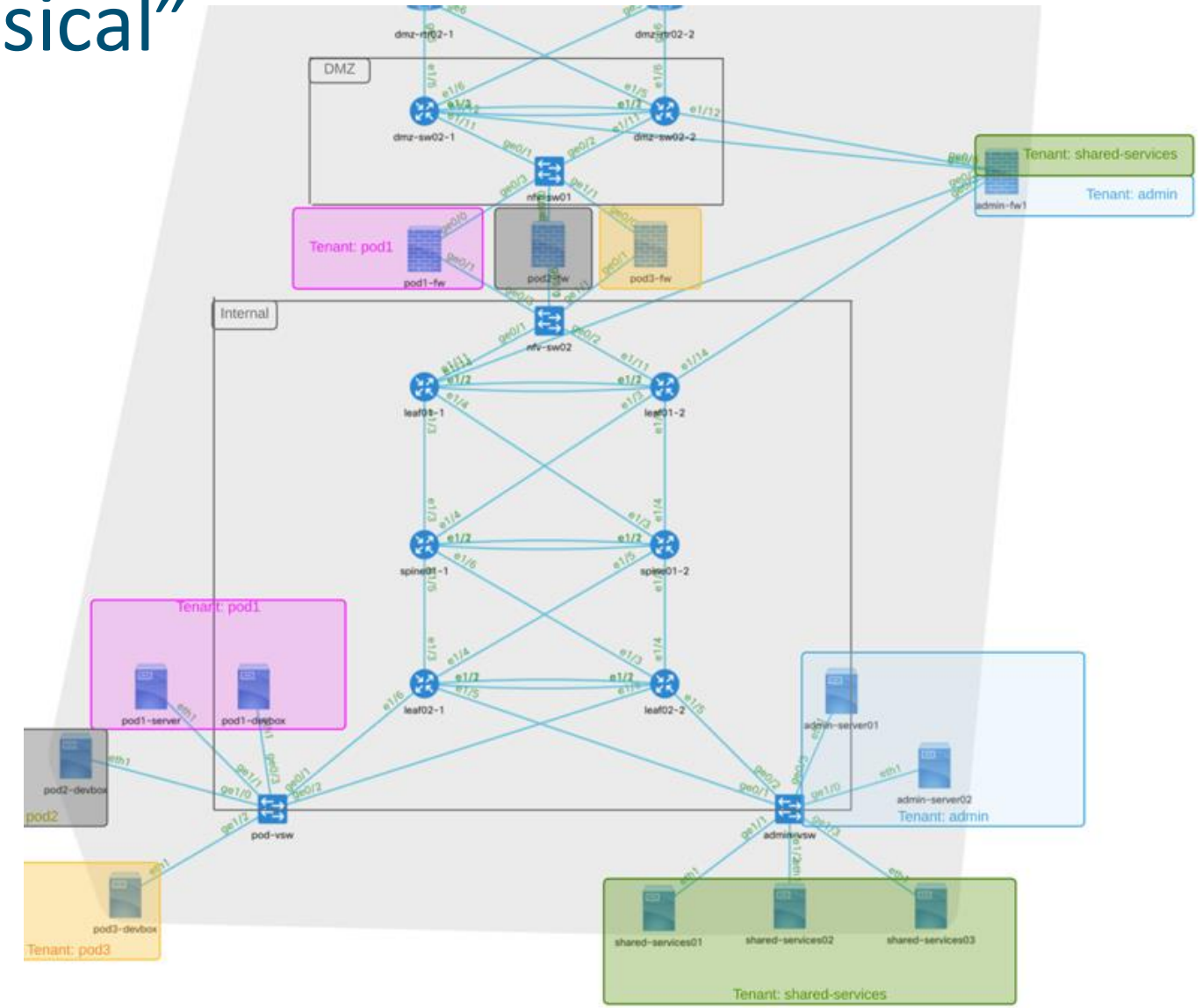
- Layer 2 domains are VLAN Fabrics
  - Single VLAN “scope”
  - Composed of multiple “switches”
    - Nexus, VMware, UCS



Twitter: @hfpreston | Email: hapresto@cisco.com

Putting “Logical” on ”Physical”

- Layer 3 domains are “VLAN Tenants”
  - Unique layer 3 IP space
  - Security boundary at firewalls

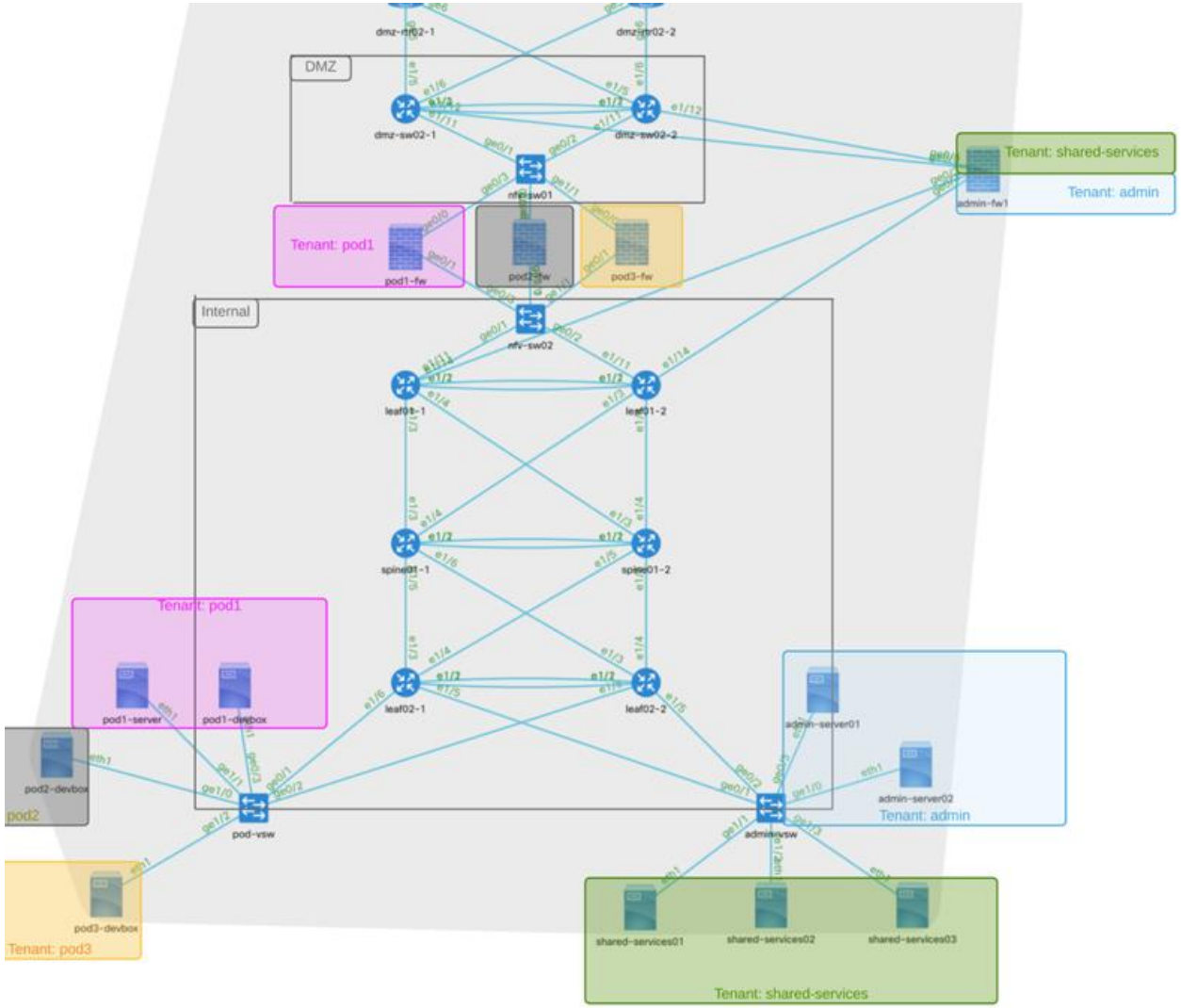


Twitter: @hfpreston | Email: hapresto@cisco.com

Cisco NSO and Network Service Based Automation

Initial Services Built

- **vlan-fabric**: Physical underlay
  - MLAG domains & interswitch trunks
- **vlan-tenant**: Overlay tenants
  - L2 and L3 domains
  - Physical network attachments
- **firewall**: Simplify and Consistency
  - Interfaces, Access Lists, Public Services, VPN management



Twitter: @hfpreston | Email: hapresto@cisco.com

Configuring a VLAN Fabric

`vlan-fabric`

- Describe underlay connectivity
- Cover “traditional” switches as well as “non-traditional” ones

```
vlan-fabric internal
 switch-pair leaf01
  layer3    true
  primary   leaf01-1
  secondary leaf01-2
  vpc-peerlink id 1
  vpc-peerlink interface 1/53
  vpc-peerlink interface 1/54
  fabric-trunk 2
   interface 1/49
   interface 1/50

 fabric-interconnect fi01
  vnic-template-trunks myorg1 vm-network-a
  vnic-template-trunks myorg2 esxi-vnic-a

 vmware-dvs vcenter1 mydatacenter mydvs
```

Note: Configurations, templates, code, etc have been simplified for this presentation.

Twitter: @hfpreston | Email: hapresto@cisco.com

Configuring a VLAN Tenant

`vlan-tenant`

- Describe the L2/L3 environment
- Focus on unique details per network

```
vlan-tenant admin
 fabric internal
 static-routes 0.0.0.0/0
  gateway 172.23.250.4

 network admin-containers
  vlanid              25
  network             172.23.4.0/23
  layer3-on-fabric    true
  dhcp-relay-address 172.23.2.11

 network admin-main
  vlanid             11
  network            172.23.2.0/23
  layer3-on-fabric true
  connections switch-pair leaf01
   interface 1/33
    description "Link to NUC ESXI"
```

Note: Configurations, templates, code, etc have been simplified for this presentation.

Twitter: @hfpreston | Email: hapresto@cisco.com

But what about NetBox?

NetBox is our Source of Truth

- The Cisco NSO CDB (Configuration Database) drives network state
- NetBox drives the CDB

Twitter: @hfpreston | Email: hapresto@cisco.com

Mapping NetBox Data Model to Services

VLAN Group	→	VLAN Fabric
Tenant and VRF	→	VLAN Tenant
VLAN & Prefix	→	Network
Devices and Interfaces	→	Devices and Interfaces

Twitter: @hfpreston | Email: hapresto@cisco.com

Mapping NetBox Data Model to Services

VLAN Group → VLAN Fabric

VLAN Groups

	Name	Site	VLANs	Slug
☐	DMZ01	USW1	1	dmz01
☐	DMZ02	USW1	3	dmz02
☐	Edge	USW1	1	edge
☐	Internal	USW1	658	internal

```
nso1# show running-config vlan-fabric
vlan-fabric dmz01
vlan-fabric dmz02
vlan-fabric edge
vlan-fabric internal
```


Twitter: @hfpreston | Email: hapresto@cisco.com

Mapping NetBox Data Model to Services

Tenant and VRF → VLAN Tenant

Tenants

	Name	Group
☐	USW1 Admin	USW1
☐	USW1 Admin-Private	USW1
☐	USW1 DMZ01	USW1
☐	USW1 DMZ02	USW1
☐	USW1 Edge	USW1

```
nso1# show running-config vlan-tenant
vlan-tenant admin
vlan-tenant admin-private
vlan-tenant dmz01
vlan-tenant dmz02
vlan-tenant edge
vlan-tenant pod-backdoor
vlan-tenant pod1
vlan-tenant pod10
vlan-tenant pod100
vlan-tenant pod101
vlan-tenant pod102
```


Twitter: @hfpreston | Email: hapresto@cisco.com

Mapping NetBox Data Model to Services

VLAN & Prefix → Network

VLANs

	ID	Site	Group	Name	Prefixes
☐	5	USW1	Internal	oobmgmt-transit	10.17.251.0/29
☐	10	USW1	Internal	admin-fw-transit	10.17.250.0/29
☐	11	USW1	Internal	admin-main	10.17.2.0/23
☐	15	USW1	Internal	pod-fw-mgmt	10.17.232.0/21

```
vlan-tenant admin
 network oobmgmt-transit
  vlanid          5
  network         10.17.251.0/29
 network admin-fw-transit
  vlanid          10
  network         10.17.250.0/29
 network admin-main
  vlanid          11
  network         10.17.2.0/23
 network pod-fw-mgmt
  vlanid          15
  network         10.17.232.0/21
```


Twitter: @hfpreston | Email: hapresto@cisco.com

Mapping NetBox Data Model to Services

Devices and Interfaces

Devices and Interfaces

VLAN | Members 40 | Changelog

VLAN Members

Parent	Interface
usw1-leaf01-1	Ethernet1/3
usw1-leaf01-2	Ethernet1/3
usw1-leaf01-1	
usw1-leaf01-2	
usw1-leaf01-1	
usw1-leaf01-2	

VLANs

ID	Tagged	Site	Group	Name
15	✔	USW1	Internal	pod-fw-mgmt
30	✔	USW1	Internal	esxi-mgmt
101	✔	USW1	Internal	pod1-backend

```
vlan-tenant admin
 network esxi-mgmt
  connections switch-pair usw1-leaf01
   interface 1/3
    mode trunk
   !
   interface 1/4
    mode trunk
   !
   interface 1/5
    mode trunk
```


Twitter: @hfpreston | Email: hapresto@cisco.com

Generating NSO Configurations from NetBox

```
python nso_tenant_config.py --tenant admin
✅ Processing Tenant: admin
❌ Skipping Tenant: admin-private because it was NOT listed in `tenant`
```

- Python script uses pynetbox to read all tenants, vlan-groups, prefixes, etc
- Jinja2 templates used to create both CLI and XML versions of NSO Service Configuration
- Generated configurations “load merged” into Cisco NSO

```
<config xmlns="http://tail-f.com/ns/config/1.0">
 <vlan-tenant xmlns="http://example.com/vlan-tenant">
  <name>admin</name>
  <fabric>internal</fabric>
  <network>
   <name>oobmgmt-transit</name>
   <vlanid>5</vlanid>
   <network>10.17.251.0/29</network>
   <layer3-on-fabric>true</layer3-on-fabric>
   <build-route-neighbors>true</build-route-neighbors>
   <connections>
    <switch-pair>
     <name>usw1-leaf01</name>
    <port-channel>
      <portchannel-id>100</portchannel-id>
      <description>Routed link to OOB</description>
      <mode>access</mode>
      <interface>
       <interface>1/48</interface>
       </interface>
     </port-channel>
     </switch-pair>
   </connections>
```


Twitter: @hfpreston | Email: hapresto@cisco.com

<close-session />

Explore it some more!

- Deeper Dive into Network Service Automation in Sandbox from Cisco Live Europe 2020
- Checkout the NSO Service Code and NetBox Scripts

Twitter: @hfpreston | Email: hapresto@cisco.com

Got more questions? Stay in touch!

Hank Preston

hapresto@cisco.com

@hfpreston

hfpreston (Network to Code)

http://github.com/hpreston

CISCO DEVNET

LEARN CODE INSPIRE CONNECT

developer.cisco.com

@CiscoDevNet

facebook.com/ciscodevnet/

http://github.com/CiscoDevNet

https://developer.cisco.com/sandbox

Twitter: @hfpreston | Email: hapresto@cisco.com