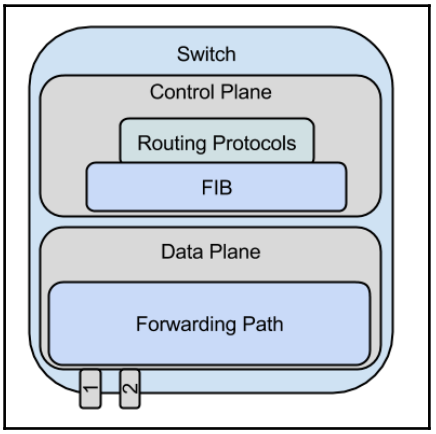
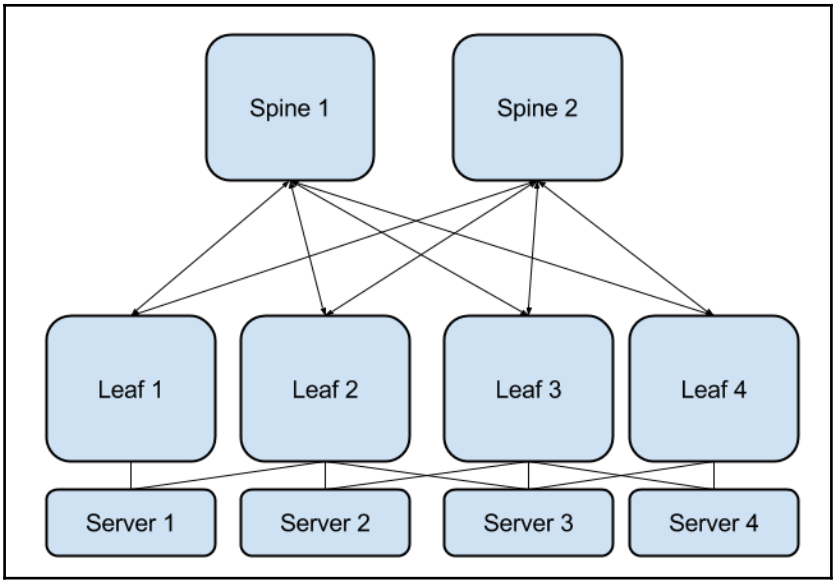
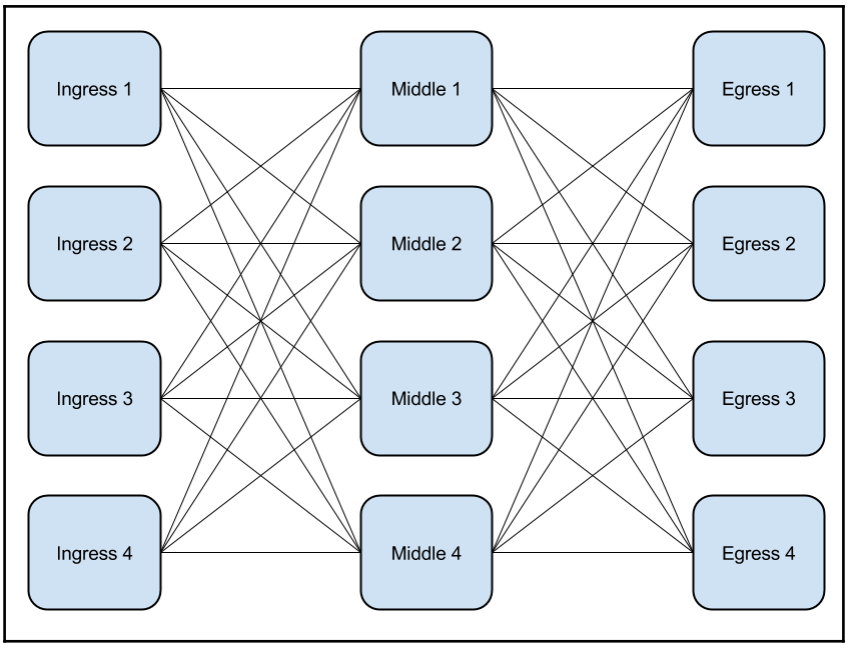
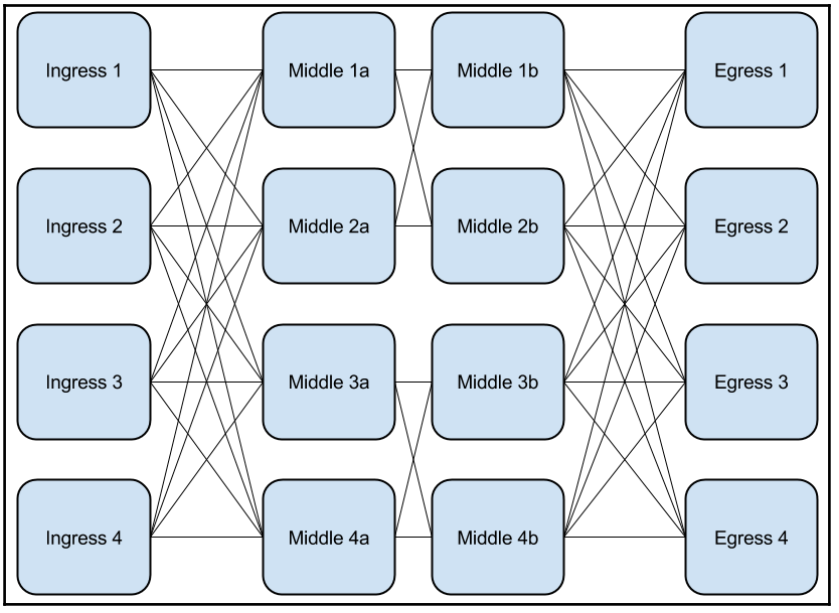
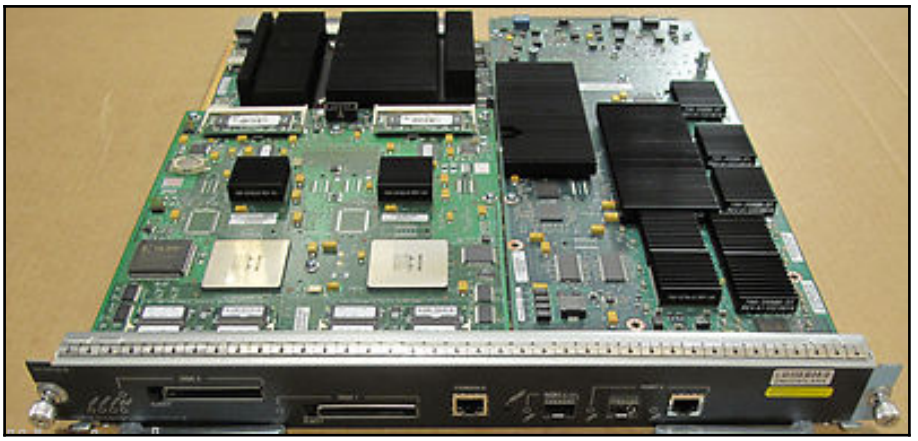
Chapter 1: Open and Proprietary Next Generation Networks

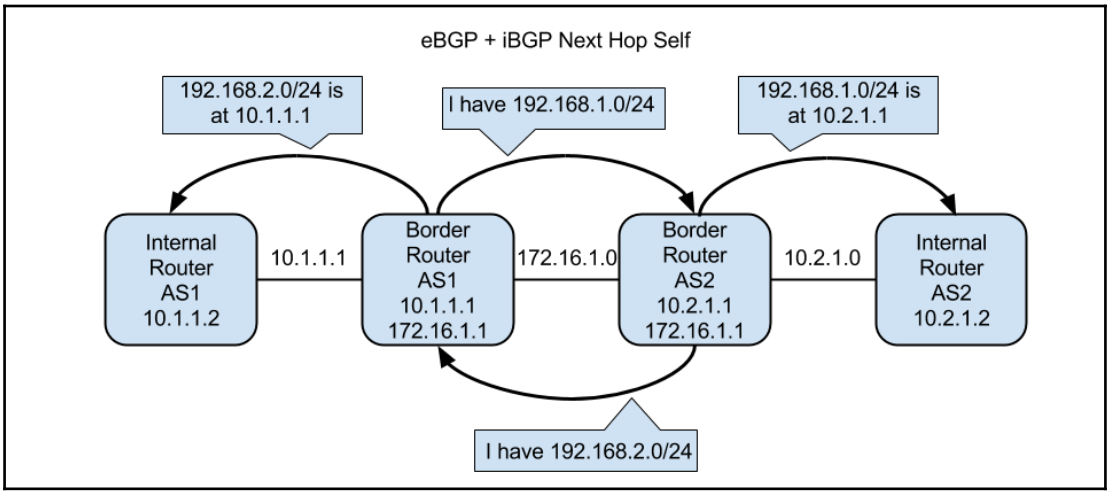


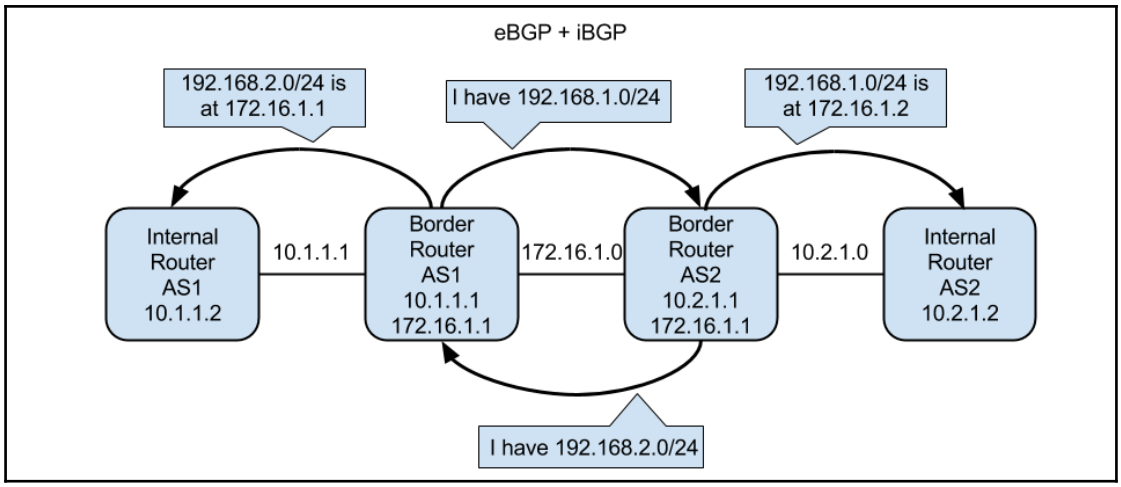


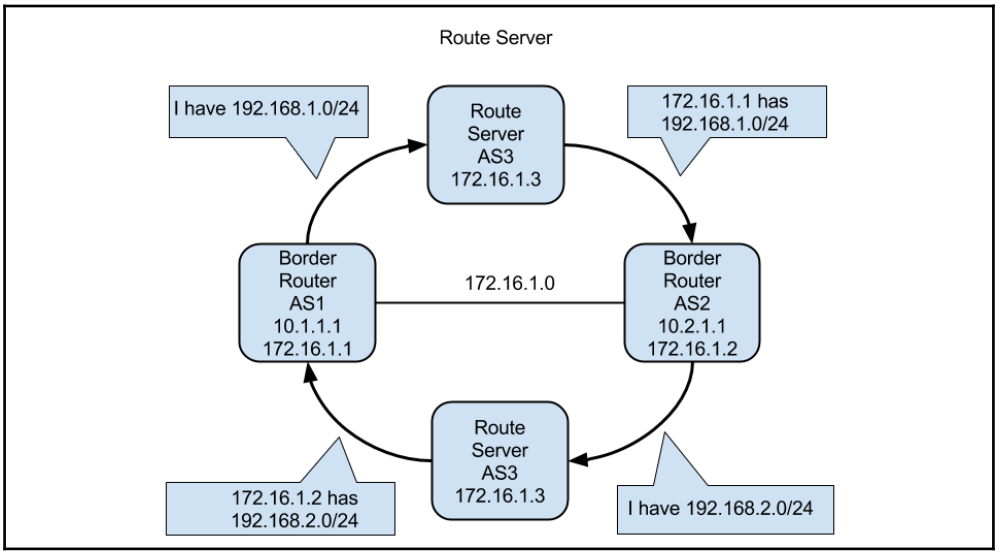

Ingress 1
Ingress 2
Ingress 3
Ingress 4
Middle 1
Middle 2
Middle 3
Middle 4
Egress 1
Egress 2
Egress 3
Egress 4

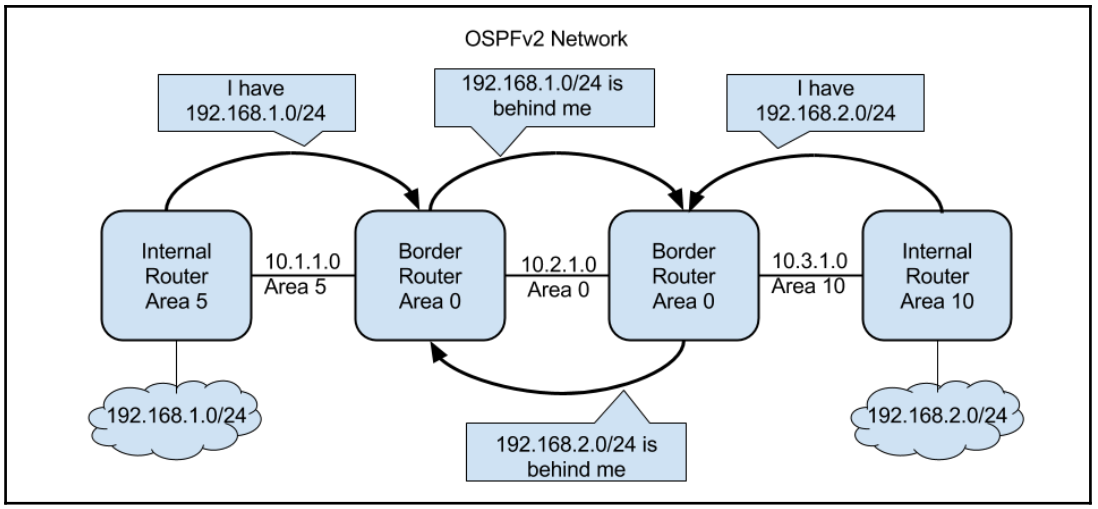

Ingress 1
Ingress 2
Ingress 3
Ingress 4
Middle 1a
Middle 2a
Middle 3a
Middle 4a
Middle 1b
Middle 2b
Middle 3b
Middle 4b
Egress 1
Egress 2
Egress 3
Egress 4

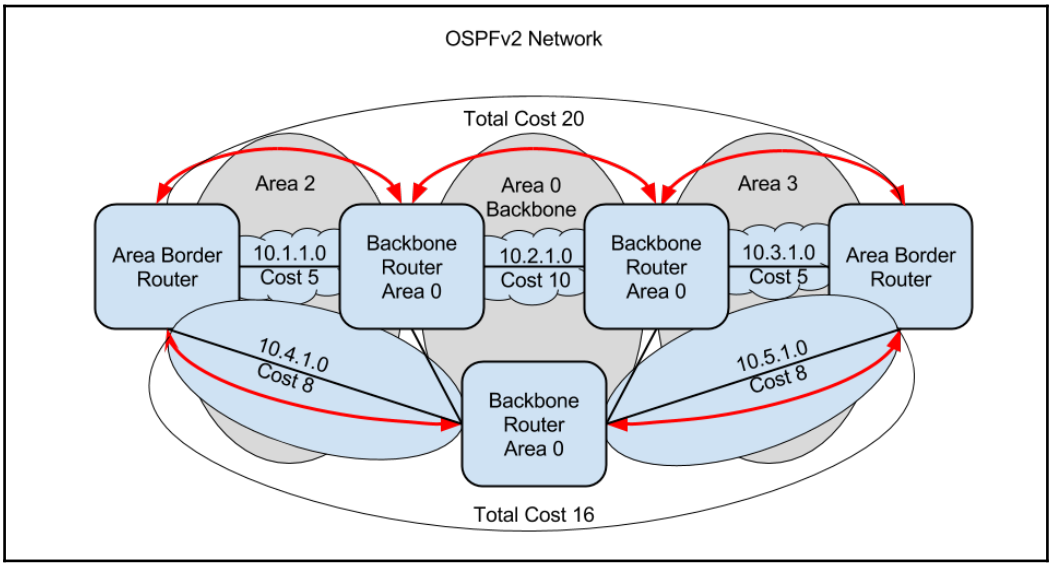


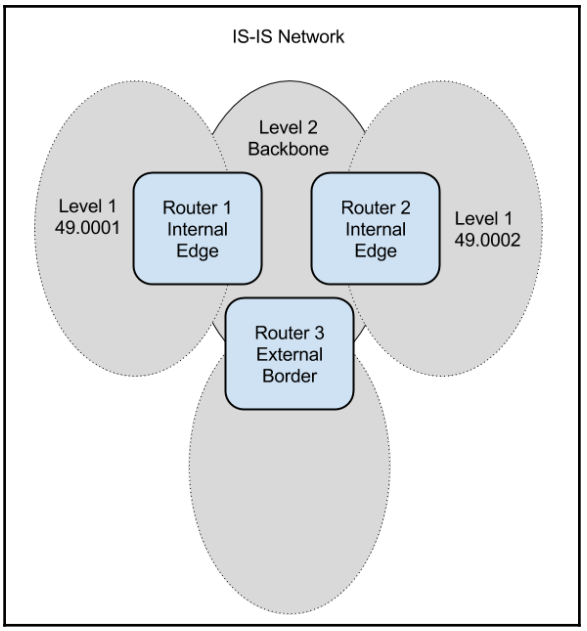

eBGP + iBGP Next Hop Self
192.168.2.0/24 is at 10.1.1.1
I have 192.168.1.0/24
192.168.1.0/24 is at 10.2.1.1
Internal Router AS1 10.1.1.2
10.1.1.1
Border Router AS1 10.1.1.1 172.16.1.1
172.16.1.0
Border Router AS2 10.2.1.1 172.16.1.1
10.2.1.0
Internal Router AS2 10.2.1.2
I have 192.168.2.0/24

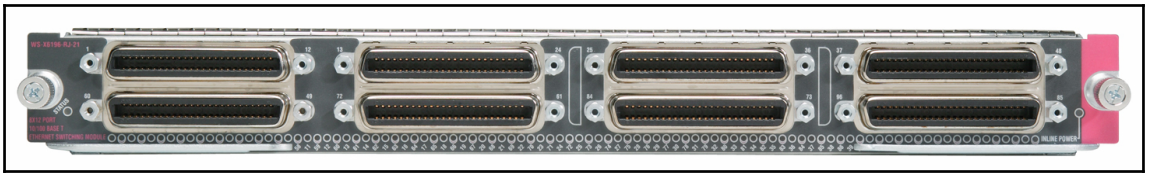

eBGP + iBGP
192.168.2.0/24 is at 172.16.1.1
I have 192.168.1.0/24
192.168.1.0/24 is at 172.16.1.2
Internal Router AS1 10.1.1.2
10.1.1.1
Border Router AS1 10.1.1.1 172.16.1.1
172.16.1.0
Border Router AS2 10.2.1.1 172.16.1.1
10.2.1.0
Internal Router AS2 10.2.1.2
I have 192.168.2.0/24


Route Server
I have 192.168.1.0/24
Route Server AS3 172.16.1.3
172.16.1.1 has 192.168.1.0/24
Border Router AS1 10.1.1.1 172.16.1.1
172.16.1.0
Border Router AS2 10.2.1.1 172.16.1.2
Route Server AS3 172.16.1.3
172.16.1.2 has 192.168.2.0/24
I have 192.168.2.0/24

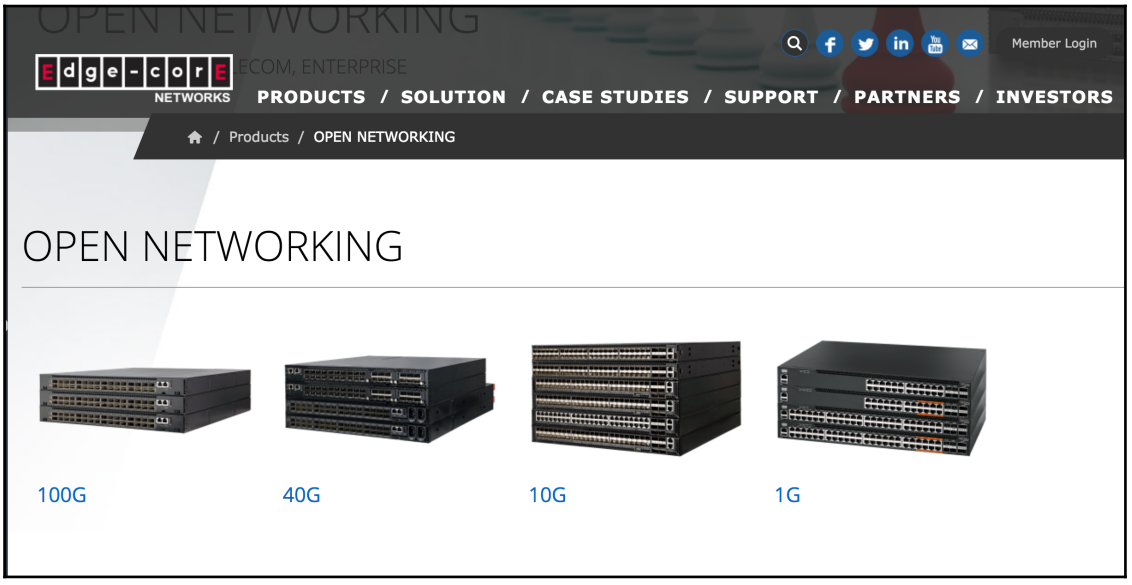

OSPFv2 Network
I have
192.168.1.0/24
192.168.1.0/24 is
behind me
I have
192.168.2.0/24
Internal
Router
Area 5
10.1.1.0
Area 5
Border
Router
Area 0
10.2.1.0
Area 0
Border
Router
Area 0
10.3.1.0
Area 10
Internal
Router
Area 10
192.168.1.0/24
192.168.2.0/24 is
behind me
192.168.2.0/24


OSPFv2 Network
Total Cost 20
Area 2
Area 0
Backbone
Area 3
Area Border
Router
10.1.1.0
Cost 5
Backbone
Router
Area 0
10.2.1.0
Cost 10
Backbone
Router
Area 0
10.3.1.0
Cost 5
Area Border
Router
10.4.1.0
Cost 8
10.5.1.0
Cost 8
Backbone
Router
Area 0
Total Cost 16

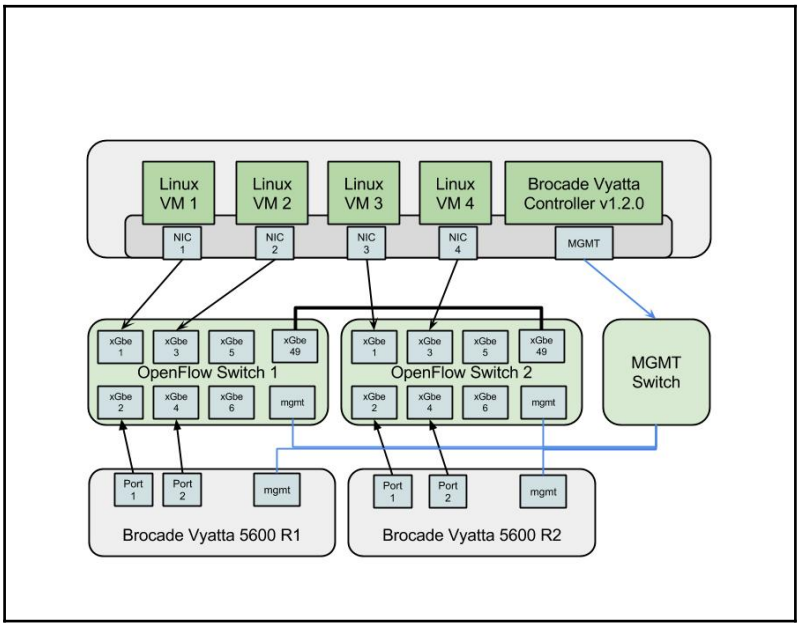

IS-IS Network
Level 2
Backbone
Level 1
49.0001
Router 1
Internal
Edge
Router 2
Internal
Edge
Level 1
49.0002
Router 3
External
Border

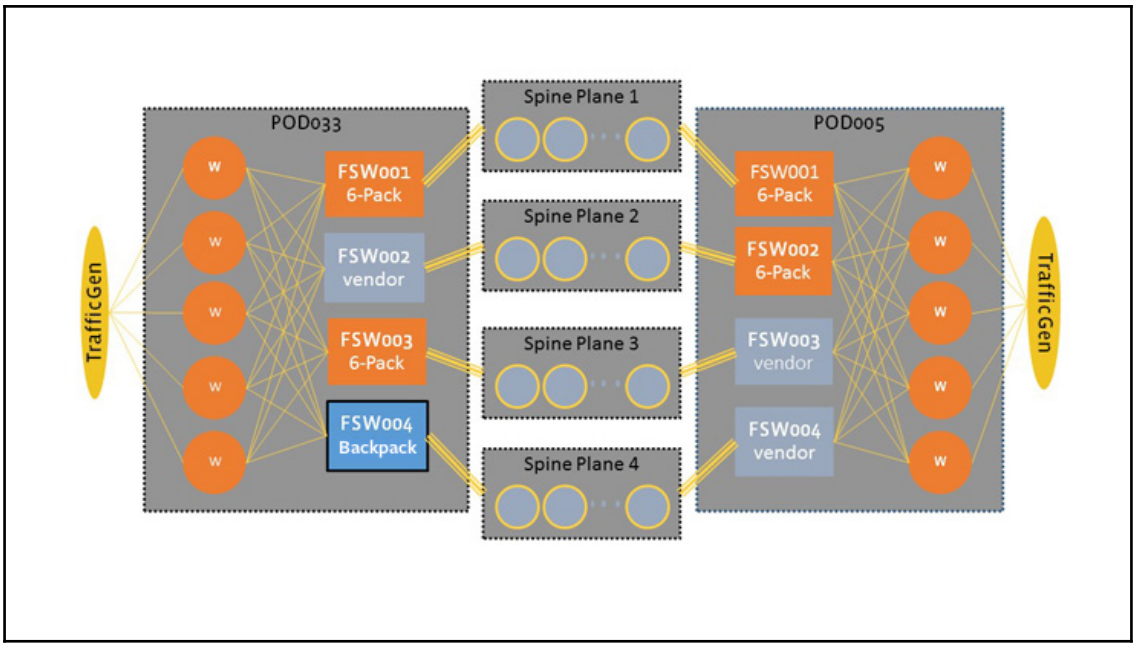


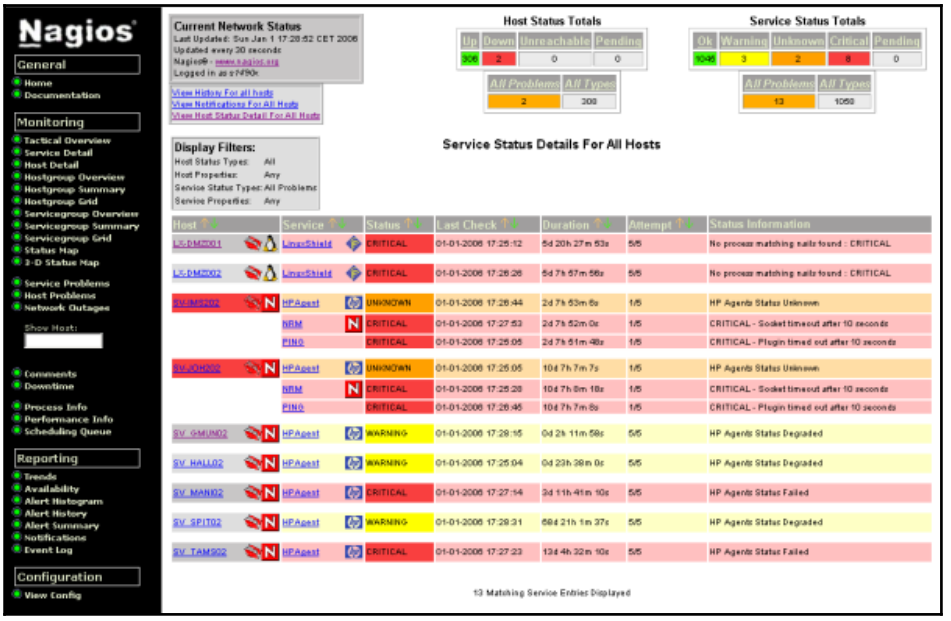
Juniper
M40
M40

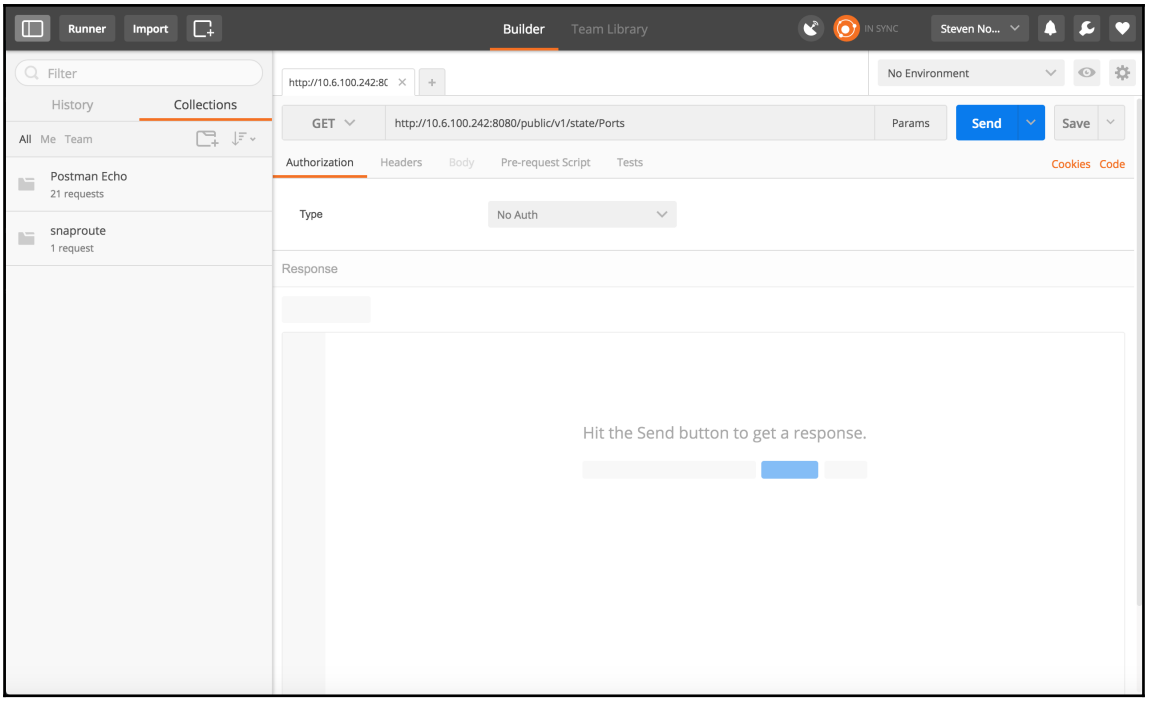

OPEN NETWORKING
Edge-corE
NETWORKS
ECOM, ENTERPRISE
Member Login
PRODUCTS / SOLUTION / CASE STUDIES / SUPPORT / PARTNERS / INVESTORS
/ Products / OPEN NETWORKING
OPEN NETWORKING
100G
40G
10G
1G

6-pack
Wedge-100


Linux VM 1
Linux VM 2
Linux VM 3
Linux VM 4
Brocade Vyatta Controller v1.2.0
NIC 1
NIC 2
NIC 3
NIC 4
MGMT
xGbe 1
xGbe 3
xGbe 5
xGbe 49
OpenFlow Switch 1
xGbe 2
xGbe 4
xGbe 6
mgmt
OpenFlow Switch 2
MGMT Switch
Port 1
Port 2
Brocade Vyatta 5600 R1
Brocade Vyatta 5600 R2

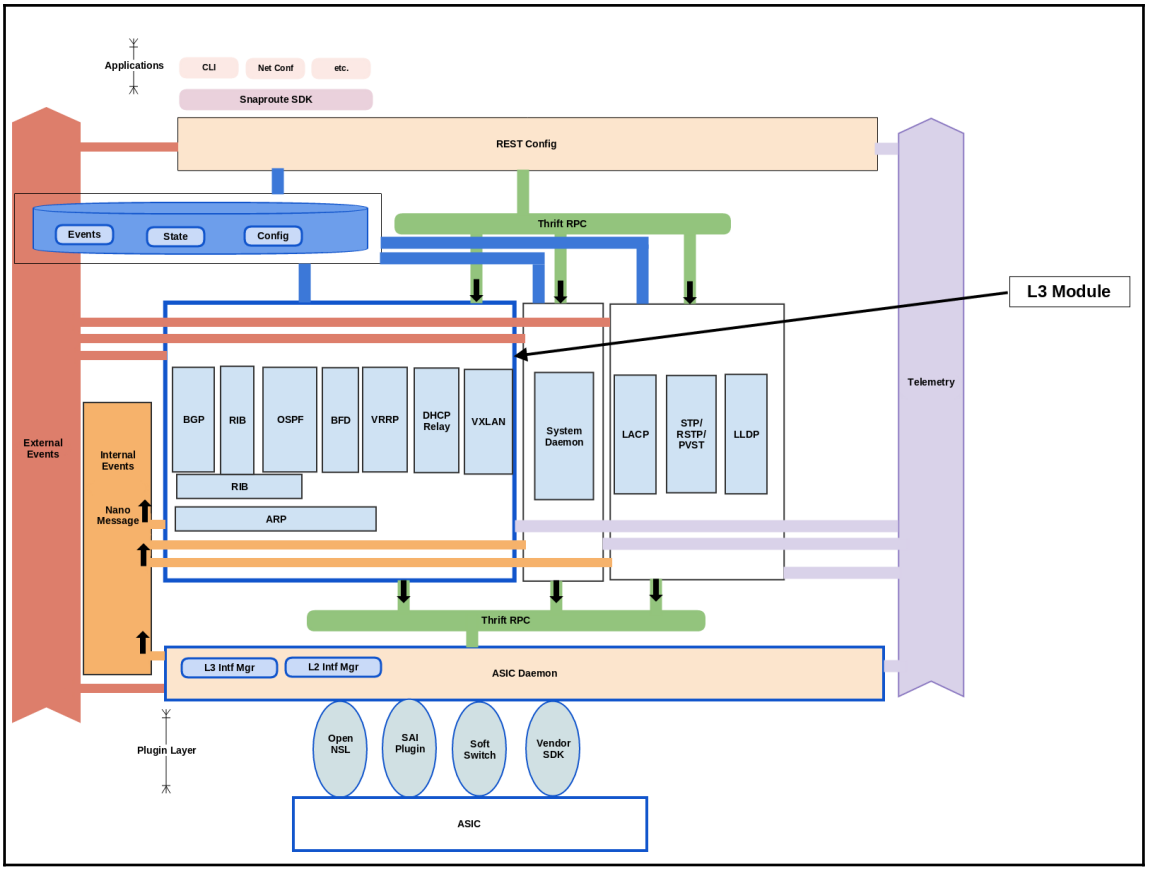

POD033
W
W
W
W
W
FSW001
6-Pack
FSW002
vendor
FSW003
6-Pack
FSW004
Backpack
Spine Plane 1
Spine Plane 2
Spine Plane 3
Spine Plane 4
POD005
FSW001
6-Pack
FSW002
6-Pack
FSW003
vendor
FSW004
vendor
W
W
W
W
W
TrafficGen
TrafficGen


Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overview
Servicegroup Summary
Servicegroup Grid
Status Map
3-D Status Map
Service Problems
Host Problems
Network Outages
Show Host:
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Current Network Status
Last Update: Sun Jan 1 17:28:52 CET 2006
Updated every 30 seconds
Nagios® - www.nagios.org
Logged in as n7490x
View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts
Display Filters:
Host Status Types: All
Host Properties: Any
Service Status Types: All Problems
Service Properties: Any
Host Status Totals
Up Down Unreachable Pending
306 2 0 0
All Problems All Types
2 308
Service Status Totals
Ok Warning Unknown Critical Pending
1045 3 2 8 0
All Problems All Types
13 1058
Service Status Details For All Hosts
Host Service Status Last Check Duration Attempt Status Information
LX-DMZ001 LinuxShield CRITICAL 01-01-2006 17:25:12 5d 20h 27m 53s 5/5 No process matching nails found : CRITICAL
LX-DMZ002 LinuxShield CRITICAL 01-01-2006 17:26:26 5d 7h 57m 56s 5/5 No process matching nails found : CRITICAL
SV-IMS202 HPAgent UNKNOWN 01-01-2006 17:26:44 2d 7h 53m 6s 1/5 HP Agents Status Unknown
NRM CRITICAL 01-01-2006 17:27:53 2d 7h 52m 0s 1/5 CRITICAL - Socket timeout after 10 seconds
PING CRITICAL 01-01-2006 17:25:05 2d 7h 51m 48s 1/5 CRITICAL - Plugin timed out after 10 seconds
SV-JOH202 HPAgent UNKNOWN 01-01-2006 17:25:05 10d 7h 7m 7s 1/5 HP Agents Status Unknown
NRM CRITICAL 01-01-2006 17:25:28 10d 7h 6m 18s 1/5 CRITICAL - Socket timeout after 10 seconds
PING CRITICAL 01-01-2006 17:26:45 10d 7h 7m 8s 1/5 CRITICAL - Plugin timed out after 10 seconds
SV-GMUN02 HPAgent WARNING 01-01-2006 17:28:15 0d 2h 11m 58s 5/5 HP Agents Status Degraded
SV-HALL02 HPAgent WARNING 01-01-2006 17:25:04 0d 23h 38m 0s 5/5 HP Agents Status Degraded
SV-MAN02 HPAgent CRITICAL 01-01-2006 17:27:14 3d 11h 41m 10s 5/5 HP Agents Status Failed
SV-SPIT02 HPAgent WARNING 01-01-2006 17:28:31 68d 21h 1m 37s 5/5 HP Agents Status Degraded
SV-TAM902 HPAgent CRITICAL 01-01-2006 17:27:23 13d 4h 32m 10s 5/5 HP Agents Status Failed
13 Matching Service Entries Displayed


Runner
Import
Builder
Team Library
IN SYNC
Steven No...
Filter
History
Collections
All
Me
Team
Postman Echo
21 requests
snaproute
1 request
http://10.6.100.242:8C
No Environment
GET
http://10.6.100.242:8080/public/v1/state/Ports
Params
Send
Save
Authorization
Headers
Body
Pre-request Script
Tests
Cookies
Code
Type
No Auth
Response
Hit the Send button to get a response.

Chapter 2: Networking Hardware and Software

```
                    GNU GRUB  version 2.02~beta2+e4a1fe391

 +----------------------------------------------------------------------------+
 |*ONIE: Install OS                                                           |
 | ONIE: Rescue                                                               |
 | ONIE: Uninstall OS                                                         |
 | ONIE: Update ONIE                                                          |
 | ONIE: Embed ONIE                                                           |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 |                                                                            |
 +----------------------------------------------------------------------------+

      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS, `e' to edit the commands
      before booting or `c' for a command-line.
```


Applications
CLI
Net Conf
etc.
Snaproute SDK
REST Config
Events
State
Config
Thrift RPC
L3 Module
Telemetry
External Events
Internal Events
Nano Message
BGP
RIB
OSPF
BFD
VRRP
DHCP Relay
VXLAN
System Daemon
LACP
STP/ RSTP/ PVST
LLDP
RIB
ARP
Thrift RPC
L3 Intf Mgr
L2 Intf Mgr
ASIC Daemon
Plugin Layer
Open NSL
SAI Plugin
Soft Switch
Vendor SDK
ASIC

Postman

Runner Import Builder Team Library IN SYNC Steven No...

Filter

History Collections

Save to collection

Today

GET http://10.6.100.242:8080/public/v1/state/Ports

Yesterday

GET http://10.6.100.242:8080/public/v1/config/Ports

GET http://10.6.100.242:8080/public/v1/state/ArpEntrys

July 29

GET http://10.7.1.77:8080/public/v1/config/Ports

July 26

GET http://10.6.100.128:8080/public/v1/config/Ports

GET http://10.6.100.128:8080/public/v1/state/IPv4Intfs

GET http://wedge-t:8080/public/v1/state/IPv4Intfs

July 16

http://10.6.100.242:8(

No Environment

GET http://10.6.100.242:8080/public/v1/state/Ports Params Send Save

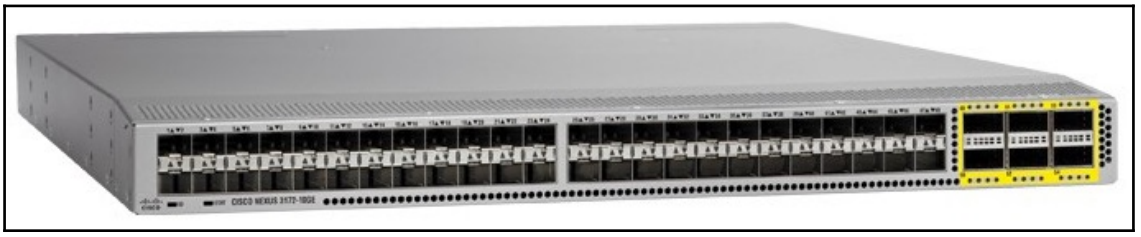
Authorization Headers Body Pre-request Script Tests Cookies Code

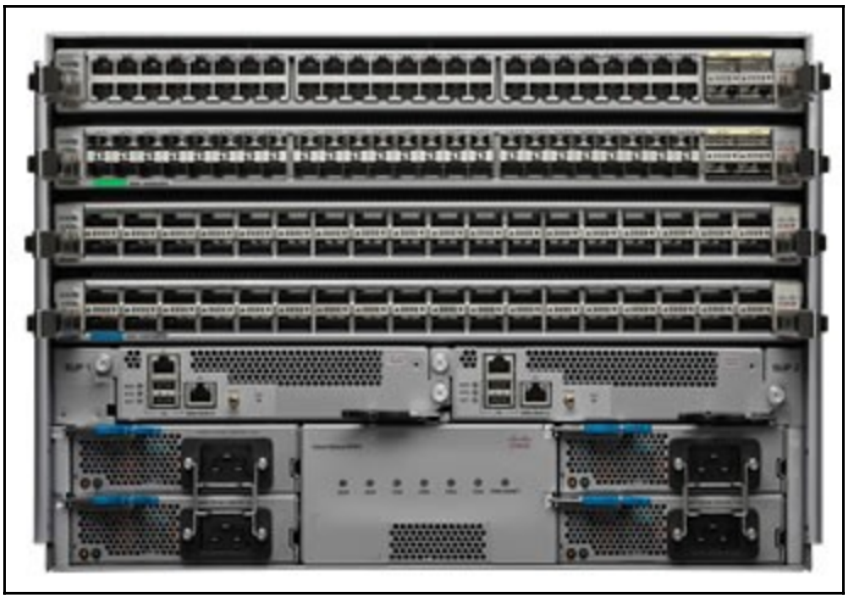
Type No Auth

Body Cookies Headers (3) Tests Status: 200 OK Time: 248 ms Size: 128.82 KB

Pretty Raw Preview JSON

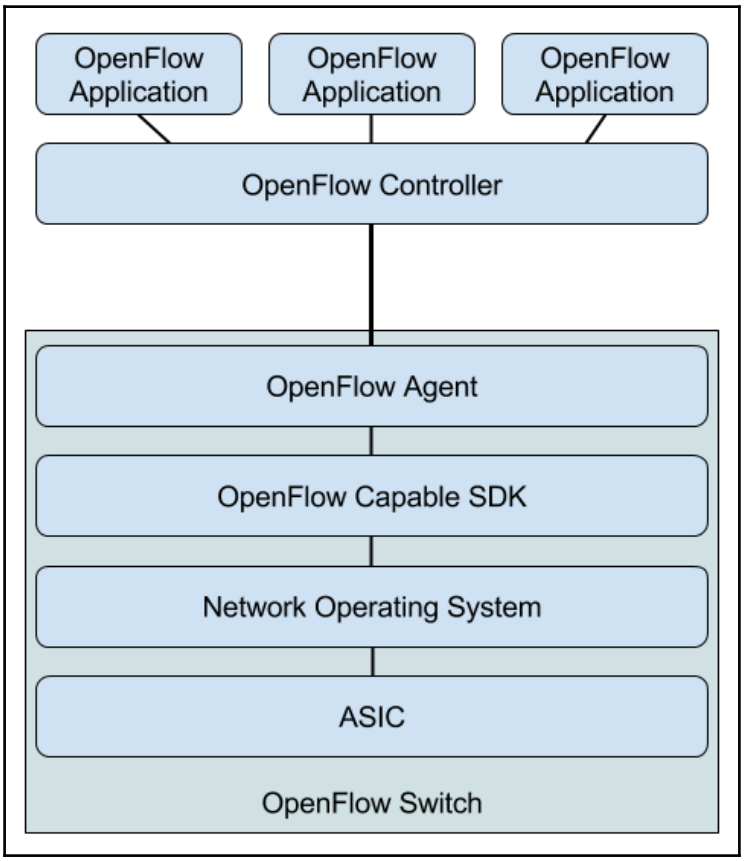

```
{
  "MoreExist": false,
  "ObjCount": 160,
  "CurrentMarker": 0,
  "NextMarker": 160,
  "Objects": [
    {
      "ObjectId": "ae0a7260-1850-4b79-4f9b-d77a8a5265a1",
      "Object": {
        "IntfRef": "fpPort6",
        "IfIndex": 0,
        "Name": "fpPort6",
        "OperState": "DOWN",
        "NumUpEvents": 0,
        "LastUpEventTime": "",
        "NumDownEvents": 0,
        "LastDownEventTime": "",
        "Pvid": 4095,
        "IfInOctets": 0,
        "IfInUcastPkts": 0,
        "IfInDiscards": 0,
        "IfInErrors": 0,
        "IfInUnknownProtos": 0,
        "IfOutOctets": 0,
```

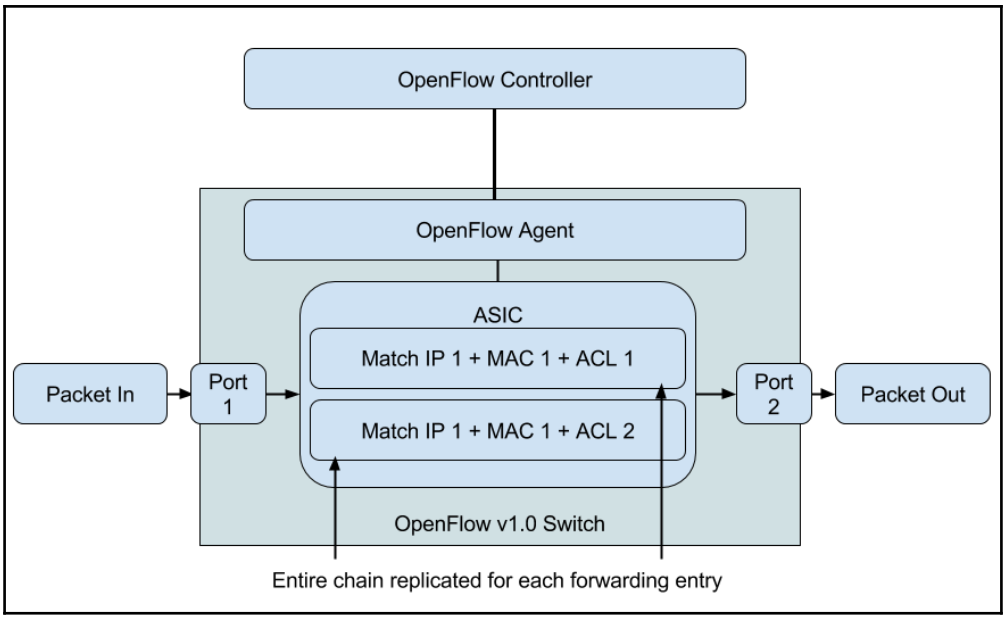


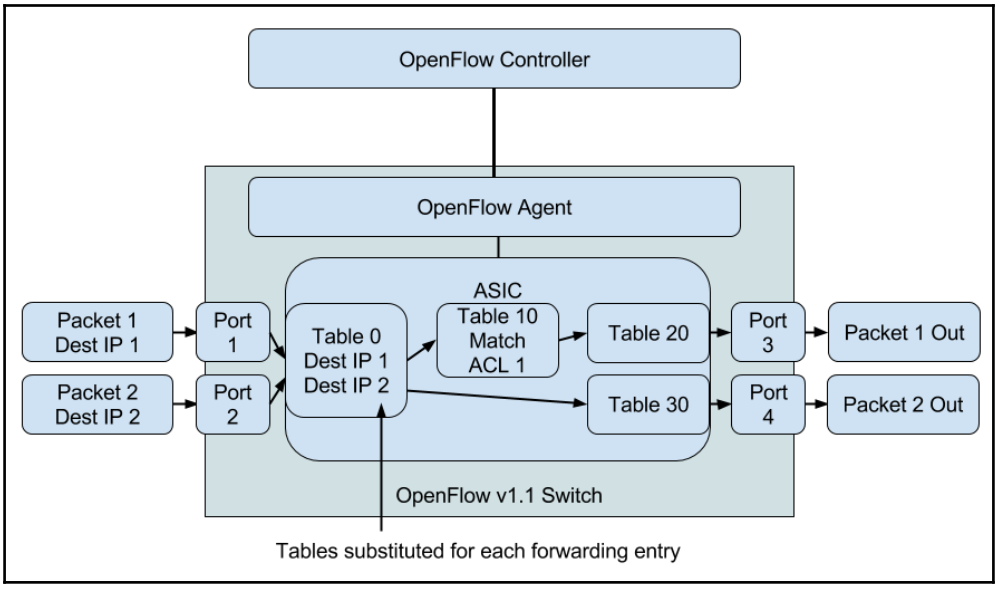


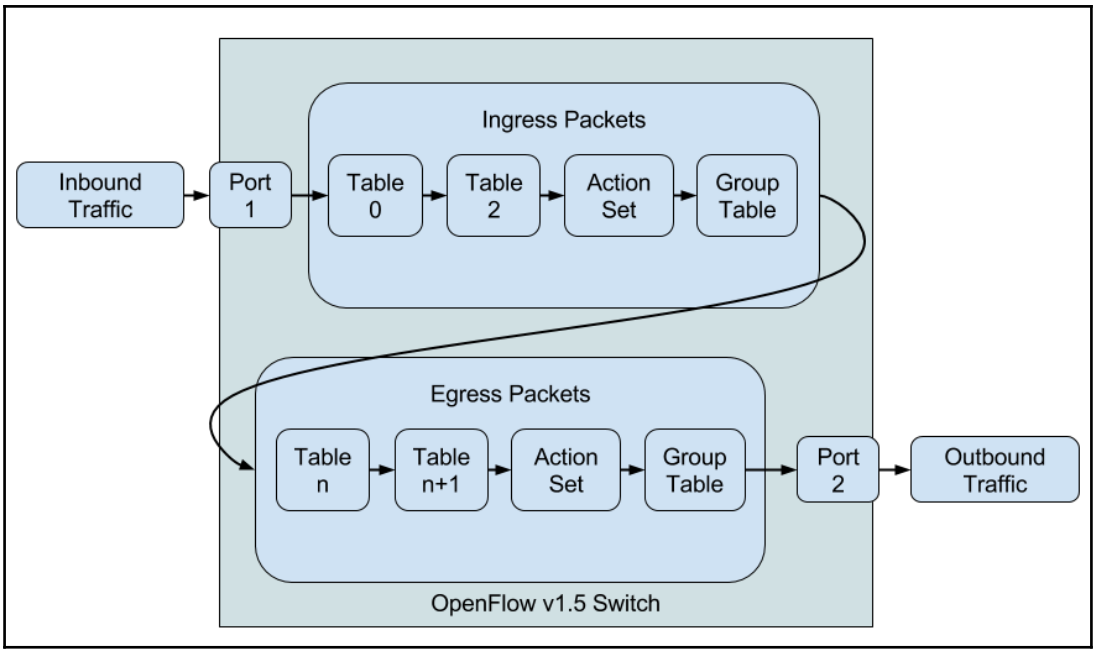
DELL
Z9100

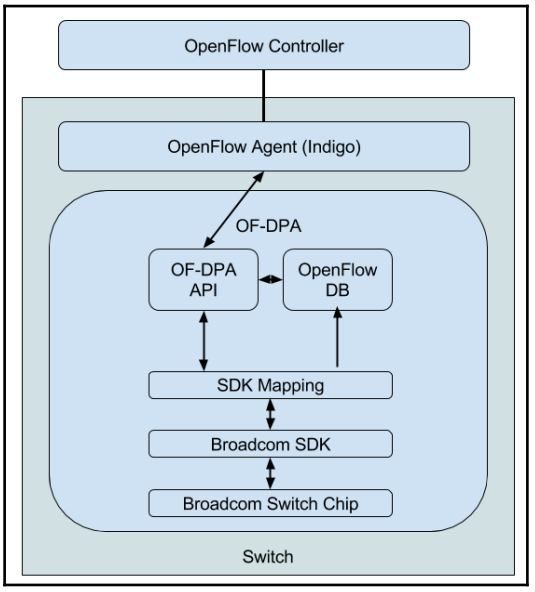
Chapter 3: Exploring OpenFlow

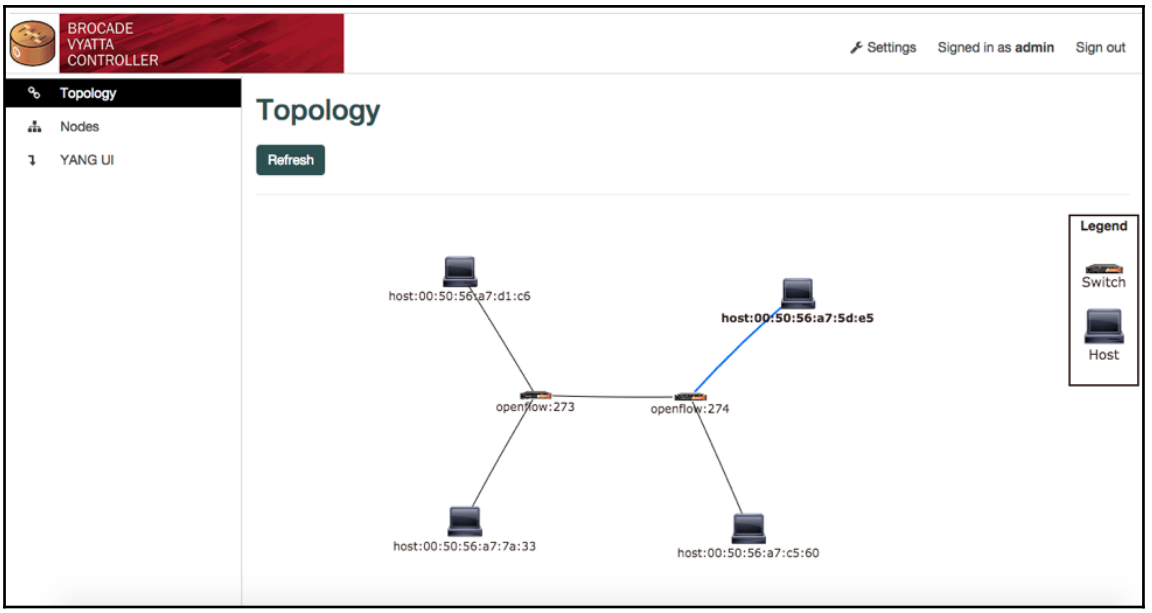


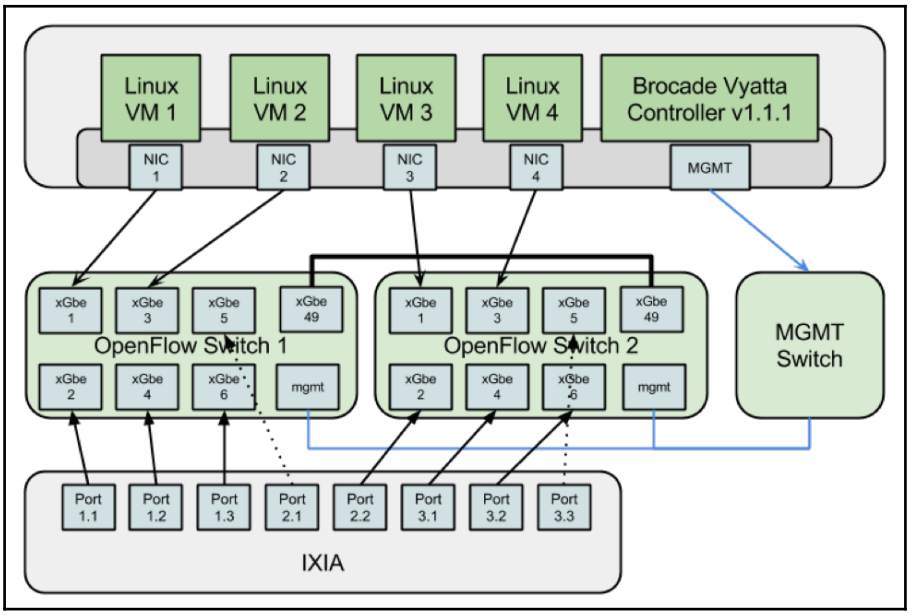

OpenFlow Controller
OpenFlow Agent
ASIC
Match IP 1 + MAC 1 + ACL 1
Match IP 1 + MAC 1 + ACL 2
Packet In
Port 1
Port 2
Packet Out
OpenFlow v1.0 Switch
Entire chain replicated for each forwarding entry


OpenFlow Controller
OpenFlow Agent
ASIC
Packet 1
Dest IP 1
Packet 2
Dest IP 2
Port 1
Port 2
Table 0
Dest IP 1
Dest IP 2
Table 10
Match
ACL 1
Table 20
Table 30
Port 3
Port 4
Packet 1 Out
Packet 2 Out
OpenFlow v1.1 Switch
Tables substituted for each forwarding entry

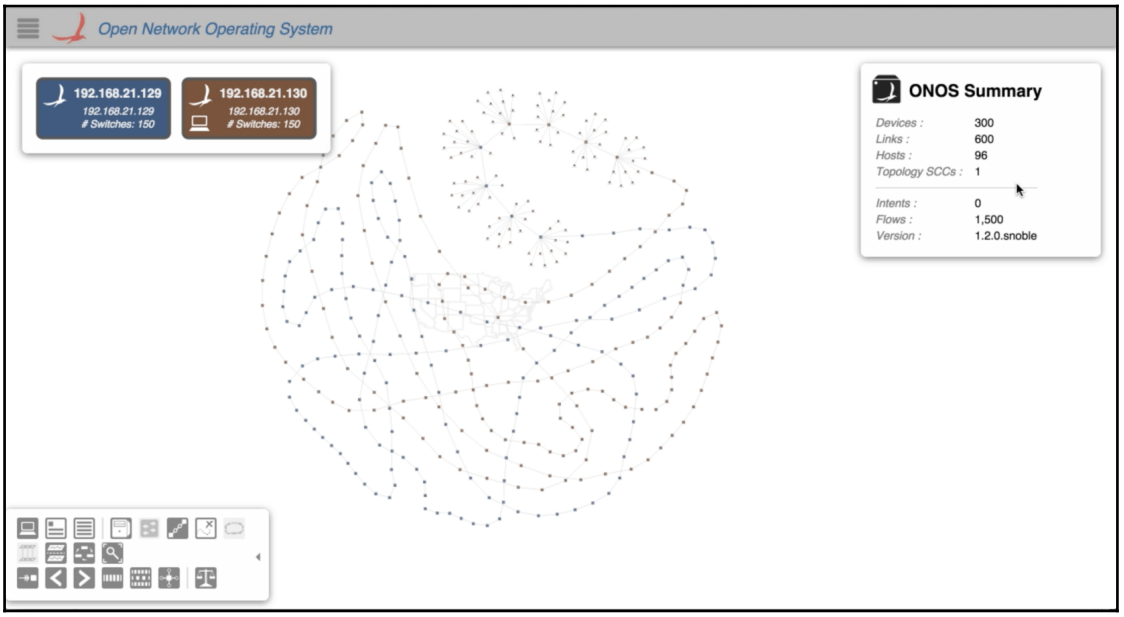

Inbound Traffic
Port 1
Ingress Packets
Table 0
Table 2
Action Set
Group Table
Egress Packets
Table n
Table n+1
Action Set
Group Table
Port 2
Outbound Traffic
OpenFlow v1.5 Switch


OpenFlow Controller
OpenFlow Agent (Indigo)
OF-DPA
OF-DPA API
OpenFlow DB
SDK Mapping
Broadcom SDK
Broadcom Switch Chip
Switch

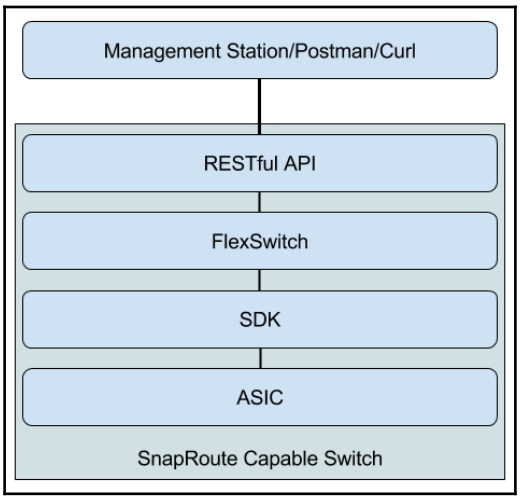

BROCADE
VYATTA
CONTROLLER
Settings
Signed in as admin
Sign out
Topology
Nodes
YANG UI
Topology
Refresh
Legend
Switch
Host
host:00:50:56:a7:d1:c6
host:00:50:56:a7:5d:e5
openflow:273
openflow:274
host:00:50:56:a7:7a:33
host:00:50:56:a7:c5:60

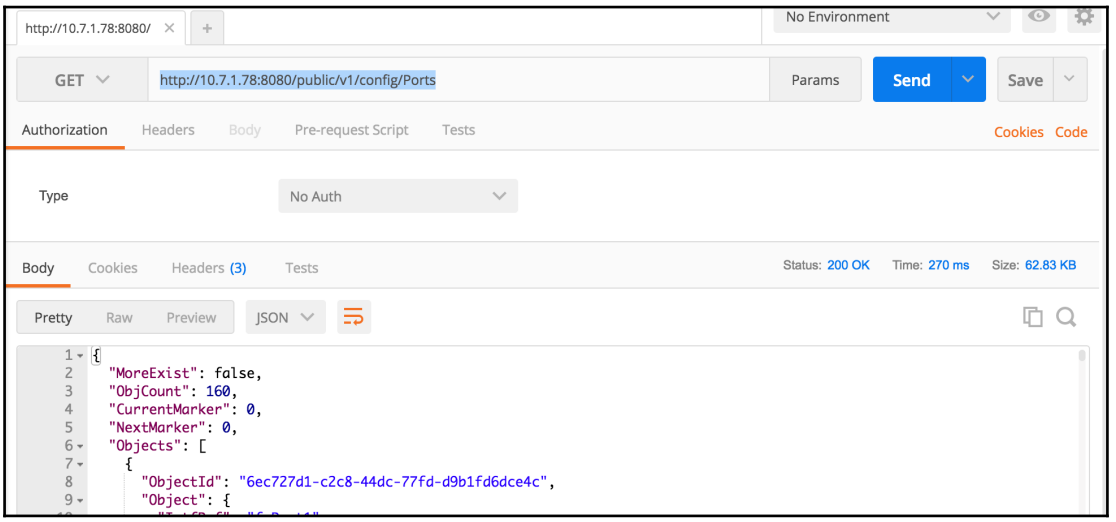

Linux VM 1
Linux VM 2
Linux VM 3
Linux VM 4
Brocade Vyatta Controller v1.1.1
NIC 1
NIC 2
NIC 3
NIC 4
MGMT
xGbe 1
xGbe 3
xGbe 5
xGbe 49
xGbe 2
xGbe 4
xGbe 6
mgmt
OpenFlow Switch 1
OpenFlow Switch 2
MGMT Switch
Port 1.1
Port 1.2
Port 1.3
Port 2.1
Port 2.2
Port 3.1
Port 3.2
Port 3.3
IXIA

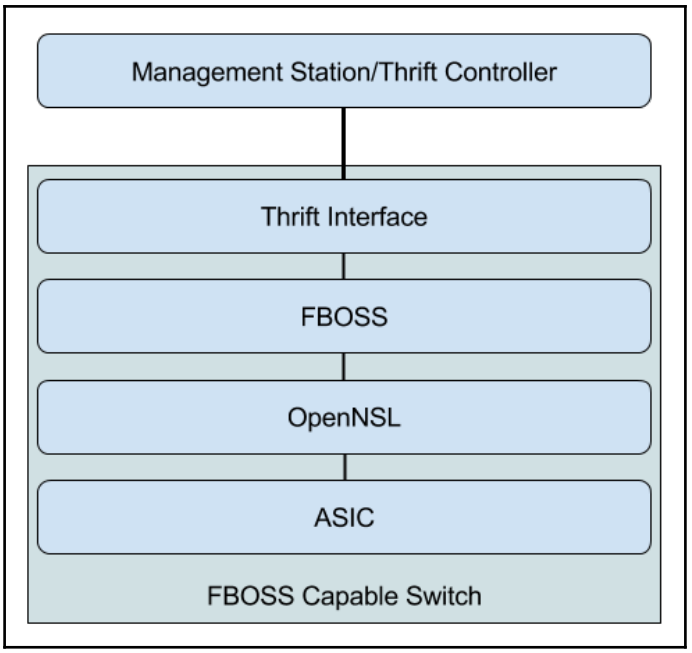
172.16.1.3 → 172.16.1.2
openflow:273
host:00:50:56:a7:7a:33:openflow:273:2 → openflow:273:2
openflow:273:1 → host:00:50:56:a7:d1:c6:openflow:273:1
172.16.1.2 → 172.16.1.3
openflow:273
host:00:50:56:a7:d1:c6:openflow:273:1 → openflow:273:1
openflow:273:2 → host:00:50:56:a7:7a:33:openflow:273:2
172.16.1.2 → 172.16.1.4
openflow:274
openflow:273
host:00:50:56:a7:d1:c6:openflow:273:1 → openflow:273:1
openflow:273:49 → openflow:274:49
openflow:274:49 → openflow:273:49
openflow:273:49 → openflow:274:49
openflow:274:1 → host:00:50:56:a7:5d:e5:openflow:274:1
Bi-directional Links
Closer
Default
Relaxed
172.16.1.2(host:00:50:56:a7:d1:c6)
172.16.1.4(host:00:50:56:a7:5d:e5)


Open Network Operating System
192.168.21.129
192.168.21.129
Switches: 150
192.168.21.130
192.168.21.130
Switches: 150
ONOS Summary
Devices : 300
Links : 600
Hosts : 96
Topology SCCs : 1
Intents : 0
Flows : 1,500
Version : 1.2.0.snoble

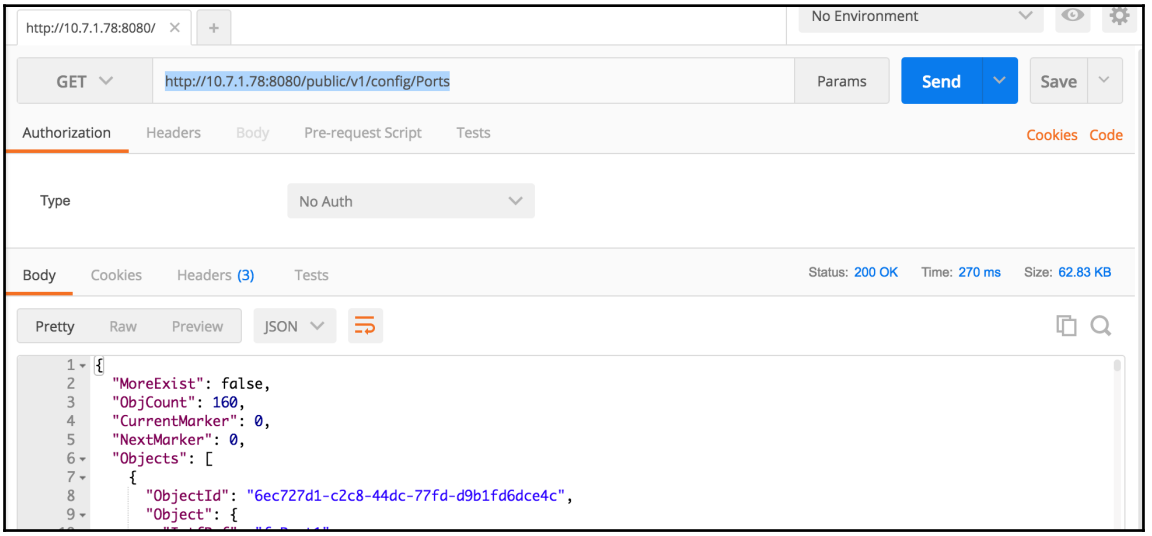
Chapter 4: Using REST and Thrift APIs to Manage Switches

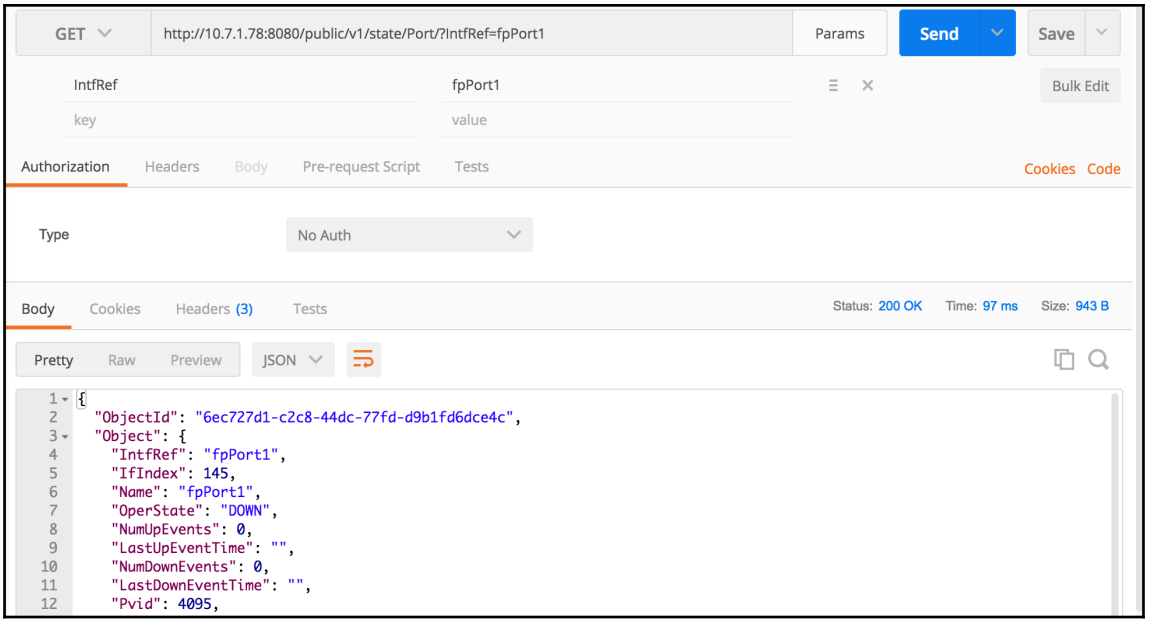


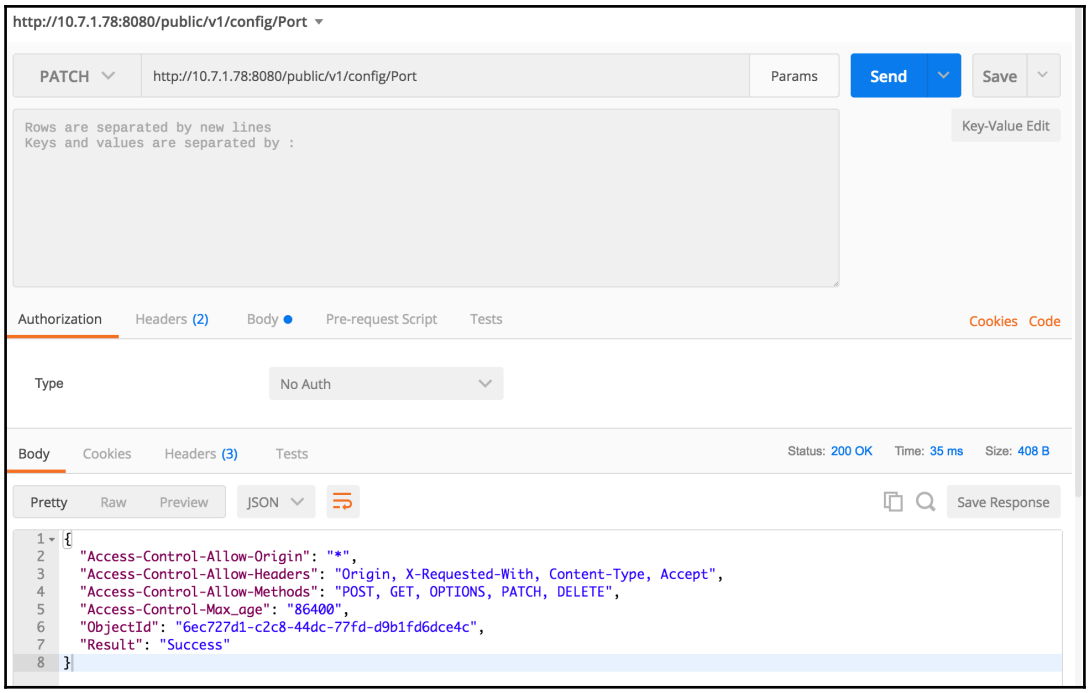



Management Station/Thrift Controller
Thrift Interface
FBOSS
OpenNSL
ASIC
FBOSS Capable Switch

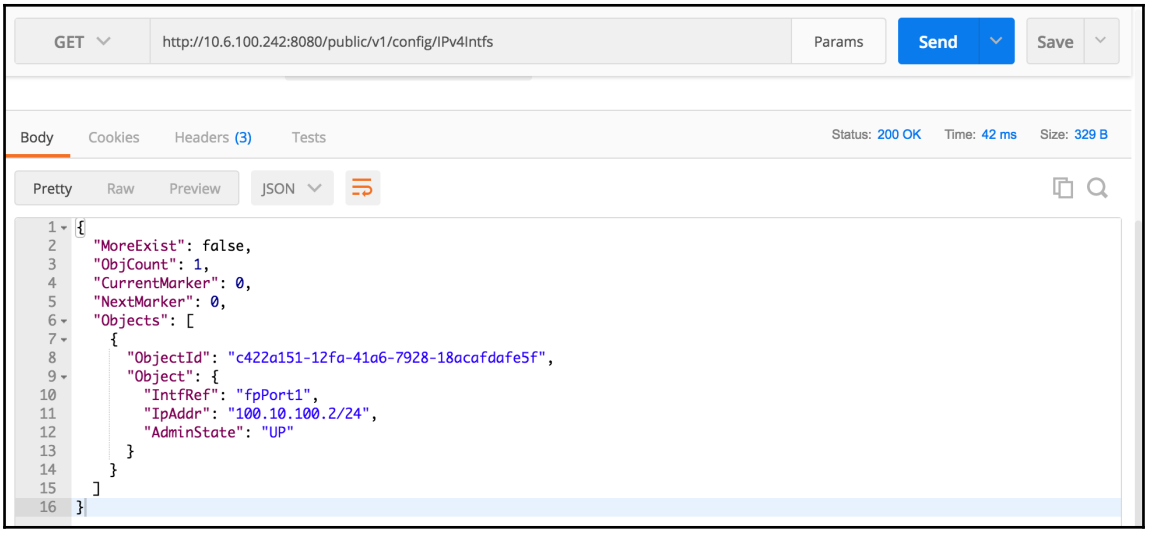
Chapter 5: Using Postman for REST API Calls

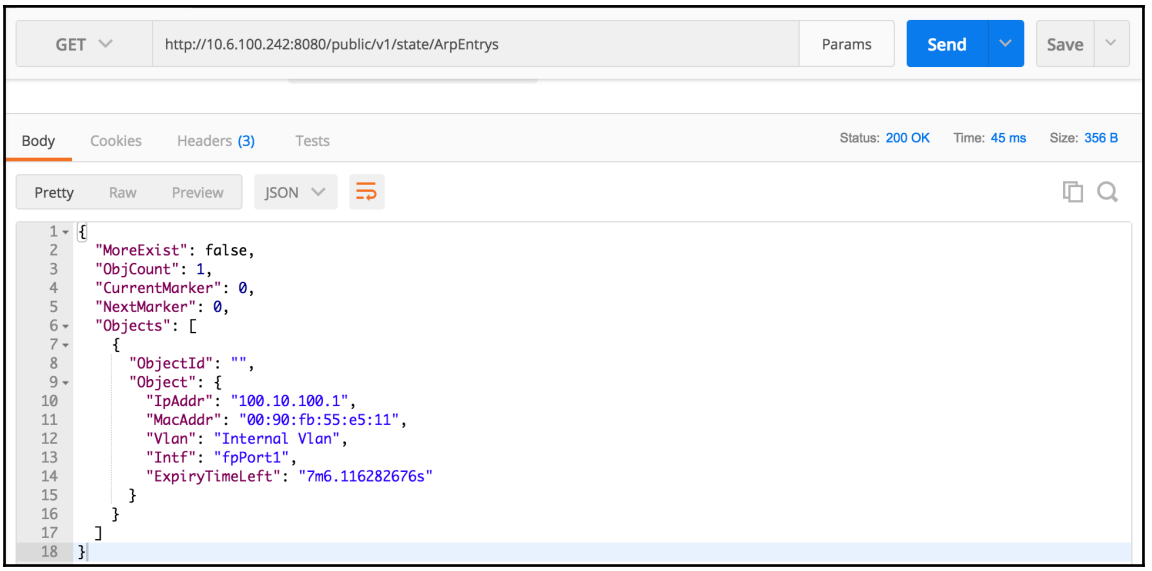




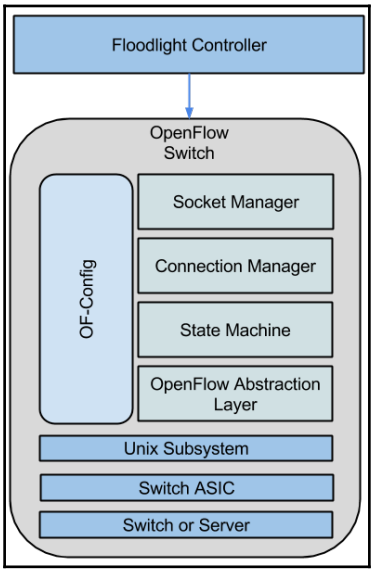

http://10.7.1.78:8080/public/v1/config/Port
PATCH
http://10.7.1.78:8080/public/v1/config/Port
Params
Send
Save
Rows are separated by new lines
Keys and values are separated by :
Key-Value Edit
Authorization
Headers (2)
Body
Pre-request Script
Tests
Cookies
Code
Type
No Auth
Body
Cookies
Headers (3)
Tests
Status: 200 OK
Time: 35 ms
Size: 408 B
Pretty
Raw
Preview
JSON
Save Response
{
"Access-Control-Allow-Origin": "*",
"Access-Control-Allow-Headers": "Origin, X-Requested-With, Content-Type, Accept",
"Access-Control-Allow-Methods": "POST, GET, OPTIONS, PATCH, DELETE",
"Access-Control-Max_age": "86400",
"ObjectId": "6ec727d1-c2c8-44dc-77fd-d9b1fd6dce4c",
"Result": "Success"
}

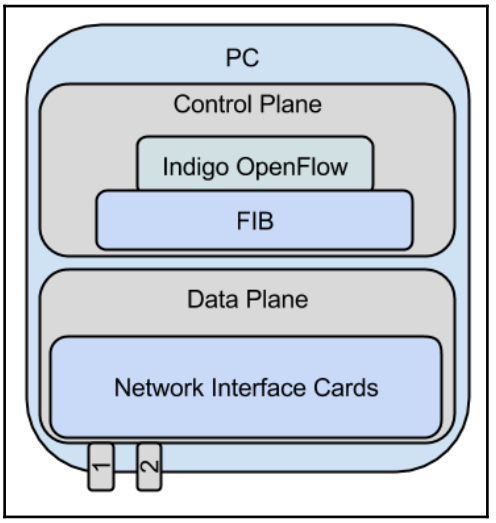
http://10.7.1.78:8080/public/v1/config/Port
PATCH
http://10.7.1.78:8080/public/v1/config/Port
Params
Send
Save
Rows are separated by new lines
Keys and values are separated by :
Key-Value Edit
Authorization
Headers (2)
Body
Pre-request Script
Tests
Cookies
Code
form-data
x-www-form-urlencoded
raw
binary
JSON (application/json)
{"IntfRef":"fpPort1","AdminState":"UP"}

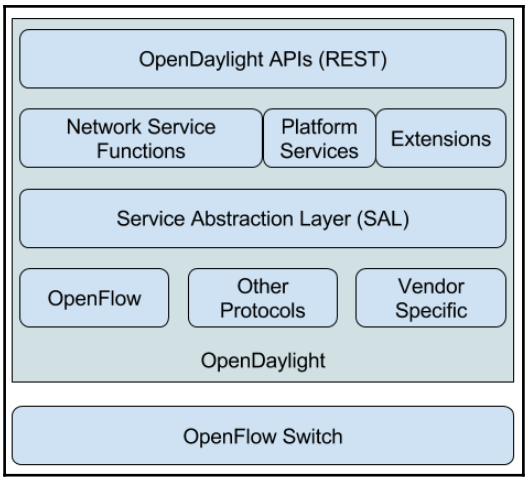

GET
http://10.6.100.242:8080/public/v1/config/IPv4Intfs
Params
Send
Save
Body
Cookies
Headers (3)
Tests
Status: 200 OK
Time: 42 ms
Size: 329 B
Pretty
Raw
Preview
JSON
{
"MoreExist": false,
"ObjCount": 1,
"CurrentMarker": 0,
"NextMarker": 0,
"Objects": [
{
"ObjectId": "c422a151-12fa-41a6-7928-18acafdafe5f",
"Object": {
"IntfRef": "fpPort1",
"IpAddr": "100.10.100.2/24",
"AdminState": "UP"
}
}
]
}


GET
http://10.6.100.242:8080/public/v1/state/ArpEntrys
Params
Send
Save
Body
Cookies
Headers (3)
Tests
Status: 200 OK
Time: 45 ms
Size: 356 B
Pretty
Raw
Preview
JSON
{
"MoreExist": false,
"ObjCount": 1,
"CurrentMarker": 0,
"NextMarker": 0,
"Objects": [
{
"ObjectId": "",
"Object": {
"IpAddr": "100.10.100.1",
"MacAddr": "00:90:fb:55:e5:11",
"Vlan": "Internal Vlan",
"Intf": "fpPort1",
"ExpiryTimeLeft": "7m6.116282676s"
}
}
]
}

Chapter 6: OpenFlow Deep Dive







THE LINUX FOUNDATION PROJECTS

OPENDAYLIGHT

About What We Do Use Cases and Users Ecosystem & Solutions Technical Community Support OpenDaylight

Downloads

Release	Edition	Version	Release date	Downloads	Virtual Machines	Documentation
Carbon	n/a	n/a	May 26, 2017	• Pre-Built Tar • Pre-Built Zip • NeXT UI • Virtual Tenant Network (VTN) Coordinator		• Getting Started Guide • Developers Guide • User Guide • Installation Guide • Using OpenDaylight with OpenStack • Release Notes

Download Ubuntu Server

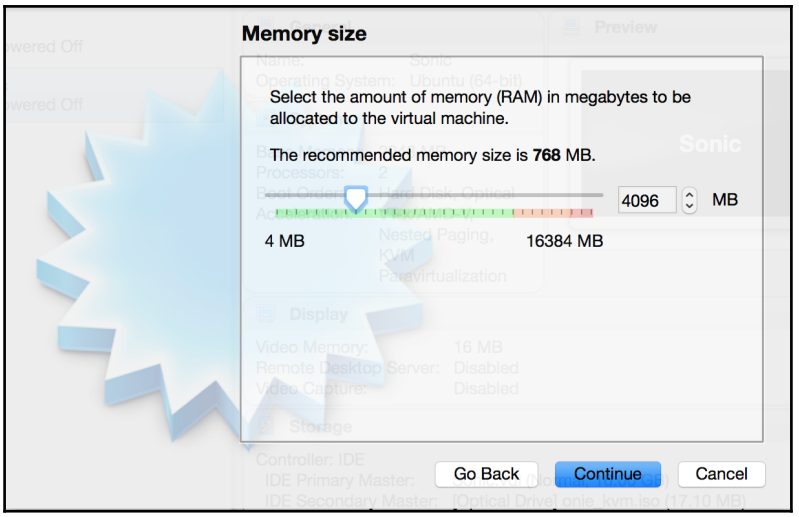
Ubuntu Server 16.04.2 LTS

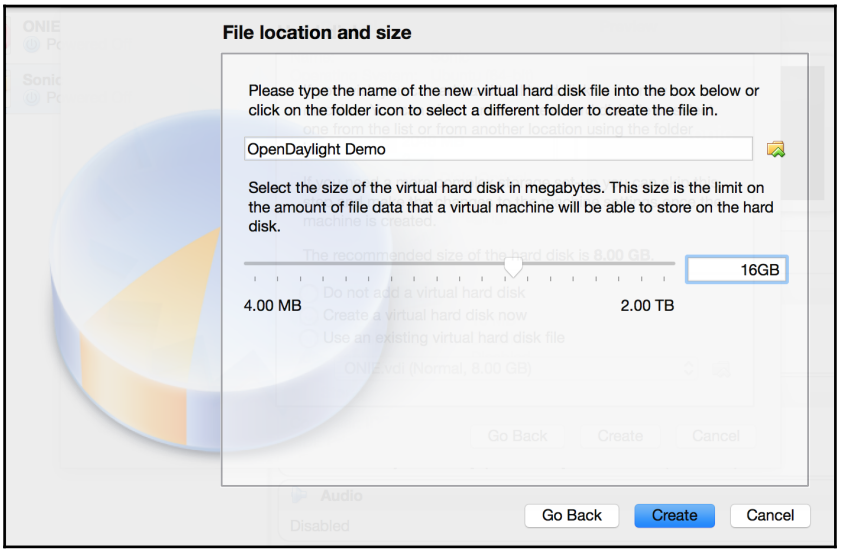
The Long Term Support version of Ubuntu Server, including the Mitaka release of OpenStack and support guaranteed until April 2021 — 64-bit only.

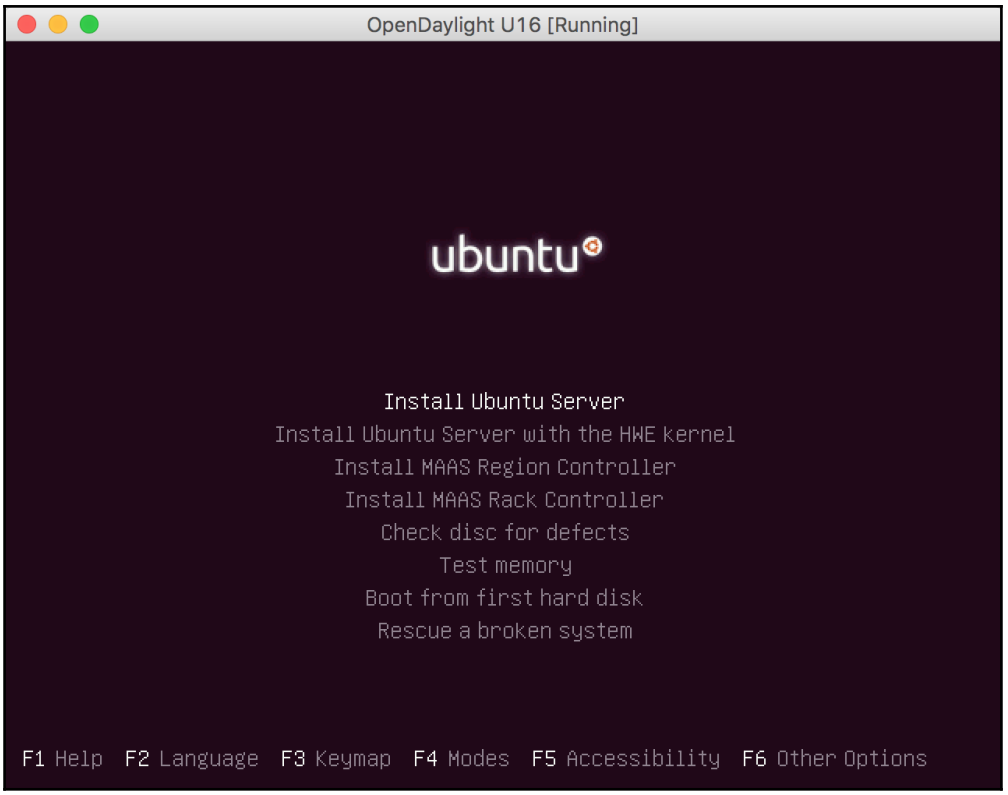
Ubuntu Server 16.04.2 LTS release notes

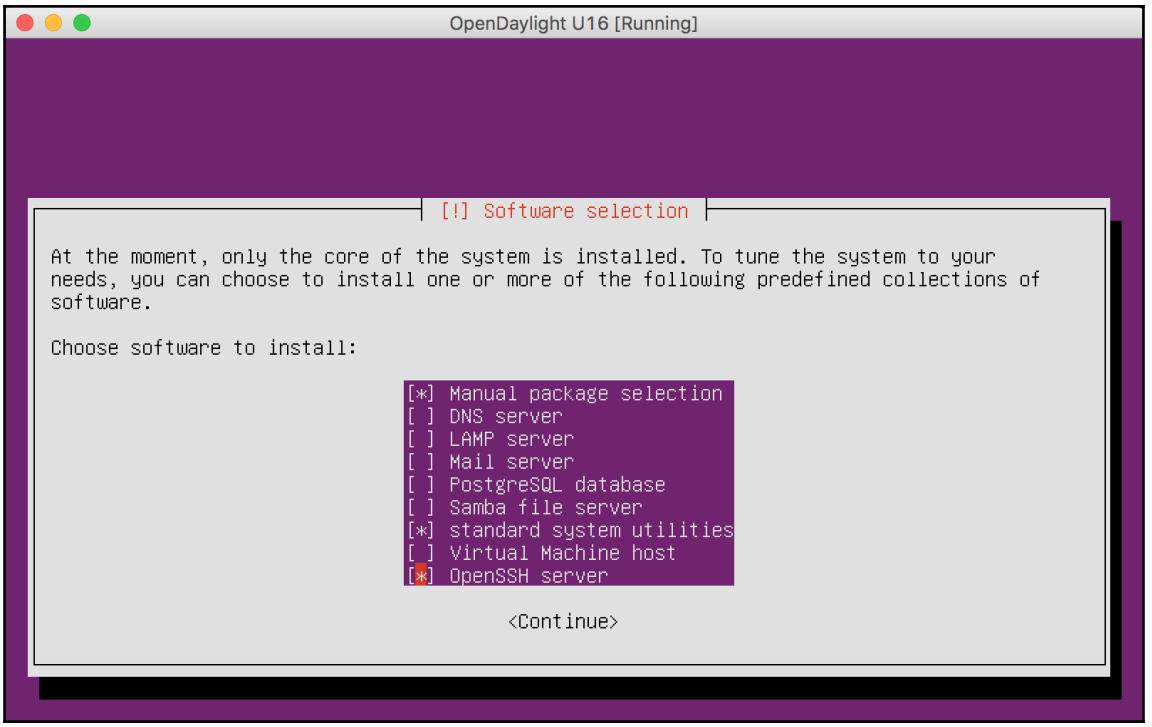
Download

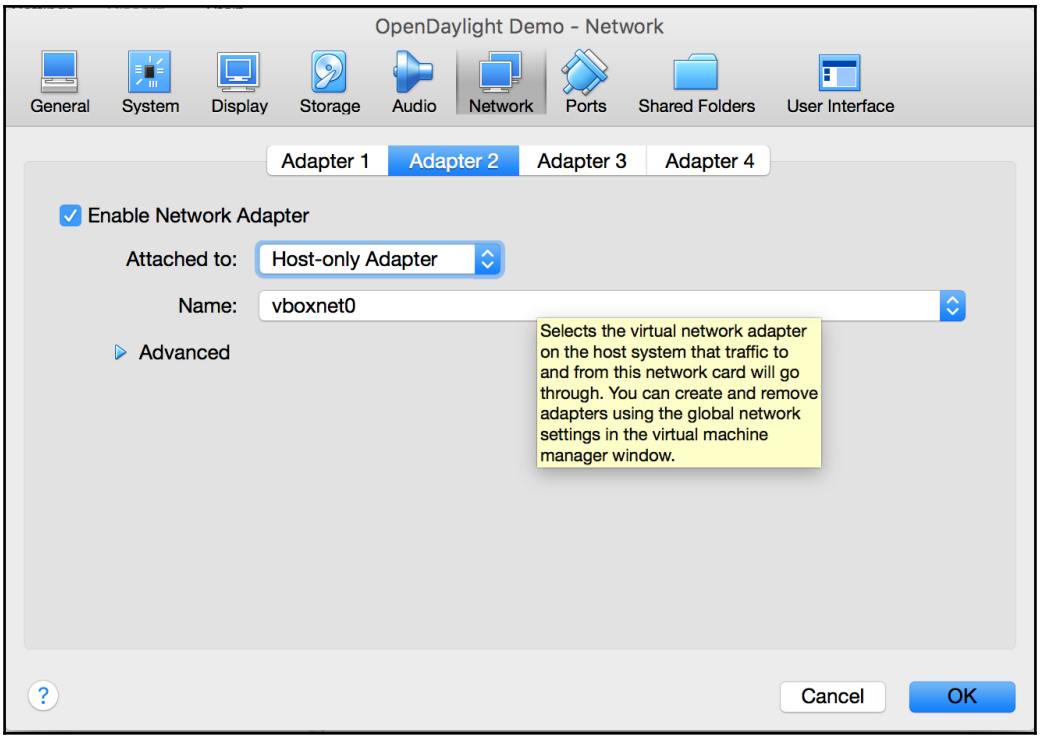
Alternative downloads and torrents ›

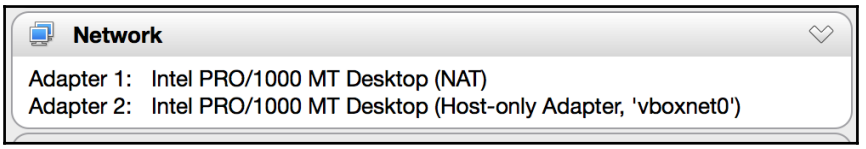

Memory size
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.
The recommended memory size is 768 MB.
4096
MB
4 MB
16384 MB
Go Back
Continue
Cancel


File location and size
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.
OpenDaylight Demo
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.
16GB
4.00 MB
2.00 TB
Go Back
Create
Cancel

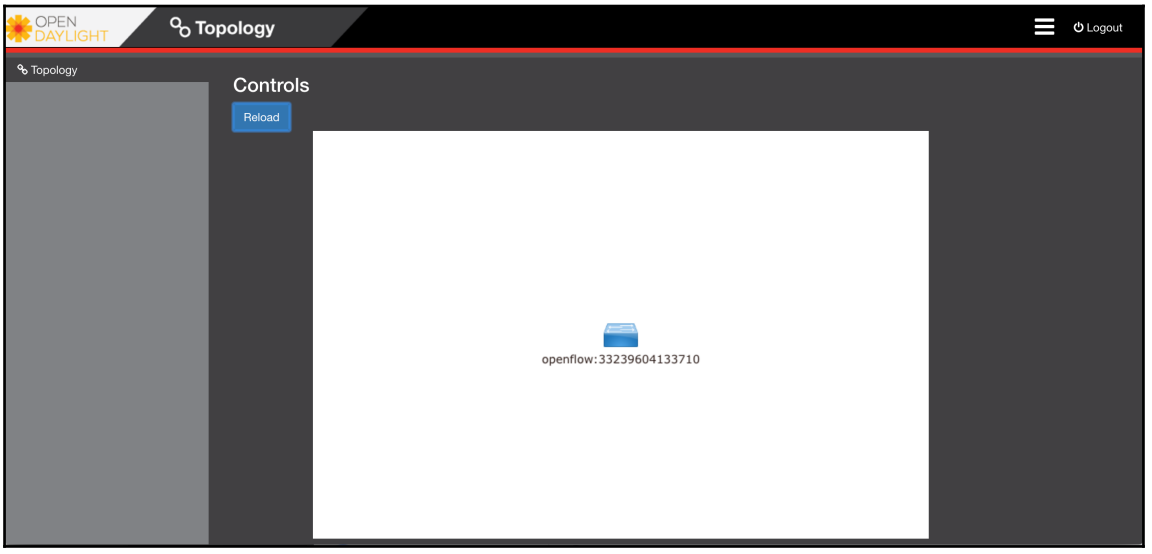

OpenDaylight U16 [Running]
ubuntu
Install Ubuntu Server
Install Ubuntu Server with the HWE kernel
Install MAAS Region Controller
Install MAAS Rack Controller
Check disc for defects
Test memory
Boot from first hard disk
Rescue a broken system
F1 Help F2 Language F3 Keymap F4 Modes F5 Accessibility F6 Other Options

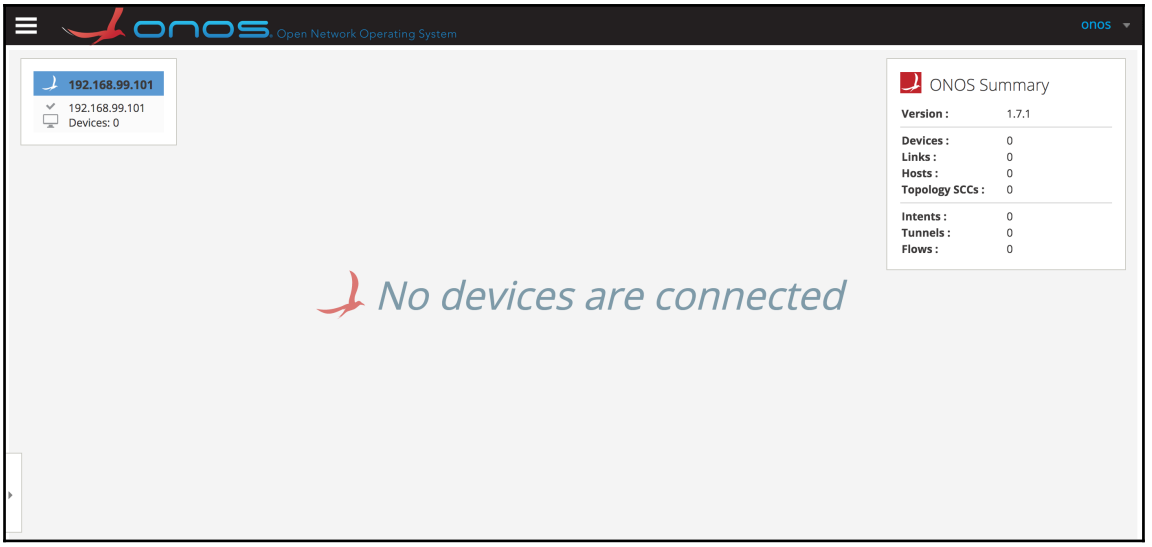

OpenDaylight U16 [Running]
[!] Software selection
At the moment, only the core of the system is installed. To tune the system to your needs, you can choose to install one or more of the following predefined collections of software.
Choose software to install:
[*] Manual package selection
[ ] DNS server
[ ] LAMP server
[ ] Mail server
[ ] PostgreSQL database
[ ] Samba file server
[*] standard system utilities
[ ] Virtual Machine host
[*] OpenSSH server
<Continue>

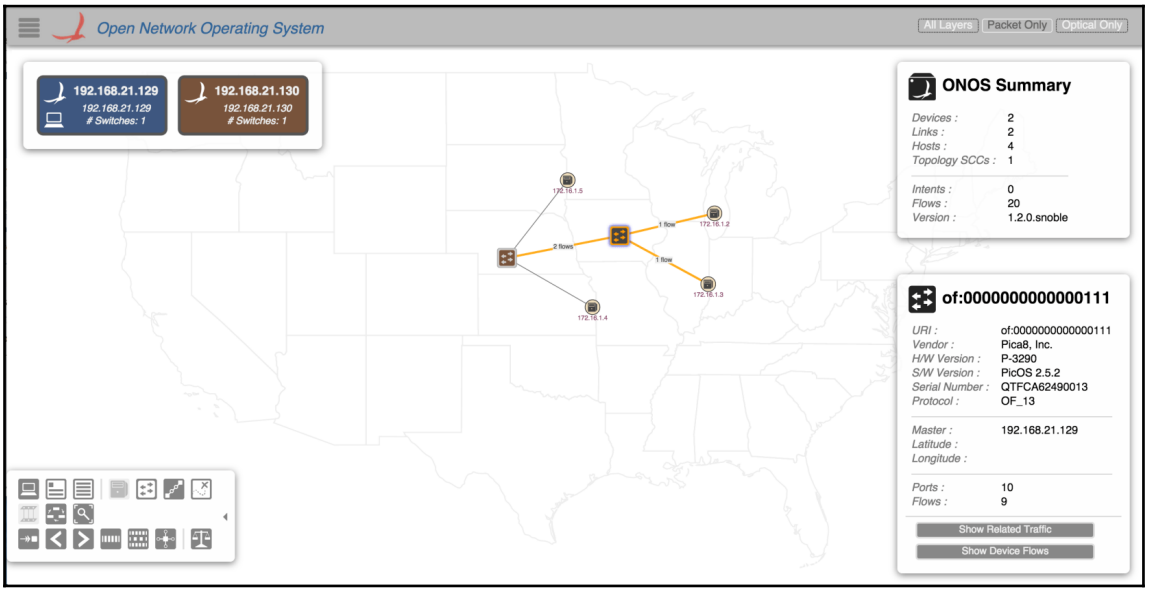

OpenDaylight Demo - Network
General
System
Display
Storage
Audio
Network
Ports
Shared Folders
User Interface
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Host-only Adapter
Name:
vboxnet0
Advanced
Selects the virtual network adapter on the host system that traffic to and from this network card will go through. You can create and remove adapters using the global network settings in the virtual machine manager window.
Cancel
OK


Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)
Adapter 2: Intel PRO/1000 MT Desktop (Host-only Adapter, 'vboxnet0')

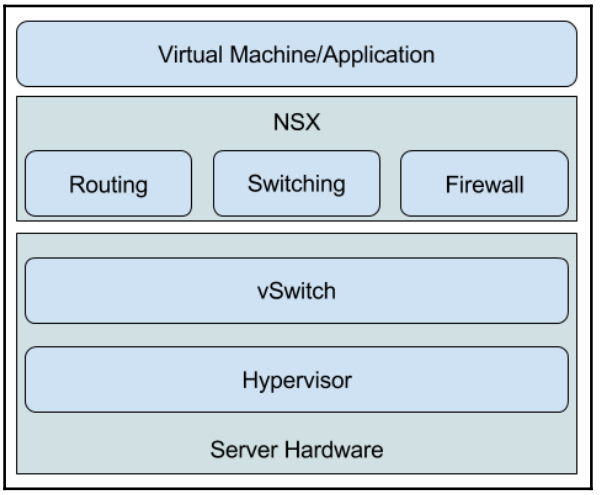
```
Apache Karaf starting up. Press Enter to open the shell now...
100% [========================================================================]

Karaf started in 4s. Bundle stats: 64 active, 64 total

    ________                       ________                .__  .__       .__     __
    \_____  \ ______   ____   ____ \_____  \ ______ ____ |__| |__| ____ |  |___/  |_
     /   |   \\____ \_/ __ \ /    \ |    |  \\__  \ <   | |  | |  |/ ___\|  |  \   __\
    /    |    \  |_> >  ___/|   |  \|    `   \/ __ \\___ ||  |_|  / /_/  >   Y  \  |
    \_______  /   __/ \___  >___|  /_______  (____  / ____||____/__\___  /|___|  /__|
            \/|__|        \/     \/        \/     \/\/                 /_____/     \/


Hit '<tab>' for a list of available commands
and '[cmd] --help' for help on a specific command.
Hit '<ctrl-d>' or type 'system:shutdown' or 'logout' to shutdown OpenDaylight.

opendaylight-user@root>
```

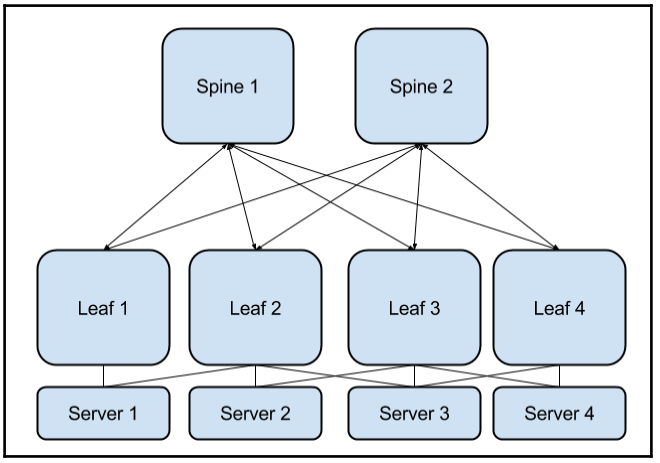


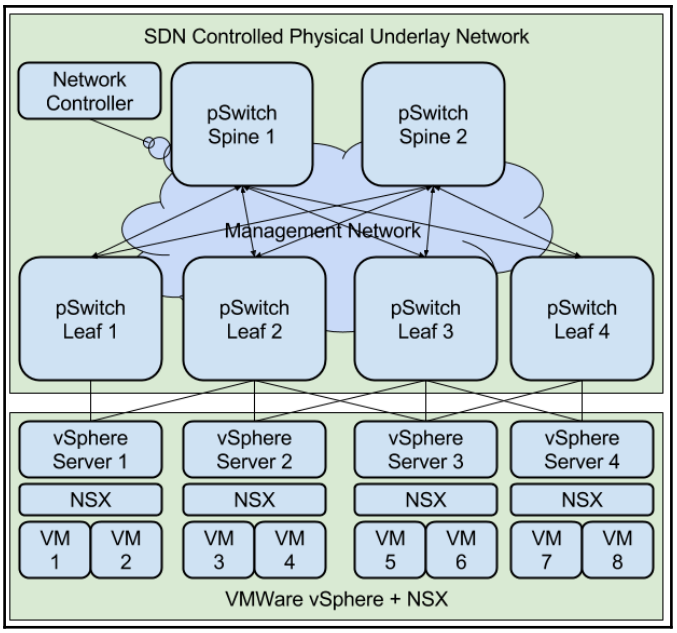

onos
Open Network Operating System
onos
192.168.99.101
192.168.99.101
Devices: 0
ONOS Summary
Version : 1.7.1
Devices : 0
Links : 0
Hosts : 0
Topology SCCs : 0
Intents : 0
Tunnels : 0
Flows : 0
No devices are connected

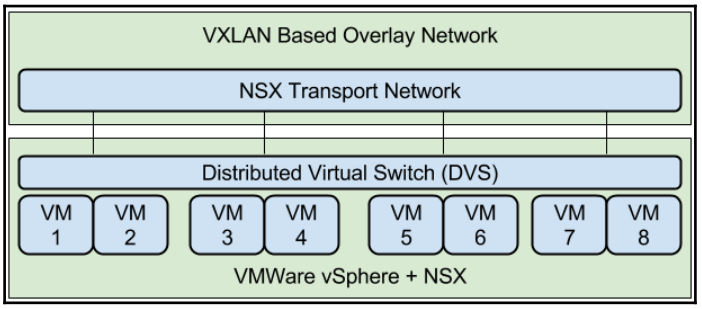

Open Network Operating System
All Layers
Packet Only
Optical Only
192.168.21.129
192.168.21.129
Switches: 1
192.168.21.130
192.168.21.130
Switches: 1
ONOS Summary
Devices : 2
Links : 2
Hosts : 4
Topology SCCs : 1
Intents : 0
Flows : 20
Version : 1.2.0.snoble
of:0000000000000111
URI : of:0000000000000111
Vendor : Pica8, Inc.
H/W Version : P-3290
S/W Version : PicOS 2.5.2
Serial Number : QTFCA62490013
Protocol : OF_13
Master : 192.168.21.129
Latitude :
Longitude :
Ports : 10
Flows : 9
Show Related Traffic
Show Device Flows

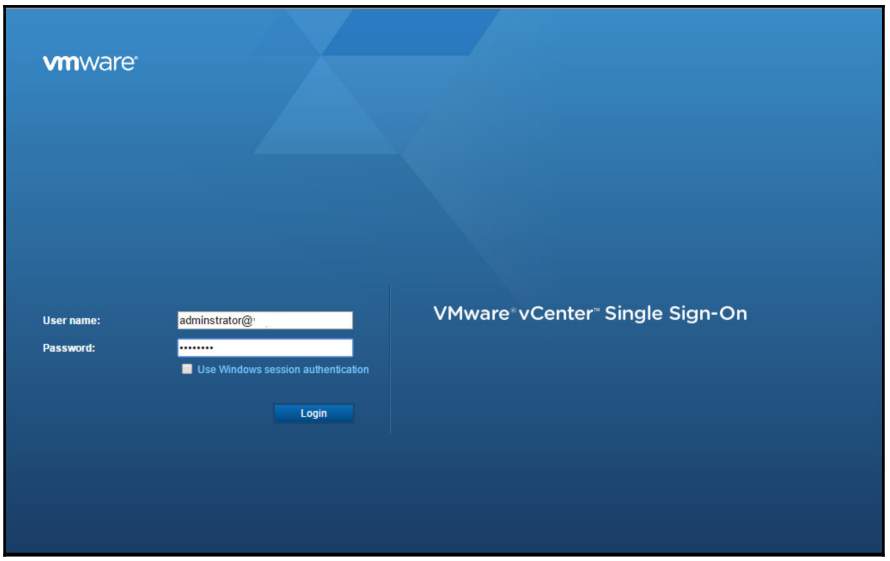
Chapter 7: VMware NSX

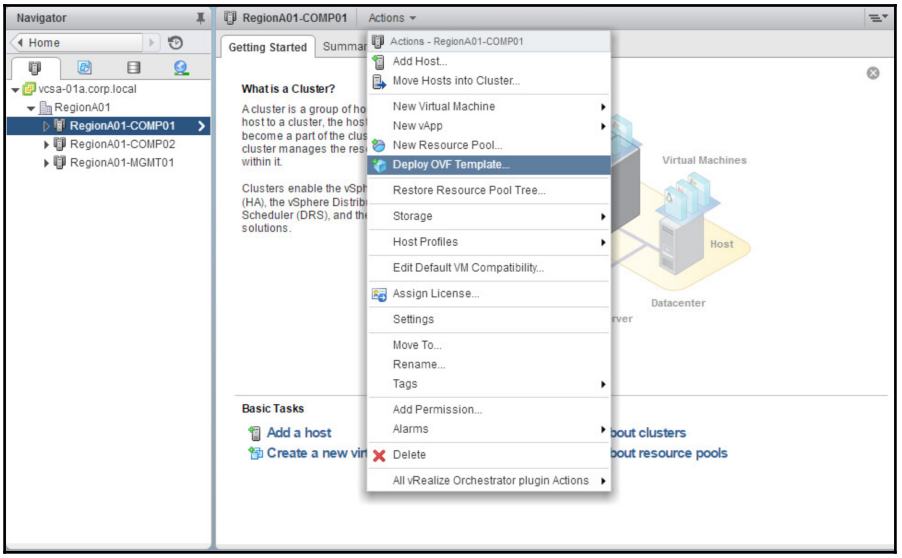


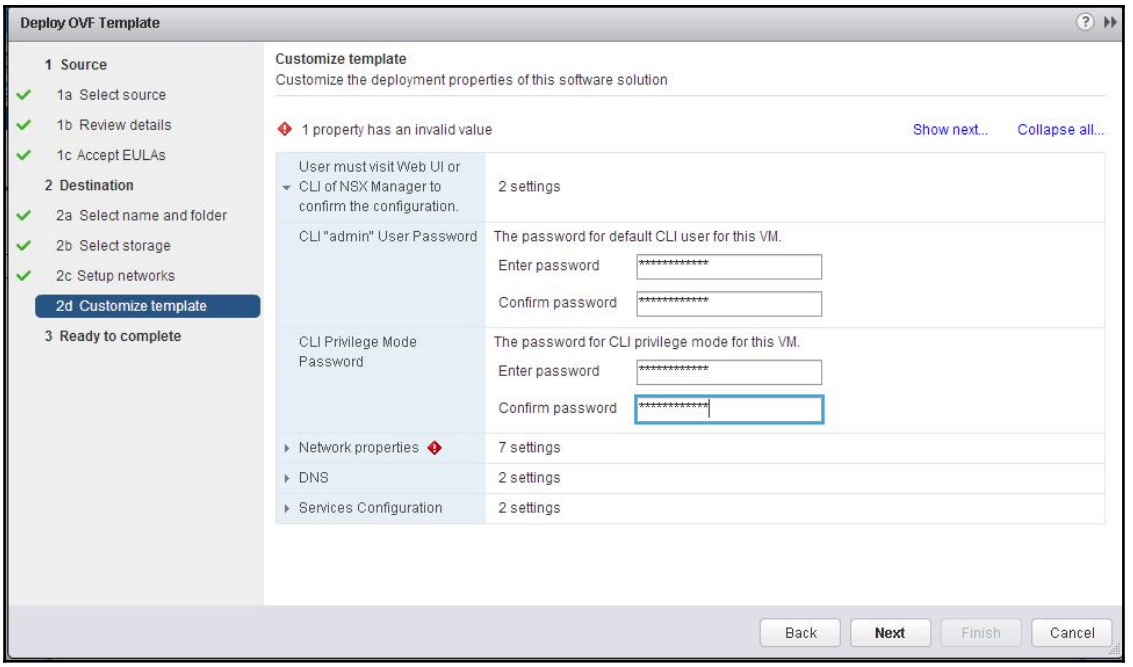


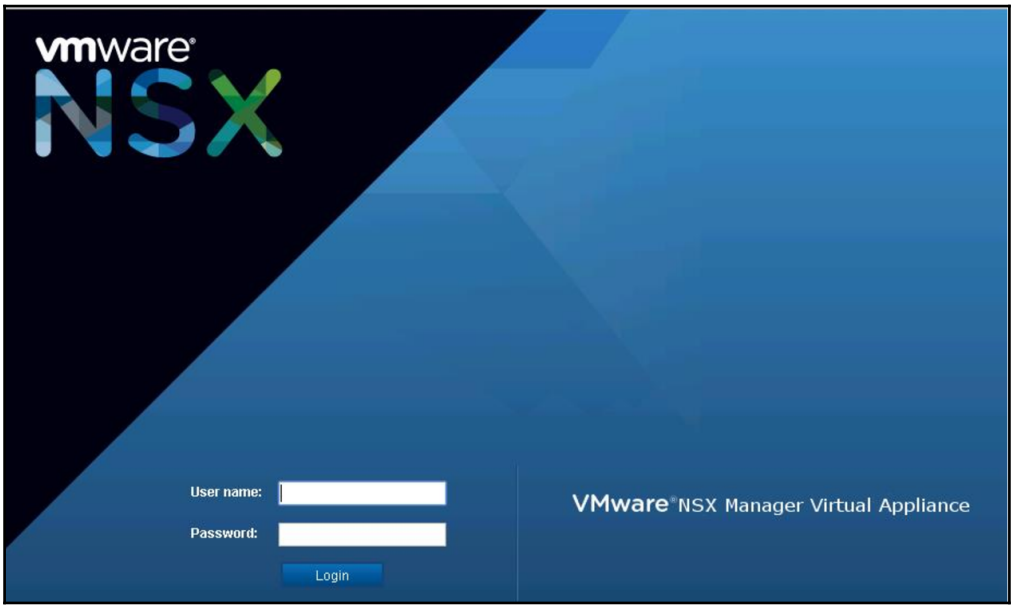

SDN Controlled Physical Underlay Network
Network Controller
pSwitch Spine 1
pSwitch Spine 2
Management Network
pSwitch Leaf 1
pSwitch Leaf 2
pSwitch Leaf 3
pSwitch Leaf 4
vSphere Server 1
vSphere Server 2
vSphere Server 3
vSphere Server 4
NSX
NSX
NSX
NSX
VM 1
VM 2
VM 3
VM 4
VM 5
VM 6
VM 7
VM 8
VMWare vSphere + NSX

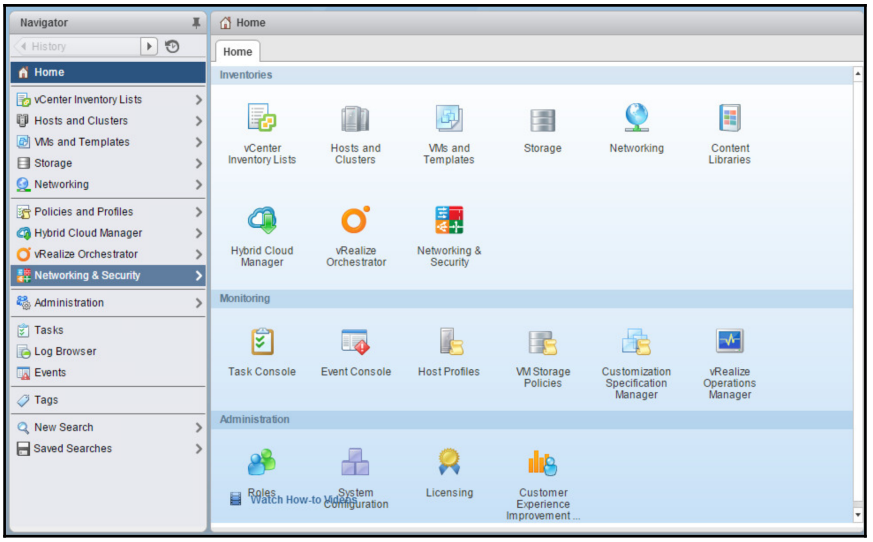

VXLAN Based Overlay Network
NSX Transport Network
Distributed Virtual Switch (DVS)
VM 1
VM 2
VM 3
VM 4
VM 5
VM 6
VM 7
VM 8
VMWare vSphere + NSX

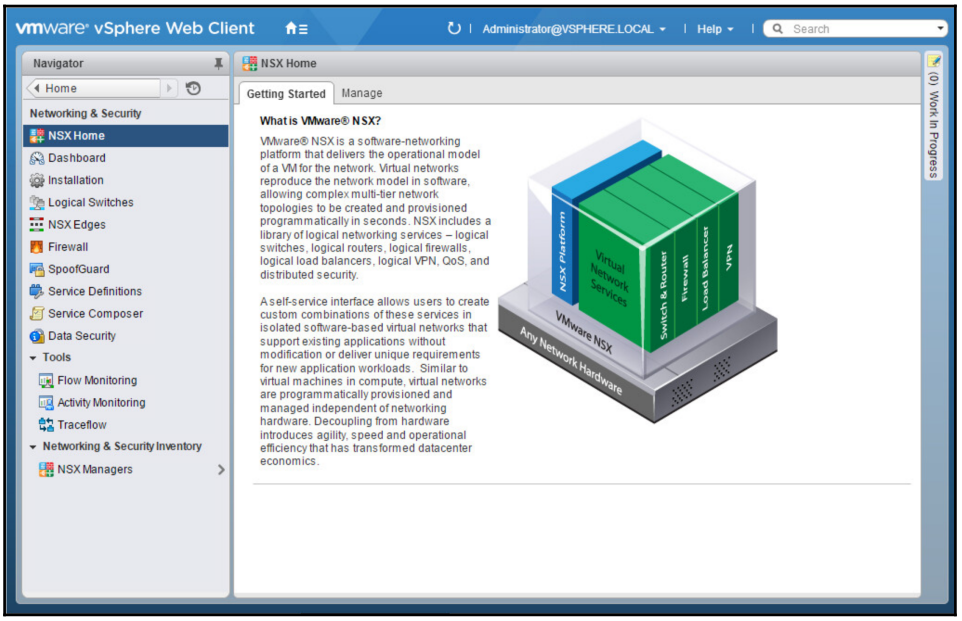

vmware
User name:
adminstrator@
Password:
Use Windows session authentication
Login
VMware vCenter Single Sign-On

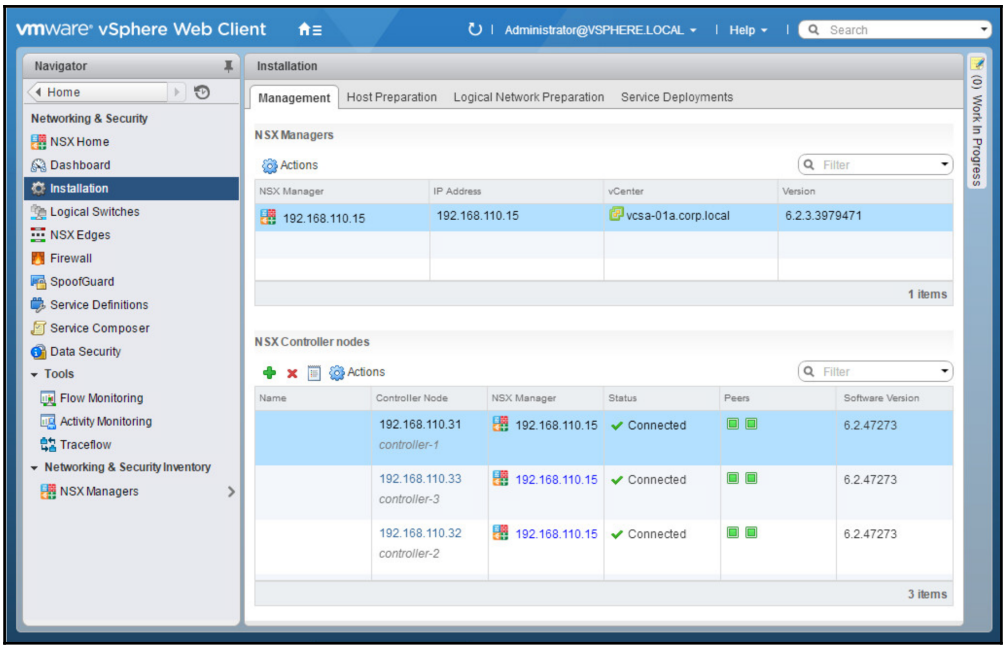

Navigator
Home
vcsa-01a.corp.local
RegionA01
RegionA01-COMP01
RegionA01-COMP02
RegionA01-MGMT01
RegionA01-COMP01
Actions
Getting Started
What is a Cluster?
Actions - RegionA01-COMP01
Add Host...
Move Hosts into Cluster...
New Virtual Machine
New vApp
New Resource Pool...
Deploy OVF Template...
Restore Resource Pool Tree...
Storage
Host Profiles
Edit Default VM Compatibility...
Assign License...
Settings
Move To...
Rename...
Tags
Add Permission...
Alarms
Delete
All vRealize Orchestrator plugin Actions
Virtual Machines
Host
Datacenter
Basic Tasks
Add a host

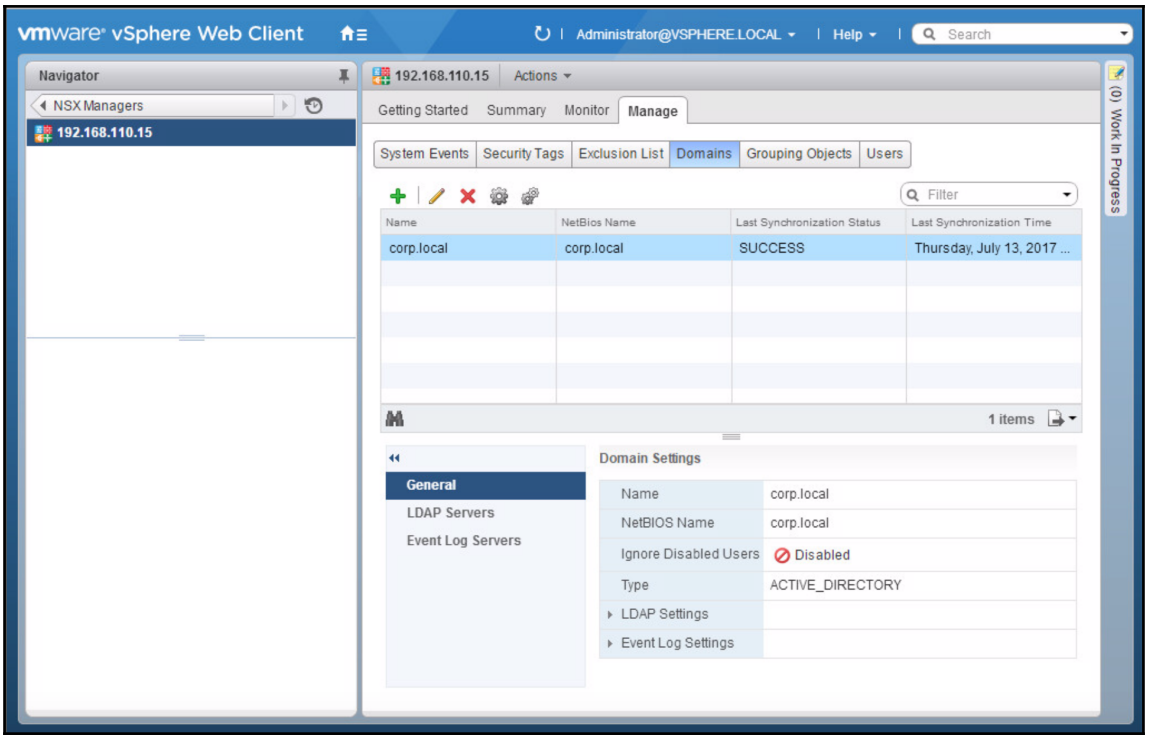

Deploy OVF Template
1 Source
1a Select source
1b Review details
1c Accept EULAs
2 Destination
2a Select name and folder
2b Select storage
2c Setup networks
2d Customize template
3 Ready to complete
Customize template
Customize the deployment properties of this software solution
1 property has an invalid value
Show next...
Collapse all...
User must visit Web UI or CLI of NSX Manager to confirm the configuration.
2 settings
CLI "admin" User Password
The password for default CLI user for this VM.
Enter password
Confirm password
CLI Privilege Mode Password
The password for CLI privilege mode for this VM.
Enter password
Confirm password
Network properties
7 settings
DNS
2 settings
Services Configuration
2 settings
Back
Next
Finish
Cancel

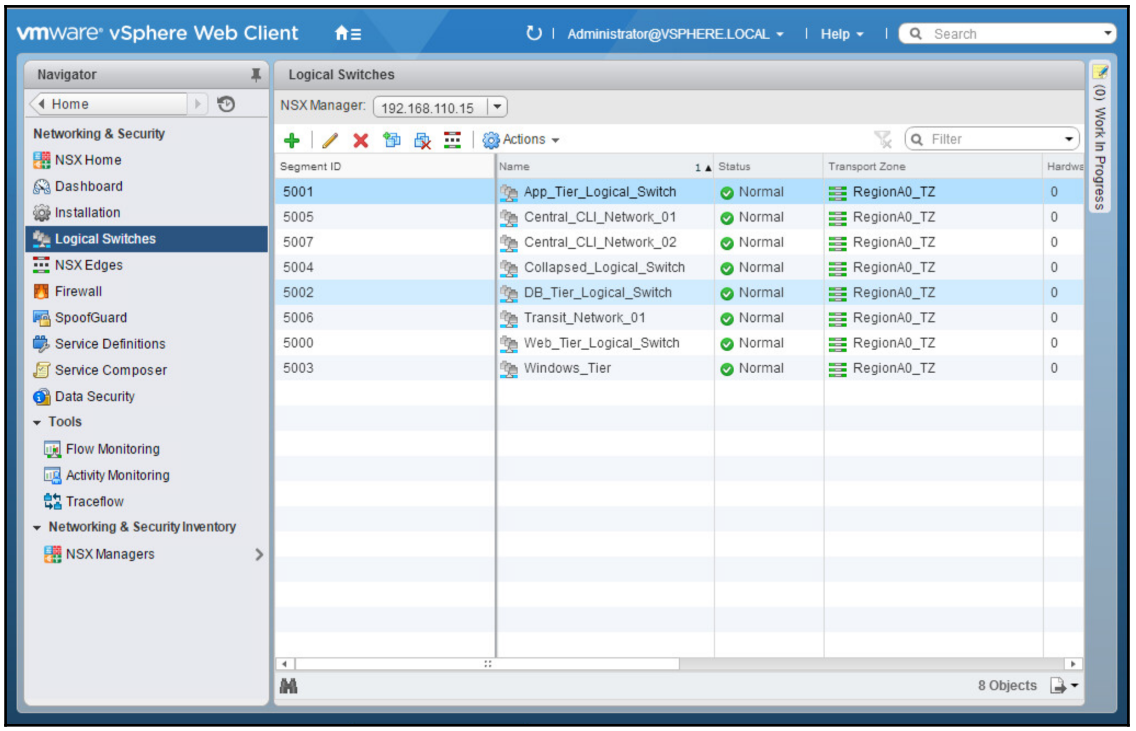

vmware
NSX
User name:
Password:
Login
VMware NSX Manager Virtual Appliance

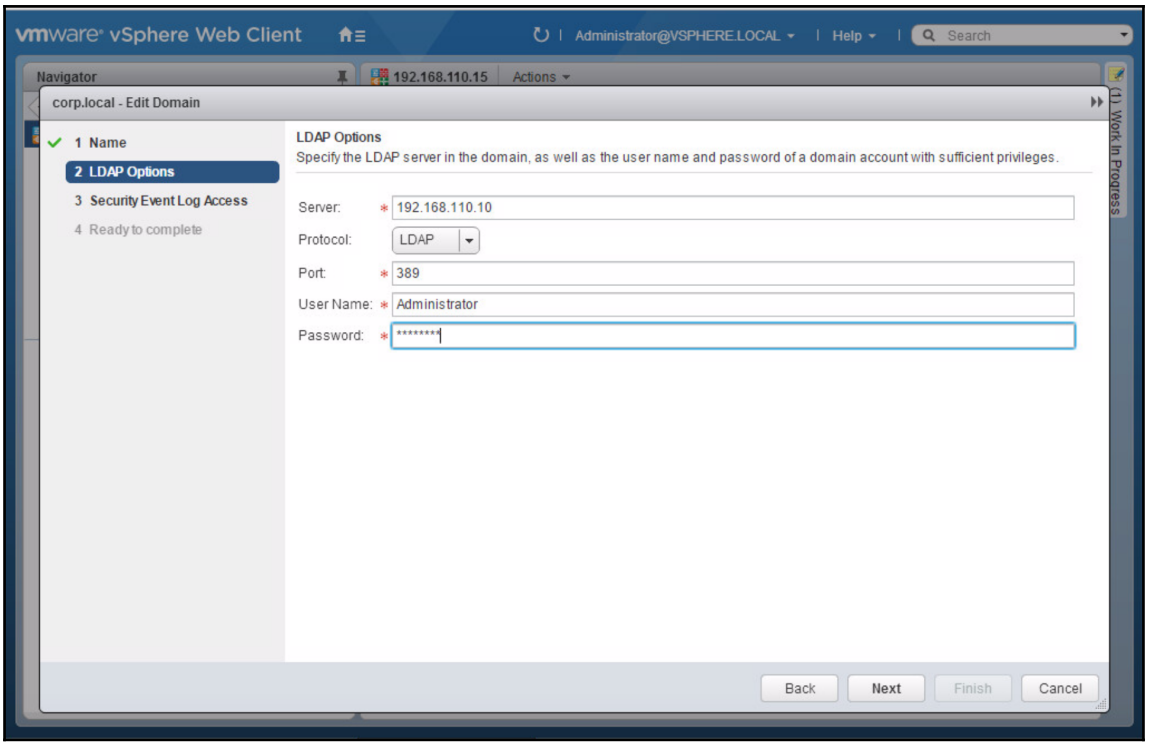

Navigator
History
Home
vCenter Inventory Lists
Hosts and Clusters
VMs and Templates
Storage
Networking
Policies and Profiles
Hybrid Cloud Manager
vRealize Orchestrator
Networking & Security
Administration
Tasks
Log Browser
Events
Tags
New Search
Saved Searches
Home
Home
Inventories
vCenter Inventory Lists
Hosts and Clusters
VMs and Templates
Storage
Networking
Content Libraries
Hybrid Cloud Manager
vRealize Orchestrator
Networking & Security
Monitoring
Task Console
Event Console
Host Profiles
VM Storage Policies
Customization Specification Manager
vRealize Operations Manager
Administration
Roles
System Configuration
Licensing
Customer Experience Improvement ...
Watch How-to Videos

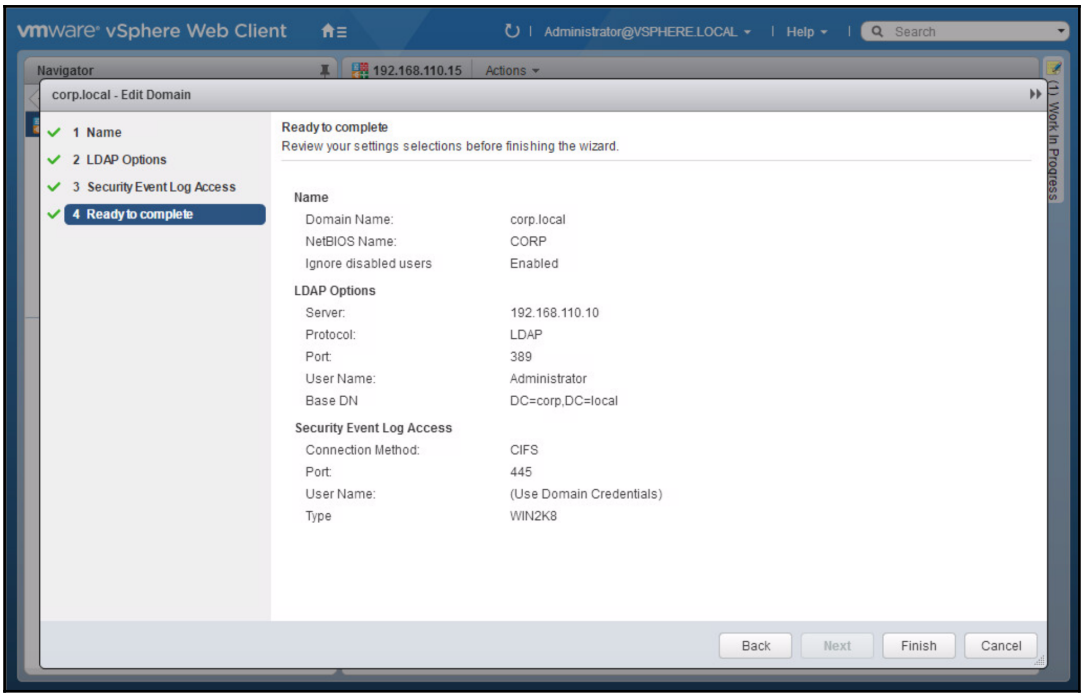

vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Home
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Data Security
Tools
Flow Monitoring
Activity Monitoring
Traceflow
Networking & Security Inventory
NSX Managers
NSX Home
Getting Started
Manage
What is VMware® NSX?
VMware® NSX is a software-networking platform that delivers the operational model of a VM for the network. Virtual networks reproduce the network model in software, allowing complex multi-tier network topologies to be created and provisioned programmatically in seconds. NSX includes a library of logical networking services – logical switches, logical routers, logical firewalls, logical load balancers, logical VPN, QoS, and distributed security.
A self-service interface allows users to create custom combinations of these services in isolated software-based virtual networks that support existing applications without modification or deliver unique requirements for new application workloads. Similar to virtual machines in compute, virtual networks are programmatically provisioned and managed independent of networking hardware. Decoupling from hardware introduces agility, speed and operational efficiency that has transformed datacenter economics.
NSX Platform
Virtual Network Services
Switch & Router
Firewall
Load Balancer
VPN
VMware NSX
Any Network Hardware
(0) Work in Progress

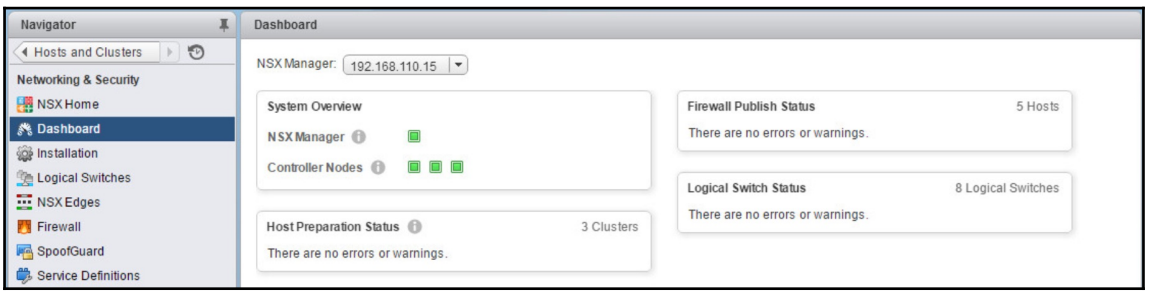

vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Home
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Data Security
Tools
Flow Monitoring
Activity Monitoring
Traceflow
Networking & Security Inventory
NSX Managers
Installation
Management
Host Preparation
Logical Network Preparation
Service Deployments
NSX Managers
Actions
Filter
NSX Manager
IP Address
vCenter
Version
192.168.110.15
192.168.110.15
vcsa-01a.corp.local
6.2.3.3979471
1 items
NSX Controller nodes
Actions
Filter
Name
Controller Node
NSX Manager
Status
Peers
Software Version
192.168.110.31
controller-1
192.168.110.15
Connected
6.2.47273
192.168.110.33
controller-3
192.168.110.15
Connected
6.2.47273
192.168.110.32
controller-2
192.168.110.15
Connected
6.2.47273
3 items
(0) Work In Progress

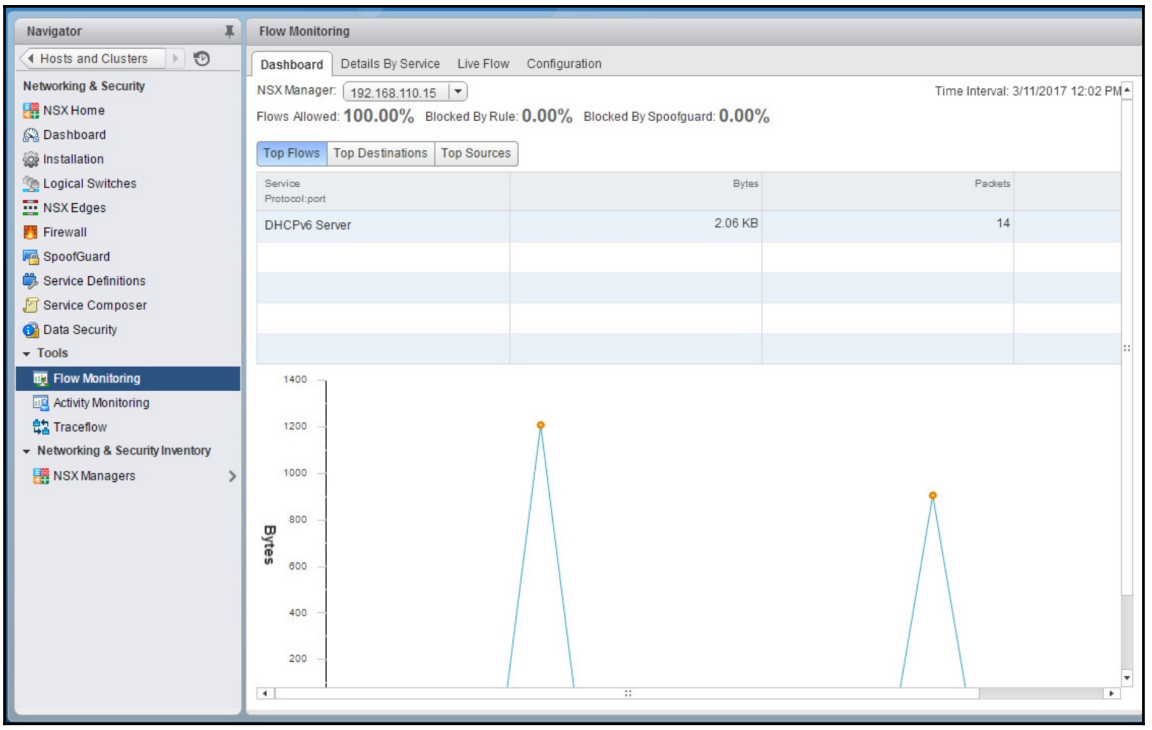

vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
NSX Managers
192.168.110.15
192.168.110.15
Actions
Getting Started
Summary
Monitor
Manage
System Events
Security Tags
Exclusion List
Domains
Grouping Objects
Users
Filter
Name
NetBios Name
Last Synchronization Status
Last Synchronization Time
corp.local
corp.local
SUCCESS
Thursday, July 13, 2017 ...
1 items
General
LDAP Servers
Event Log Servers
Domain Settings
Name
corp.local
NetBIOS Name
corp.local
Ignore Disabled Users
Disabled
Type
ACTIVE_DIRECTORY
LDAP Settings
Event Log Settings
(0) Work In Progress

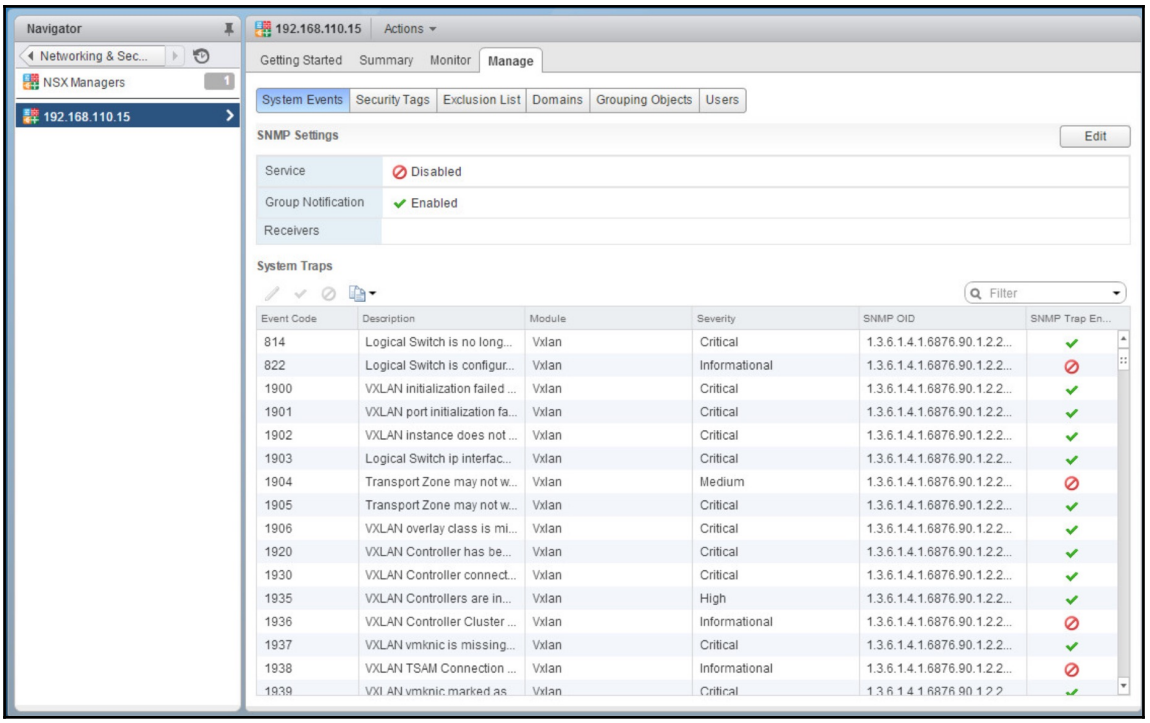

vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Home
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Data Security
Tools
Flow Monitoring
Activity Monitoring
Traceflow
Networking & Security Inventory
NSX Managers
Logical Switches
NSX Manager: 192.168.110.15
Actions
Filter
Segment ID
Name
Status
Transport Zone
Hardwa
5001 App_Tier_Logical_Switch Normal RegionA0_TZ 0
5005 Central_CLI_Network_01 Normal RegionA0_TZ 0
5007 Central_CLI_Network_02 Normal RegionA0_TZ 0
5004 Collapsed_Logical_Switch Normal RegionA0_TZ 0
5002 DB_Tier_Logical_Switch Normal RegionA0_TZ 0
5006 Transit_Network_01 Normal RegionA0_TZ 0
5000 Web_Tier_Logical_Switch Normal RegionA0_TZ 0
5003 Windows_Tier Normal RegionA0_TZ 0
8 Objects
(0) Work In Progress

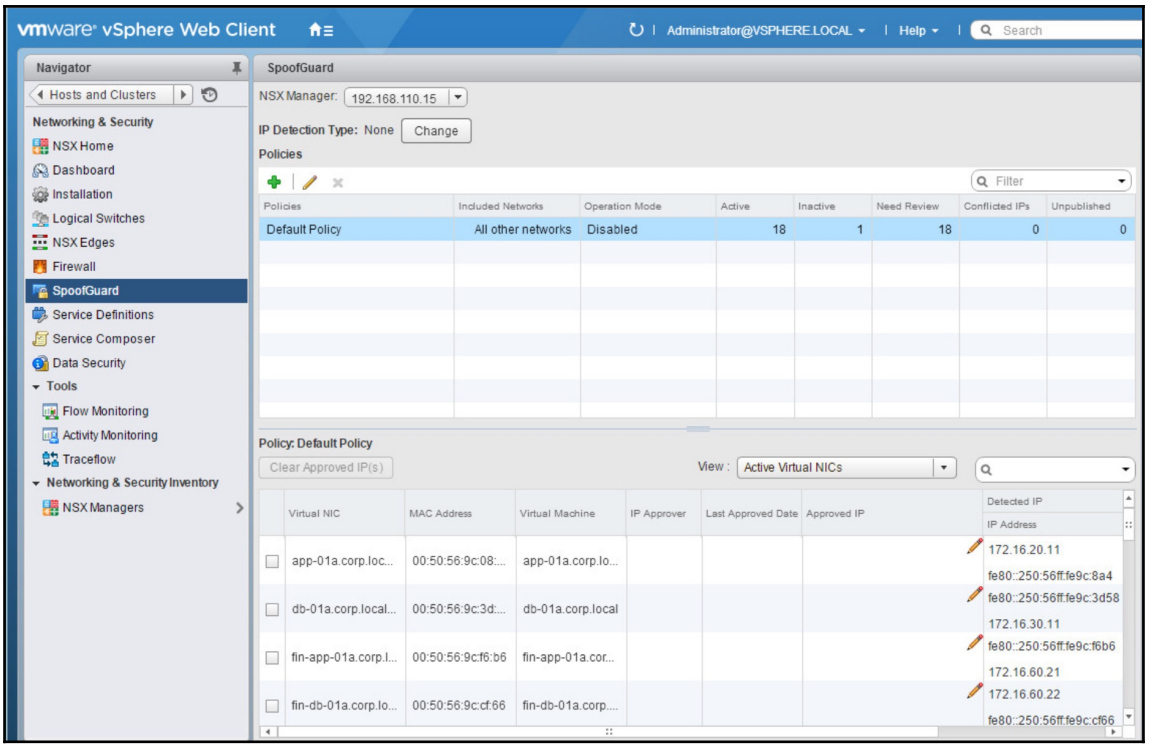

vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
192.168.110.15
Actions
corp.local - Edit Domain
1 Name
2 LDAP Options
3 Security Event Log Access
4 Ready to complete
LDAP Options
Specify the LDAP server in the domain, as well as the user name and password of a domain account with sufficient privileges.
Server: * 192.168.110.10
Protocol: LDAP
Port: * 389
User Name: * Administrator
Password: * ********
Back
Next
Finish
Cancel
(1) Work in Progress

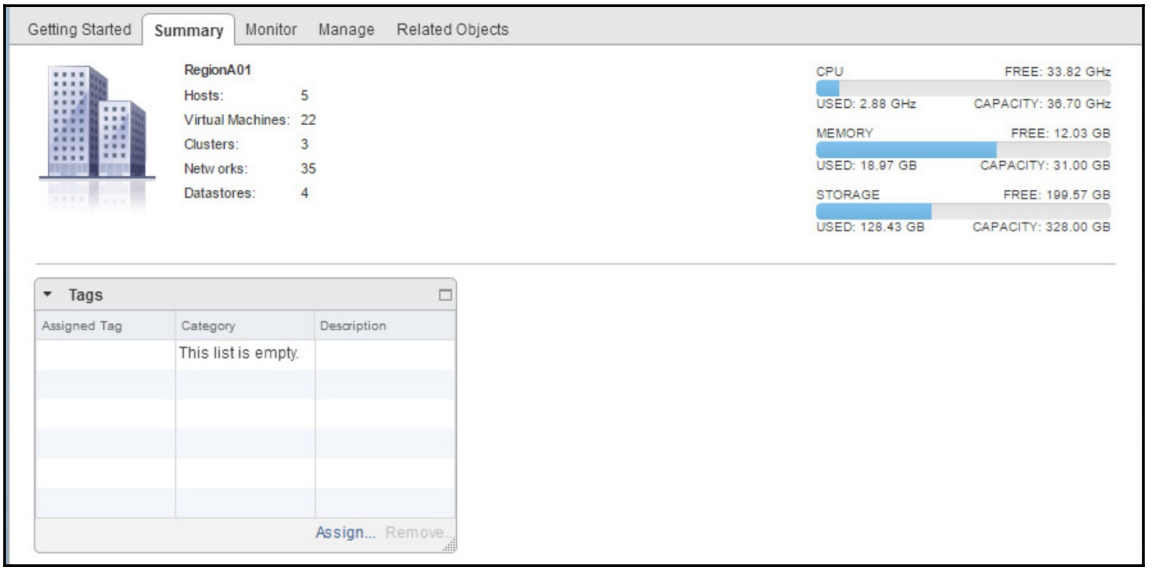

vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
192.168.110.15
Actions
corp.local - Edit Domain
1 Name
2 LDAP Options
3 Security Event Log Access
4 Ready to complete
Ready to complete
Review your settings selections before finishing the wizard.
Name
Domain Name: corp.local
NetBIOS Name: CORP
Ignore disabled users Enabled
LDAP Options
Server: 192.168.110.10
Protocol: LDAP
Port: 389
User Name: Administrator
Base DN DC=corp,DC=local
Security Event Log Access
Connection Method: CIFS
Port: 445
User Name: (Use Domain Credentials)
Type WIN2K8
Back
Next
Finish
Cancel
(1) Work In Progress


Navigator
Hosts and Clusters
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Dashboard
NSX Manager: 192.168.110.15
System Overview
NSX Manager
Controller Nodes
Host Preparation Status
3 Clusters
There are no errors or warnings.
Firewall Publish Status
5 Hosts
There are no errors or warnings.
Logical Switch Status
8 Logical Switches
There are no errors or warnings.

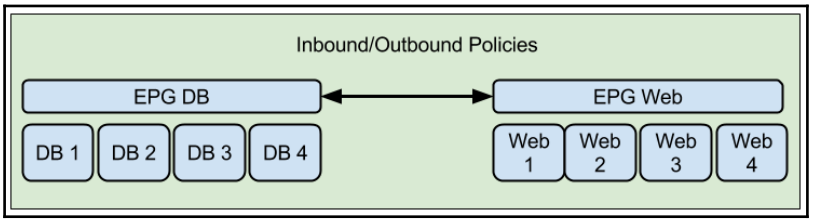

Navigator
Hosts and Clusters
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Data Security
Tools
Flow Monitoring
Activity Monitoring
Traceflow
Networking & Security Inventory
NSX Managers
Flow Monitoring
Dashboard
Details By Service
Live Flow
Configuration
NSX Manager: 192.168.110.15
Time Interval: 3/11/2017 12:02 PM
Flows Allowed: 100.00% Blocked By Rule: 0.00% Blocked By Spoofguard: 0.00%
Top Flows
Top Destinations
Top Sources
Service
Protocol:port
Bytes
Packets
DHCPv6 Server
2.06 KB
14
1400
1200
1000
800
600
400
200
Bytes

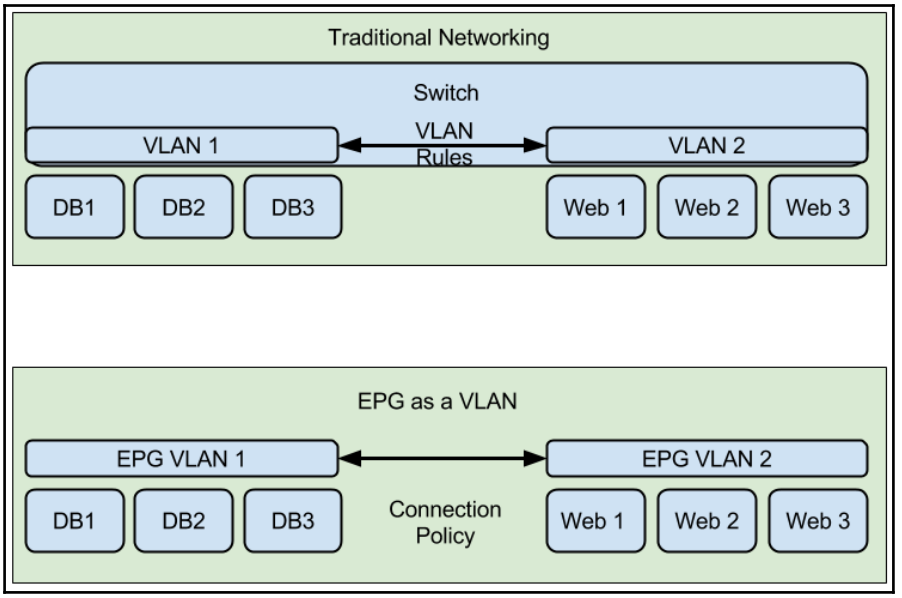

Navigator
Networking & Sec...
NSX Managers
1
192.168.110.15
192.168.110.15
Actions
Getting Started
Summary
Monitor
Manage
System Events
Security Tags
Exclusion List
Domains
Grouping Objects
Users
SNMP Settings
Edit
Service
Disabled
Group Notification
Enabled
Receivers
System Traps
Filter
Event Code
Description
Module
Severity
SNMP OID
SNMP Trap En...
814
Logical Switch is no long...
Vxlan
Critical
1.3.6.1.4.1.6876.90.1.2.2...
822
Logical Switch is configur...
Vxlan
Informational
1.3.6.1.4.1.6876.90.1.2.2...
1900
VXLAN initialization failed ...
Vxlan
Critical
1.3.6.1.4.1.6876.90.1.2.2...
1901
VXLAN port initialization fa...
Vxlan
Critical
1.3.6.1.4.1.6876.90.1.2.2...
1902
VXLAN instance does not ...
Vxlan
Critical
1.3.6.1.4.1.6876.90.1.2.2...
1903
Logical Switch ip interfac...
Vxlan
Critical
1.3.6.1.4.1.6876.90.1.2.2...
1904
Transport Zone may not w...
Vxlan
Medium
1.3.6.1.4.1.6876.90.1.2.2...
1905
Transport Zone may not w...
Vxlan
Critical
1.3.6.1.4.1.6876.90.1.2.2...
1906
VXLAN overlay class is mi...
Vxlan
Critical
1.3.6.1.4.1.6876.90.1.2.2...
1920
VXLAN Controller has be...
Vxlan
Critical
1.3.6.1.4.1.6876.90.1.2.2...
1930
VXLAN Controller connect...
Vxlan
Critical
1.3.6.1.4.1.6876.90.1.2.2...
1935
VXLAN Controllers are in...
Vxlan
High
1.3.6.1.4.1.6876.90.1.2.2...
1936
VXLAN Controller Cluster ...
Vxlan
Informational
1.3.6.1.4.1.6876.90.1.2.2...
1937
VXLAN vmknic is missing...
Vxlan
Critical
1.3.6.1.4.1.6876.90.1.2.2...
1938
VXLAN TSAM Connection ...
Vxlan
Informational
1.3.6.1.4.1.6876.90.1.2.2...
1939
VXLAN vmknic marked as ...
Vxlan
Critical
1.3.6.1.4.1.6876.90.1.2.2...

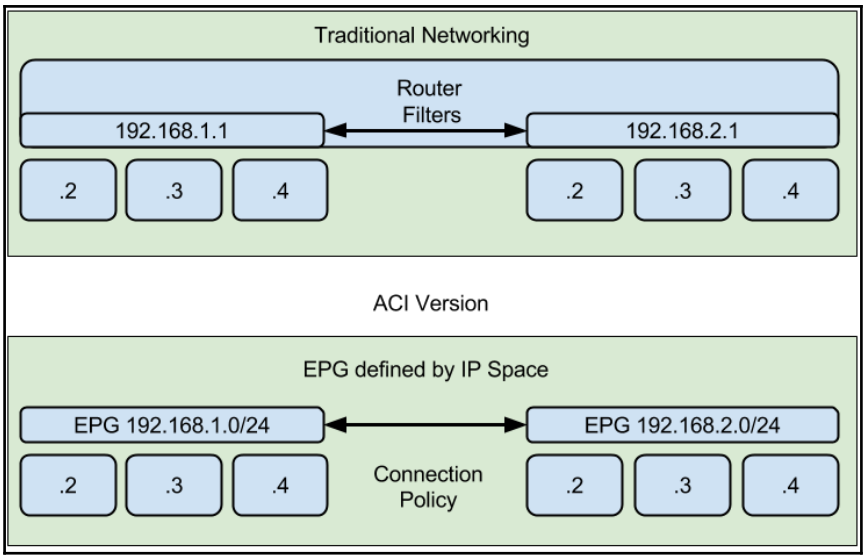

vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Hosts and Clusters
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Data Security
Tools
Flow Monitoring
Activity Monitoring
Traceflow
Networking & Security Inventory
NSX Managers
SpoofGuard
NSX Manager: 192.168.110.15
IP Detection Type: None
Change
Policies
Filter
Policies
Included Networks
Operation Mode
Active
Inactive
Need Review
Conflicted IPs
Unpublished
Default Policy
All other networks
Disabled
18
1
18
0
0
Policy: Default Policy
Clear Approved IP(s)
View :
Active Virtual NICs
Virtual NIC
MAC Address
Virtual Machine
IP Approver
Last Approved Date
Approved IP
Detected IP
IP Address
app-01a.corp.loc...
00:50:56:9c:08:...
app-01a.corp.lo...
172.16.20.11
fe80::250:56ff:fe9c:8a4
db-01a.corp.local...
00:50:56:9c:3d:...
db-01a.corp.local
fe80::250:56ff:fe9c:3d58
172.16.30.11
fin-app-01a.corp.l...
00:50:56:9c:f6:b6
fin-app-01a.cor...
fe80::250:56ff:fe9c:f6b6
172.16.60.21
fin-db-01a.corp.lo...
00:50:56:9c:cf:66
fin-db-01a.corp....
172.16.60.22
fe80::250:56ff:fe9c:cf66

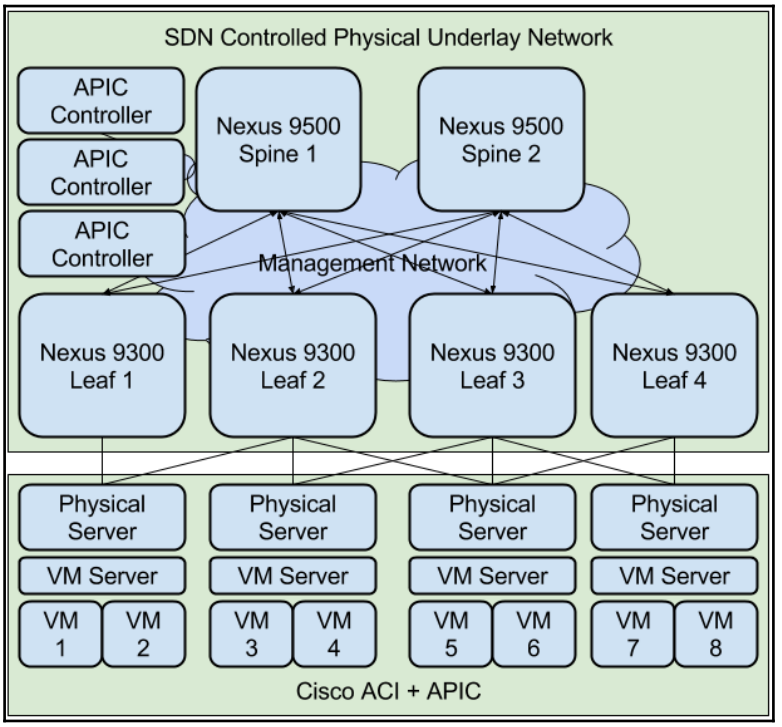

Getting Started
Summary
Monitor
Manage
Related Objects
RegionA01
Hosts: 5
Virtual Machines: 22
Clusters: 3
Networks: 35
Datastores: 4
CPU
FREE: 33.82 GHz
USED: 2.88 GHz
CAPACITY: 36.70 GHz
MEMORY
FREE: 12.03 GB
USED: 18.97 GB
CAPACITY: 31.00 GB
STORAGE
FREE: 199.57 GB
USED: 128.43 GB
CAPACITY: 328.00 GB
Tags
Assigned Tag
Category
Description
This list is empty.
Assign...
Remove

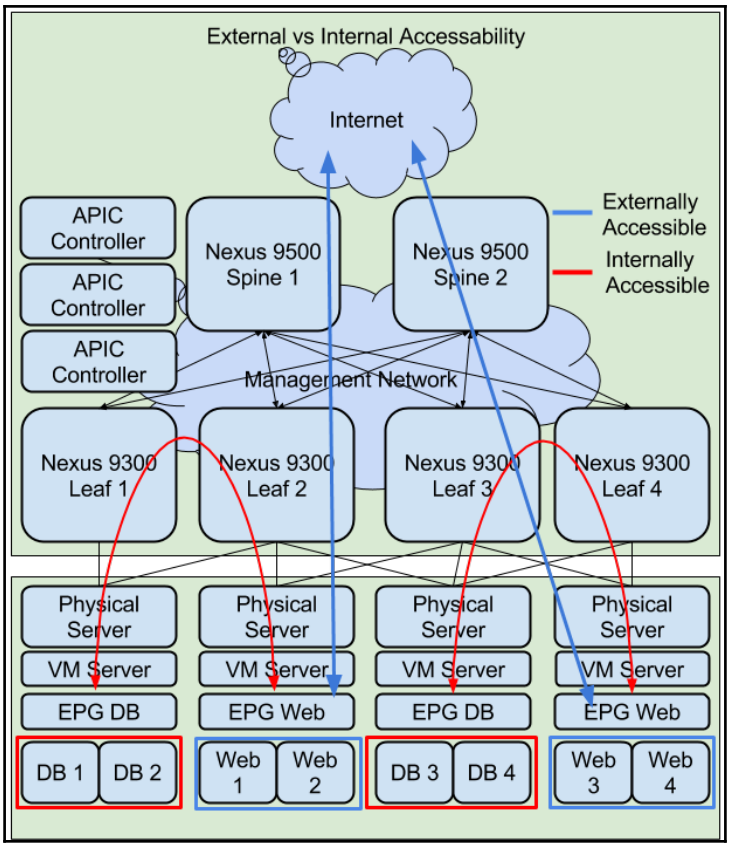
Chapter 8: Cisco ACI

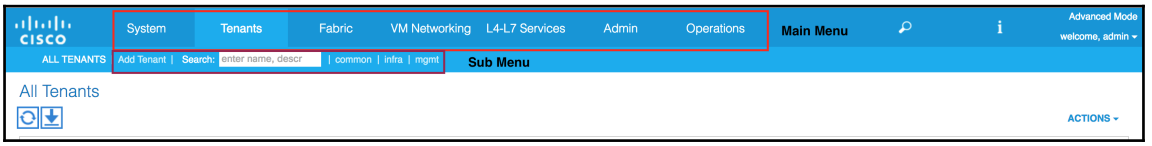


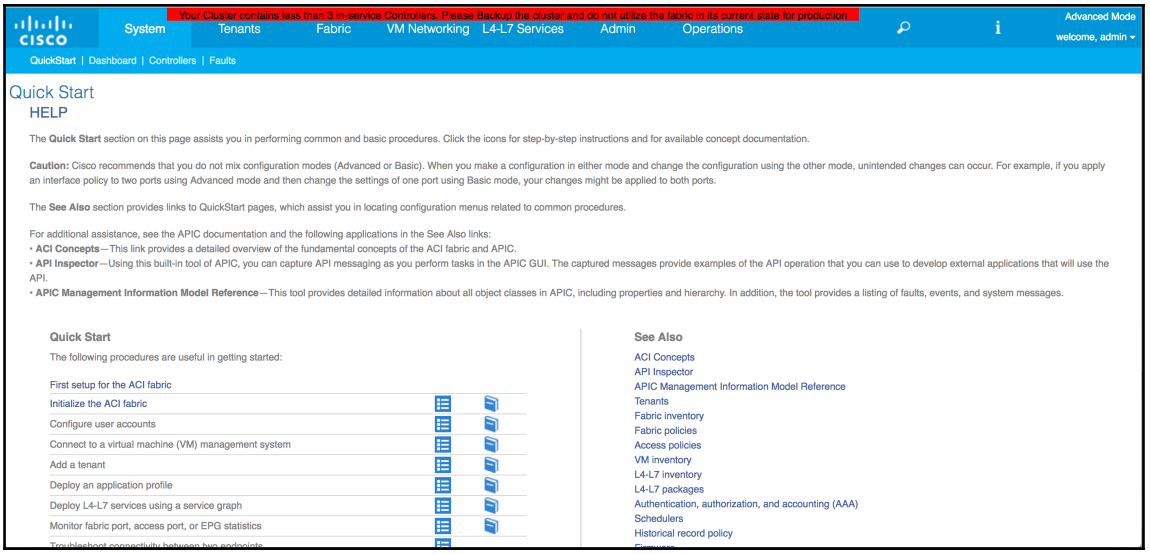


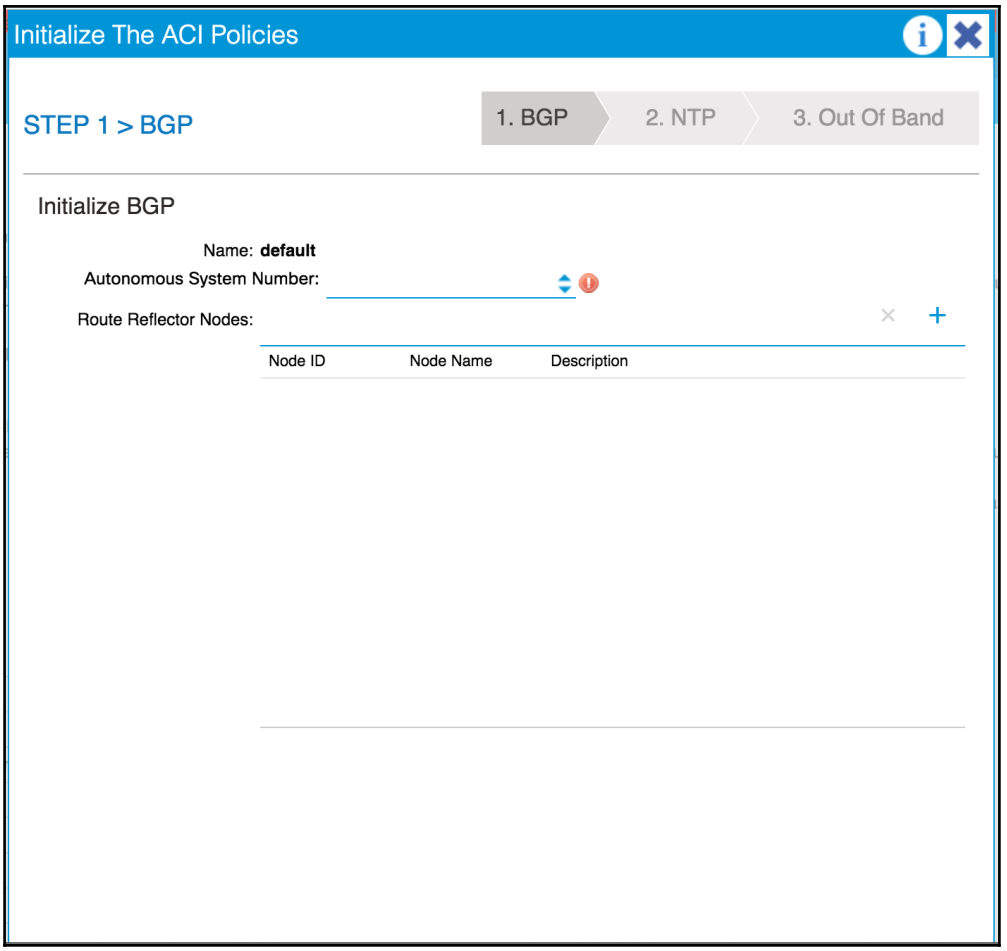

Traditional Networking
Router
Filters
192.168.1.1
192.168.2.1
.2
.3
.4
.2
.3
.4
ACI Version
EPG defined by IP Space
EPG 192.168.1.0/24
EPG 192.168.2.0/24
.2
.3
.4
Connection
Policy
.2
.3
.4

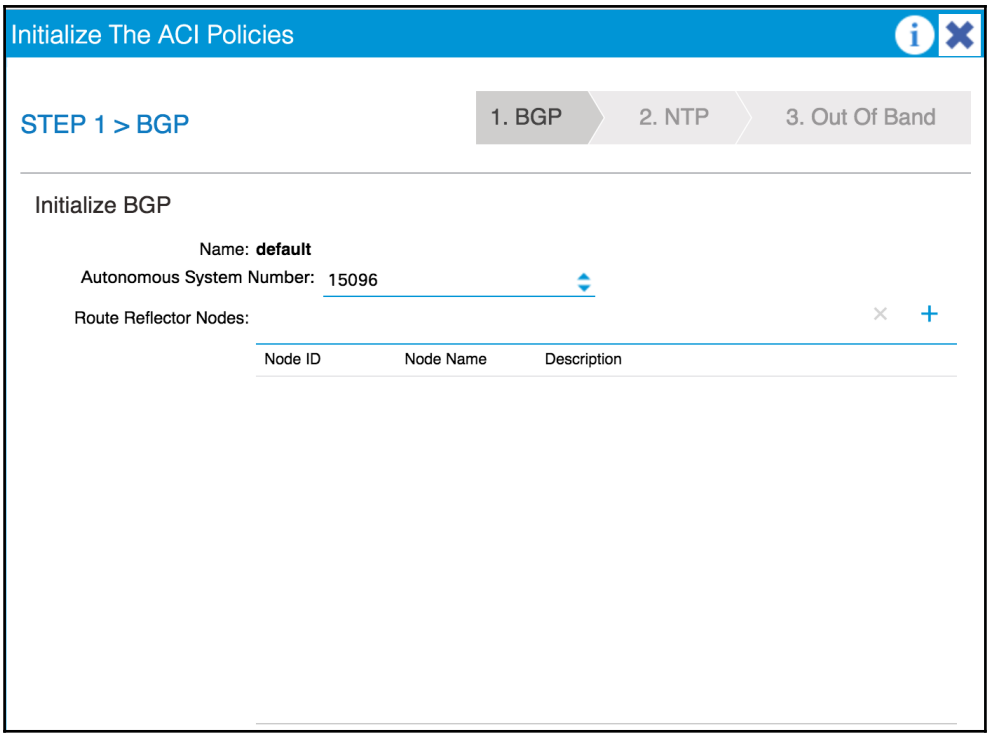

SDN Controlled Physical Underlay Network
APIC
Controller
APIC
Controller
APIC
Controller
Nexus 9500
Spine 1
Nexus 9500
Spine 2
Management Network
Nexus 9300
Leaf 1
Nexus 9300
Leaf 2
Nexus 9300
Leaf 3
Nexus 9300
Leaf 4
Physical
Server
Physical
Server
Physical
Server
Physical
Server
VM Server
VM Server
VM Server
VM Server
VM
1
VM
2
VM
3
VM
4
VM
5
VM
6
VM
7
VM
8
Cisco ACI + APIC

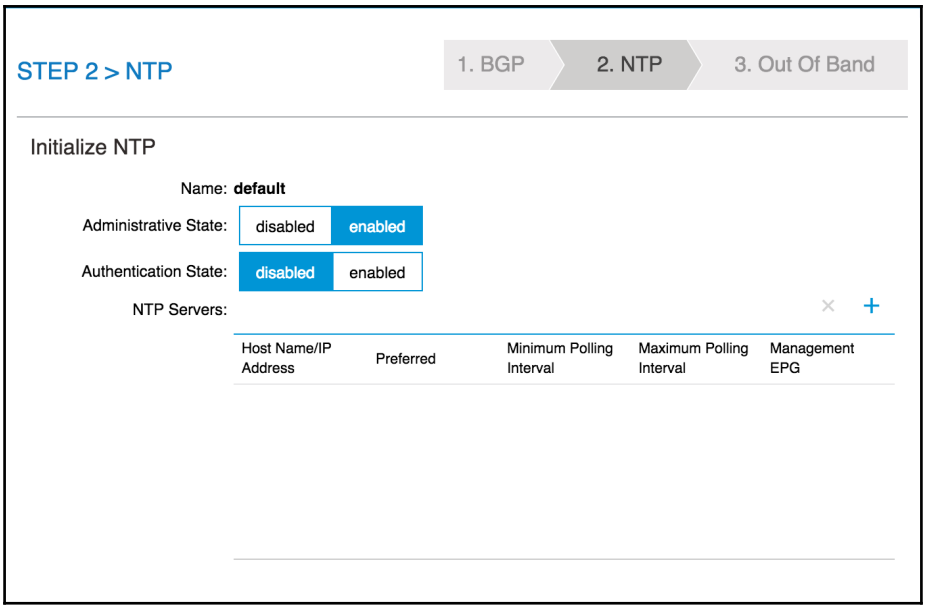

External vs Internal Accessability
Internet
APIC Controller
APIC Controller
APIC Controller
Nexus 9500 Spine 1
Nexus 9500 Spine 2
Externally Accessible
Internally Accessible
Management Network
Nexus 9300 Leaf 1
Nexus 9300 Leaf 2
Nexus 9300 Leaf 3
Nexus 9300 Leaf 4
Physical Server
VM Server
EPG DB
Physical Server
VM Server
EPG Web
Physical Server
VM Server
EPG DB
Physical Server
VM Server
EPG Web
DB 1
DB 2
Web 1
Web 2
DB 3
DB 4
Web 3
Web 4

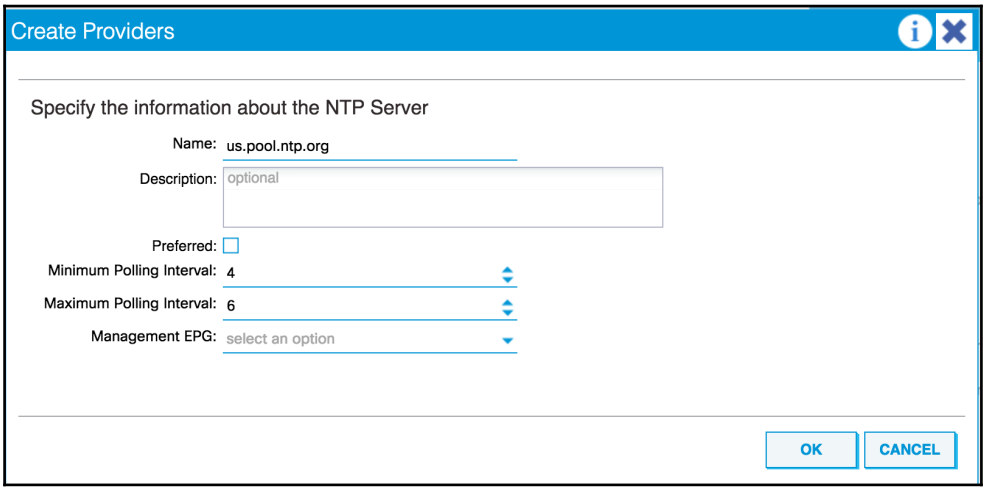

System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Main Menu
Advanced Mode
welcome, admin
ALL TENANTS
Add Tenant
Search:
enter name, descr
common
infra
mgmt
Sub Menu
All Tenants
ACTIONS

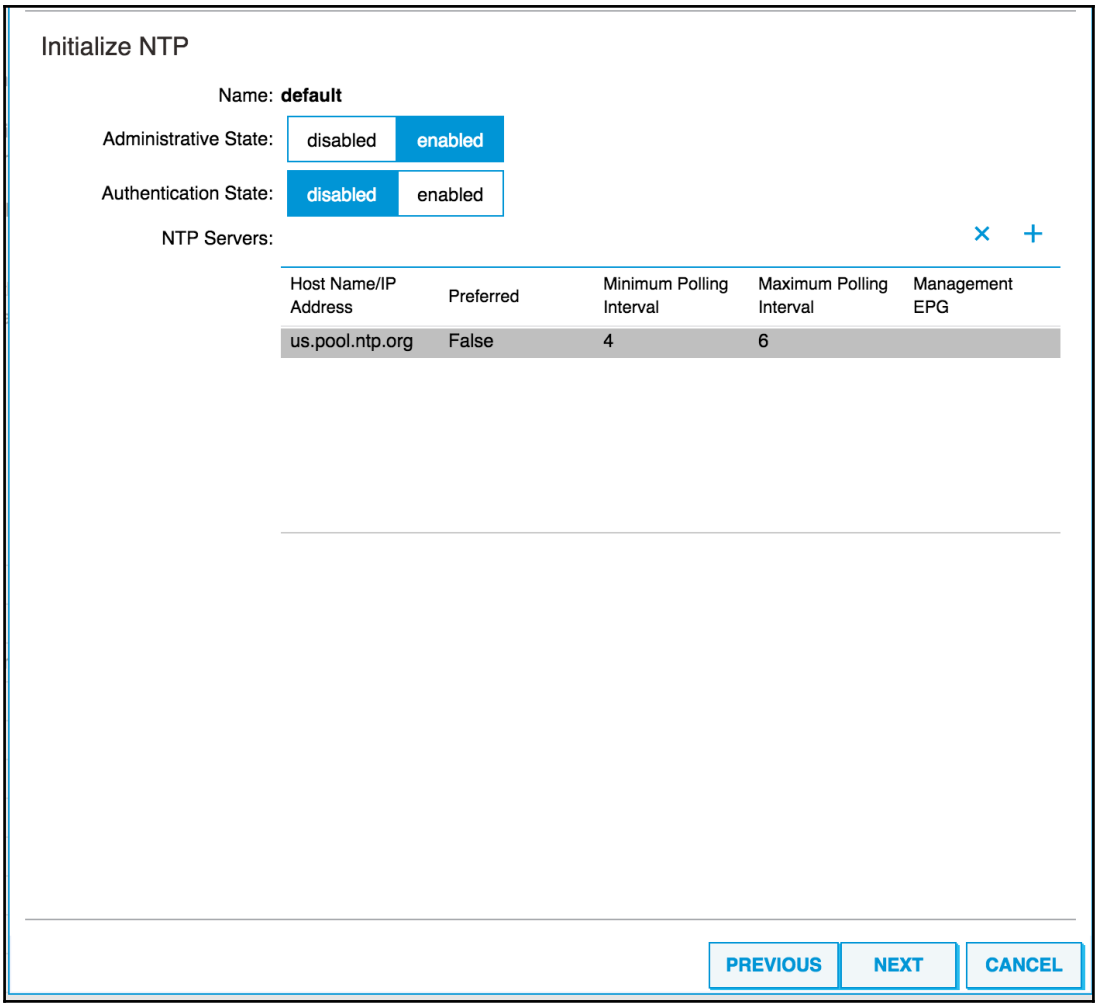

Your Cluster contains less than 3 in-service Controllers. Please Backup the cluster and do not utilize the fabric in its current state for production.
System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Advanced Mode
welcome, admin
QuickStart | Dashboard | Controllers | Faults
Quick Start
HELP
The Quick Start section on this page assists you in performing common and basic procedures. Click the icons for step-by-step instructions and for available concept documentation.
Caution: Cisco recommends that you do not mix configuration modes (Advanced or Basic). When you make a configuration in either mode and change the configuration using the other mode, unintended changes can occur. For example, if you apply an interface policy to two ports using Advanced mode and then change the settings of one port using Basic mode, your changes might be applied to both ports.
The See Also section provides links to QuickStart pages, which assist you in locating configuration menus related to common procedures.
For additional assistance, see the APIC documentation and the following applications in the See Also links:
• ACI Concepts—This link provides a detailed overview of the fundamental concepts of the ACI fabric and APIC.
• API Inspector—Using this built-in tool of APIC, you can capture API messaging as you perform tasks in the APIC GUI. The captured messages provide examples of the API operation that you can use to develop external applications that will use the API.
• APIC Management Information Model Reference—This tool provides detailed information about all object classes in APIC, including properties and hierarchy. In addition, the tool provides a listing of faults, events, and system messages.
Quick Start
The following procedures are useful in getting started:
First setup for the ACI fabric
Initialize the ACI fabric
Configure user accounts
Connect to a virtual machine (VM) management system
Add a tenant
Deploy an application profile
Deploy L4-L7 services using a service graph
Monitor fabric port, access port, or EPG statistics
Troubleshoot connectivity between two endpoints
See Also
ACI Concepts
API Inspector
APIC Management Information Model Reference
Tenants
Fabric inventory
Fabric policies
Access policies
VM inventory
L4-L7 inventory
L4-L7 packages
Authentication, authorization, and accounting (AAA)
Schedulers
Historical record policy
Firmware

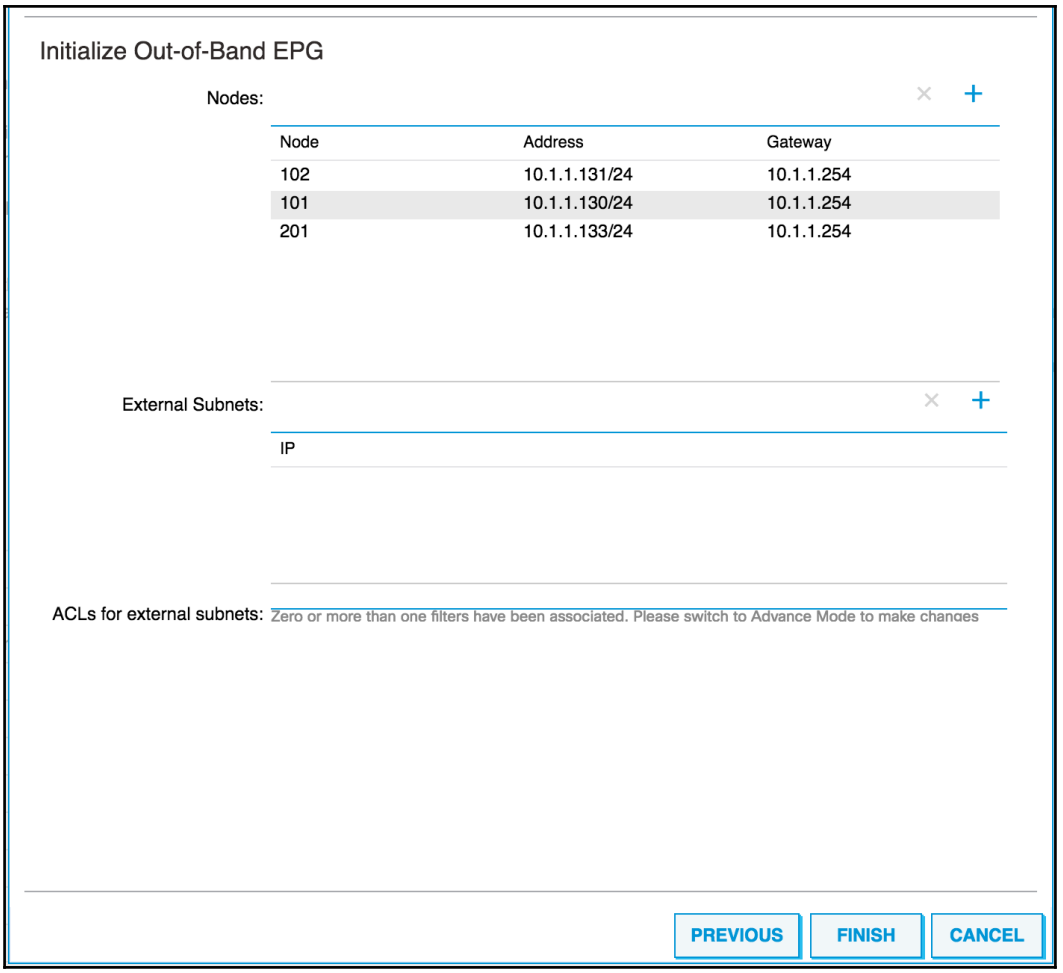

Initialize The ACI Policies
STEP 1 > BGP
1. BGP
2. NTP
3. Out Of Band
Initialize BGP
Name: default
Autonomous System Number:
Route Reflector Nodes:
Node ID
Node Name
Description

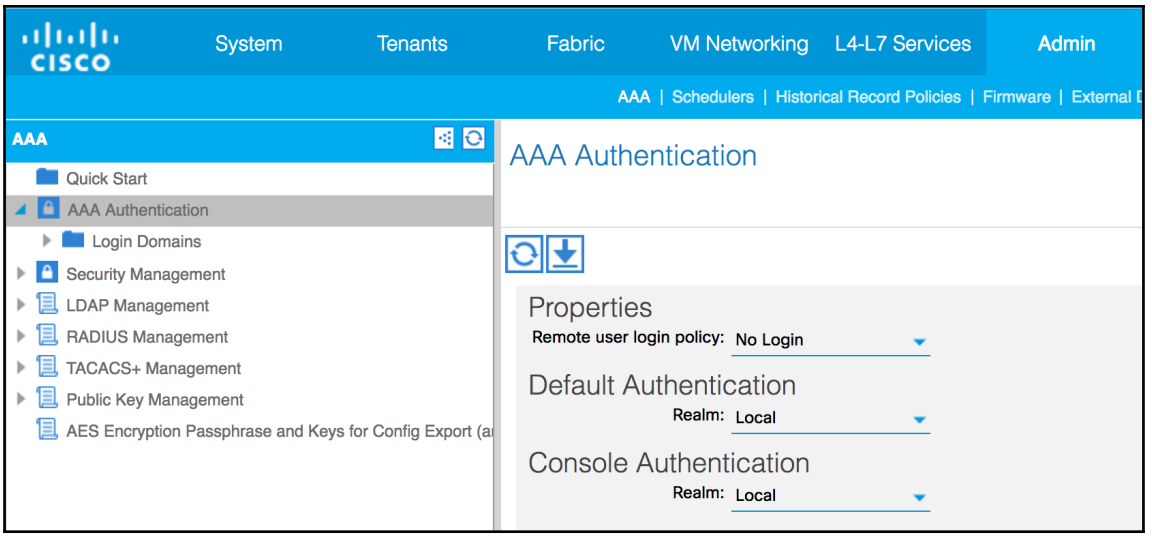

Initialize The ACI Policies
STEP 1 > BGP
1. BGP
2. NTP
3. Out Of Band
Initialize BGP
Name: default
Autonomous System Number: 15096
Route Reflector Nodes:
Node ID
Node Name
Description

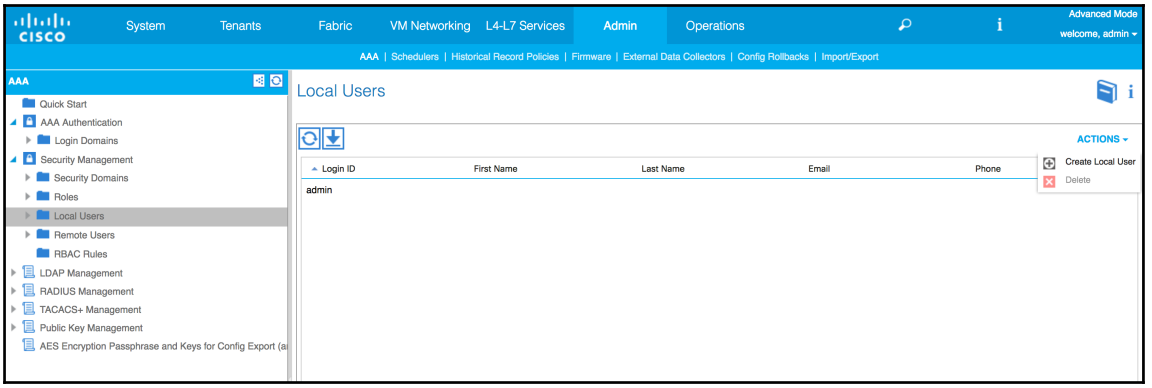

STEP 2 > NTP
1. BGP
2. NTP
3. Out Of Band
Initialize NTP
Name: default
Administrative State:
disabled
enabled
Authentication State:
disabled
enabled
NTP Servers:
Host Name/IP Address
Preferred
Minimum Polling Interval
Maximum Polling Interval
Management EPG

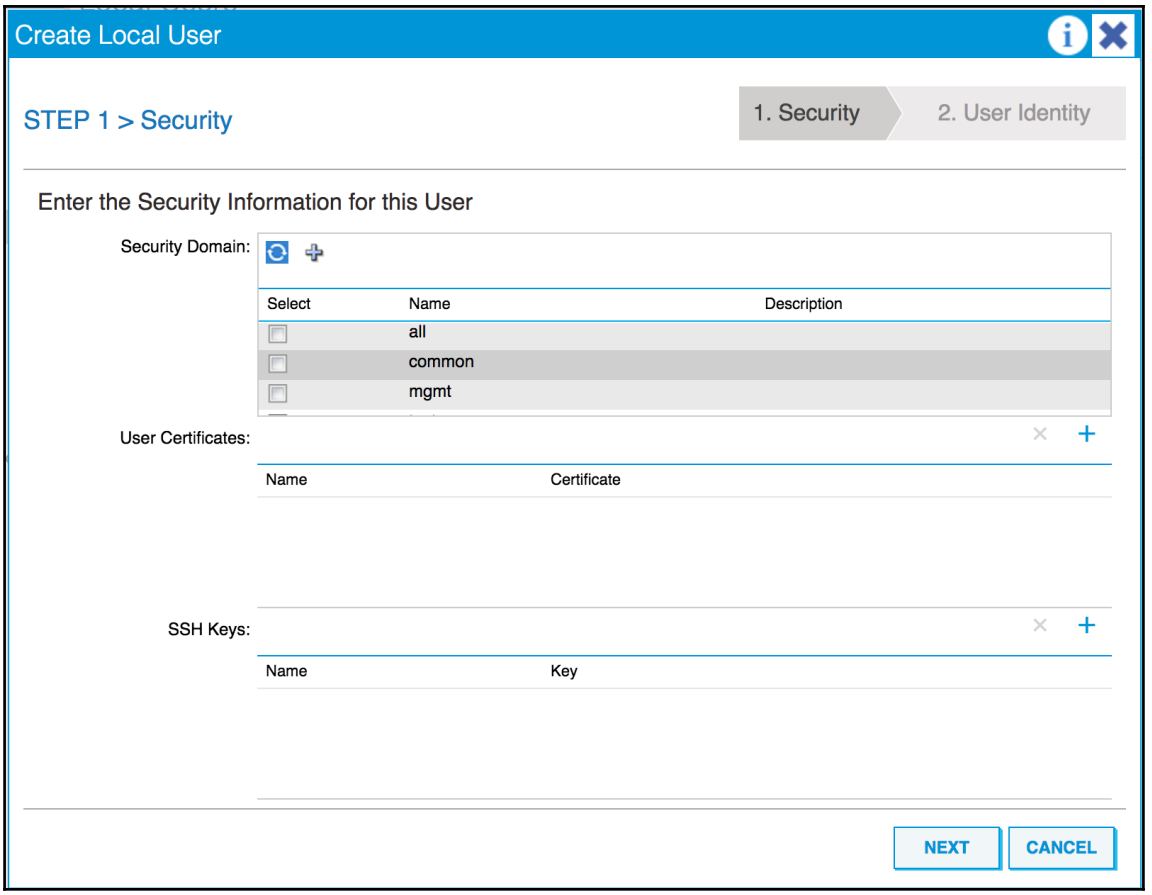

Create Providers
Specify the information about the NTP Server
Name: us.pool.ntp.org
Description: optional
Preferred:
Minimum Polling Interval: 4
Maximum Polling Interval: 6
Management EPG: select an option
OK
CANCEL

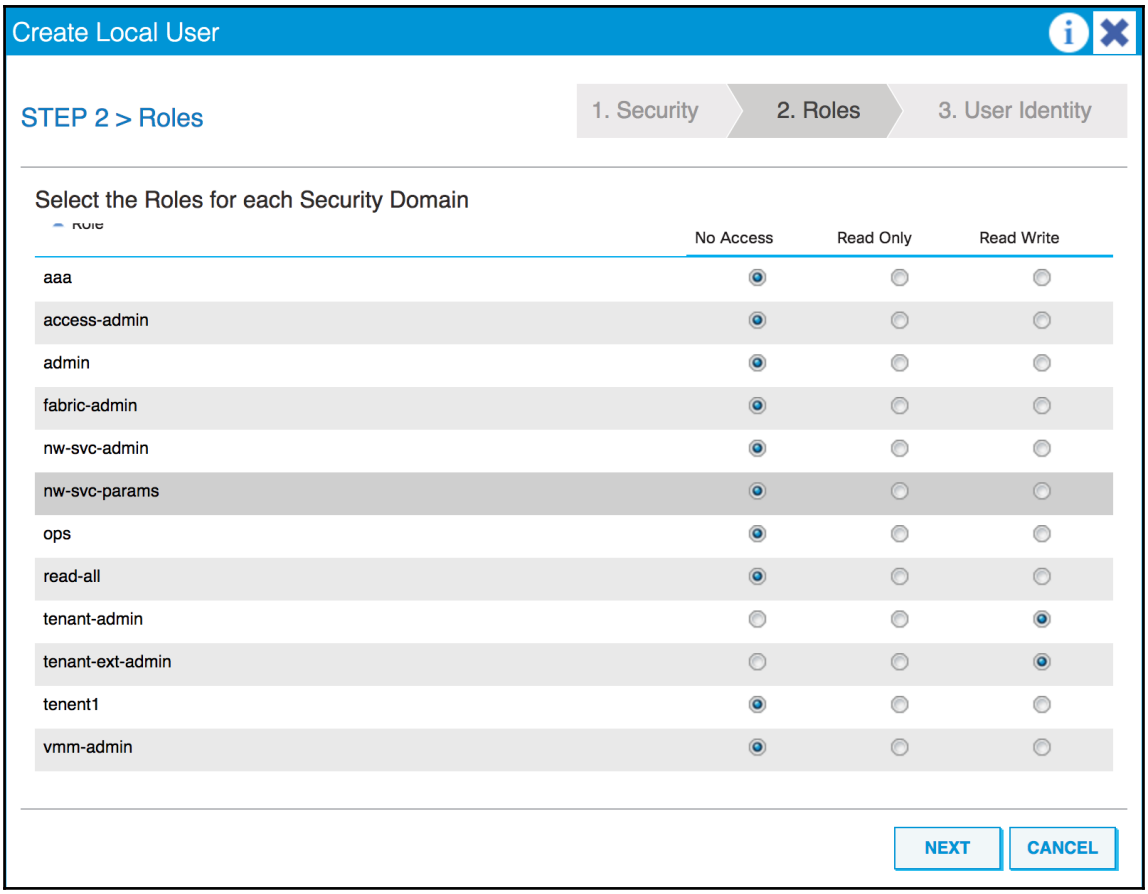

Initialize NTP
Name: default
Administrative State:
disabled
enabled
Authentication State:
disabled
enabled
NTP Servers:
Host Name/IP Address
Preferred
Minimum Polling Interval
Maximum Polling Interval
Management EPG
us.pool.ntp.org
False
4
6
PREVIOUS
NEXT
CANCEL

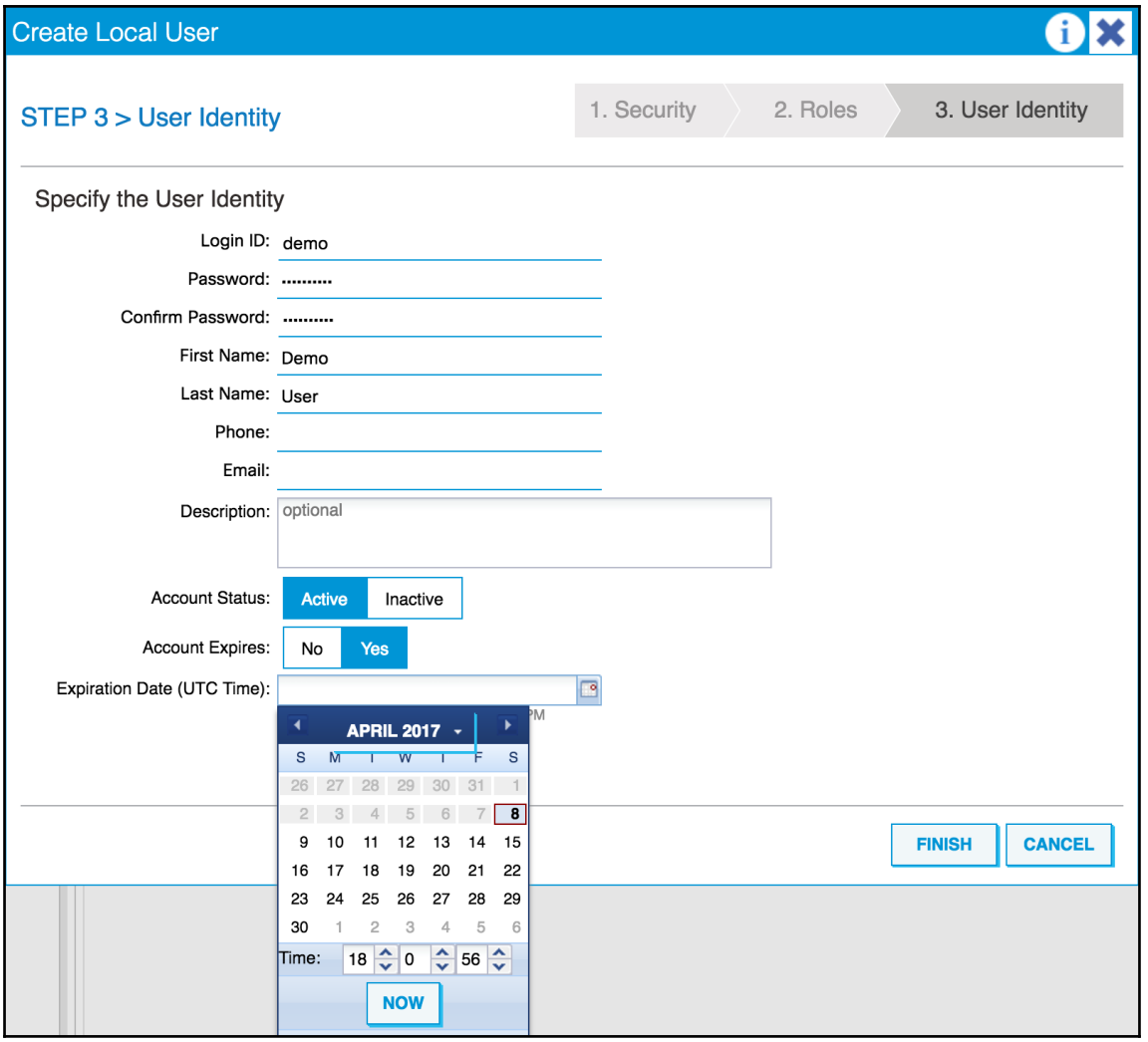

Initialize Out-of-Band EPG
Nodes:
Node
Address
Gateway
102
10.1.1.131/24
10.1.1.254
101
10.1.1.130/24
10.1.1.254
201
10.1.1.133/24
10.1.1.254
External Subnets:
IP
ACLs for external subnets:
Zero or more than one filters have been associated. Please switch to Advance Mode to make changes
PREVIOUS
FINISH
CANCEL

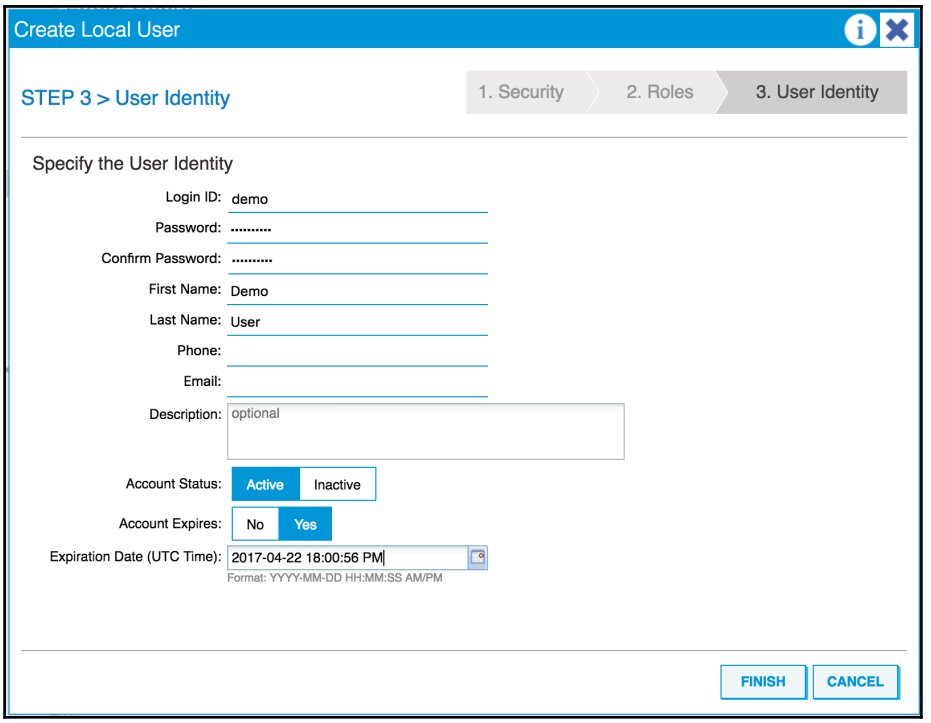

System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
AAA | Schedulers | Historical Record Policies | Firmware | External
AAA
Quick Start
AAA Authentication
Login Domains
Security Management
LDAP Management
RADIUS Management
TACACS+ Management
Public Key Management
AES Encryption Passphrase and Keys for Config Export (a
AAA Authentication
Properties
Remote user login policy: No Login
Default Authentication
Realm: Local
Console Authentication
Realm: Local

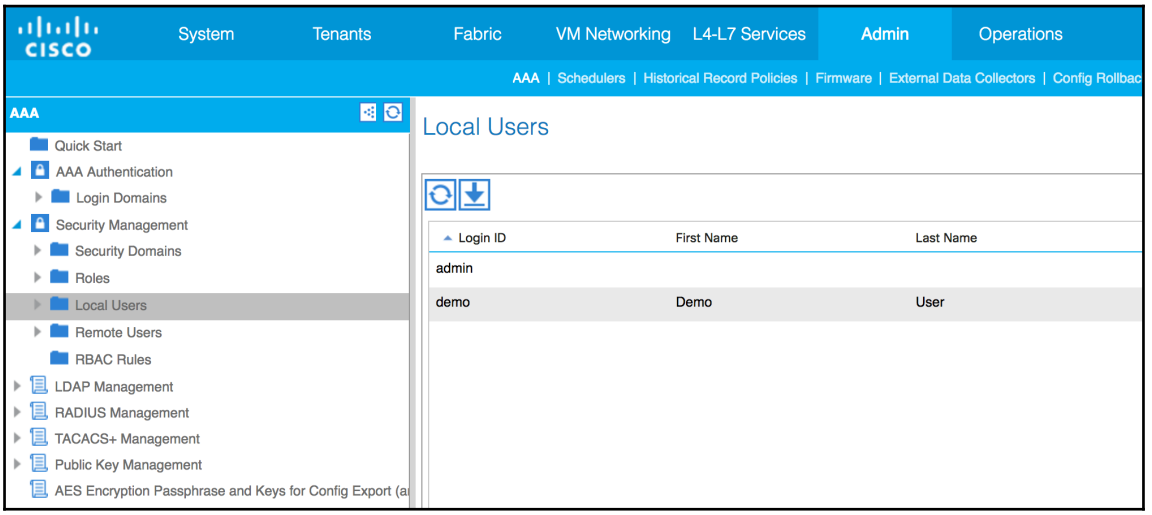

System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Advanced Mode
welcome, admin
AAA | Schedulers | Historical Record Policies | Firmware | External Data Collectors | Config Rollbacks | Import/Export
AAA
Quick Start
AAA Authentication
Login Domains
Security Management
Security Domains
Roles
Local Users
Remote Users
RBAC Rules
LDAP Management
RADIUS Management
TACACS+ Management
Public Key Management
AES Encryption Passphrase and Keys for Config Export (a
Local Users
ACTIONS
Create Local User
Delete
Login ID
First Name
Last Name
Email
Phone
admin

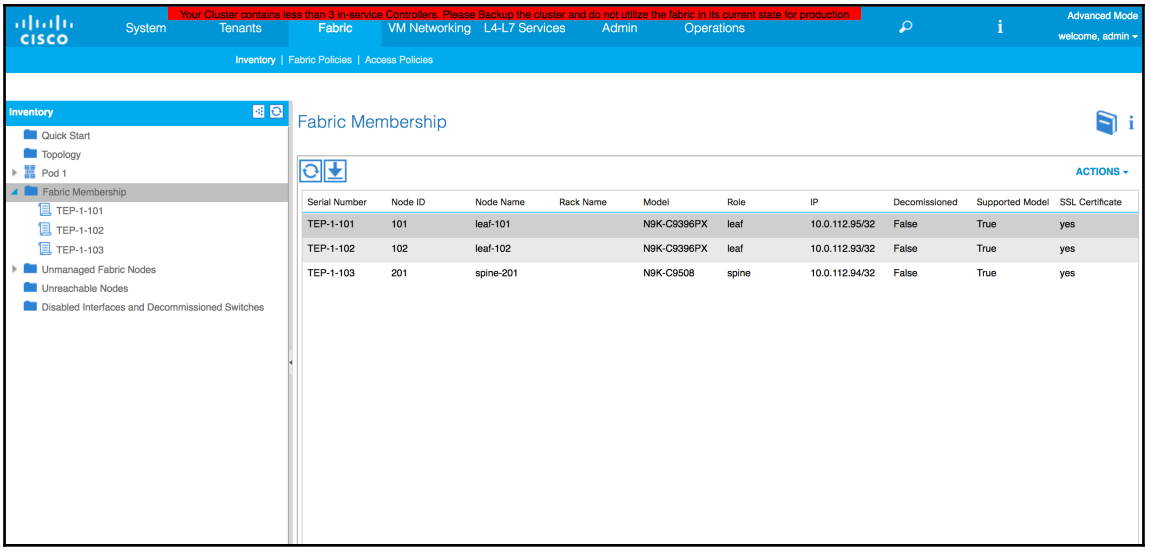

Create Local User
STEP 1 > Security
1. Security
2. User Identity
Enter the Security Information for this User
Security Domain:
Select
Name
Description
all
common
mgmt
User Certificates:
Name
Certificate
SSH Keys:
Name
Key
NEXT
CANCEL

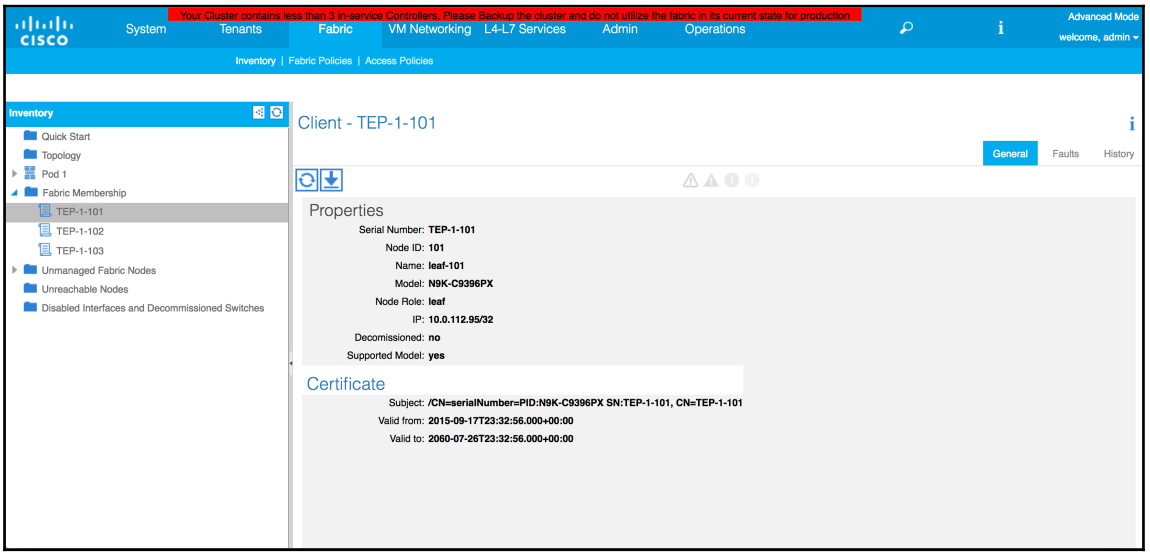

Create Local User
STEP 2 > Roles
1. Security
2. Roles
3. User Identity
Select the Roles for each Security Domain
Role
No Access
Read Only
Read Write
aaa
access-admin
admin
fabric-admin
nw-svc-admin
nw-svc-params
ops
read-all
tenant-admin
tenant-ext-admin
tenent1
vmm-admin
NEXT
CANCEL


Create Local User
STEP 3 > User Identity
1. Security
2. Roles
3. User Identity
Specify the User Identity
Login ID: demo
Password: .....
Confirm Password: .....
First Name: Demo
Last Name: User
Phone:
Email:
Description: optional
Account Status: Active Inactive
Account Expires: No Yes
Expiration Date (UTC Time):
APRIL 2017
S M T W T F S
26 27 28 29 30 31 1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 1 2 3 4 5 6
Time: 18 0 56
NOW
FINISH
CANCEL

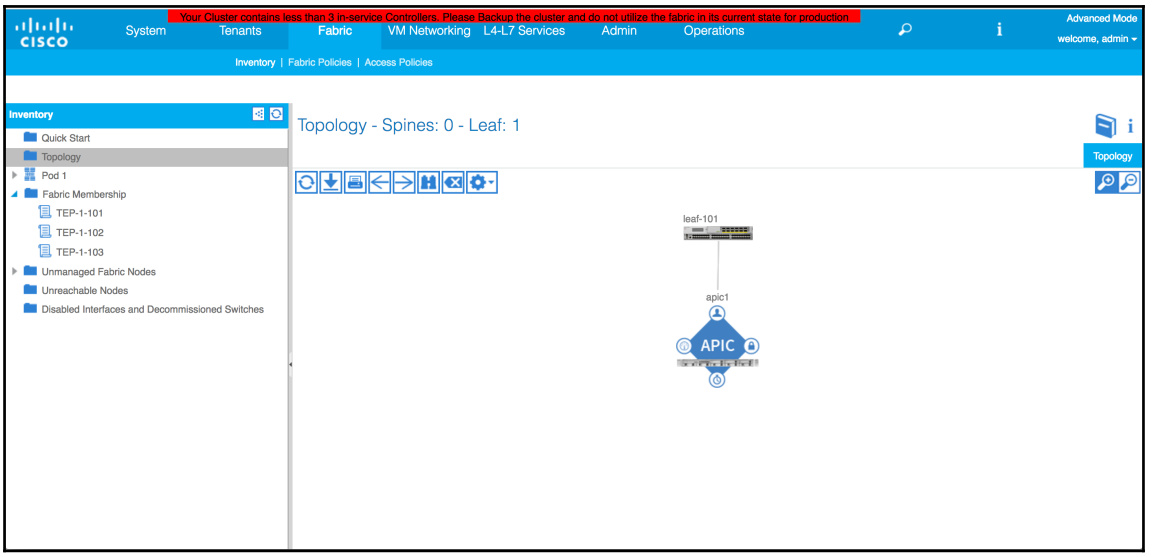

Create Local User
STEP 3 > User Identity
1. Security
2. Roles
3. User Identity
Specify the User Identity
Login ID: demo
Password: .....
Confirm Password: .....
First Name: Demo
Last Name: User
Phone:
Email:
Description: optional
Account Status: Active Inactive
Account Expires: No Yes
Expiration Date (UTC Time): 2017-04-22 18:00:56 PM
Format: YYYY-MM-DD HH:MM:SS AM/PM
FINISH
CANCEL

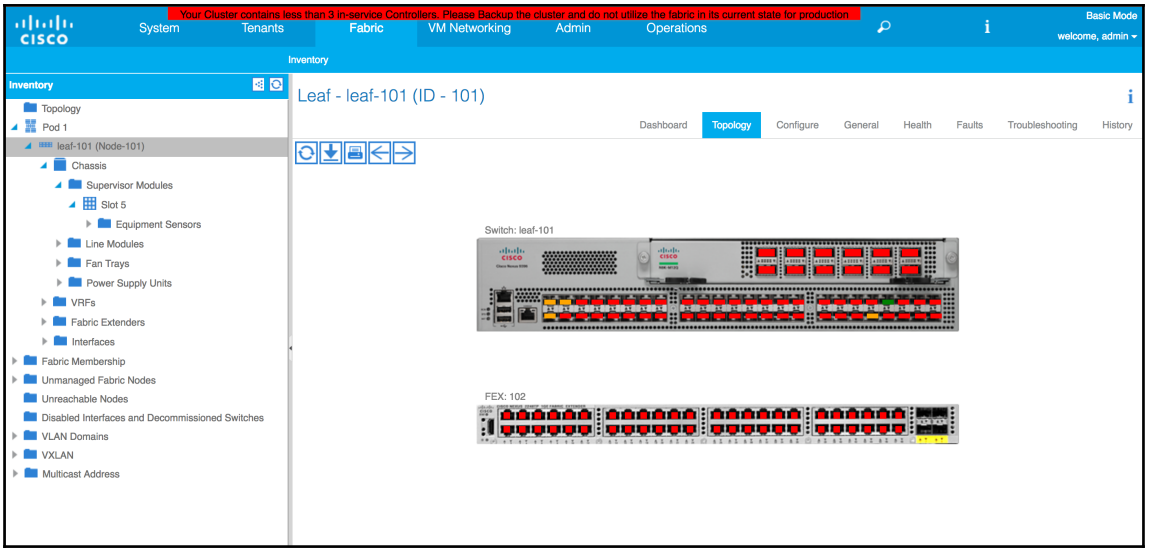

System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
AAA | Schedulers | Historical Record Policies | Firmware | External Data Collectors | Config Rollbac
AAA
Quick Start
AAA Authentication
Login Domains
Security Management
Security Domains
Roles
Local Users
Remote Users
RBAC Rules
LDAP Management
RADIUS Management
TACACS+ Management
Public Key Management
AES Encryption Passphrase and Keys for Config Export (a
Local Users
Login ID
First Name
Last Name
admin
demo
Demo
User

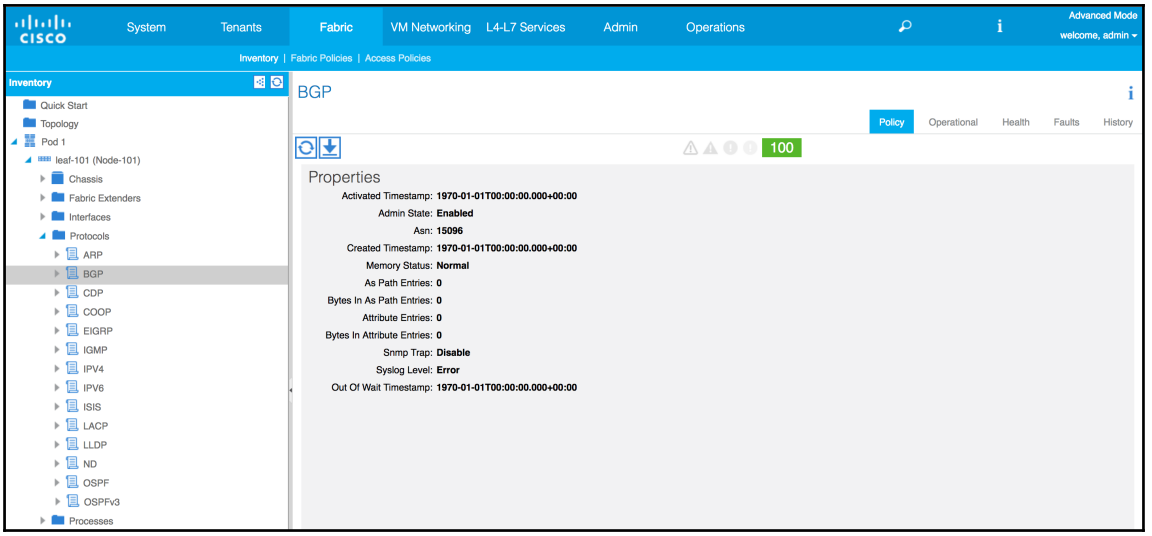

Your Cluster contains less than 3 in-service Controllers. Please Backup the cluster and do not utilize the fabric in its current state for production
System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Advanced Mode
welcome, admin
Inventory | Fabric Policies | Access Policies
Inventory
Quick Start
Topology
Pod 1
Fabric Membership
TEP-1-101
TEP-1-102
TEP-1-103
Unmanaged Fabric Nodes
Unreachable Nodes
Disabled Interfaces and Decommissioned Switches
Fabric Membership
ACTIONS
Serial Number Node ID Node Name Rack Name Model Role IP Decomissioned Supported Model SSL Certificate
TEP-1-101 101 leaf-101 N9K-C9396PX leaf 10.0.112.95/32 False True yes
TEP-1-102 102 leaf-102 N9K-C9396PX leaf 10.0.112.93/32 False True yes
TEP-1-103 201 spine-201 N9K-C9508 spine 10.0.112.94/32 False True yes

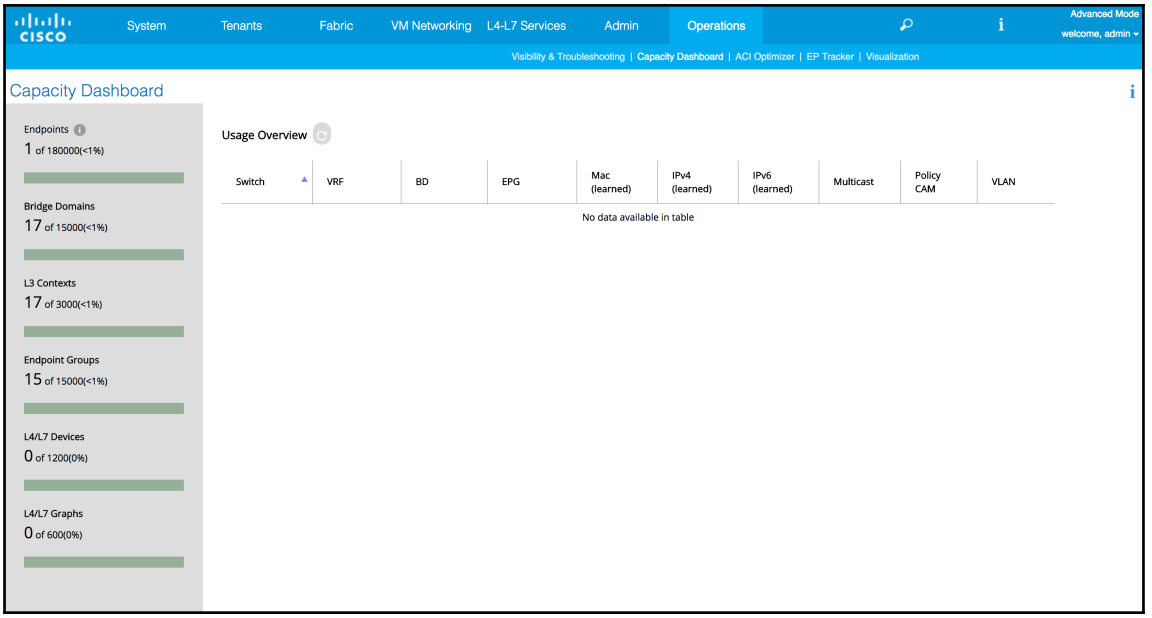

Your Cluster contains less than 3 in-service Controllers. Please Backup the cluster and do not utilize the fabric in its current state for production
System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Advanced Mode
welcome, admin
Inventory | Fabric Policies | Access Policies
Inventory
Quick Start
Topology
Pod 1
Fabric Membership
TEP-1-101
TEP-1-102
TEP-1-103
Unmanaged Fabric Nodes
Unreachable Nodes
Disabled Interfaces and Decommissioned Switches
Client - TEP-1-101
General
Faults
History
Properties
Serial Number: TEP-1-101
Node ID: 101
Name: leaf-101
Model: N9K-C9396PX
Node Role: leaf
IP: 10.0.112.95/32
Decomissioned: no
Supported Model: yes
Certificate
Subject: /CN=serialNumber=PID:N9K-C9396PX SN:TEP-1-101, CN=TEP-1-101
Valid from: 2015-09-17T23:32:56.000+00:00
Valid to: 2060-07-26T23:32:56.000+00:00

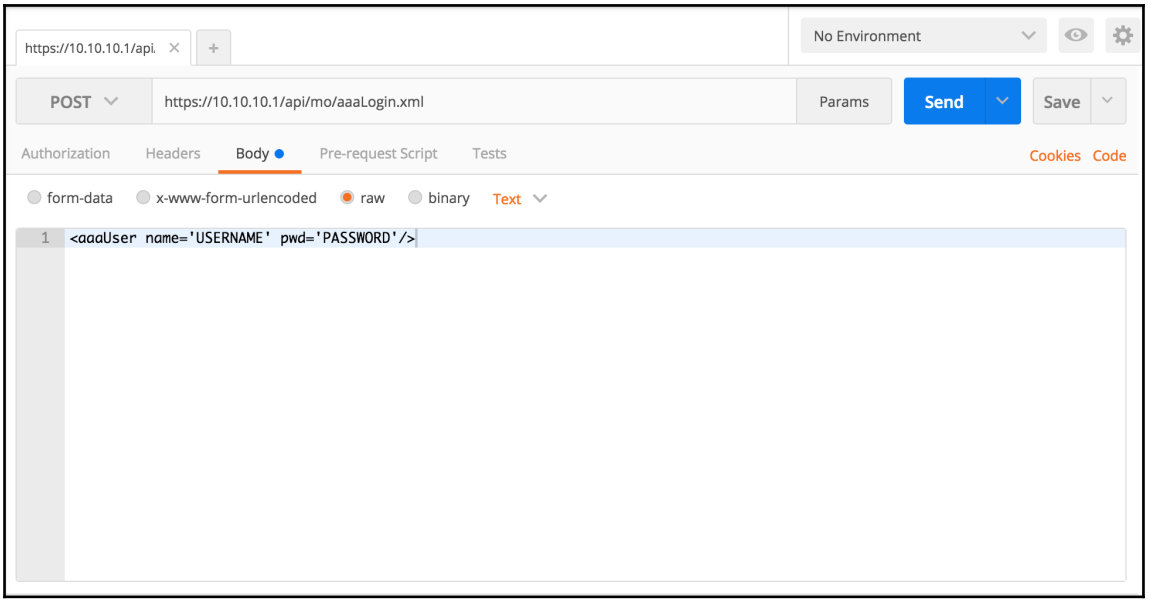
Your Cluster contains less than 3 in-service Controllers. Please Backup the cluster and do not utilize the fabric in its current state for production
System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Advanced Mode
welcome, admin
Inventory | Fabric Policies | Access Policies
Inventory
Quick Start
Topology
Pod 1
Fabric Membership
TEP-1-101
TEP-1-102
TEP-1-103
Unmanaged Fabric Nodes
Unreachable Nodes
Disabled Interfaces and Decommissioned Switches
POD - 1
Dashboard
Topology
Operational
Faults
Troubleshooting
History
Pod Health
0
score
4. Apr
04:00
08:00
12:00
16:00
20:00
Time
Nodes With Health ≤ 99
99
Name
Type
Health Score
leaf-101
leaf
90
Fault Counts By Domain
Fault Level:
SYSTEM WIDE 3 13 21 121
Access 0 0 0 2
External 0 1 0 0
Framework 0 7 0 0
Infra 3 5 8 119
Management 0 0 0 0
Security 0 0 0 0
Tenant 0 0 13 0
Fault Counts By Type
Communicatio... 0 1 0 0
Config 0 3 19 14

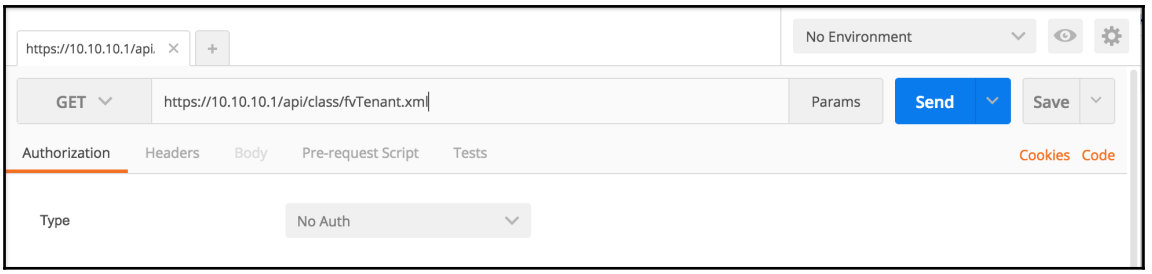

Your Cluster contains less than 3 in-service Controllers. Please Backup the cluster and do not utilize the fabric in its current state for production
System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Advanced Mode
welcome, admin
Inventory | Fabric Policies | Access Policies
Inventory
Quick Start
Topology
Pod 1
Fabric Membership
TEP-1-101
TEP-1-102
TEP-1-103
Unmanaged Fabric Nodes
Unreachable Nodes
Disabled Interfaces and Decommissioned Switches
Topology - Spines: 0 - Leaf: 1
Topology
leaf-101
apic1
APIC


Your Cluster contains less than 3 in-service Controllers. Please Backup the cluster and do not utilize the fabric in its current state for production
System
Tenants
Fabric
VM Networking
Admin
Operations
Basic Mode
welcome, admin
Inventory
Inventory
Topology
Pod 1
leaf-101 (Node-101)
Chassis
Supervisor Modules
Slot 5
Equipment Sensors
Line Modules
Fan Trays
Power Supply Units
VRFs
Fabric Extenders
Interfaces
Fabric Membership
Unmanaged Fabric Nodes
Unreachable Nodes
Disabled Interfaces and Decommissioned Switches
VLAN Domains
VXLAN
Multicast Address
Leaf - leaf-101 (ID - 101)
Dashboard
Topology
Configure
General
Health
Faults
Troubleshooting
History
Switch: leaf-101
FEX: 102

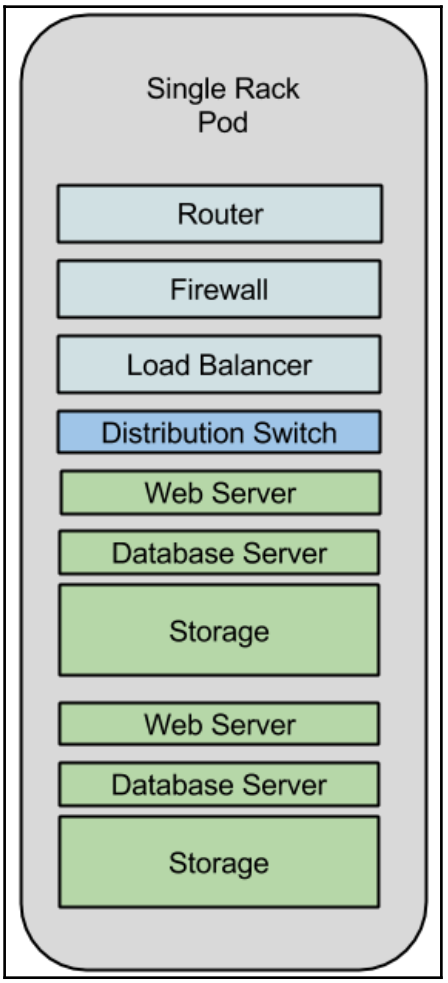

System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Advanced Mode
welcome, admin
Inventory | Fabric Policies | Access Policies
Inventory
Quick Start
Topology
Pod 1
leaf-101 (Node-101)
Chassis
Fabric Extenders
Interfaces
Protocols
ARP
BGP
CDP
COOP
EIGRP
IGMP
IPV4
IPV6
ISIS
LACP
LLDP
ND
OSPF
OSPFv3
Processes
BGP
Policy
Operational
Health
Faults
History
100
Properties
Activated Timestamp: 1970-01-01T00:00:00.000+00:00
Admin State: Enabled
Asn: 15096
Created Timestamp: 1970-01-01T00:00:00.000+00:00
Memory Status: Normal
As Path Entries: 0
Bytes In As Path Entries: 0
Attribute Entries: 0
Bytes In Attribute Entries: 0
Snmp Trap: Disable
Syslog Level: Error
Out Of Wait Timestamp: 1970-01-01T00:00:00.000+00:00

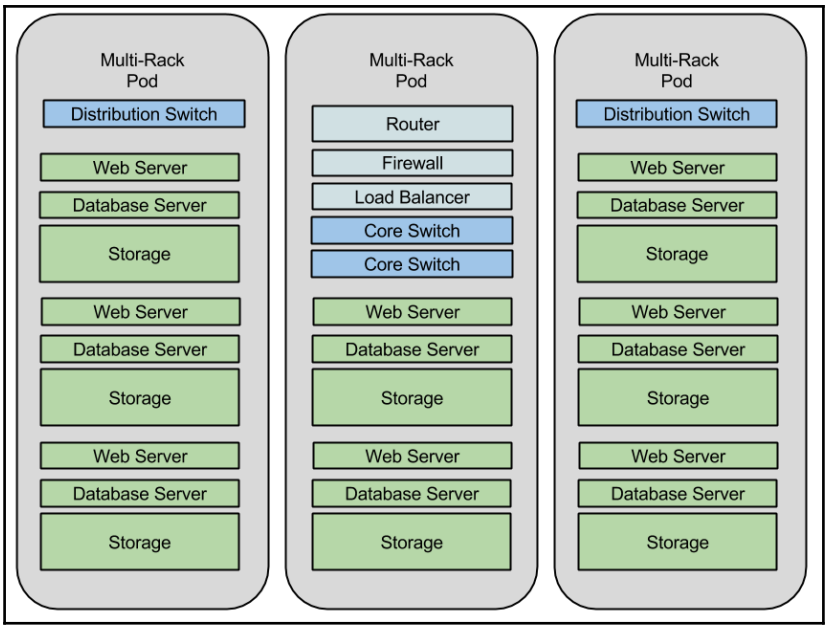

System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Advanced Mode
welcome, admin
Visibility & Troubleshooting | Capacity Dashboard | ACI Optimizer | EP Tracker | Visualization
Capacity Dashboard
Endpoints
1 of 180000(<1%)
Bridge Domains
17 of 15000(<1%)
L3 Contexts
17 of 3000(<1%)
Endpoint Groups
15 of 15000(<1%)
L4/L7 Devices
0 of 1200(0%)
L4/L7 Graphs
0 of 600(0%)
Usage Overview
Switch
VRF
BD
EPG
Mac (learned)
IPv4 (learned)
IPv6 (learned)
Multicast
Policy CAM
VLAN
No data available in table

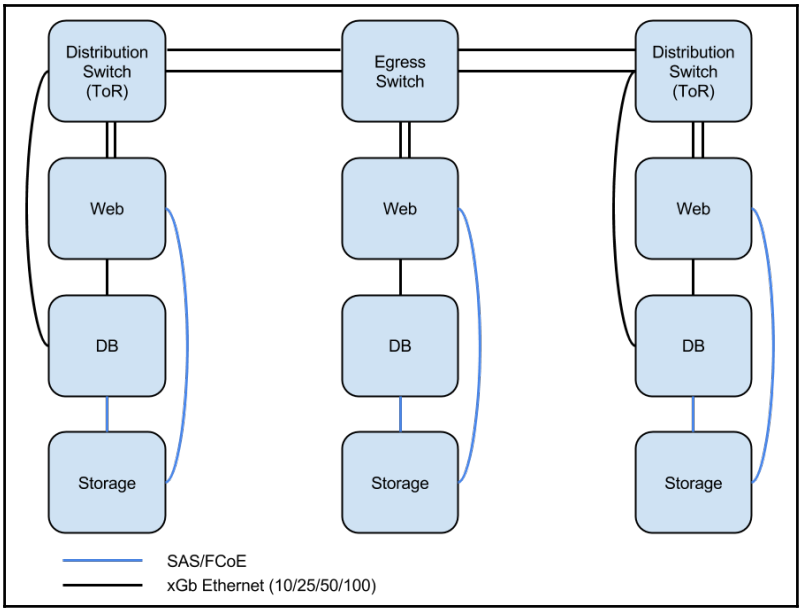

https://10.10.10.1/api.
No Environment
POST
https://10.10.10.1/api/mo/aaaLogin.xml
Params
Send
Save
Authorization
Headers
Body
Pre-request Script
Tests
Cookies
Code
form-data
x-www-form-urlencoded
raw
binary
Text
1
<aaaUser name='USERNAME' pwd='PASSWORD'/>

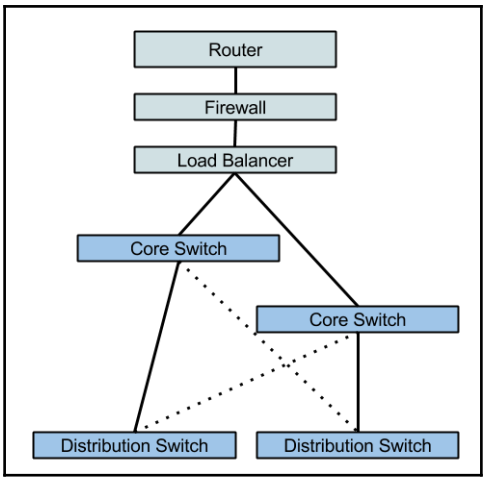

https://10.10.10.1/api.
No Environment
GET
https://10.10.10.1/api/class/fvTenant.xml
Params
Send
Save
Authorization
Headers
Body
Pre-request Script
Tests
Cookies
Code
Type
No Auth

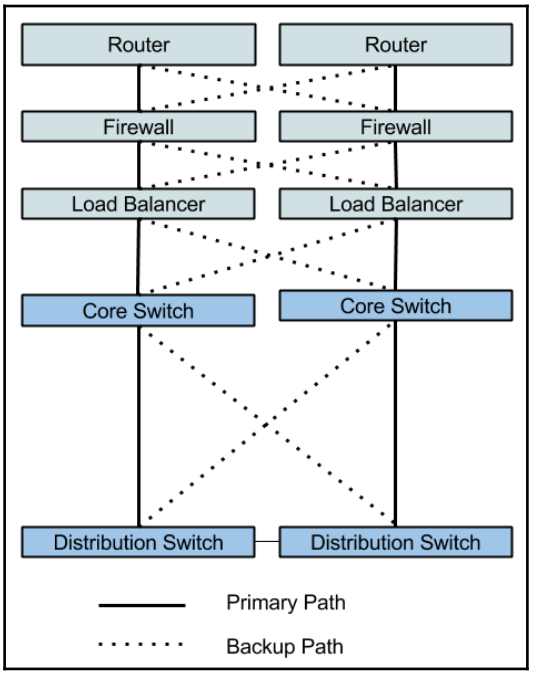
Chapter 9: Where to Start When Building a Next Generation Network

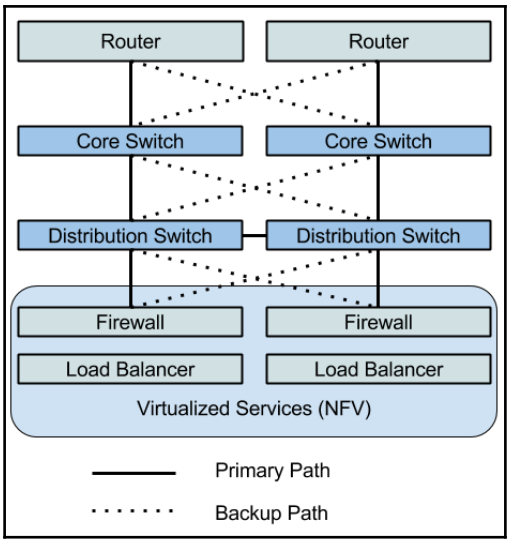


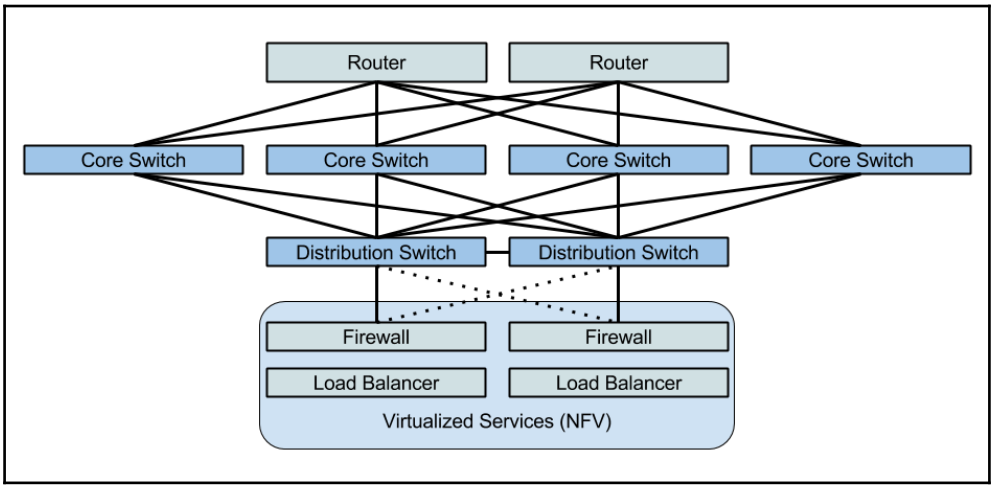

Multi-Rack Pod
Distribution Switch
Web Server
Database Server
Storage
Web Server
Database Server
Storage
Web Server
Database Server
Storage
Multi-Rack Pod
Router
Firewall
Load Balancer
Core Switch
Core Switch
Web Server
Database Server
Storage
Web Server
Database Server
Storage
Multi-Rack Pod
Distribution Switch
Web Server
Database Server
Storage
Web Server
Database Server
Storage
Web Server
Database Server
Storage


Distribution Switch (ToR)
Egress Switch
Distribution Switch (ToR)
Web
DB
Storage
Web
DB
Storage
Web
DB
Storage
SAS/FCoE
xGb Ethernet (10/25/50/100)


Router
Firewall
Load Balancer
Core Switch
Core Switch
Distribution Switch
Distribution Switch


Router
Router
Firewall
Firewall
Load Balancer
Load Balancer
Core Switch
Core Switch
Distribution Switch
Distribution Switch
Primary Path
Backup Path


Router
Router
Core Switch
Core Switch
Distribution Switch
Distribution Switch
Firewall
Firewall
Load Balancer
Load Balancer
Virtualized Services (NFV)
Primary Path
Backup Path


Router
Router
Core Switch
Core Switch
Core Switch
Core Switch
Distribution Switch
Distribution Switch
Firewall
Firewall
Load Balancer
Load Balancer
Virtualized Services (NFV)

Core & SDDC Services Switch

Engineering Request for Information

(RFI)

Customer is seeking responses for two classes of switching solutions:

1. **Core Services**
   A service-provider, carrier-grade platform supporting multiple interfaces and the ability to forward switched and routed packets at very high data rates. Addtionally, it must support various routing protocols and network service delivery mechanisms.
   Must include high availability and resiliency features and best-in-class manageability and health visability.

2. **SDDC Services**
   A service-provider, carrier-grade platform supporting multiple interfaces and the ability to forward, filter and modify switched and routed local and PoD specific packets and streams (IPv4 and IPv6) at very high data rates. It also includes but is not limited to, the termination of VLXAN based services, appliances, storage devices, etc.
   Must include high availability and resiliency features and best-in-class manageability and health visability.

Core & SDDC Services Switch - Engineering Request for Information (RFI)

I. Description / Objectives:

1. This request for information (RFI) is being issued by Customer's Engineering and Technology Team.
   Material contained within represents requirements from both Engineering and Customer's Network Management Department.
   Review and evaluation of submitted material will likewise be conducted by both the Engineering and Network Management teams.

2. It is understood that there may have been (or is currently underway), similar RFI/RFQ/RFP/etc. exercises originating from other departments within Customer. This particular request should be viewed (and completed) independently of said exercises.
   That said, information gleaned from the response to this request may be used in conjunction with prior/concurrently submitted material.

3. Customer is actively looking to quantify and qualify various capabilities of switches and switching solutions.

4. Customer is actively looking to understand the availability and timelines of switches and switching devices/solutions that meet specific criteria.

5. Customer is actively looking to understand the licensing and fee model(s) associated with switches and switching devices/solutions.

6. Customer is actively looking at various switch architectures and deployment models.

7. No assumption should be made with respect to differentiating various deployment models. That said, Customer is looking for two **solutions. One that is appropriate for servicing the "core" of a network and a second that is appropriate for SDDC services.**
   Respondents may submit different products/solutions to satiate the different requirements outlined immediately above.
   Respondents may also submit a single product/solution if they feel it well suited in either or both applications; please indicate as such.

   It is expected and required that respondents will submit a **SEPARATE and DISCRETE WORKSHEET** (Response Section "B") **for each product / solution presented** (e.g. one for a core switching solution and another for a SDDC switching solution).

8. The information contained within this RFI (plus all associated attachments, articles, appendicies, etc.) and the reponses thereto are to be considered confidential and under non-disclosure. This material is intended only for the person(s) or entity to which it is addressed and may contain proprietary information, which is privileged, confidential, or subject to copyright belonging to Customer. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited.

9. No contract will be awarded as a result of this RFI. This RFI does not in any way constitute a contractual obligation on the behalf of either party.

10. Customer shall not incur any obligation, liability, or cause of action whatsoever by reason of this RFI or any actions or inactions relative hereto. Respondents are solely responsible for all expenses associated with preparing and responding to this RFI. All RFI responses shall become the property of Customer and will not be returned to respondents.

11. Customer may, at its sole discretion, issue a follow-up Request for Proposal ("RFP") to some or all of the RFI respondents.
    Customer shall have no obligation to issue a follow-up RFP to any RFI respondent.

12. Customer is committed to a policy of nondiscrimination in its vendors, contractors and other suppliers. All qualified vendors, contractors and suppliers are reviewed without regard to race, color, religion, sex, national origin, ancestry, age, marital or veteran status, sexual orientation/ preferences or non-disqualifying physical or mental handicaps.

Core & SDDC Services Switch - Engineering Request for Information (RFI)

II. Instructions / Response Sections:

A. Respondent must include a one-page, executive-summary style descriptive outlining key differentiators of the submitted product/solution.

B. Respondent must complete the "Respondent Section" of the attached requirements worksheet in its entirety.
- A separate worksheet should be filled out for each viable product/solution submitted for consideration.
- No assumptions should be made regarding the network architecture in which the respondent's product/solution will be placed/integrated.
- The approximate retail "street" price must be included for each unit involved in the solution. No assumption of discounts should be made.

Capability field of the worksheet should be completed using the following values:
- "**5**" - Submitted product/solution **fully delivers** required functionality today.
- "**4**" - Submitted product/solution **can** fully deliver required functionality with only minor changes needed (< 1 month development time).
- "**3**" - Submitted product/solution **can** fully deliver required functionality with 1 - 3 months development time.
- "**2**" - Submitted product/solution **can** fully deliver required functionality with 4 - 8 months development time.
- "**1**" - Submitted product/solution **can not** deliver required functionality **but** there is a product roadmap to do so (future hardware platform, etc.).
- "**0**" - Submitted product/solution **can not** deliver required functionality nor is there a product roadmap to do so.
- "**NA**" - Required functionality is not applicable to the submitted product/solution

Notes:
- *Please use the "Notes" field to provide relevant details pertaining to the product or solution's ability to deliver required functionality.*
- *Please use the "Notes" field to describe capabilities that may exist above and beyond the required functionality.*
- *If capabilty "1" is used, please use the "Notes" field to indicate the timeframe and details surrounding the product/solution roadmap.*
- *If **any** amount of development time is needed to satiate the requirement, please use the "Notes" field to detail motivators:*
  - *NRE*
  - *Quantity commitments*
  - *Financial commitments*
  - *Etc.*

IPv4 and IPv6 fields should be completed as follows:
- "**Yes**" - Submitted product/solution **IS** fully "aware" and capable as it relates to the referenced protocol and to the stated line item.
- "**No**" - Submitted product/solution **IS NOT** fully "aware" and capable as it relates to the referenced protocol and to the stated line item.
- "**NA**" - The referenced protocol is not applicable or relevant to the stated line item.
- "**Notes**" - Submitted product/solution may be partially "aware" and capable as it relates to the referenced protocol and to the stated line item. Please use the "Notes" field to provide relevant details and/or time lines associated with full compatibility

B/L field of the worksheet should be completed as follows:
- "**B**" - Capability is included as a "base" feature; no additional licencing fees, procedural costs, labor fees or other financial dependancies are needed to enable or leverage the capability.
- "**L**" - Capability is available. However, additional licencing fees, procedural costs, labor fees or financial dependancies are needed to enable or leverage the capability.

C. Respondent must include and attach relevant product literature, specification sheets and diagrams with their submission(s).

D. Respondent must include a full list of protocols of which the solution is capable of routing and on which it can operate and report.

E. Respondent must include a description of both the process and fee structure associated with inserting a new feature request into the development queue.

F. A relevant, itemized example pricing worksheet for the suggested solution (with clearly noted assumptions), must be included.

Corporate Engineering Team

Core & SDDC Services Switch - Engineering RFI

Response Section B

RESPONDENT SECTION

Response Target:
- [✓] Core Switch
- [ ] SDDC Switch

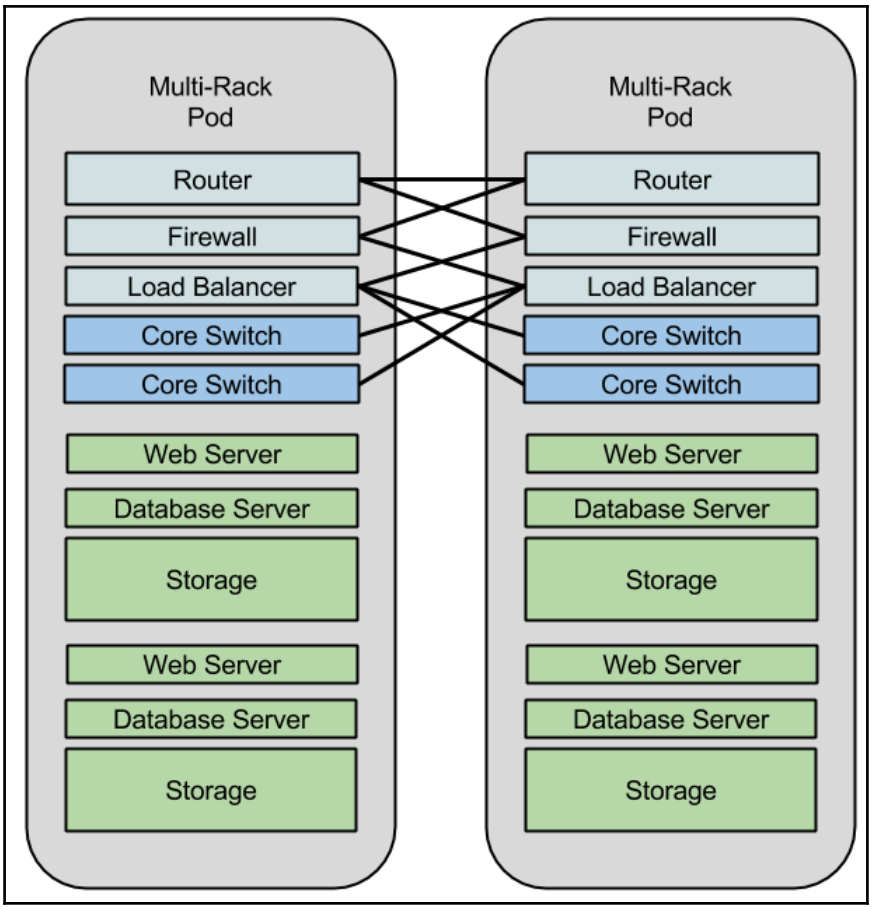
Vendor / Product Name: .....
Model No.: .....
Approx. Unit "Street" $: .....

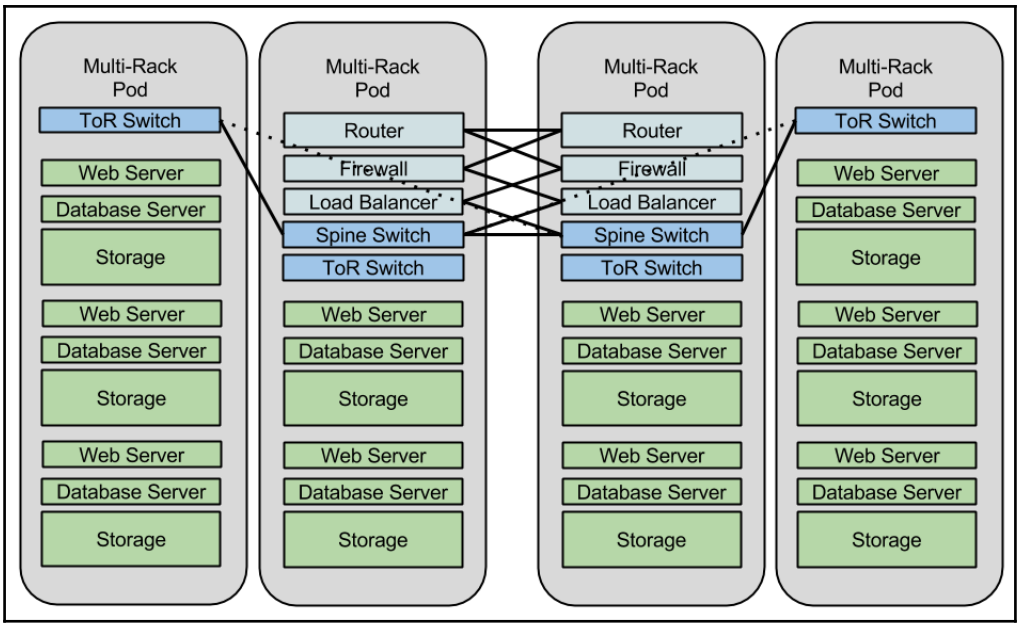
CUSTOMER REQUIREMENTS			*please see instructions*				
ITEM NO.	CATEGORY	DESCRIPTION	CAPABILITY (Value =5,4,3,2,1,0,NA)	IPv4	IPv6	B/L	NOTES
		FOUNDATIONS - PHYSICAL & PERFORMANCE					
1	Physical	Please detail physical dimensions and weight of all included components and indicate ability to rack-mount said equipment		NA	NA		
2	Physical	Please detail redundancy schemes available for the network and redundant components within the device		NA	NA		
3	Physical	N+1 and 1+1 redundancy capabilities (switch fabric, fan, power, etc)		NA	NA		
4	Physical	Please document what management and craft interface are available on the platform					
5	Physical	Please document solution's MTBF (mean time between failure) and MTTR (mean time to repair)					
6	Physical	Support for AC or -48 volt DC power. Please document start-up and operating amperages & how the number and type of cards influence the power requirements of the solution.		NA	NA		
7	Physical	Support for redundant power supplies (indicate how many)		NA	NA		
8	Physical	NEBS (network equipment-building system design guidelines) Level 3 certification		NA	NA		
9	Physical	Support for 10GigE interfaces (indicate port/card density and how many total supported in each box and across a pair/cluster). Please also indicate whether the ports are " blocking" or non-blocking"		NA	NA		
10	Physical	Support for GigE interfaces (indicate port/card density and how many total supported in each box and across a pair/cluster)		NA	NA		
11	Physical	Port support for: 1 Gbps (gigabit per second)		NA	NA		
12	Physical	Port support for: 10 Gbps		NA	NA		
13	Physical	Port support for: 40 Gbps (if not present today, please detail roadmap and time line. Also please describe what dependencies are required: e.g. upgrades to power supplies, augmentation or replacement of route processor modules, etc.)		NA	NA		
14	Physical	Port support for: 100 Gbps (if not present today, please detail roadmap and time line. Also please describe what dependencies are required: e.g. upgrades to power supplies, augmentation or replacement of route processor modules, etc.)		NA	NA		
15	Physical	Port support for: Logical (Null, Loopback, sub-interface, pseudo) (please detail)		NA	NA		
16	Physical	Please detail plans for terabit forwarding / switching capabilities					
17	Physical	Please document all available, supported physical interfaces and speeds		NA	NA		
18	Physical	Please detail the number of interface slots available and the available throughput per slot. Also please indicate if oversubscription is present and if so, please detail how this oversubscription is architected/handled.		NA	NA		
19	Physical	Please detail the maximum number of interfaces that can be operational in the switch		NA	NA		
20	Physical	Please detail any constraints on mixing different interface types in the switch		NA	NA		
21	Physical	Please detail any constraints on the number of operational interfaces due to addition of router resilience/redundancy features		NA	NA		
22	Physical	Please detail whether any type of interface restricts or limits the features supported by the router. Are particular features (QoS (quality of service), multicast, IPv6 Access Control Lists, GRE (generic routing encapsulation), etc.) restricted to, or limited by particular interfaces?		NA	NA		

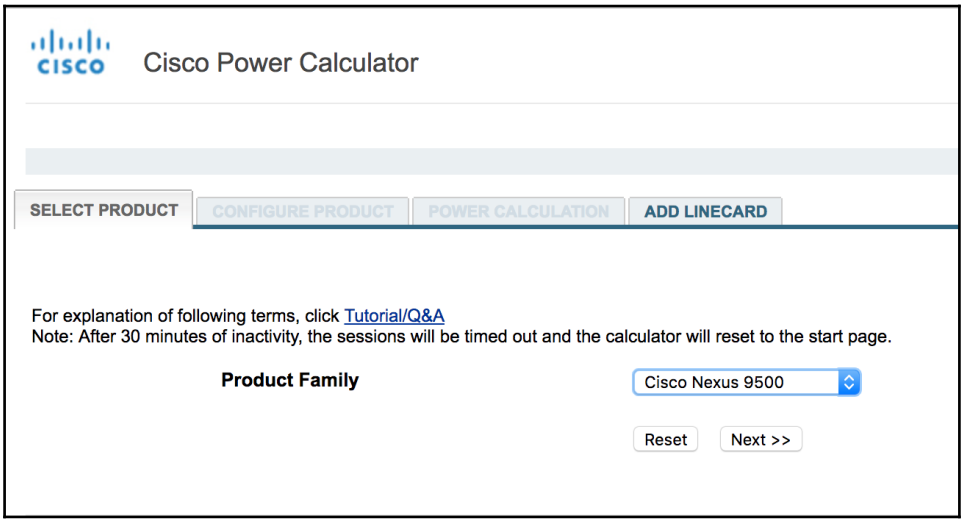
CUSTOMER REQUIREMENTS			*please see instructions*				
ITEM NO.	CATEGORY	DESCRIPTION	CAPABILITY (Value =5,4,3,2,1,0,NA)	IPv4	IPv6	B/L	NOTES
48	Performance	Ability to scale beyond 10G of traffic throughput. Please document capabilities					
49	Performance	Ability to operate as either a complete Layer 3 router or purely Layer 2 switch					
50	Performance	Distributed processing of routing protocols					
51	Performance	Distributed processing of data forwarding plane					
52	Performance	Distributed processing of management plane					
53	Performance	Distributed processing of infrastructure services		NA	NA		
54	Performance	Please detail the number of hardware queues per port					
55	Performance	Nonstop forwarding (NSF)					
56	Performance	Ability to support software upgrades without impacting the deployed solution and with no subscriber traffic or state being lost (hit-less upgrades) (e.g. ISSU or In Service Software Upgrade)		NA	NA		
57	Performance	Ability to support hardware upgrades without impacting the deployed solution and with no subscriber traffic or state being lost		NA	NA		
58	Performance	Please detail which hardware components in the router may be hot swapped, which may not, and the impact on the router, and on packet forwarding of controlled and uncontrolled hot swapping.		NA	NA		
59	Performance	Please indicate and detail any other mechanisms, apart from redundancy, that enhance the overall reliability of the proposed router/solution					
60	Performance	"Feature Blades" - Please detail and describe available blades and their purpose/capabilities		NA	NA		
61	IPv6	IPv6 hardware compatibility		NA	Yes		

SOFTWARE / ROUTING / POLICY DECISION & ENFORCEMENT / TRAFFIC MANAGEMENT							
62	General	Possess any embedded, included or underlying technologies and/or features that would permit derivative financial gain by the enablement thereof (please explain)					
63	IP Routing	IPv4 and IPv6 services and routing protocols (please detail supported service and protocols)					
64	Security	Modular operating system (please detail specific available modules if applicable)		NA	NA		
65	MPLS	MPLS (Multi-Protocol Label Switching) forwarding		NA	NA		
66	MPLS	MPLS L3 (layer 3) VPN					
67	MPLS	MPLS L2 (layer 2) VPN		NA	NA		
68	MPLS	MPLS TE (Multi-Protocol Label Switching Traffic Engineering)					
69	MPLS	MPLS-Label Distribution Protocol (MPLS-LDP)		NA	NA		
70	General	Ability to terminate MPLS Pseudo-wires into VPLS (virtual private LAN service) instances					
71	General	VPLS & LSP (label switch path) ping to isolate fault in the core					
72	General	L3VPN (please detail supported protocols)					
73	General	L2VPN (please detail supported protocols)					
74	General	L2 Circuits					
75	General	PPP encapsulation		NA	NA		
76	General	HDLC (High-Level Data Link Control) encapsulation		NA	NA		
77	General	Frame Relay encapsulation		NA	NA		

Chapter 10: Designing a Next Generation Network


Multi-Rack
Pod
Router
Firewall
Load Balancer
Core Switch
Core Switch
Web Server
Database Server
Storage
Web Server
Database Server
Storage
Multi-Rack
Pod
Router
Firewall
Load Balancer
Core Switch
Core Switch
Web Server
Database Server
Storage
Web Server
Database Server
Storage


Multi-Rack Pod
ToR Switch
Web Server
Database Server
Storage
Web Server
Database Server
Storage
Web Server
Database Server
Storage
Multi-Rack Pod
Router
Firewall
Load Balancer
Spine Switch
ToR Switch
Web Server
Database Server
Storage
Web Server
Database Server
Storage
Multi-Rack Pod
Router
Firewall
Load Balancer
Spine Switch
ToR Switch
Web Server
Database Server
Storage
Web Server
Database Server
Storage
Multi-Rack Pod
ToR Switch
Web Server
Database Server
Storage
Web Server
Database Server
Storage
Web Server
Database Server
Storage


Cisco Power Calculator
SELECT PRODUCT
CONFIGURE PRODUCT
POWER CALCULATION
ADD LINECARD
For explanation of following terms, click Tutorial/Q&A
Note: After 30 minutes of inactivity, the sessions will be timed out and the calculator will reset to the start page.
Product Family
Cisco Nexus 9500
Reset
Next >>

Chassis	N9K-C9504
Supervisor Engine	N9K-SUP-B
Redundant Supervisor Engine	NO
System Controller	N9K-SC-A
Redundant System Controller	YES
Fantray	N9K-C9504-FAN
Fabric Module	N9K-C9504-FM
How many Fabric modules?	3
Input Voltage	200-240 Volts AC

Next >>

Quick Facts

Selected Chassis	N9K-C9504
Selected Supervisor Engine	N9K-SUP-B
Selected System Controller	N9K-SC-A
Selected Voltage	200-240 Volts AC
Selected Fantray	N9K-C9504-FAN
Selected Fabric Module	N9K-C9504-FM
Selected Number of Fabric Modules	3
Chassis Slots	4

Power Consumption/Heat Dissipation Summary

Slot	Line Card
1	N9K-X9636PQ
2	N9K-X9564PX
3	--EMPTY-SLOT--
4	--EMPTY-SLOT--

Minimum Power Supply	Percentage Of Power Used
Single N9K-PAC-3000W-B in Combined mode	59.68 %
First Alternative Power Supply	**Percentage of Power used**
Dual N9K-PAC-3000W-B in Combined mode	29.85 %

Total Output Current	Total Output Power	Total Typical Output Power	Total Heat Dissipation
8.14 Amps	**2380.00 Watts**	**1723.00 Watts**	**7850.30 BTU/Hr**

Chassis	N9K-C9504
Supervisor Engine	N9K-SUP-B
Redundant Supervisor Engine	NO
System Controller	N9K-SC-A
Redundant System Controller	YES
Fantray	N9K-C9504-FAN
Fabric Module	N9K-C9504-FM-E
How many Fabric modules?	4
Input Voltage	200-240 Volts AC

Next >>

Quick Facts

Selected Chassis	N9K-C9504
Selected Supervisor Engine	N9K-SUP-B
Selected System Controller	N9K-SC-A
Selected Voltage	200-240 Volts AC
Selected Fantray	N9K-C9504-FAN
Selected Fabric Module	N9K-C9504-FM-E
Selected Number of Fabric Modules	4
Chassis Slots	4

Power Consumption/Heat Dissipation Summary

Slot	Line Card
1	N9K-X9732C-EX
2	N9K-X97160YC-EX
3	-- EMPTY-SLOT --
4	-- EMPTY-SLOT --

Minimum Power Supply	Percentage of Power Used
Single N9K-PAC-3000W-B in Combined mode	77.64%
First Alternative Power Supply	**Percentage of Power Used**
Dual N9K-PAC-3000W-B in Combined mode	38.83%

Total Output Current	Total Output Power	Total Typical Output Power	Total Heat Dissipation
10.59 Amps	**3089.00 Watts**	**2242.00 Watts**	**10507.90 BTU/Hr**

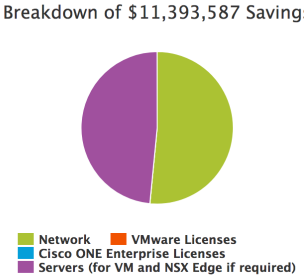
Power Consumption/Heat Dissipation Summary

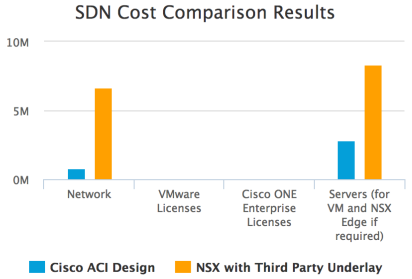
Slot	Line Card
1	N9K-X9732C-EX
2	N9K-X9732C-EX
3	N9K-X9732C-EX
4	N9K-X9732C-EX
5	N9K-X9732C-EX
6	N9K-X9732C-EX
7	N9K-X9732C-EX
8	N9K-X9732C-EX

Minimum Power Supply	Percentage of Power Used
Three N9K-PAC-3000W-B in Combined mode	77.54%
First Alternative Power Supply	**Percentage of Power Used**
Four N9K-PAC-3000W-B in Combined mode	58.15%

Total Output Current	Total Output Power	Total Typical Output Power	Total Heat Dissipation
31.72 Amps	**10128.00 Watts**	**6874.00 Watts**	**36999.53 BTU/Hr**

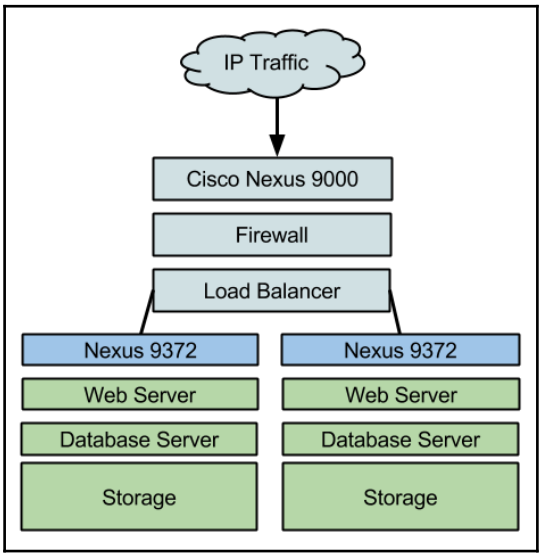
SDN Cost Comparison

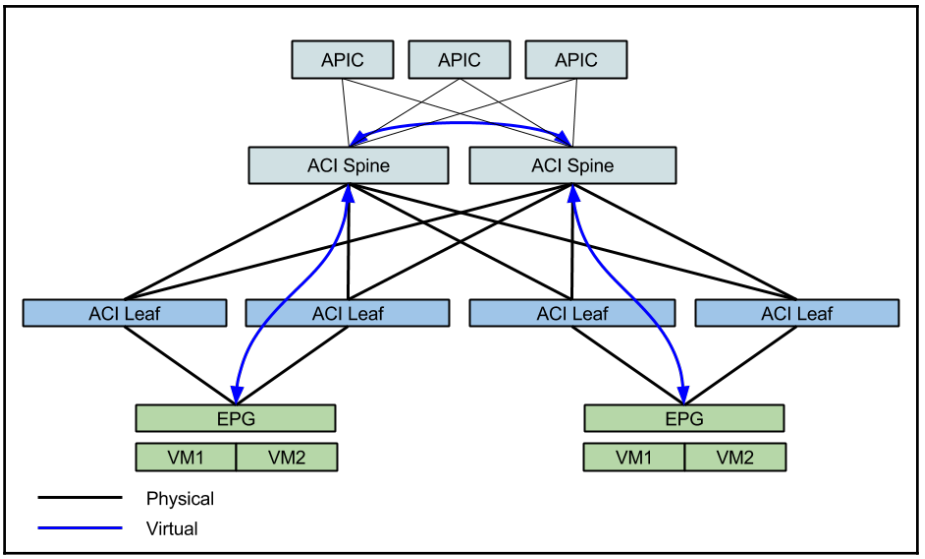


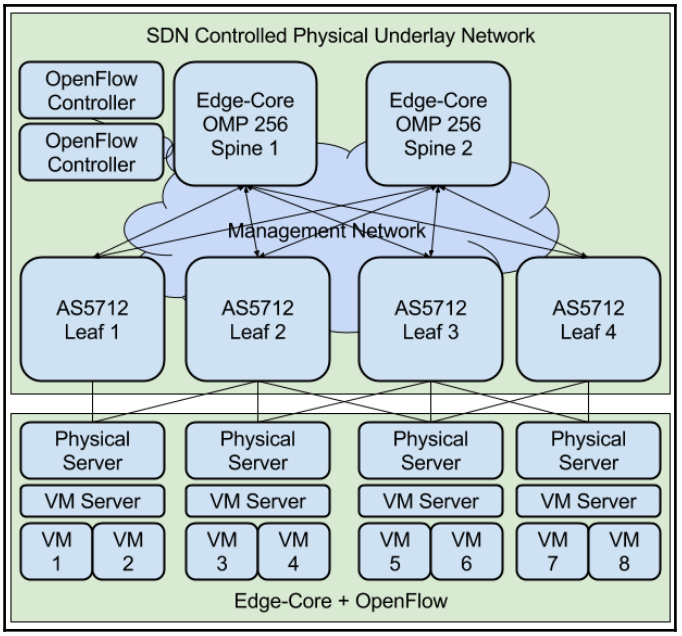


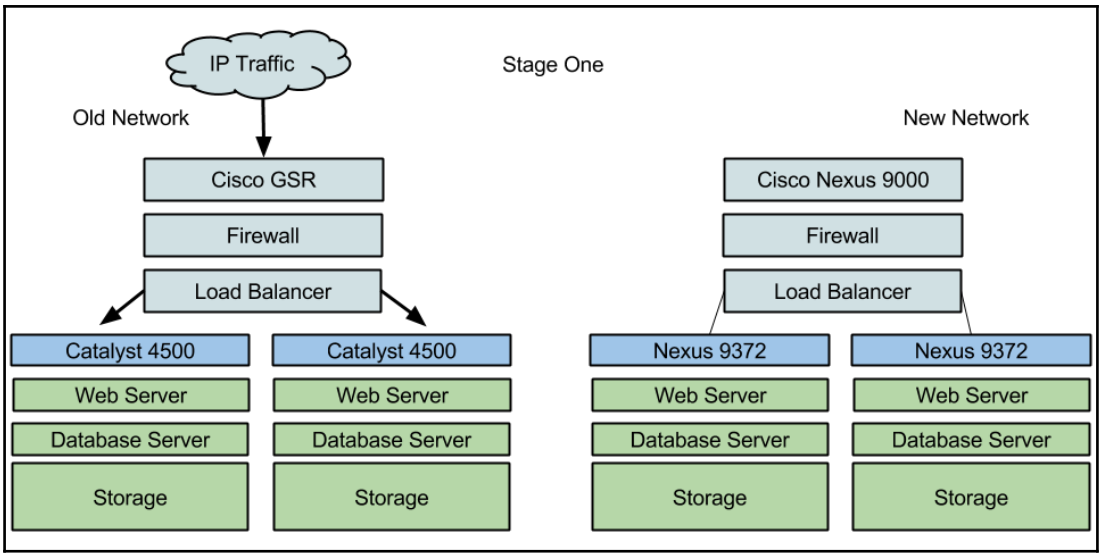
	Cisco ACI Design	NSX with Third Party Underlay	Cisco ACI Savings	Cisco ACI Savings, %
Network (switches, transceivers and SDN licenses)	$787,784	$6,660,076	$5,872,292	**88.17%**
VMware vCloud Suite or vSphere Enterprise+ licenses	$0	$0	$0	**0.00%**
Cisco ONE Enterprise Licenses	$0	$0	$0	**0.00%**
Servers (for VM and NSX Edge if required)	$2,821,818	$8,343,112	$5,521,295	**66.18%**
Total	**$3,609,601**	**$15,003,188**	**$11,393,587**	**75.94%**

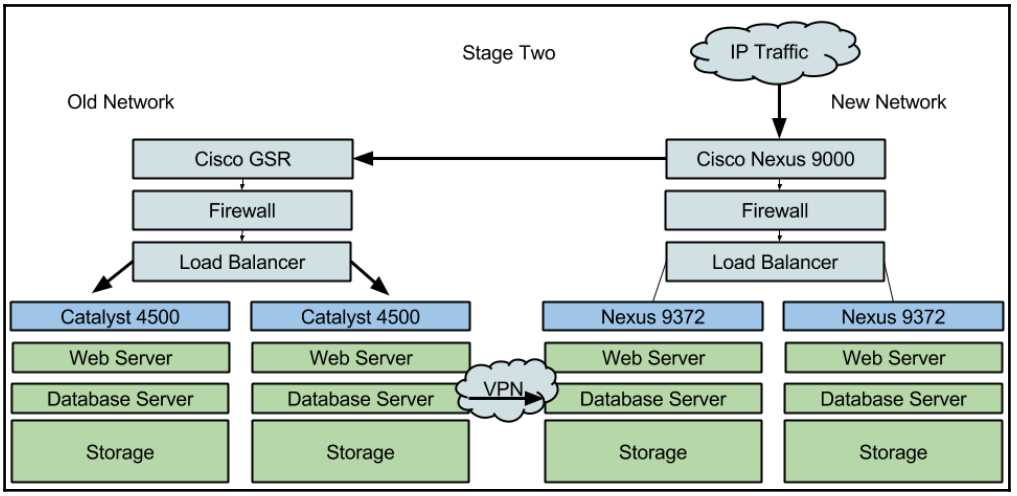
Simulation with 2,500 VM, 5 vCenter, 15 tenants and 28:1 oversubscription to the WAN (1 year) TCO

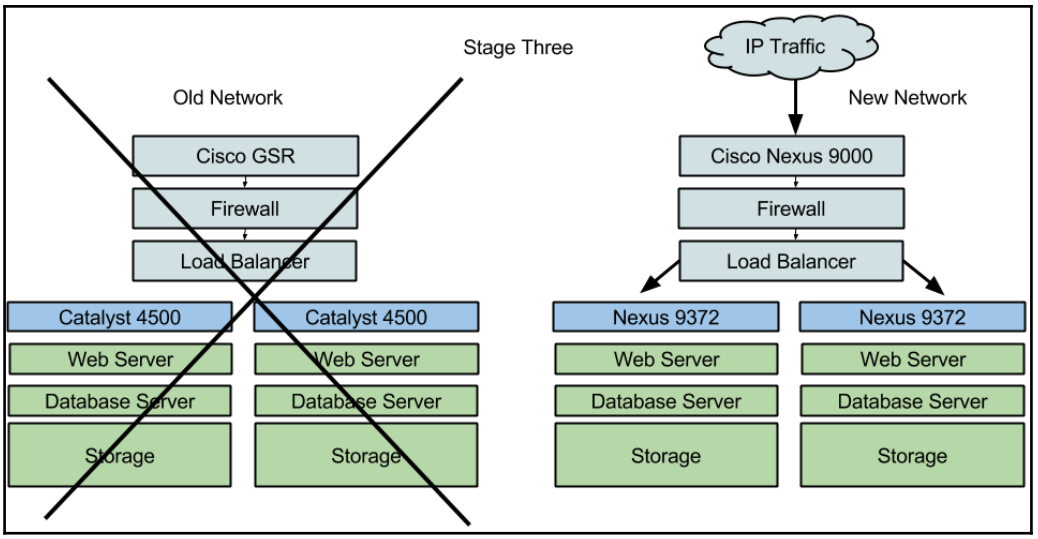



APIC
APIC
APIC
ACI Spine
ACI Spine
ACI Leaf
ACI Leaf
ACI Leaf
ACI Leaf
EPG
VM1
VM2
EPG
VM1
VM2
Physical
Virtual

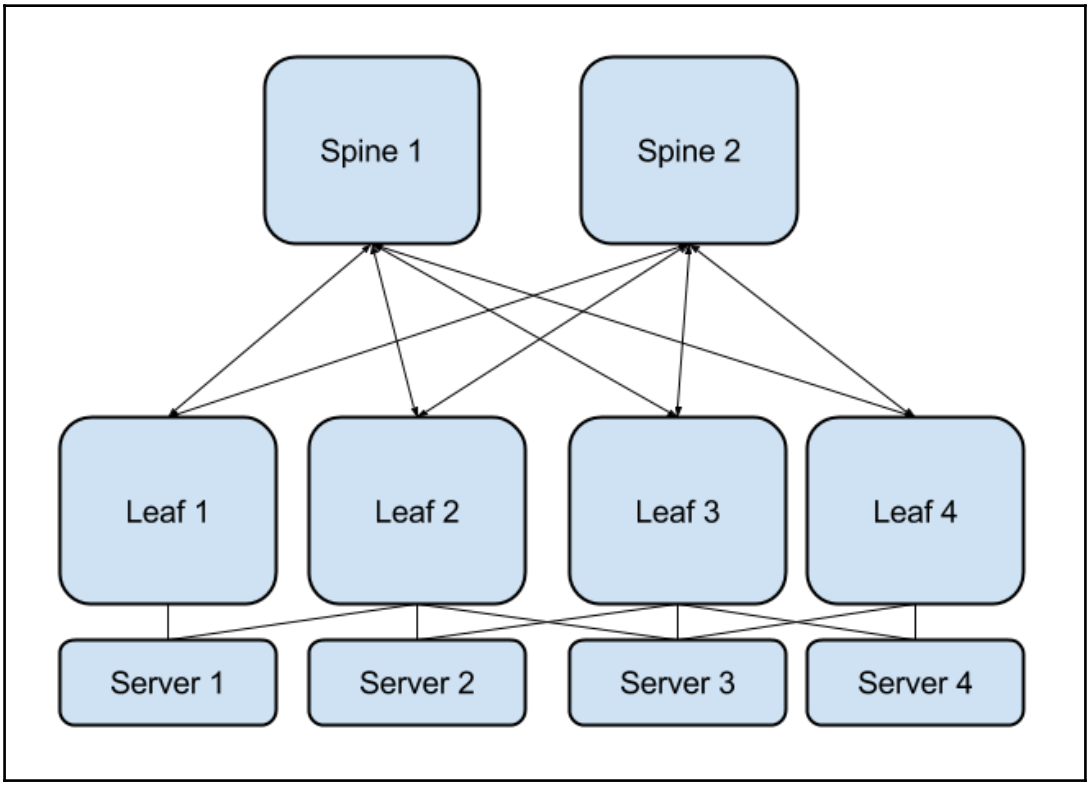

SDN Controlled Physical Underlay Network
OpenFlow Controller
OpenFlow Controller
Edge-Core OMP 256 Spine 1
Edge-Core OMP 256 Spine 2
Management Network
AS5712 Leaf 1
AS5712 Leaf 2
AS5712 Leaf 3
AS5712 Leaf 4
Physical Server
Physical Server
Physical Server
Physical Server
VM Server
VM Server
VM Server
VM Server
VM 1
VM 2
VM 3
VM 4
VM 5
VM 6
VM 7
VM 8
Edge-Core + OpenFlow

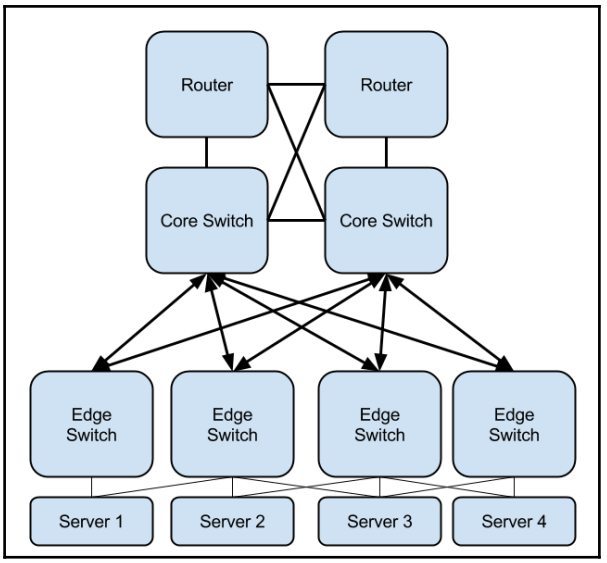

IP Traffic
Stage One
Old Network
New Network
Cisco GSR
Firewall
Load Balancer
Cisco Nexus 9000
Firewall
Load Balancer
Catalyst 4500
Catalyst 4500
Nexus 9372
Nexus 9372
Web Server
Web Server
Web Server
Web Server
Database Server
Database Server
Database Server
Database Server
Storage
Storage
Storage
Storage

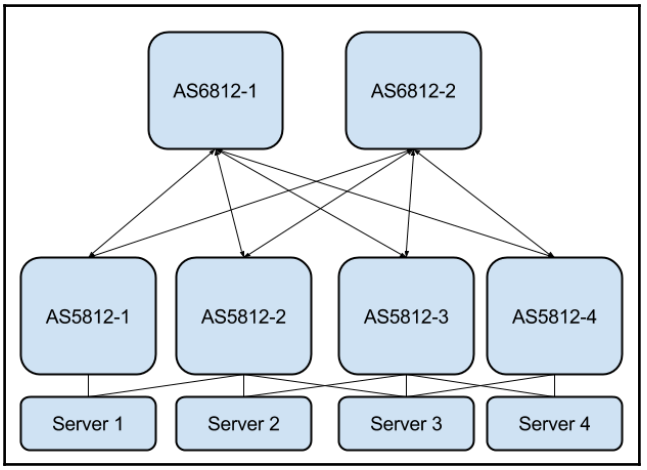

Stage Two
IP Traffic
Old Network
New Network
Cisco GSR
Cisco Nexus 9000
Firewall
Firewall
Load Balancer
Load Balancer
Catalyst 4500
Catalyst 4500
Nexus 9372
Nexus 9372
Web Server
Web Server
Web Server
Web Server
Database Server
Database Server
VPN
Database Server
Database Server
Storage
Storage
Storage
Storage

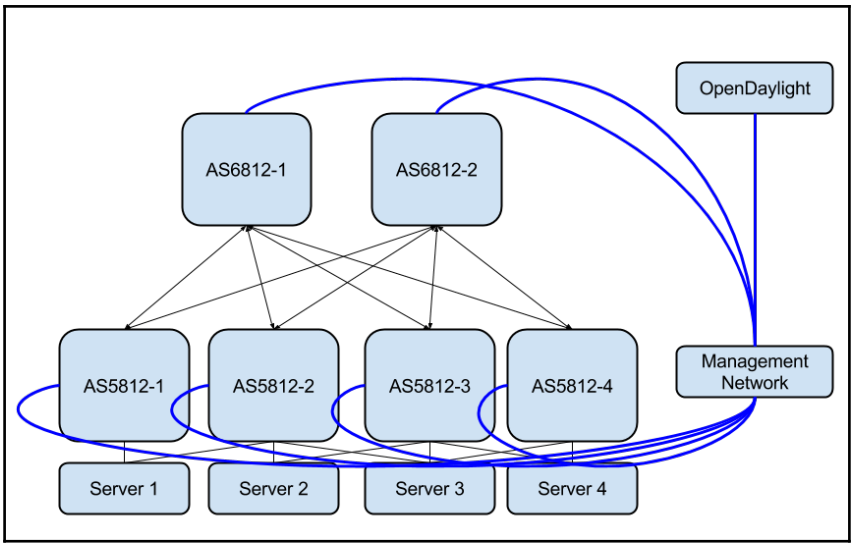

Stage Three
IP Traffic
Old Network
New Network
Cisco GSR
Firewall
Load Balancer
Cisco Nexus 9000
Firewall
Load Balancer
Catalyst 4500
Catalyst 4500
Nexus 9372
Nexus 9372
Web Server
Web Server
Web Server
Web Server
Database Server
Database Server
Database Server
Database Server
Storage
Storage
Storage
Storage

Chapter 11: Example NGN Designs

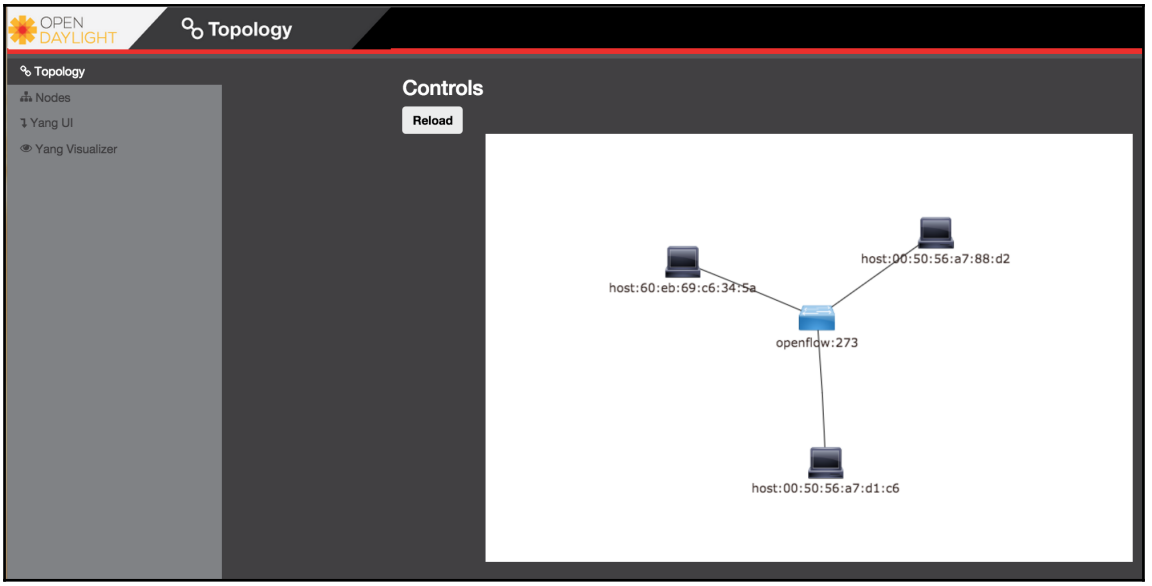


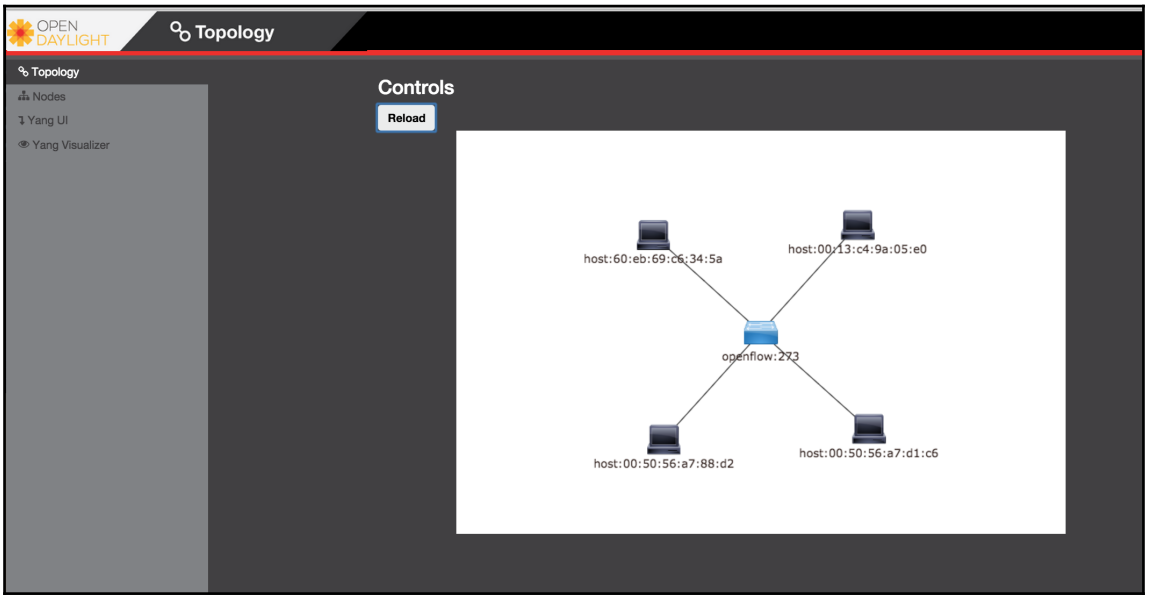

Router
Router
Core Switch
Core Switch
Edge Switch
Edge Switch
Edge Switch
Edge Switch
Server 1
Server 2
Server 3
Server 4

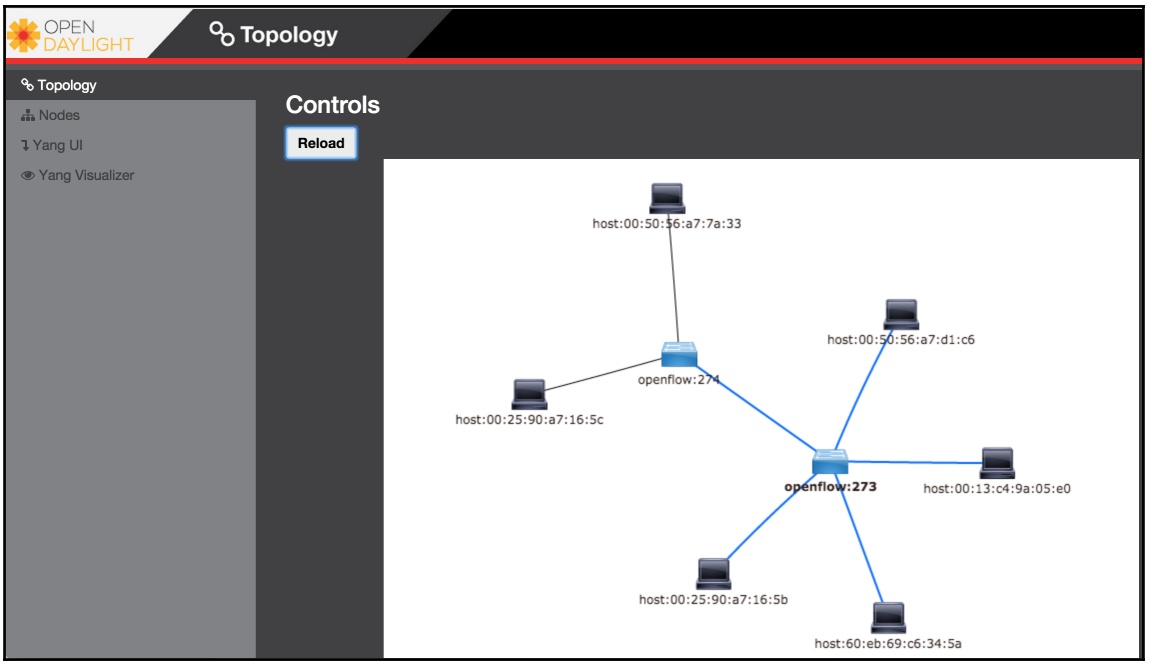

AS6812-1
AS6812-2
AS5812-1
AS5812-2
AS5812-3
AS5812-4
Server 1
Server 2
Server 3
Server 4

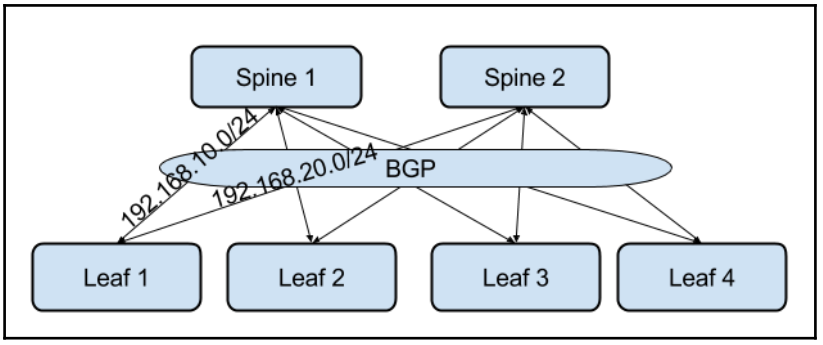

OpenDaylight
AS6812-1
AS6812-2
AS5812-1
AS5812-2
AS5812-3
AS5812-4
Management Network
Server 1
Server 2
Server 3
Server 4

OPEN DAYLIGHT
Topology
Topology
Nodes
Yang UI
Yang Visualizer
Controls
Reload


OPEN DAYLIGHT
Topology
Topology
Nodes
Yang UI
Yang Visualizer
Controls
Reload
host:00:50:56:a7:88:d2
host:60:eb:69:c6:34:5a
openflow:273
host:00:50:56:a7:d1:c6


OPEN DAYLIGHT
Topology
Topology
Nodes
Yang UI
Yang Visualizer
Controls
Reload
host:60:eb:69:c6:34:5a
host:00:13:c4:9a:05:e0
openflow:273
host:00:50:56:a7:88:d2
host:00:50:56:a7:d1:c6


OPEN DAYLIGHT
Topology
Topology
Nodes
Yang UI
Yang Visualizer
Controls
Reload
host:00:50:56:a7:7a:33
host:00:50:56:a7:d1:c6
openflow:274
host:00:25:90:a7:16:5c
openflow:273
host:00:13:c4:9a:05:e0
host:00:25:90:a7:16:5b
host:60:eb:69:c6:34:5a


Spine 1
Spine 2
192.168.10.0/24
192.168.20.0/24
BGP
Leaf 1
Leaf 2
Leaf 3
Leaf 4

GET http://10.1.1.1:8080/public/v1/state/SystemStatus Params Send Save

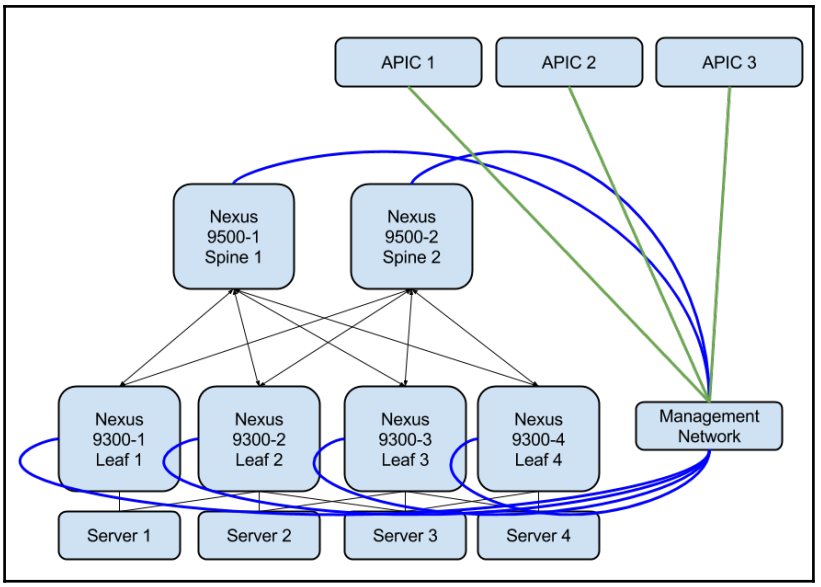
Body Cookies Headers (3) Tests Status: 200 OK Time: 62 ms Size: 3 KB

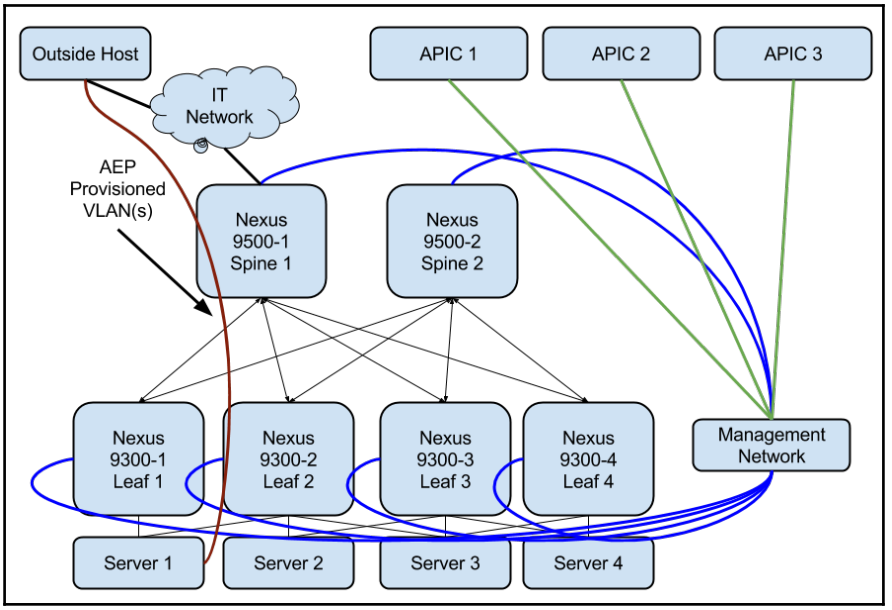
Pretty Raw Preview JSON Save Response

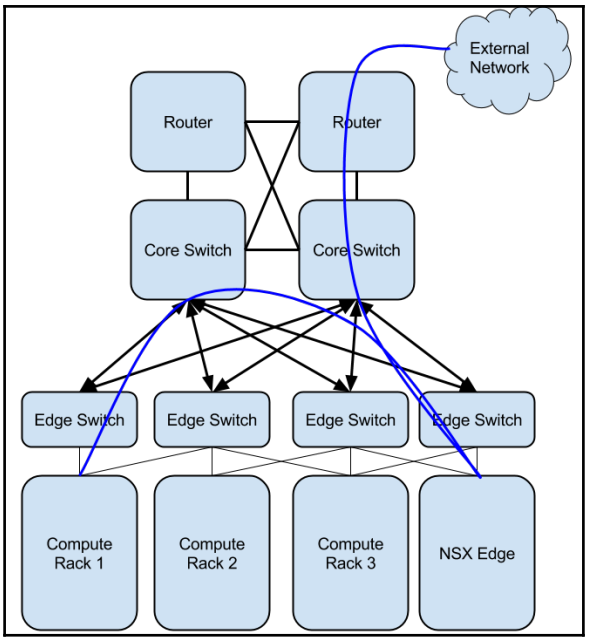

```
{
  "ObjectId": "",
  "Object": {
    "Name": "localhost",
    "Ready": true,
    "Reason": "None",
    "UpTime": "55h43m39.4793313s",
    "NumCreateCalls": "Total 8 Success 2",
    "NumDeleteCalls": "Total 0 Success 0",
    "NumUpdateCalls": "Total 0 Success 0",
    "NumGetCalls": "Total 18 Success 12",
    "NumActionCalls": "Total 0 Success 0",
    "FlexDaemons": [
      {
        "Name": "ribd",
        "Enable": true,
        "State": "up",
        "Reason": "None",
        "StartTime": "2001-07-02 19:51:07.59484187 +0000 UTC",
        "KeepAlive": "Received 5 keepalives",
        "RestartCount": 0,
        "RestartTime": "",
        "RestartReason": ""
      },
      {
        "Name": "dhcprelayd",
        "Enable": true,
        "State": "up",
        "Reason": "None",
        "StartTime": "2001-07-02 19:50:48.148455384 +0000 UTC",
        "KeepAlive": "Received 5 keepalives",
        "RestartCount": 0,
```

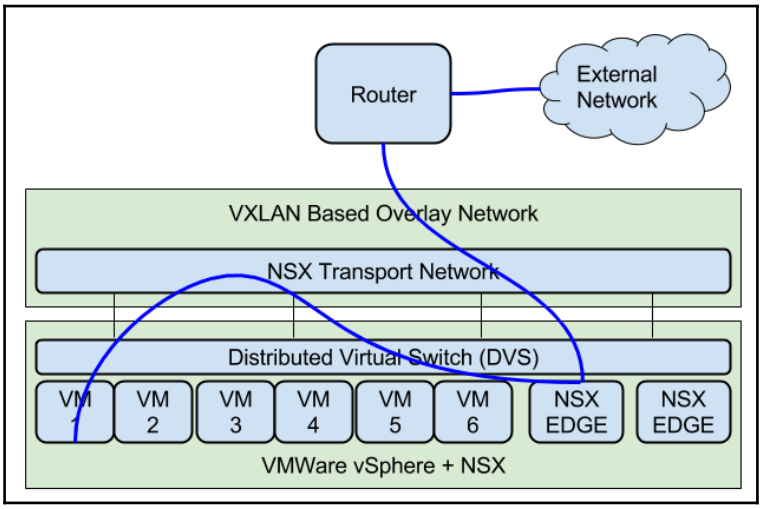


```
{
  "MoreExist": false,
  "ObjCount": 2,
  "CurrentMarker": 0,
  "NextMarker": 0,
  "Objects": [
    {
      "ObjectId": "1c4ab72c-6914-43b3-63c3-292b7401306c",
      "Object": {
        "NeighborAddress": "192.168.10.2",
        "IntfRef": "",
        "Description": "",
        "Disabled": false,
        "PeerGroup": "",
        "PeerType": 0,
        "SessionState": 6,
        "PeerAS": "15096",
        "LocalAS": "15096",
```

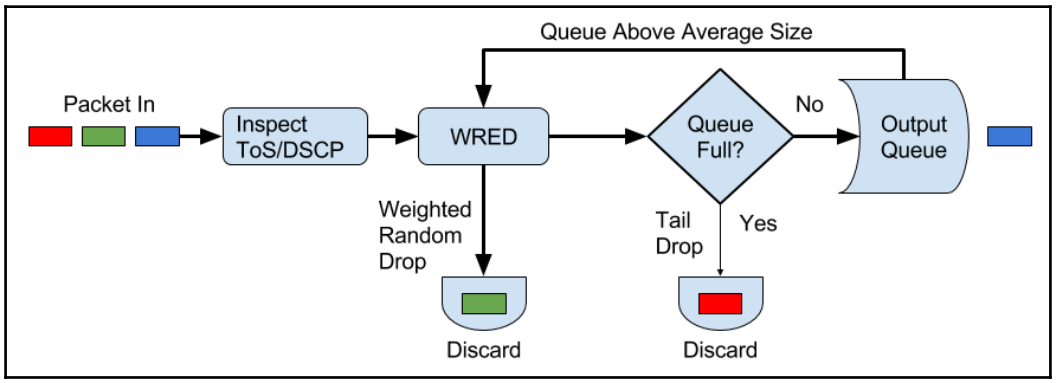

APIC 1
APIC 2
APIC 3
Nexus 9500-1 Spine 1
Nexus 9500-2 Spine 2
Nexus 9300-1 Leaf 1
Nexus 9300-2 Leaf 2
Nexus 9300-3 Leaf 3
Nexus 9300-4 Leaf 4
Management Network
Server 1
Server 2
Server 3
Server 4

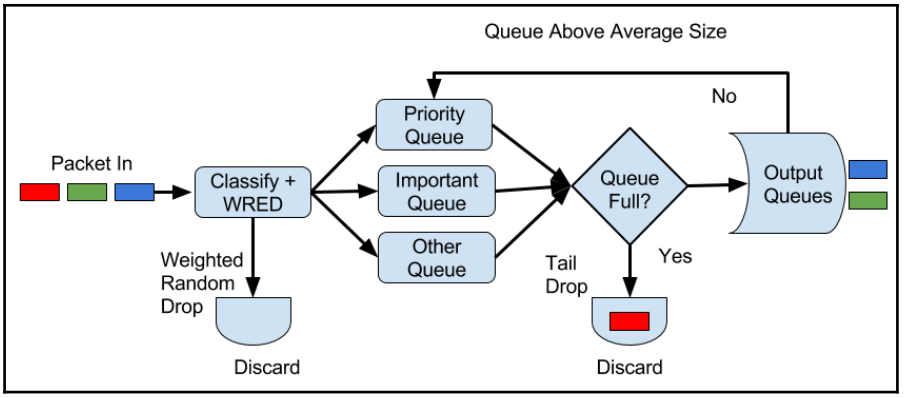

Outside Host
IT Network
AEP Provisioned VLAN(s)
APIC 1
APIC 2
APIC 3
Nexus 9500-1 Spine 1
Nexus 9500-2 Spine 2
Nexus 9300-1 Leaf 1
Nexus 9300-2 Leaf 2
Nexus 9300-3 Leaf 3
Nexus 9300-4 Leaf 4
Management Network
Server 1
Server 2
Server 3
Server 4

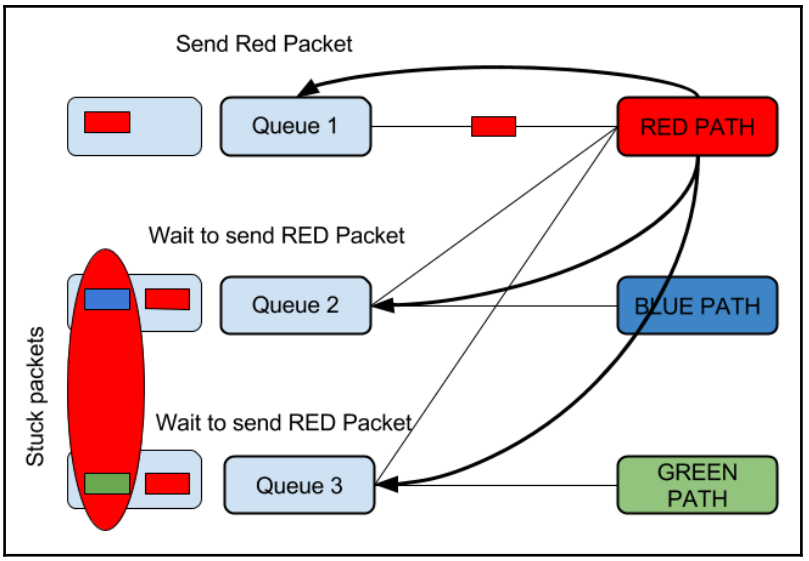

External Network
Router
Router
Core Switch
Core Switch
Edge Switch
Edge Switch
Edge Switch
Edge Switch
Compute Rack 1
Compute Rack 2
Compute Rack 3
NSX Edge

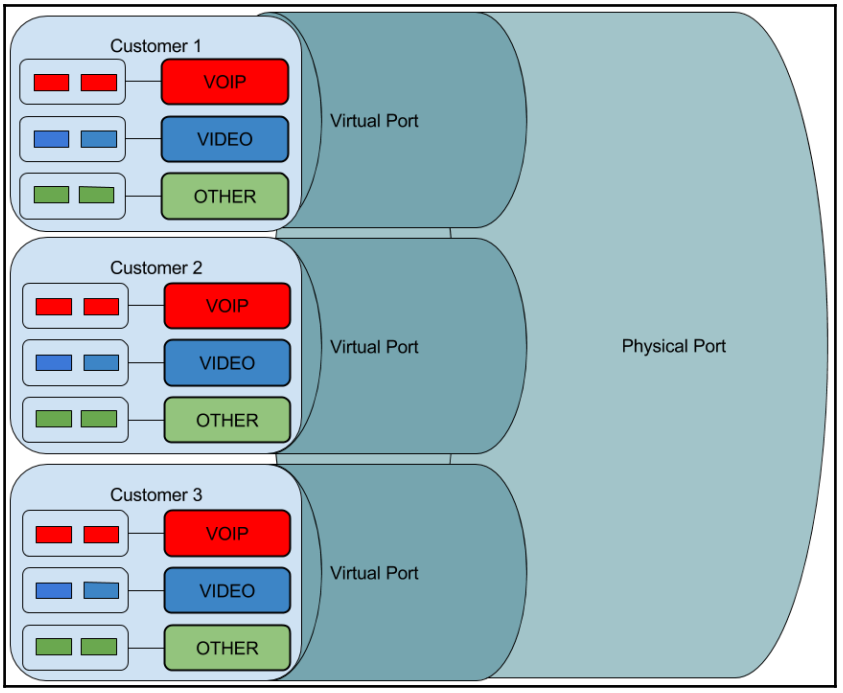

Router
External Network
VXLAN Based Overlay Network
NSX Transport Network
Distributed Virtual Switch (DVS)
VM 1
VM 2
VM 3
VM 4
VM 5
VM 6
NSX EDGE
NSX EDGE
VMWare vSphere + NSX

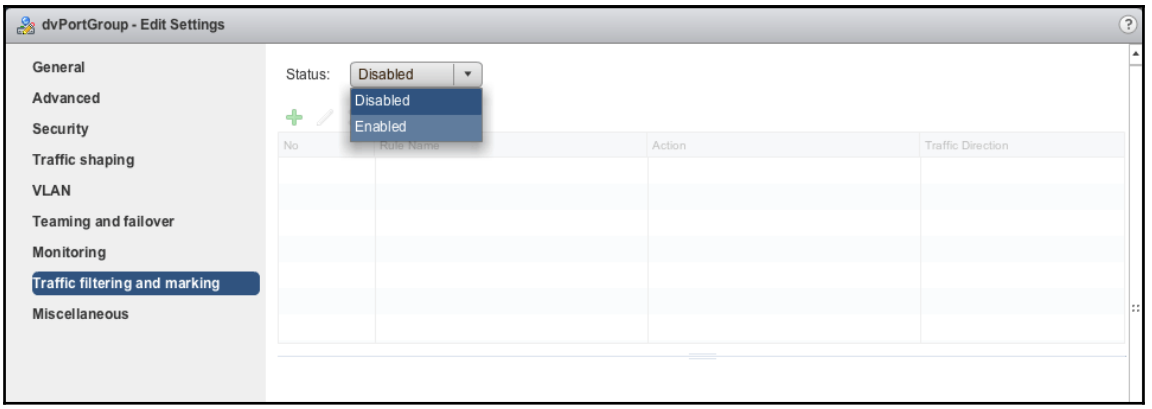
Chapter 12: Understanding and Configuring Quality of Service

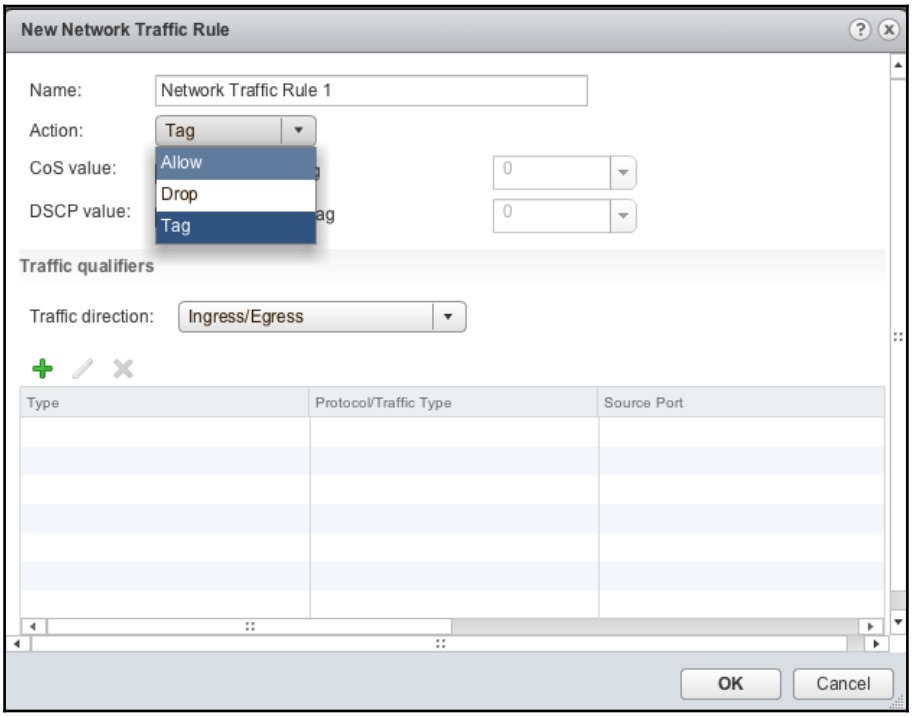


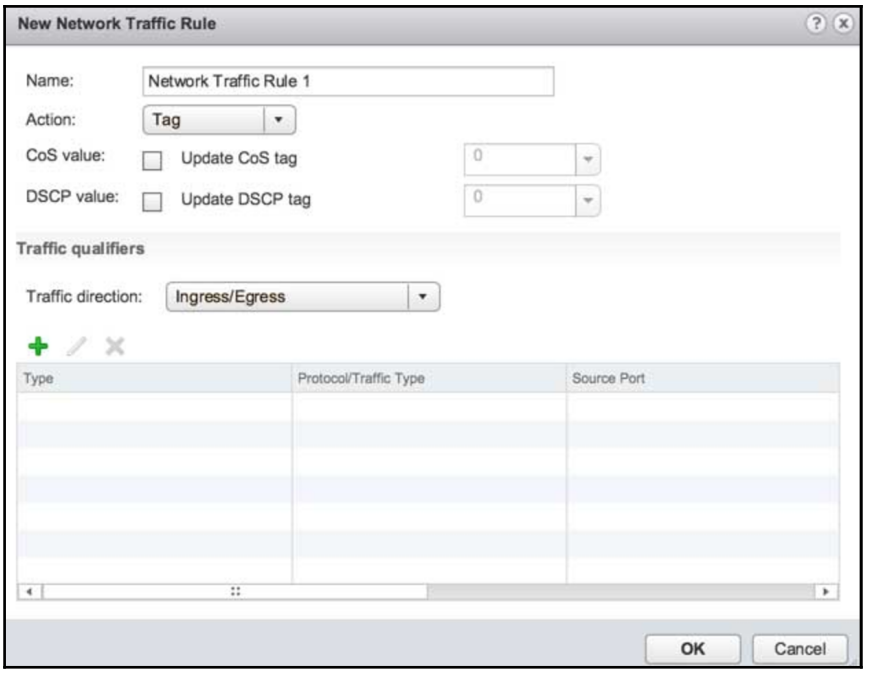


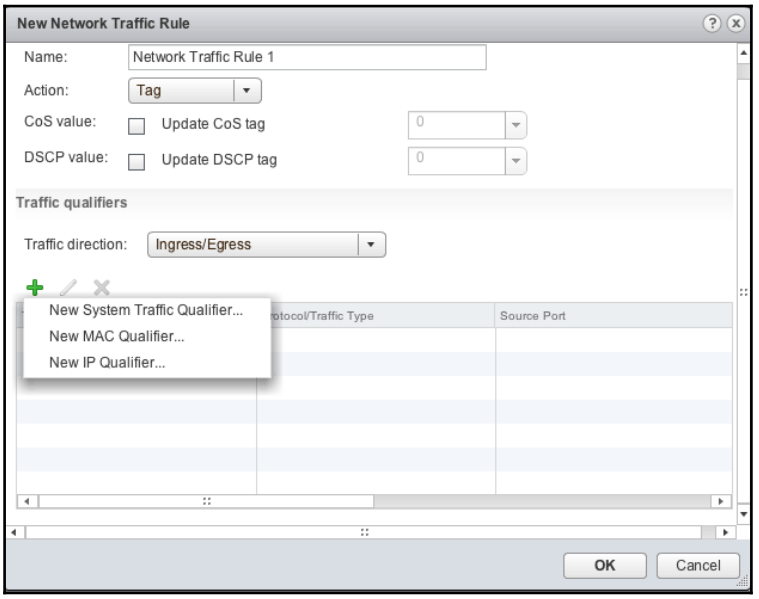

Send Red Packet
Queue 1
RED PATH
Wait to send RED Packet
Queue 2
BLUE PATH
Stuck packets
Wait to send RED Packet
Queue 3
GREEN PATH

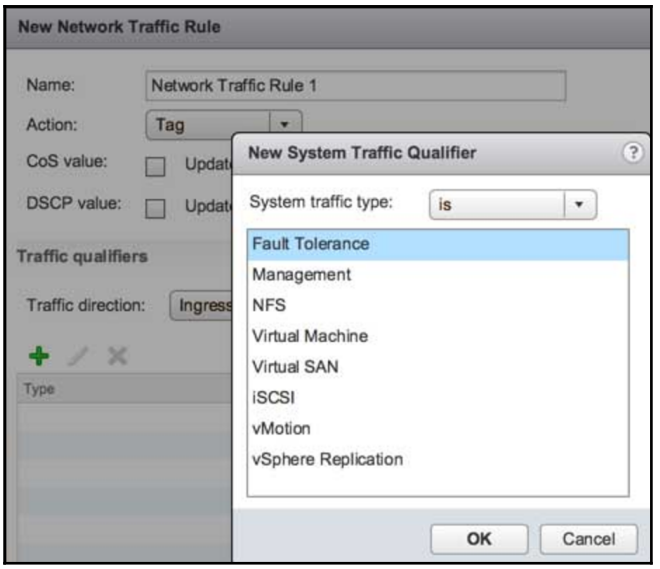

Customer 1
VOIP
VIDEO
OTHER
Virtual Port
Customer 2
VOIP
VIDEO
OTHER
Virtual Port
Physical Port
Customer 3
VOIP
VIDEO
OTHER
Virtual Port

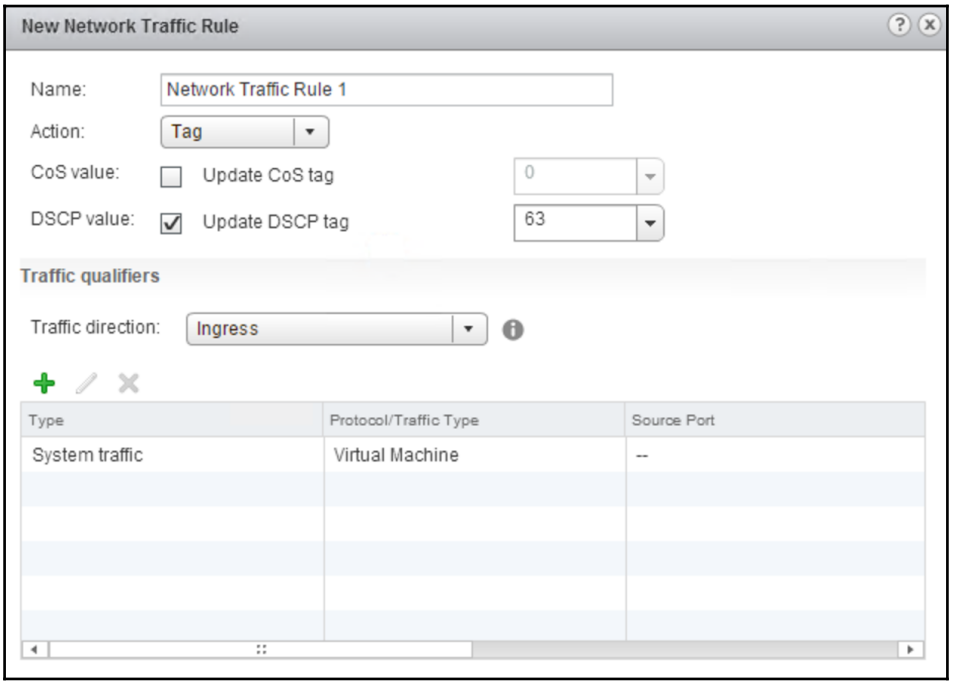

dvPortGroup - Edit Settings
General
Advanced
Security
Traffic shaping
VLAN
Teaming and failover
Monitoring
Traffic filtering and marking
Miscellaneous
Status:
Disabled
Disabled
Enabled
No
Rule Name
Action
Traffic Direction


New Network Traffic Rule
Name:
Network Traffic Rule 1
Action:
Tag
Allow
Drop
Tag
CoS value:
DSCP value:
0
0
Traffic qualifiers
Traffic direction:
Ingress/Egress
Type
Protocol/Traffic Type
Source Port
OK
Cancel

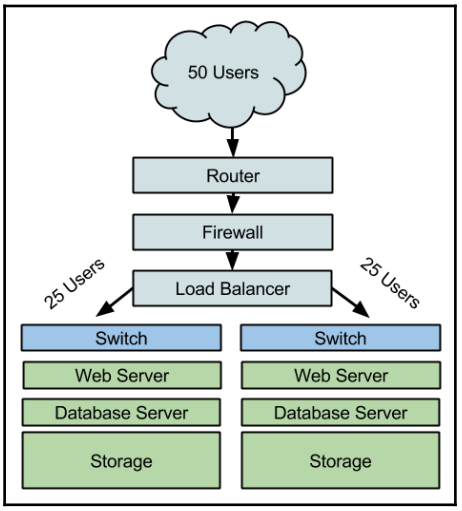

New Network Traffic Rule
Name:
Network Traffic Rule 1
Action:
Tag
CoS value:
Update CoS tag
0
DSCP value:
Update DSCP tag
0
Traffic qualifiers
Traffic direction:
Ingress/Egress
Type
Protocol/Traffic Type
Source Port
OK
Cancel

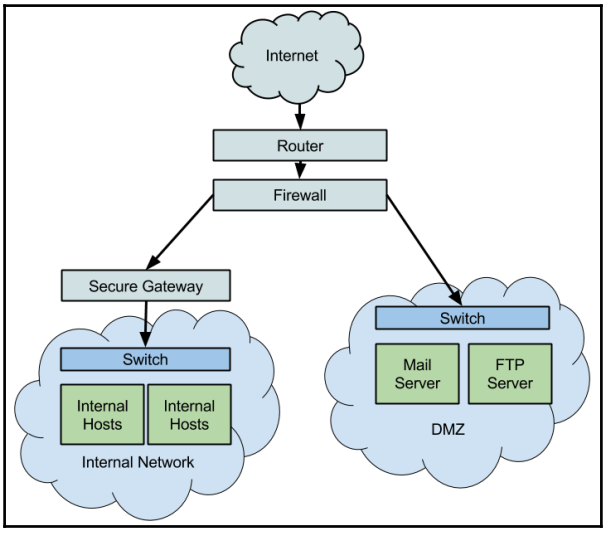

New Network Traffic Rule
Name:
Network Traffic Rule 1
Action:
Tag
CoS value:
Update CoS tag
0
DSCP value:
Update DSCP tag
0
Traffic qualifiers
Traffic direction:
Ingress/Egress
New System Traffic Qualifier...
New MAC Qualifier...
New IP Qualifier...
Source Port
OK
Cancel

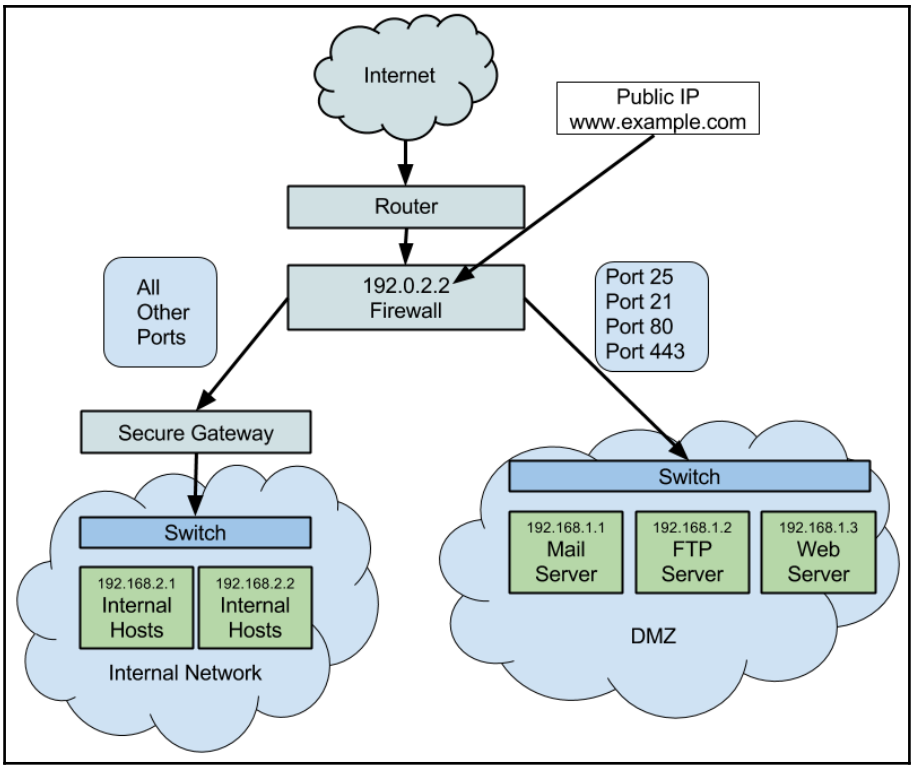

New Network Traffic Rule
Name:
Network Traffic Rule 1
Action:
Tag
CoS value:
DSCP value:
Traffic qualifiers
Traffic direction:
Type
New System Traffic Qualifier
System traffic type:
is
Fault Tolerance
Management
NFS
Virtual Machine
Virtual SAN
iSCSI
vMotion
vSphere Replication
OK
Cancel

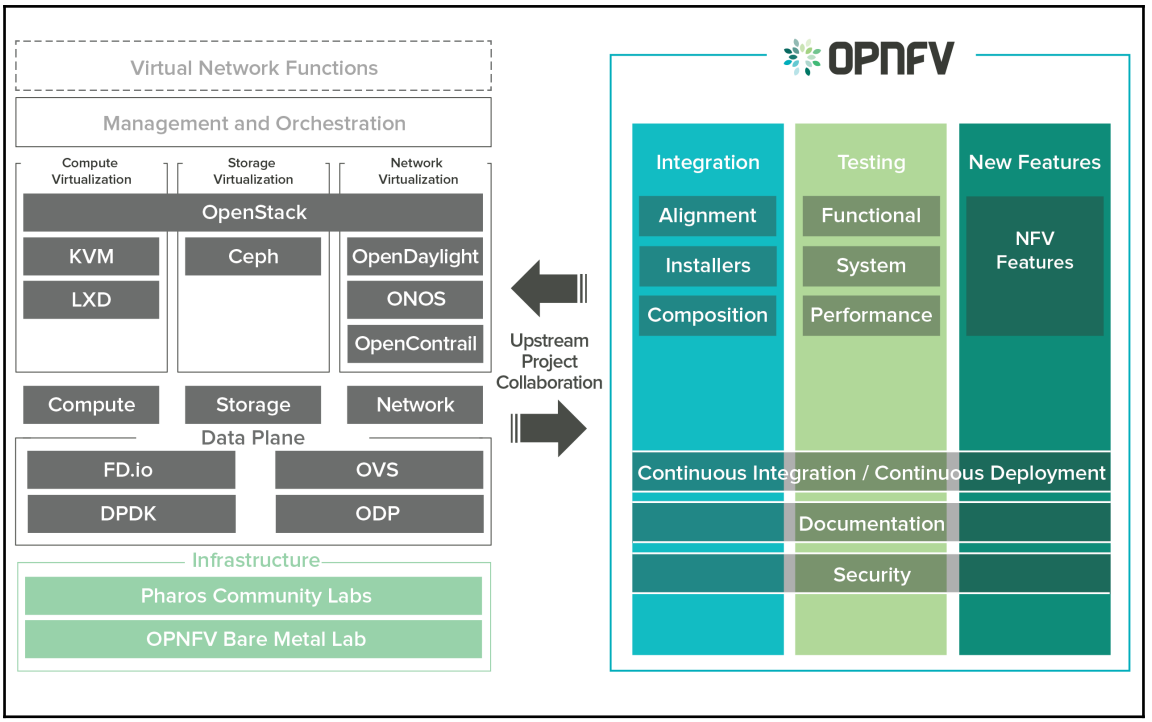

New Network Traffic Rule
Name:
Network Traffic Rule 1
Action:
Tag
CoS value:
Update CoS tag
0
DSCP value:
Update DSCP tag
63
Traffic qualifiers
Traffic direction:
Ingress
Type
Protocol/Traffic Type
Source Port
System traffic
Virtual Machine
--

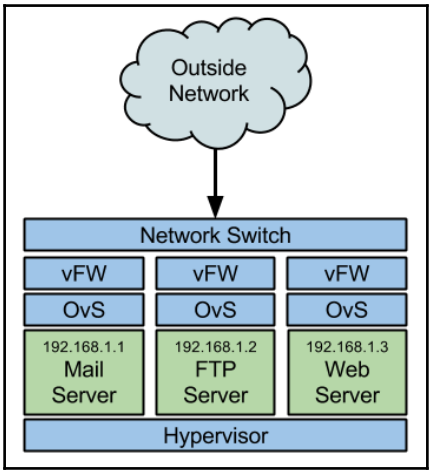
Chapter 13: Securing the Network

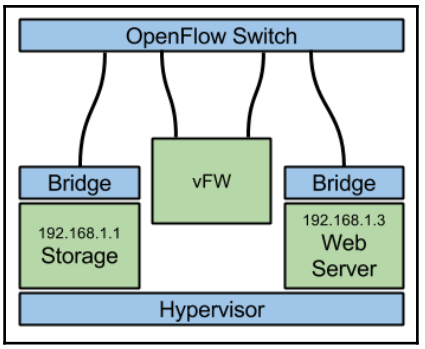


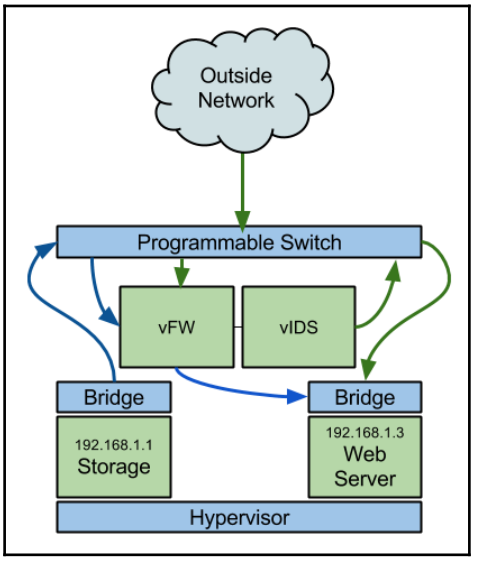


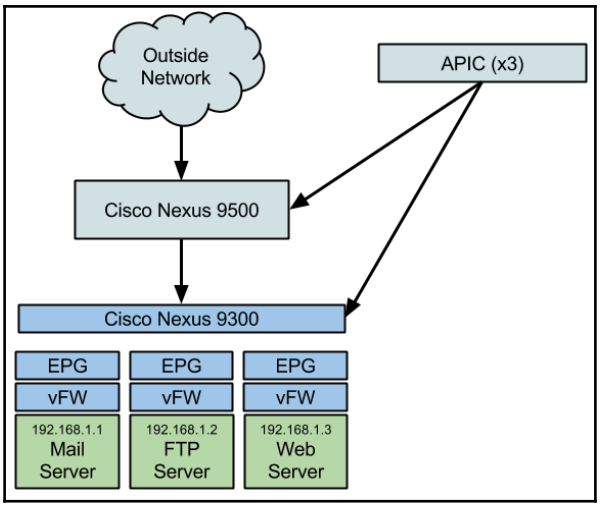

Internet
Public IP
www.example.com
Router
All
Other
Ports
192.0.2.2
Firewall
Port 25
Port 21
Port 80
Port 443
Secure Gateway
Switch
192.168.2.1
Internal
Hosts
192.168.2.2
Internal
Hosts
Internal Network
Switch
192.168.1.1
Mail
Server
192.168.1.2
FTP
Server
192.168.1.3
Web
Server
DMZ

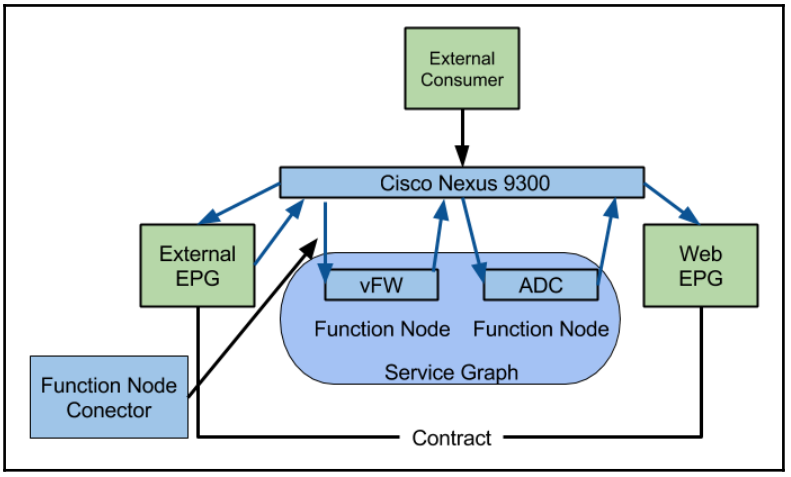

Virtual Network Functions
Management and Orchestration
Compute Virtualization
Storage Virtualization
Network Virtualization
OpenStack
KVM
LXD
Ceph
OpenDaylight
ONOS
OpenContrail
Compute
Storage
Network
Data Plane
FD.io
DPDK
OVS
ODP
Infrastructure
Pharos Community Labs
OPNFV Bare Metal Lab
Upstream Project Collaboration
OPNFV
Integration
Alignment
Installers
Composition
Testing
Functional
System
Performance
New Features
NFV Features
Continuous Integration / Continuous Deployment
Documentation
Security

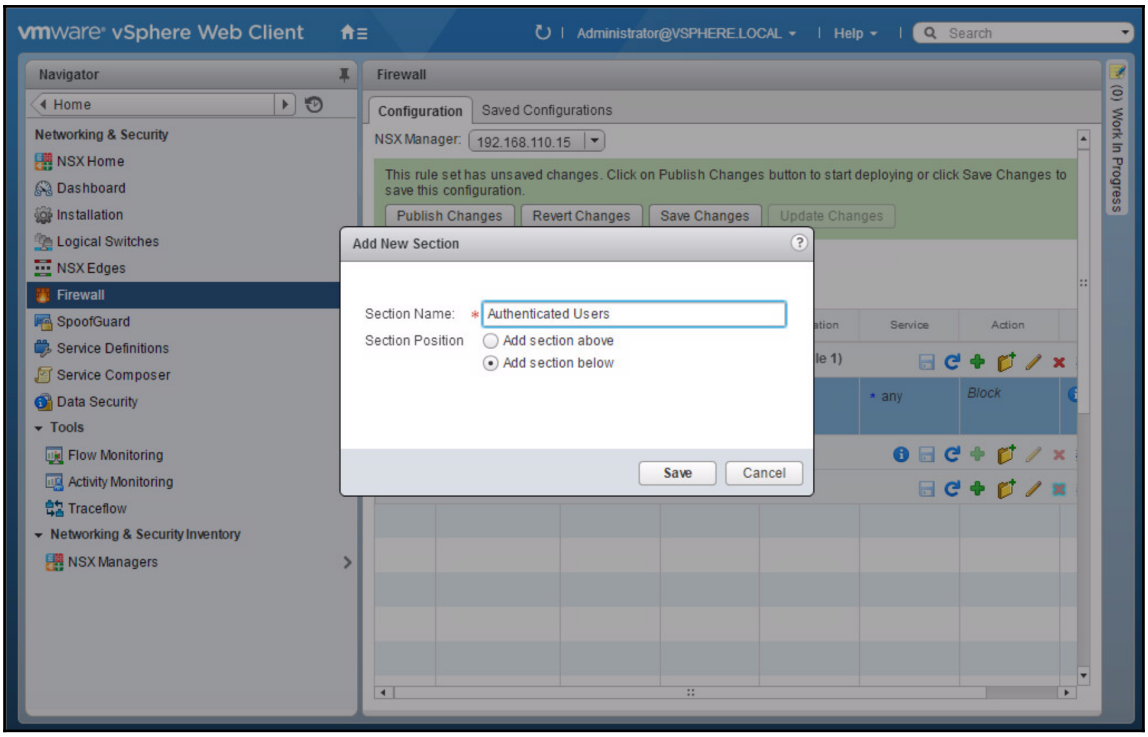

Outside Network
Network Switch
vFW
vFW
vFW
OvS
OvS
OvS
192.168.1.1 Mail Server
192.168.1.2 FTP Server
192.168.1.3 Web Server
Hypervisor

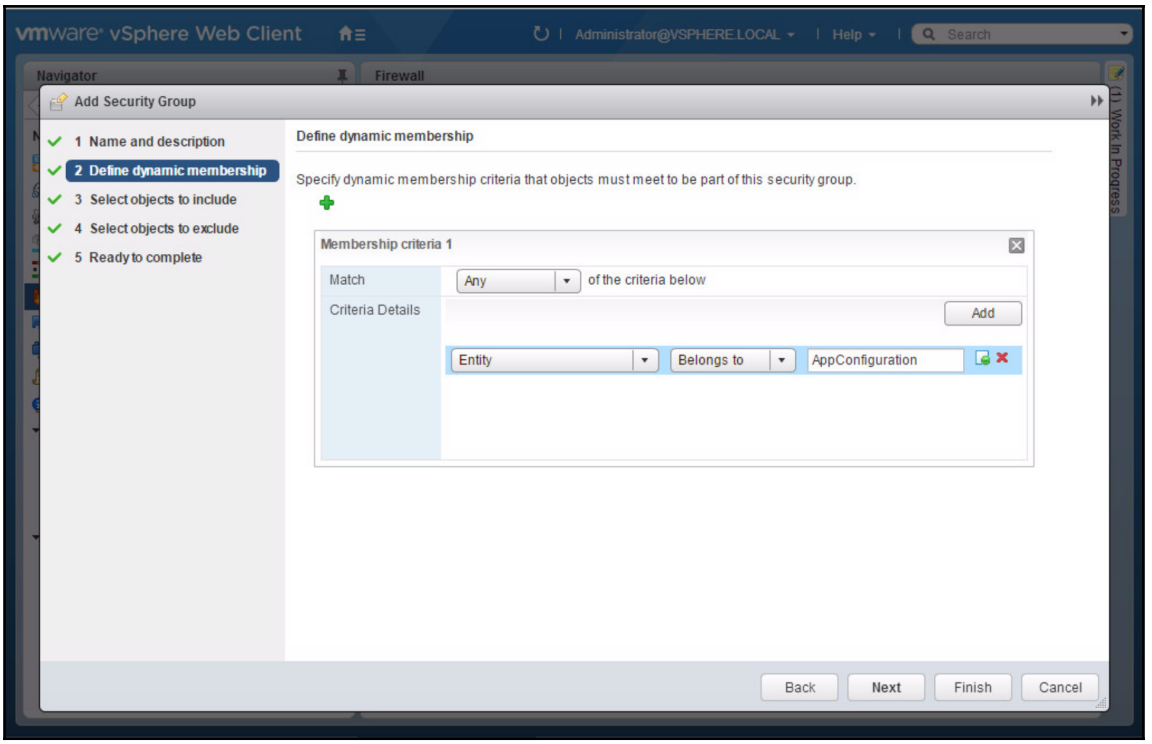

OpenFlow Switch
Bridge
vFW
Bridge
192.168.1.1
Storage
192.168.1.3
Web
Server
Hypervisor

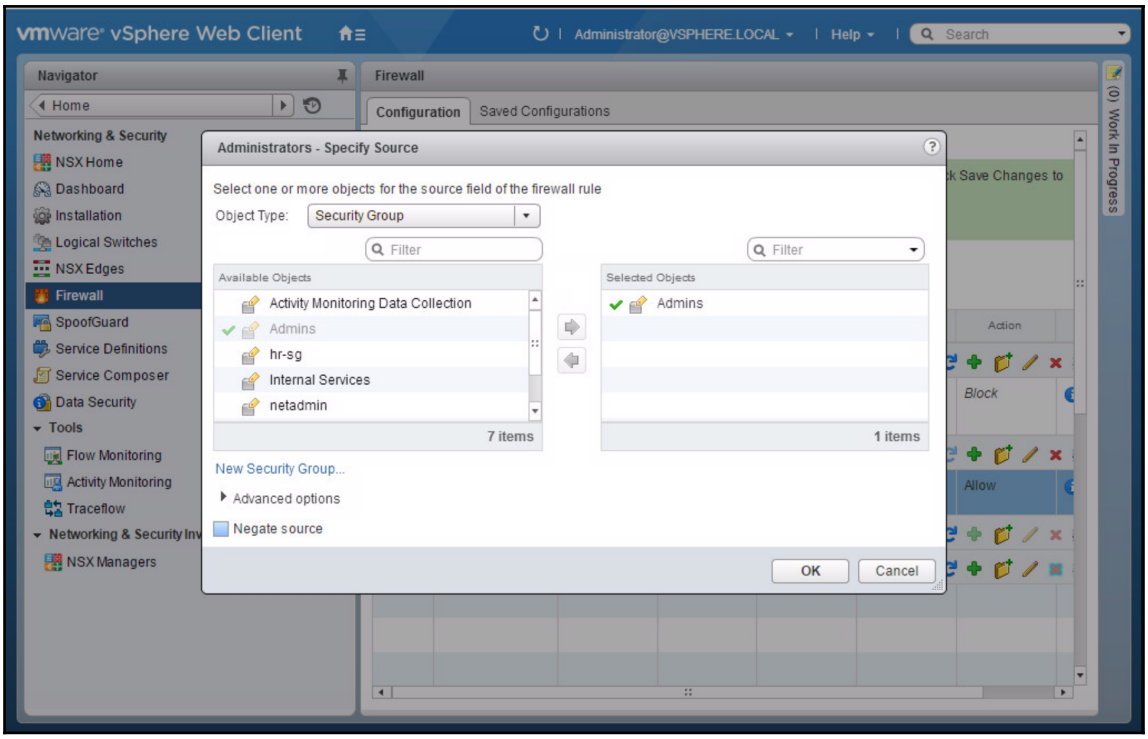

Outside
Network
Programmable Switch
vFW
vIDS
Bridge
Bridge
192.168.1.1
Storage
192.168.1.3
Web
Server
Hypervisor

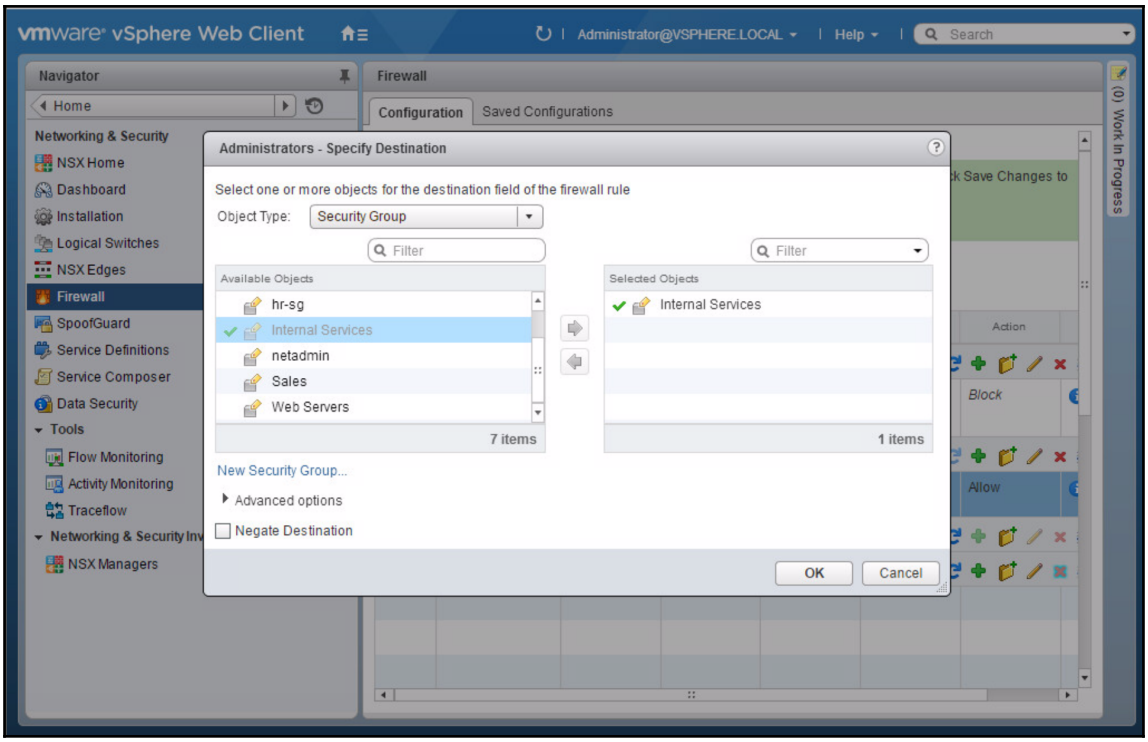

Outside Network
APIC (x3)
Cisco Nexus 9500
Cisco Nexus 9300
EPG
EPG
EPG
vFW
vFW
vFW
192.168.1.1 Mail Server
192.168.1.2 FTP Server
192.168.1.3 Web Server

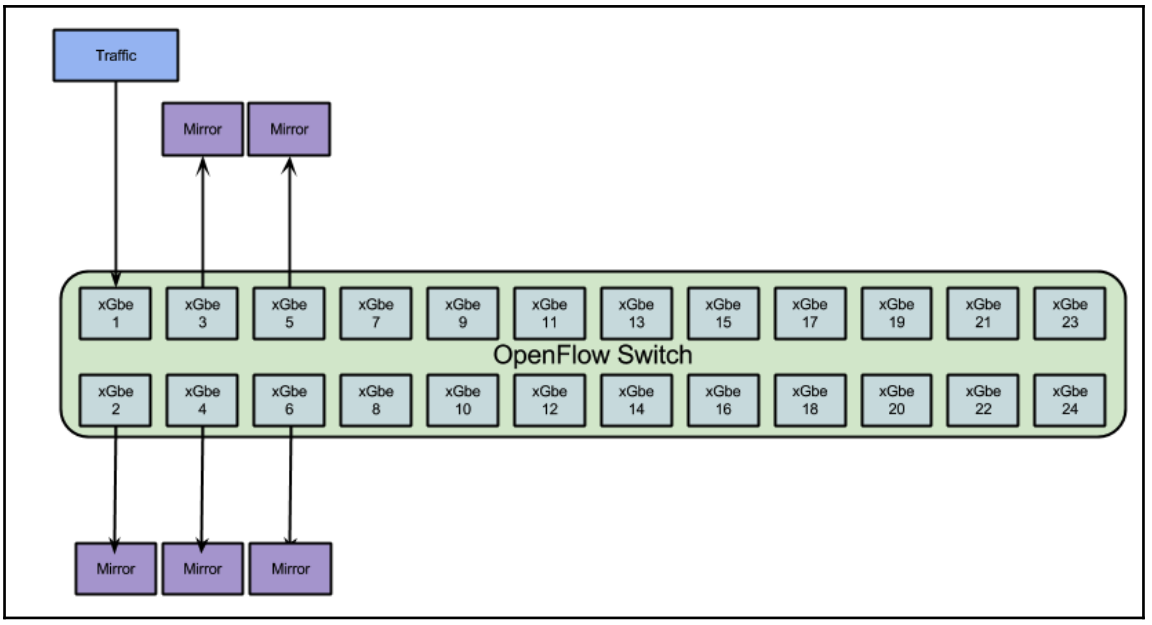

External Consumer
Cisco Nexus 9300
External EPG
vFW
ADC
Web EPG
Function Node
Function Node
Service Graph
Function Node Conector
Contract

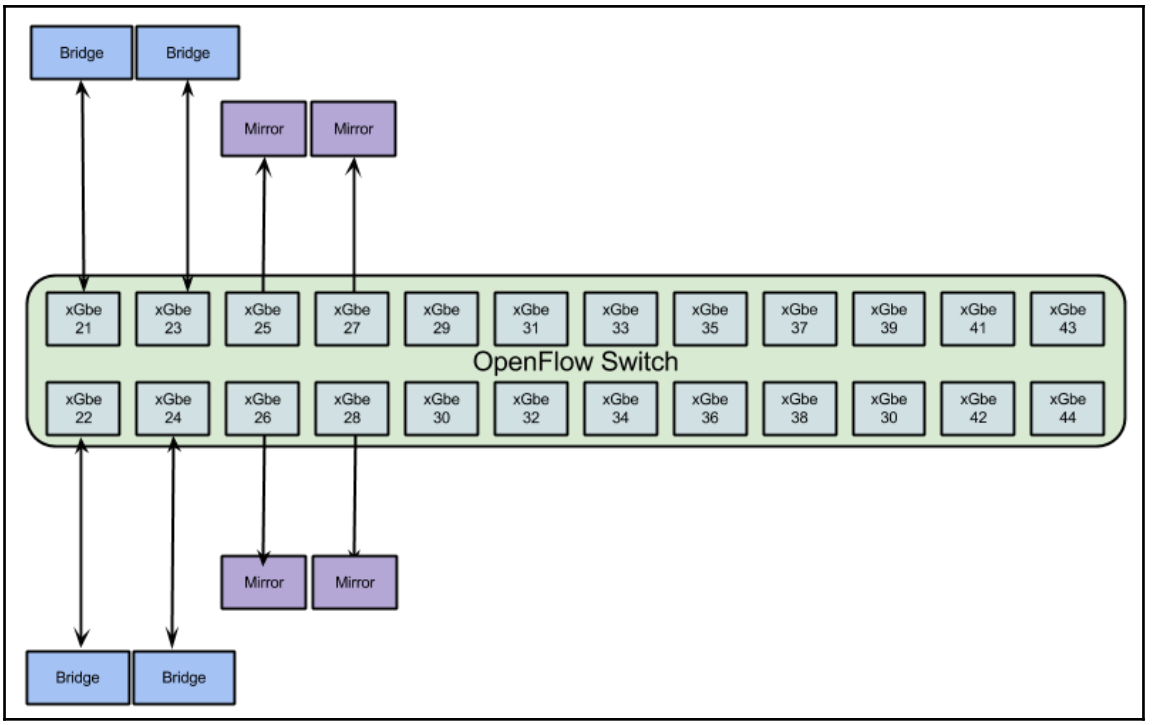

vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Home
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Data Security
Tools
Flow Monitoring
Activity Monitoring
Traceflow
Networking & Security Inventory
NSX Managers
Firewall
Configuration
Saved Configurations
NSX Manager:
192.168.110.15
This rule set has unsaved changes. Click on Publish Changes button to start deploying or click Save Changes to save this configuration.
Publish Changes
Revert Changes
Save Changes
Update Changes
(0) Work In Progress
Add New Section
Section Name:
Authenticated Users
Section Position
Add section above
Add section below
Save
Cancel
Service
Action
any
Block

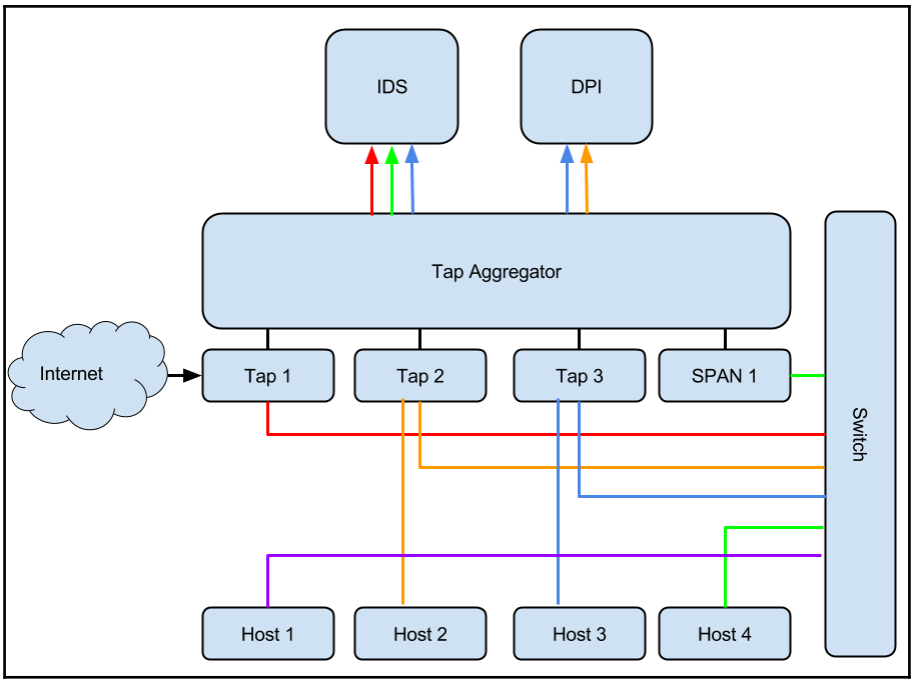

vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Firewall
Add Security Group
1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete
Define dynamic membership
Specify dynamic membership criteria that objects must meet to be part of this security group.
Membership criteria 1
Match
Any
of the criteria below
Criteria Details
Add
Entity
Belongs to
AppConfiguration
Back
Next
Finish
Cancel
(1) Work In Progress


vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Home
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Data Security
Tools
Flow Monitoring
Activity Monitoring
Traceflow
Networking & Security Inv
NSX Managers
Firewall
Configuration
Saved Configurations
(0) Work In Progress
Save Changes to
Action
Block
Allow
Administrators - Specify Source
Select one or more objects for the source field of the firewall rule
Object Type:
Security Group
Filter
Available Objects
Activity Monitoring Data Collection
Admins
hr-sg
Internal Services
netadmin
7 items
Filter
Selected Objects
Admins
1 items
New Security Group...
Advanced options
Negate source
OK
Cancel


vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Home
Networking & Security
NSX Home
Dashboard
Installation
Logical Switches
NSX Edges
Firewall
SpoofGuard
Service Definitions
Service Composer
Data Security
Tools
Flow Monitoring
Activity Monitoring
Traceflow
Networking & Security Inv
NSX Managers
Firewall
Configuration
Saved Configurations
(0) Work In Progress
Save Changes to
Action
Block
Allow
Administrators - Specify Destination
Select one or more objects for the destination field of the firewall rule
Object Type:
Security Group
Filter
Available Objects
hr-sg
Internal Services
netadmin
Sales
Web Servers
7 items
Filter
Selected Objects
Internal Services
1 items
New Security Group...
Advanced options
Negate Destination
OK
Cancel


Traffic
Mirror
Mirror
xGbe 1
xGbe 3
xGbe 5
xGbe 7
xGbe 9
xGbe 11
xGbe 13
xGbe 15
xGbe 17
xGbe 19
xGbe 21
xGbe 23
OpenFlow Switch
xGbe 2
xGbe 4
xGbe 6
xGbe 8
xGbe 10
xGbe 12
xGbe 14
xGbe 16
xGbe 18
xGbe 20
xGbe 22
xGbe 24
Mirror
Mirror
Mirror


Bridge
Bridge
Mirror
Mirror
xGbe 21
xGbe 23
xGbe 25
xGbe 27
xGbe 29
xGbe 31
xGbe 33
xGbe 35
xGbe 37
xGbe 39
xGbe 41
xGbe 43
OpenFlow Switch
xGbe 22
xGbe 24
xGbe 26
xGbe 28
xGbe 30
xGbe 32
xGbe 34
xGbe 36
xGbe 38
xGbe 30
xGbe 42
xGbe 44
Mirror
Mirror
Bridge
Bridge


IDS
DPI
Tap Aggregator
Internet
Tap 1
Tap 2
Tap 3
SPAN 1
Switch
Host 1
Host 2
Host 3
Host 4