TOMORROW
starts here.

Policy Driven Data Centre with ACI

BRKACI-1601

Chris Gascoigne

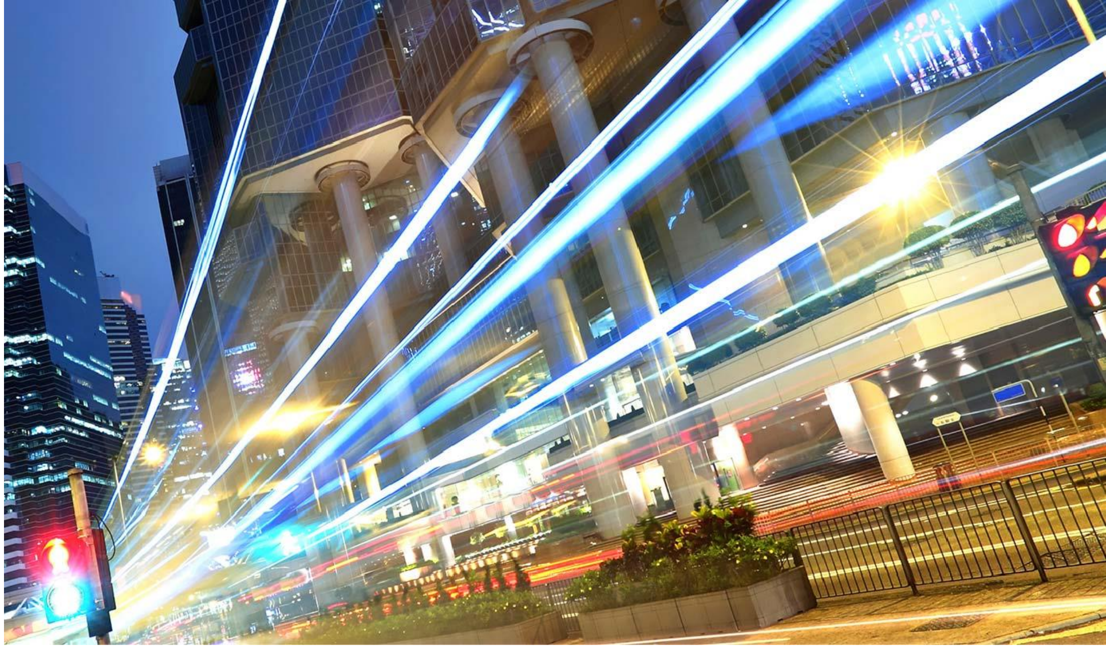
Technical Solutions Architect

#clmel

Cisco live!

Agenda

- Introduction
- What is policy
- Network policy
- Application policy
- Conclusion

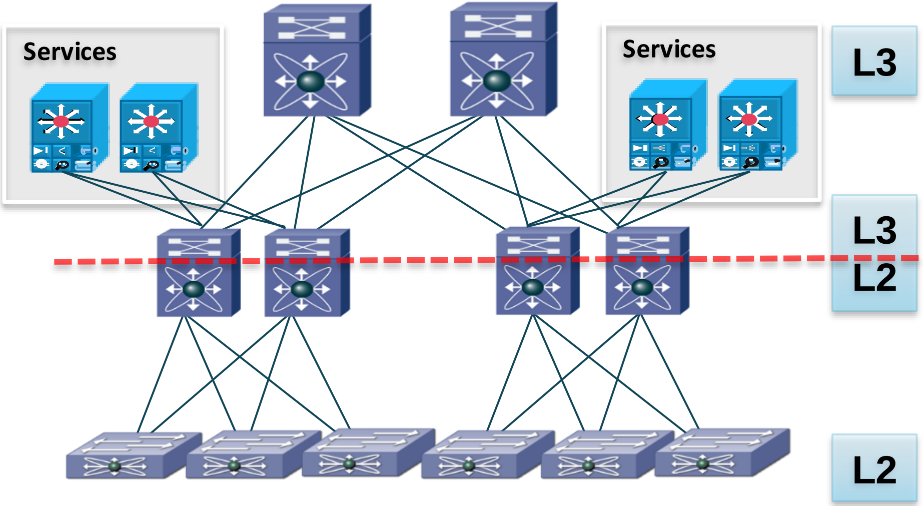


Introduction

Traditional Data Centre Networking Issues

Lack of agility

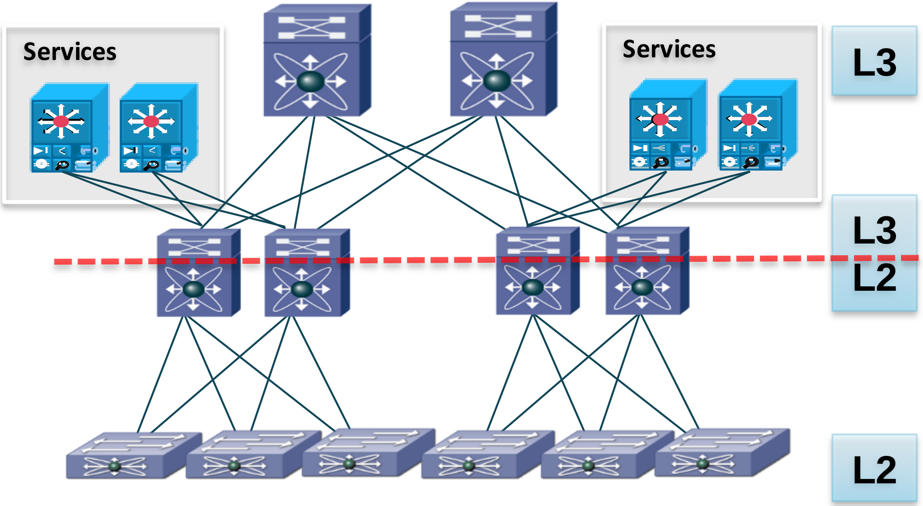
- Configuration is complex
- Configuration is error-prone
- Configuration changes require careful planning
- Many touch points
- Restricted workload placement / mobility



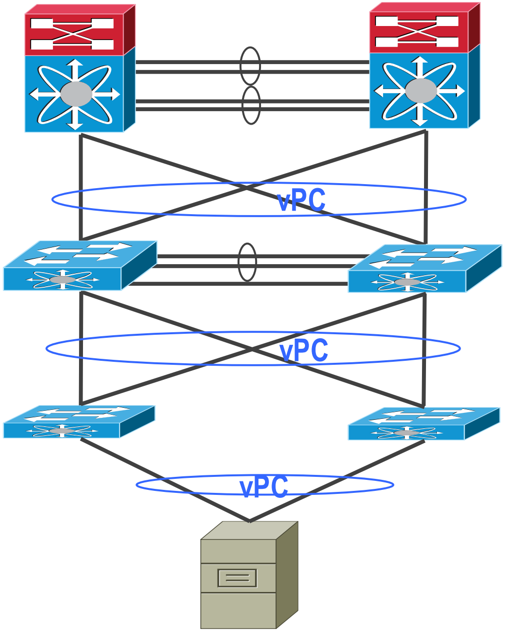
Traditional Networking Issues

Not cost effective

- Expensive hardware in core/distribution
- Intelligence/state centralised at core/distribution
- Big CapEx upgrades required to scale up

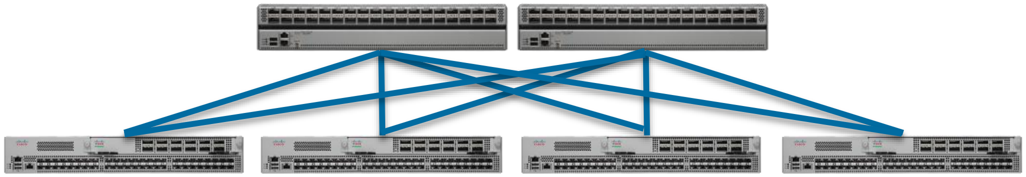


ACI Changes The Game

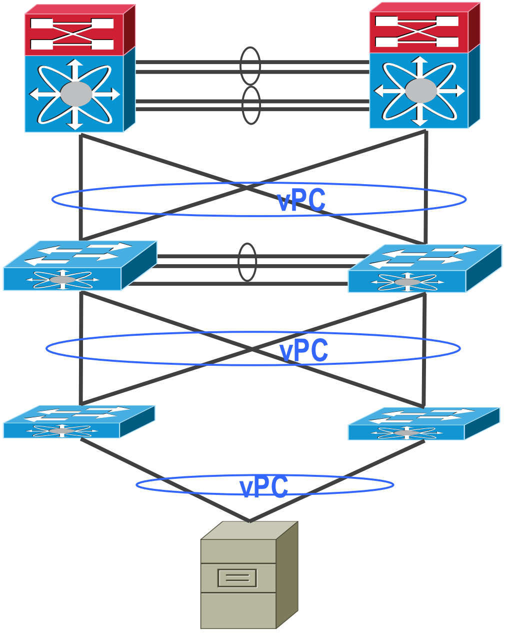


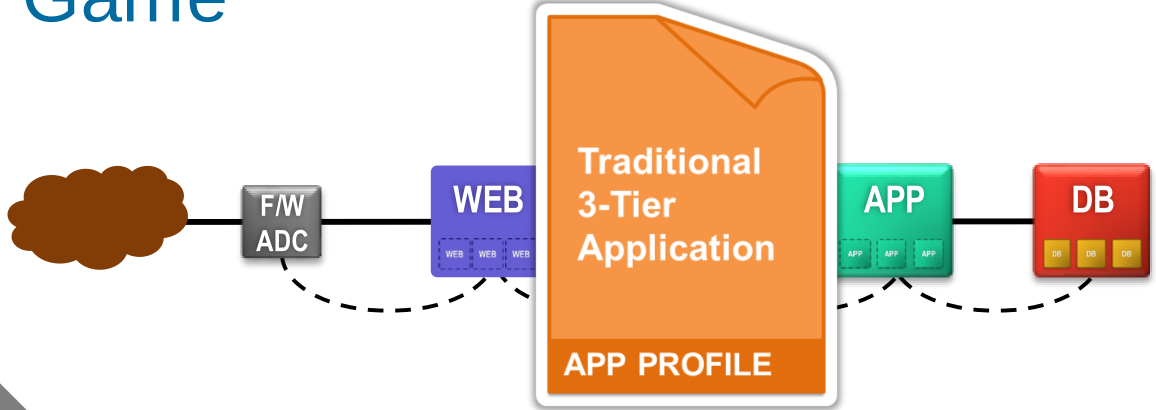
A better network

- Simplify the topology
- Self configuring
- Host mobility
- Scale out
- Penalty free fabric
- Cost effective



ACI Changes The Game



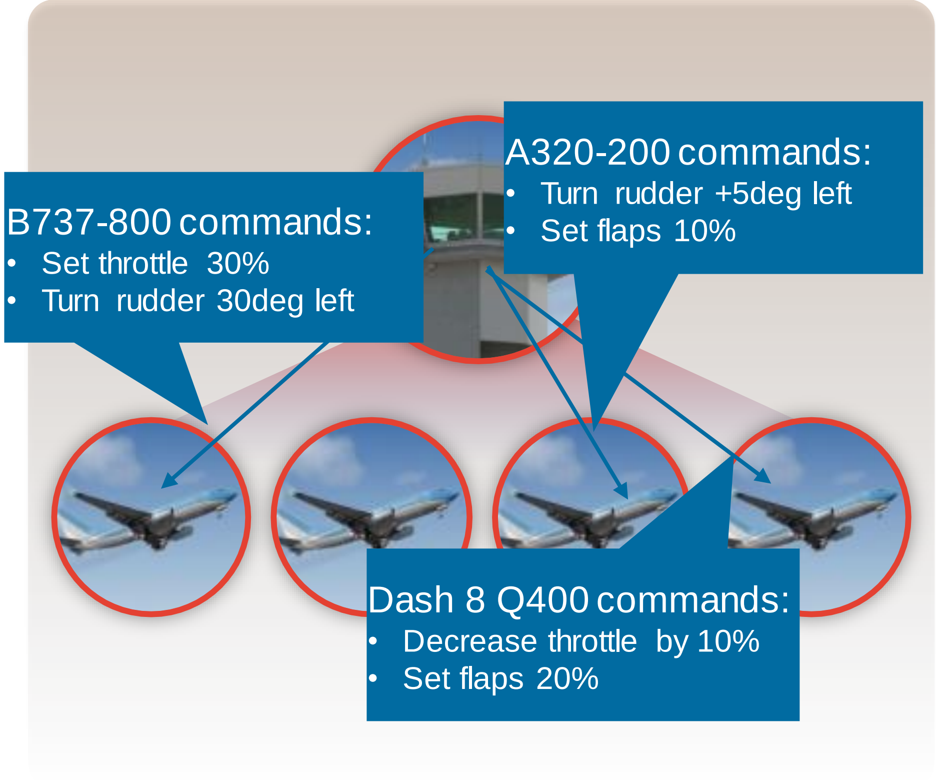


Policy

- Centralised provisioning
- Build policy, not configuration
- Profile driven
- Abstracted from topology, fowarding
- Simplify operations

Imperative Control

- Controller has full intelligence/state
- Controlled entities follow rules/instructions
- Controller knows how to control all entity types
- Good for:
  - Small systems
  - Simple problems
  - All controlled entities are the same



A320-200 commands:

- Turn rudder +5deg left
- Set flaps 10%

B737-800 commands:

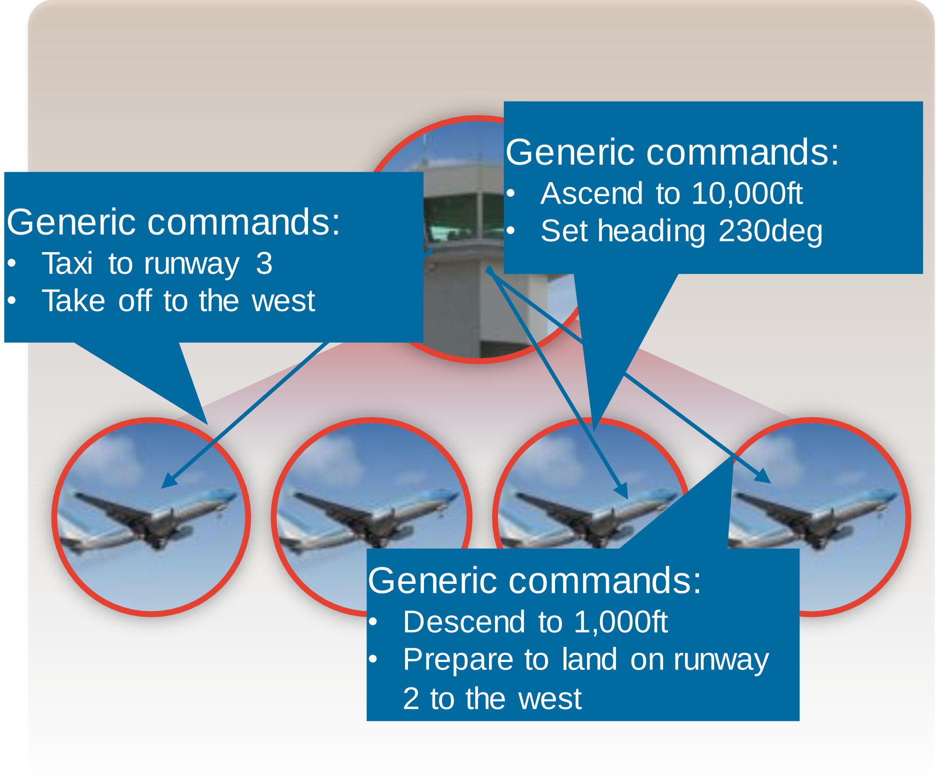
- Set throttle 30%
- Turn rudder 30deg left

Dash 8 Q400 commands:

- Decrease throttle by 10%
- Set flaps 20%

Declarative Control

- Controller stores/distributes desired state
- Controlled entities receive desired state and make changes
- Good for:
  - Large scale
  - Complex problems
  - Disparate controlled entities



Generic commands:
- Taxi to runway 3
- Take off to the west

Generic commands:
- Ascend to 10,000ft
- Set heading 230deg

Generic commands:
- Descend to 1,000ft
- Prepare to land on runway 2 to the west

Declarative vs Imperative

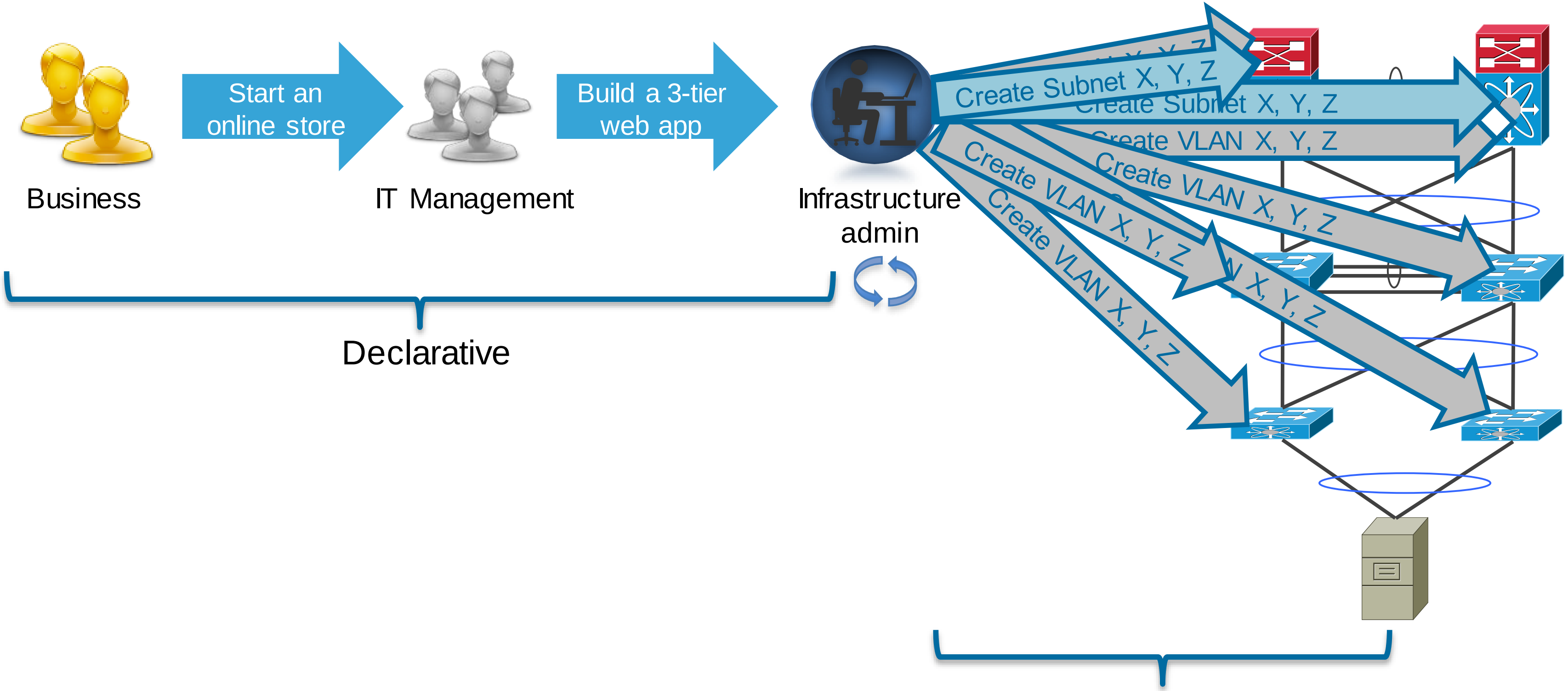
Puppet (declarative)

```
user { ‘cgascoig’ :
  ensure => present,
  gid => ‘admin’,
}

group { ‘admin’ :
  ensure => present,
}
```

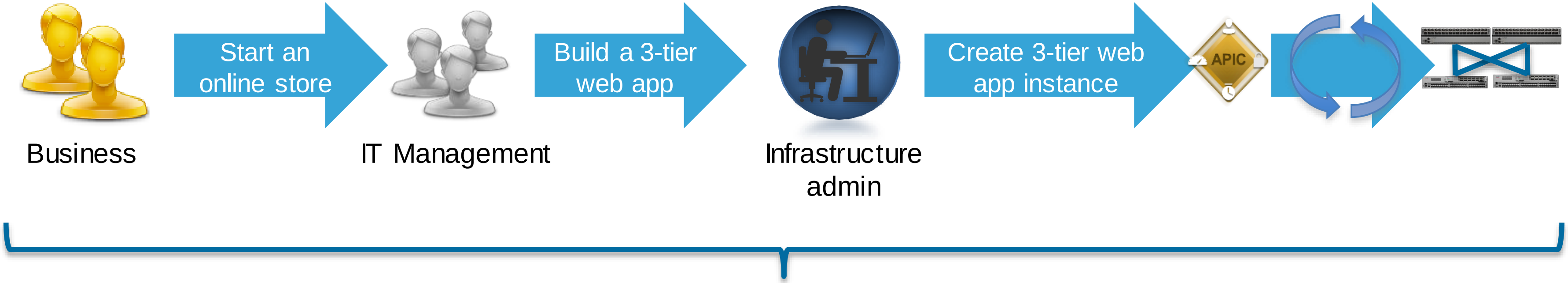
Shell script (imperative)

```
#!/bin/bash

if ! getent group sysadmin >/dev/null
then
              echo "Group sysadmin does not exist, creating"
              groupadd sysadmin
fi

if  ! getent passwd chris >/dev/null
then
              echo "User chris does not exist, creating"
              useradd --gid sysadmin chris
fi

USERGROUPID=`getent passwd chris | awk -F: '{print $4}'`
USERGROUPNAME=`getent group $USERGROUPID | awk -F: '{print
$1}'`


if [ "$USERGROUPNAME" != "sysadmin" ]
then
              echo "Primary group of user chris is not
sysadmin, updating"
              usermod --gid sysadmin chris
fi
```

Network Provisioning Today



Intent Driven Provisioning



Business

Start an online store

IT Management

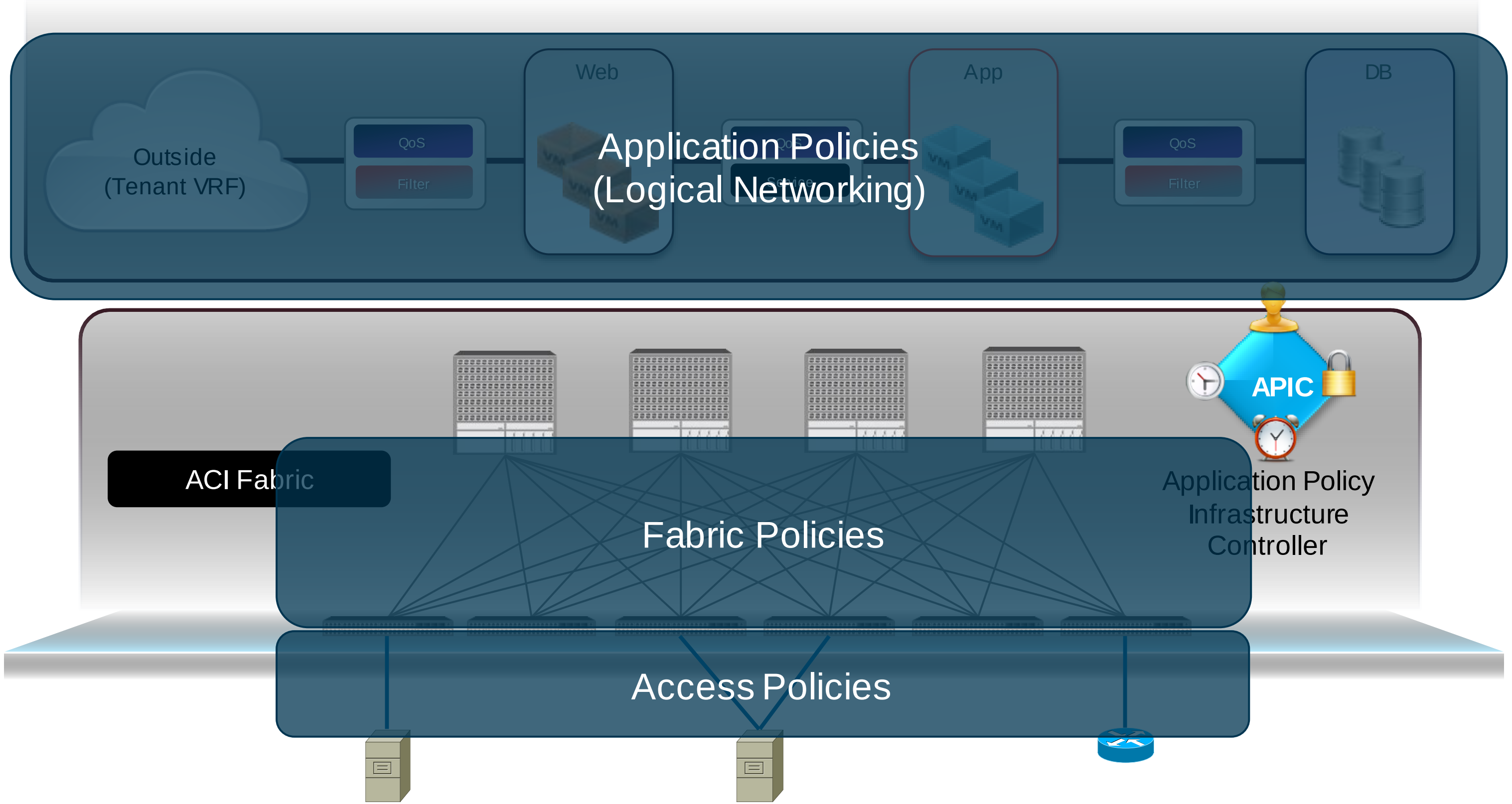
Build a 3-tier web app

Infrastructure admin

Create 3-tier web app instance

Declarative

Policy Layers in ACI

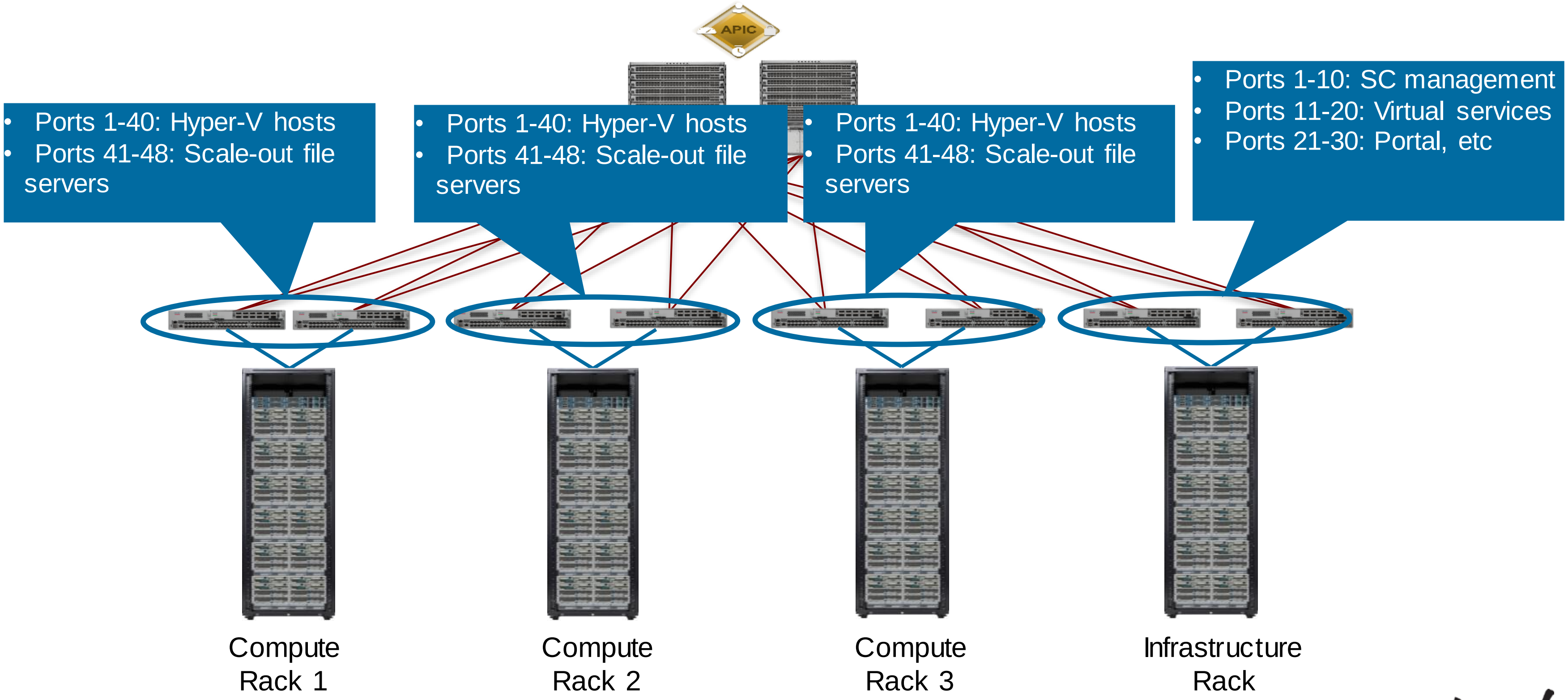


Network Policy

Network Policy

- Fabric Policies
  - Fabric interface policies
  - Pod policies
  - Fabric load balancing policies
  - Firmware / maintenance policies
  - …
- Access Policies
  - Interface policies
  - vPC
  - Attachable Access Entity Profiles
  - Quality of Service Classes
  - DHCP Policies

Switch / Interface Policy



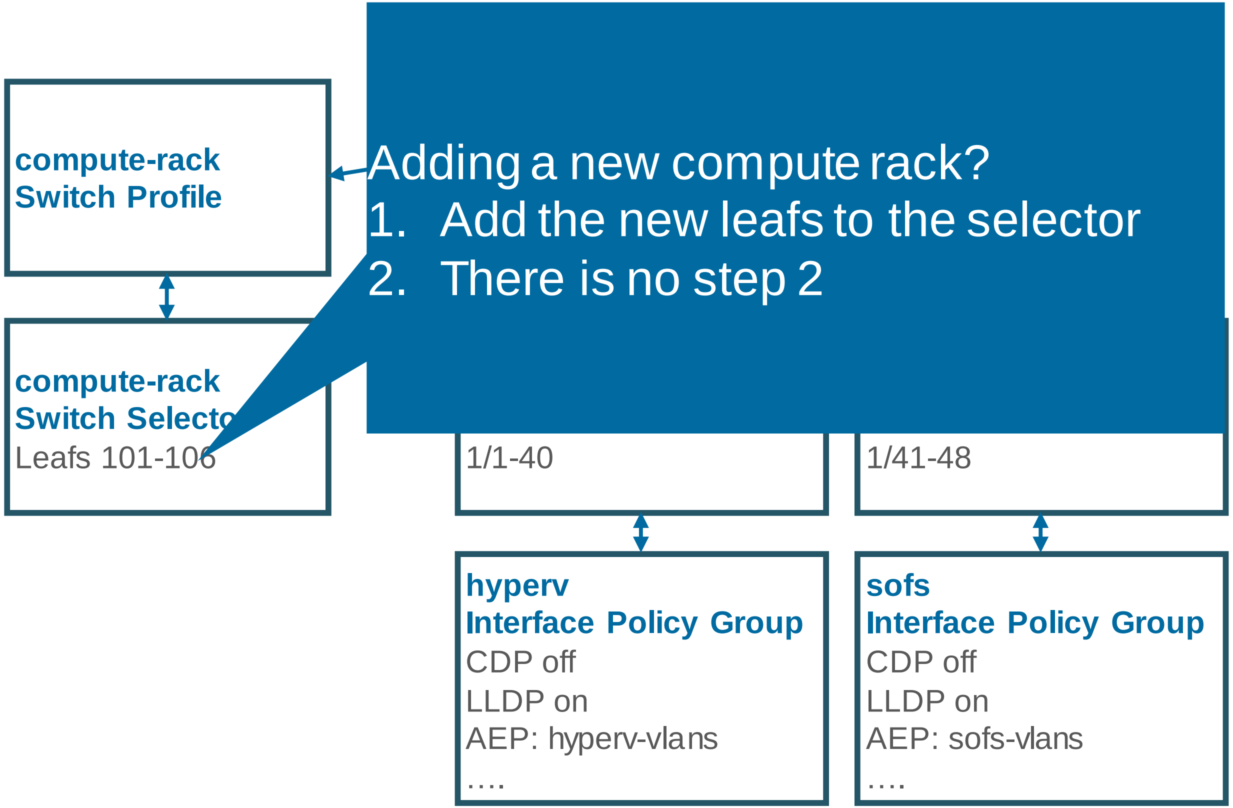
- Ports 1-40: Hyper-V hosts
- Ports 41-48: Scale-out file servers

- Ports 1-40: Hyper-V hosts
- Ports 41-48: Scale-out file servers

- Ports 1-40: Hyper-V hosts
- Ports 41-48: Scale-out file servers

- Ports 1-10: SC management
- Ports 11-20: Virtual services
- Ports 21-30: Portal, etc

Switch / Interface Policy



Adding a new compute rack?

1. Add the new leafs to the selector
2. There is no step 2

compute-rack
Switch Profile

compute-rack
Switch Selecto
Leafs 101-106

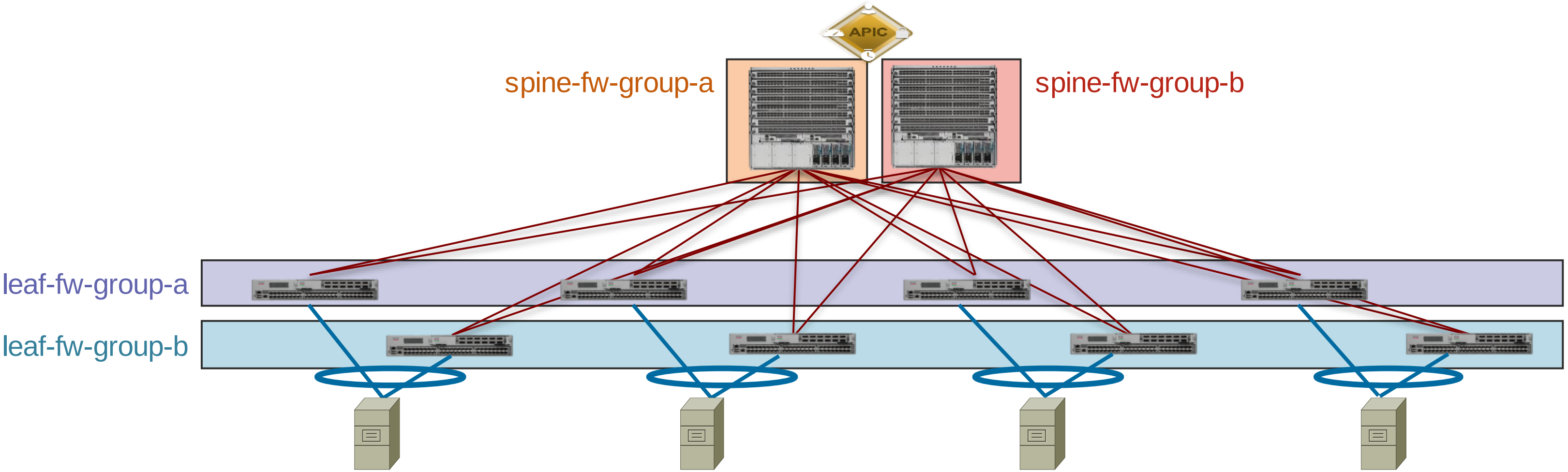
1/1-40

1/41-48

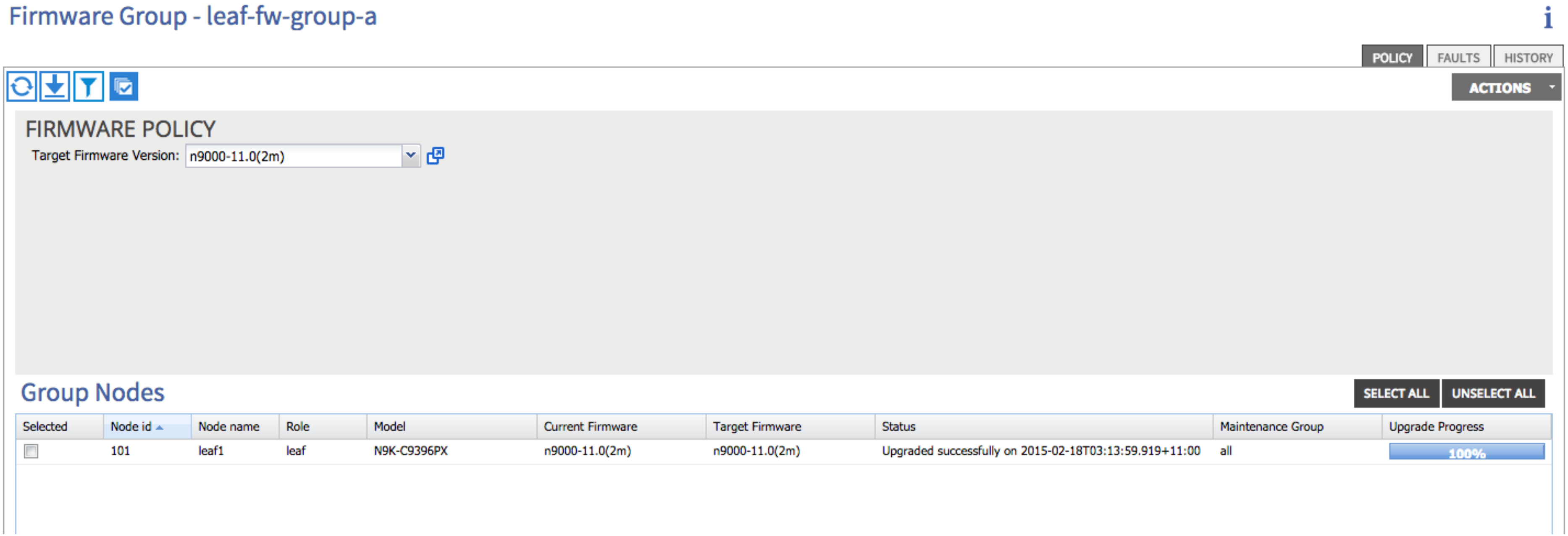
hyperv
Interface Policy Group
CDP off
LLDP on
AEP: hyperv-vlans
….

sofs
Interface Policy Group
CDP off
LLDP on
AEP: sofs-vlans
….

Firmware Policy



Firmware Policy



Firmware Group - leaf-fw-group-a

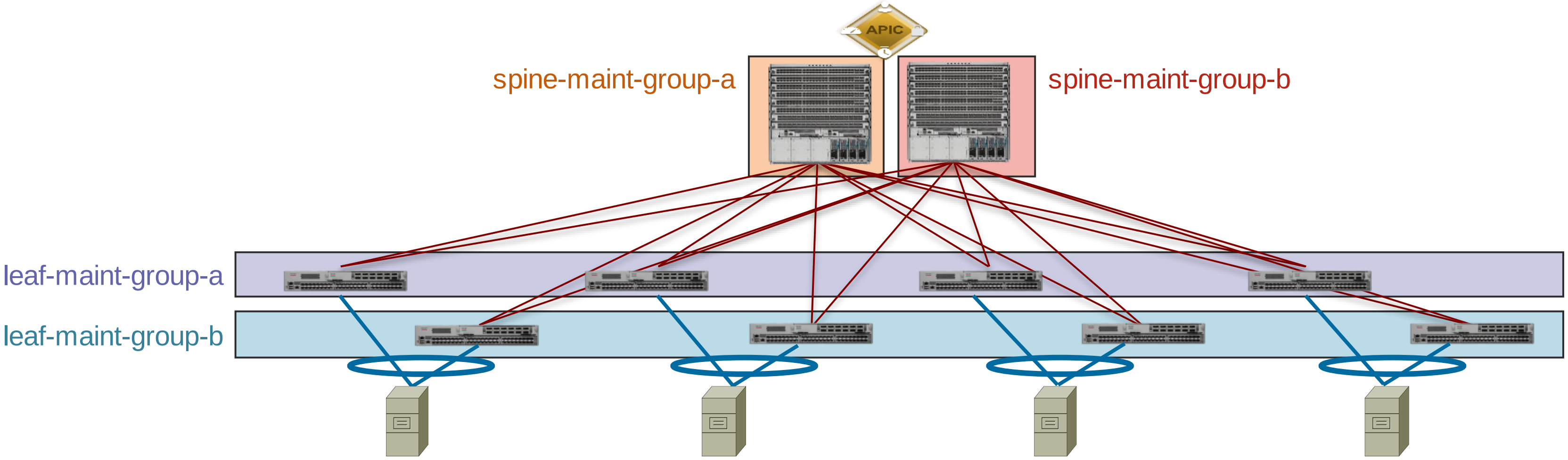
FIRMWARE POLICY

Target Firmware Version: n9000-11.0(2m)

Group Nodes

Selected	Node id	Node name	Role	Model	Current Firmware	Target Firmware	Status	Maintenance Group	Upgrade Progress
□	101	leaf1	leaf	N9K-C9396PX	n9000-11.0(2m)	n9000-11.0(2m)	Upgraded successfully on 2015-02-18T03:13:59.919+11:00	all	100%

Maintenance Policy



Maintenance Policy

leaf-maint-group-a	leaf-maint-group-b	spine-maint-group-a	spine-maint-group-b
Window:	**Window**:	**Window**:	**Window**:
Wed 22:00-23:59	Thur 22:00-23:59	Thur 00:00-01:59	Fri 00:00-01:59
Concurrent nodes:	**Concurrent nodes:**	**Concurrent nodes:**	**Concurrent nodes:**
4	4	1	1

Application Policy

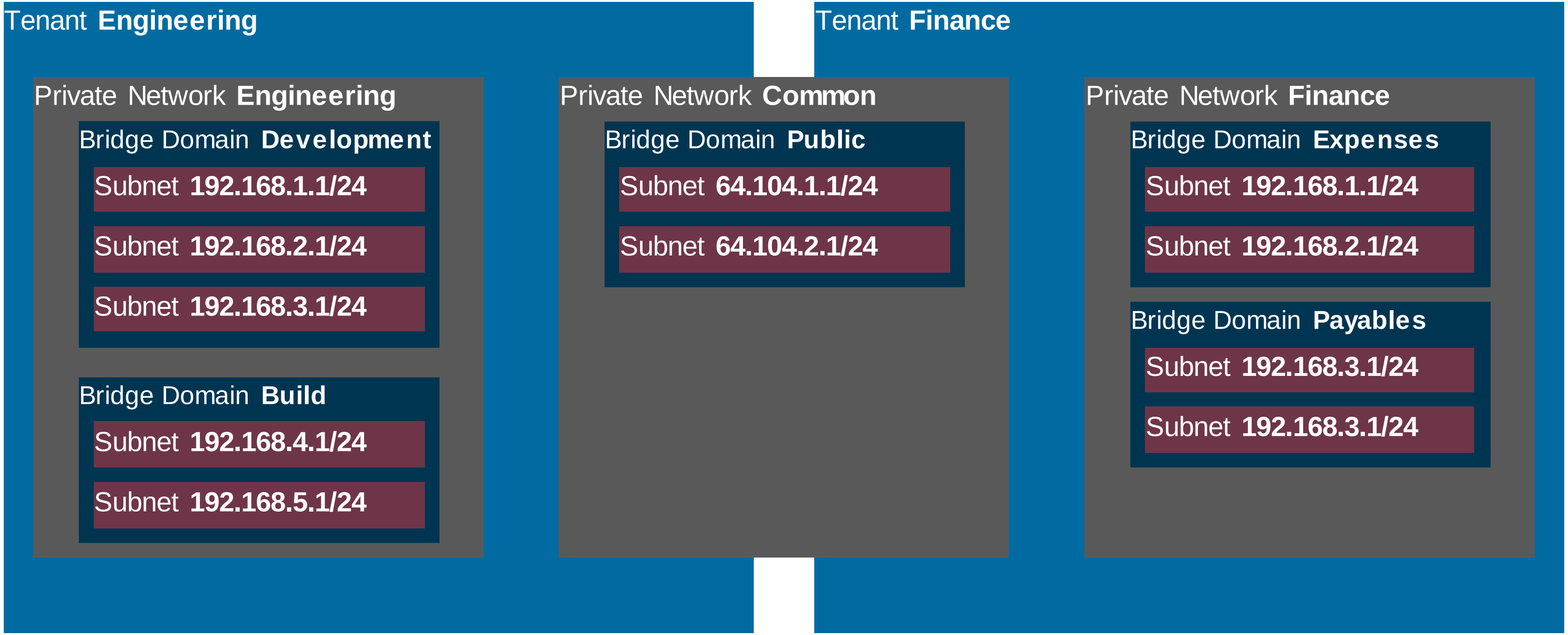
Application Policy

- Logical networking
- Application Network Profiles
- Service insertion and automation

Logical Networking

- How does A talk to B?
  - Bridged?
  - Routed?
  - Intra-VRF? Inter-VRF?
  - Inside to outside? Outside to inside?

Logical Networking



Tenant **Engineering**

Private Network **Engineering**

Bridge Domain **Development**

Subnet **192.168.1.1/24**

Subnet **192.168.2.1/24**

Subnet **192.168.3.1/24**

Bridge Domain **Build**

Subnet **192.168.4.1/24**

Subnet **192.168.5.1/24**

Private Network **Common**

Bridge Domain **Public**

Subnet **64.104.1.1/24**

Subnet **64.104.2.1/24**

Tenant **Finance**

Private Network **Finance**

Bridge Domain **Expenses**

Subnet **192.168.1.1/24**

Subnet **192.168.2.1/24**

Bridge Domain **Payables**

Subnet **192.168.3.1/24**

Subnet **192.168.3.1/24**

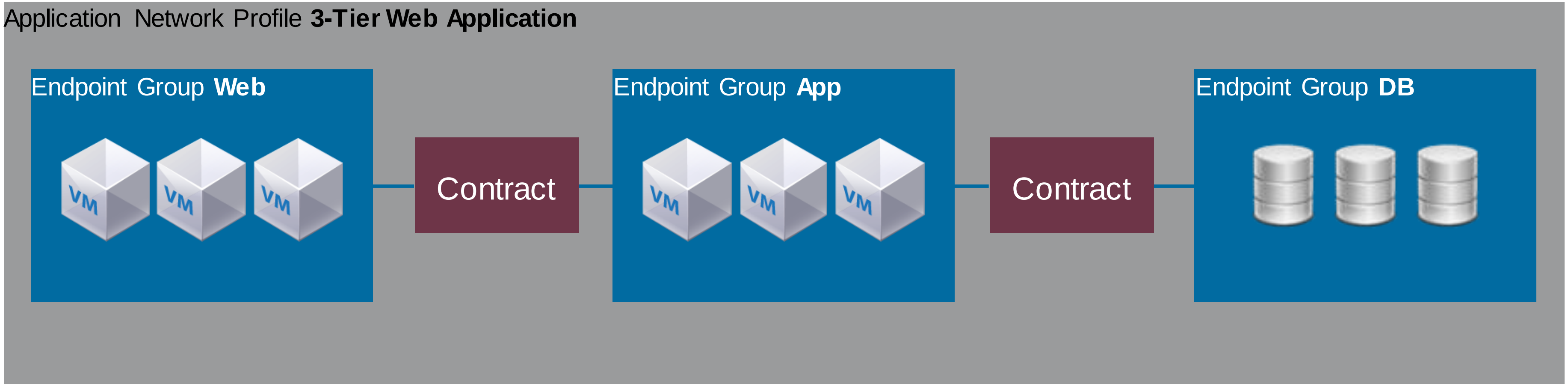
Logical Networking Terms

- **Tenant** – Logical separation for administrative domains (e.g. Business Unit, Customers, Dev/Test/Prod)
- **Private Network** – Separate routing instances == VRF
- **Bridge Domain** – Layer 2 segment; analogous to a VLAN, but not tied to a VLAN ID
- **Subnet** – Layer 3 address associated to a Bridge Domain == SVI

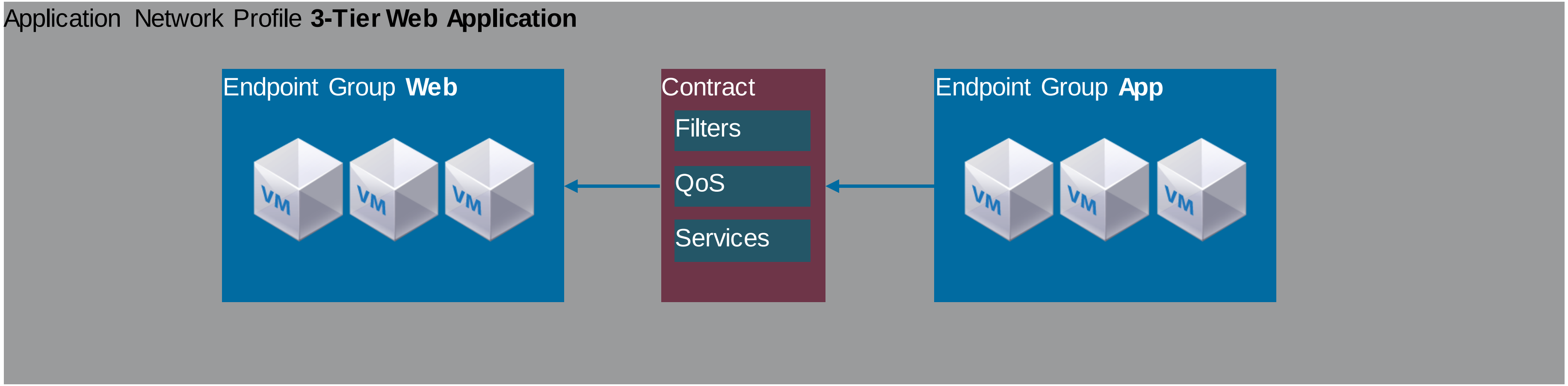
Application Network Profiles

- Logical network defines **how** A talks to B
- Application Network Profiles define **should** A talk to B?
  - Which protocols?
  - QoS?
  - Additional L4-7 services required?
  - Etc.

Application Network Profile



Application Network Profile - Contracts



Application Network Profile **3-Tier Web Application**

Endpoint Group **Web**

Contract

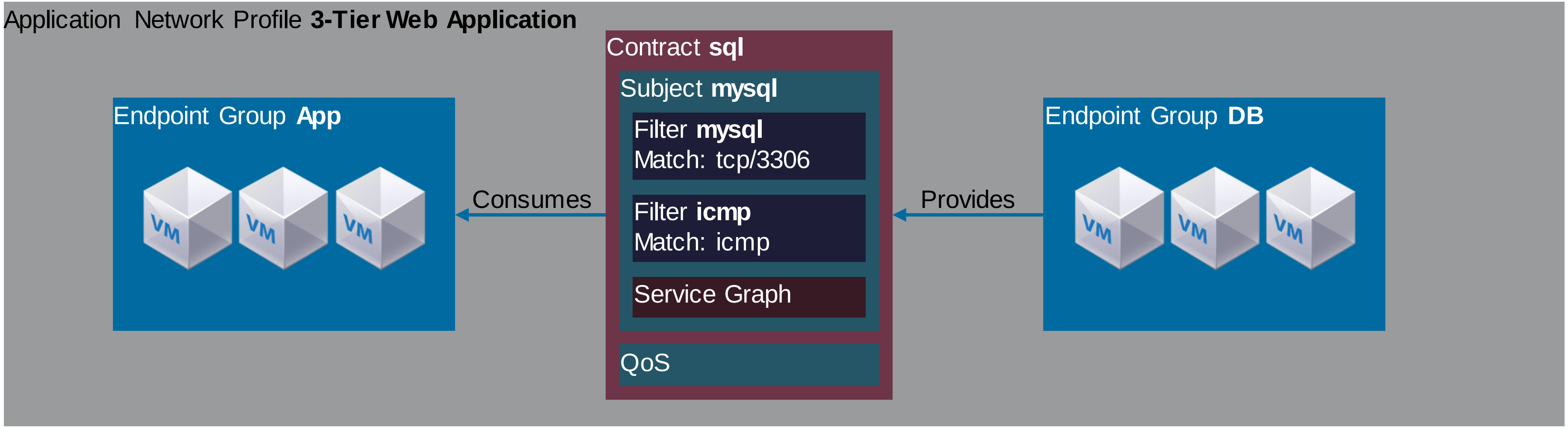
Filters

QoS

Services

Endpoint Group **App**

Application Network Profile - Contracts



Application Network Profile **3-Tier Web Application**

Contract **sql**

Subject **mysql**

Filter **mysql**
Match: tcp/3306

Filter **icmp**
Match: icmp

Service Graph

QoS

Endpoint Group **App**

Endpoint Group **DB**

Application Network Profile Terms

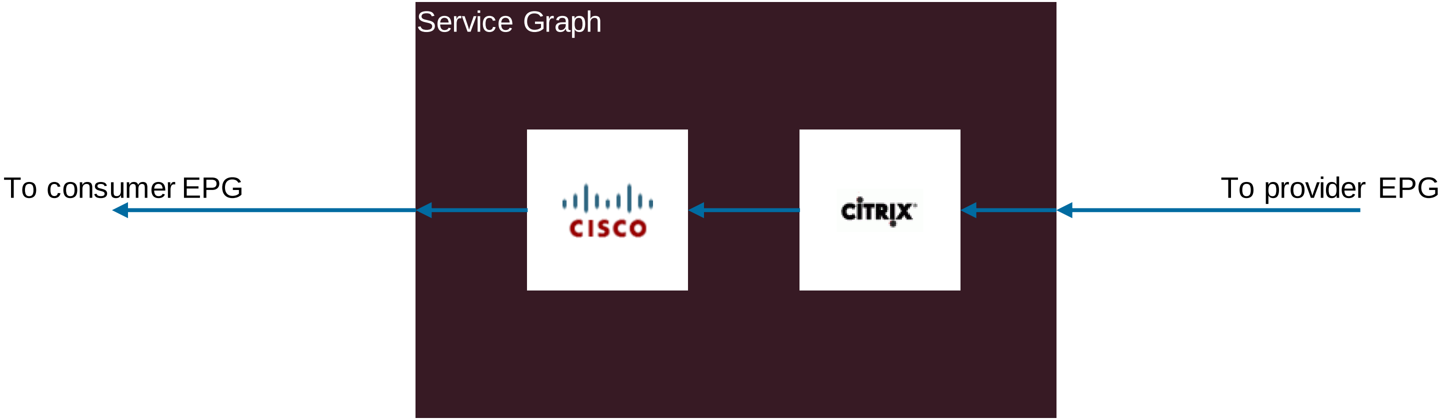
- **Endpoint Group (EPG)** – Group of endpoints (servers/VMs) with the same policy
- **Contract** – Encapsulates policy between endpoint groups
- **Subject** – Defines if (filters) and how (action) traffic can flow between endpoint groups
- **Filter** – Selector of traffic, matching up to L4 attributes
- **Action** – Action to take on matched traffic, e.g. service graph, apply QoS, etc
- **Provider** – Provides the services defined in a contract
- **Consumer** – Consumes the services defined in a contract

Endpoint Group Membership

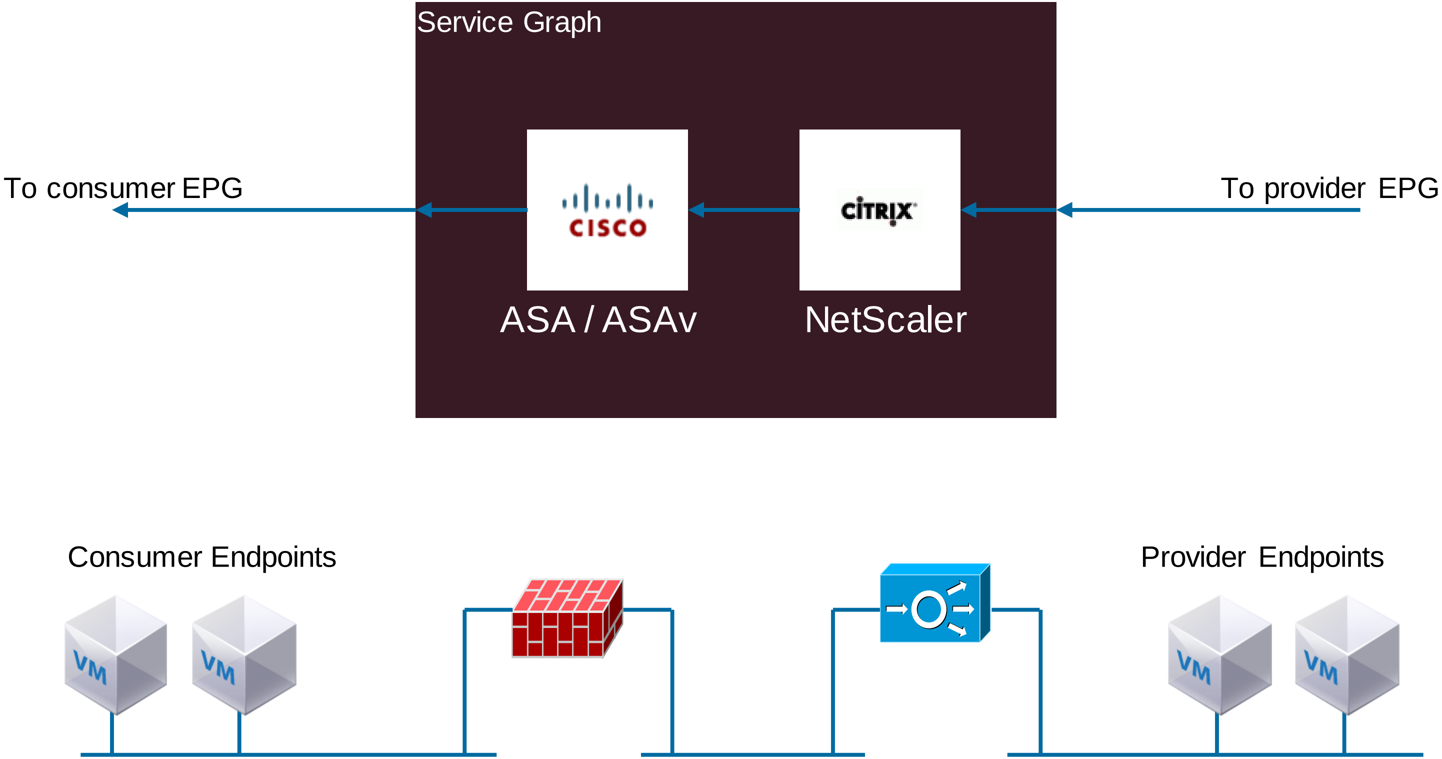
- Physical port
- VLAN Identifier on a port / switch
- VXLAN VNID on a port / switch
- NGVGE VSID on a port / switch
- Subnet
- Virtual Machine Manager grouping
  - Port Group (VMWare vCentre/vShield)
  - VM Network (Microsoft Hyper-V/SCVMM)
  - Neutron Network (OpenStack)

- VM Attribute*
- IP Address*
- MAC Address*
- …

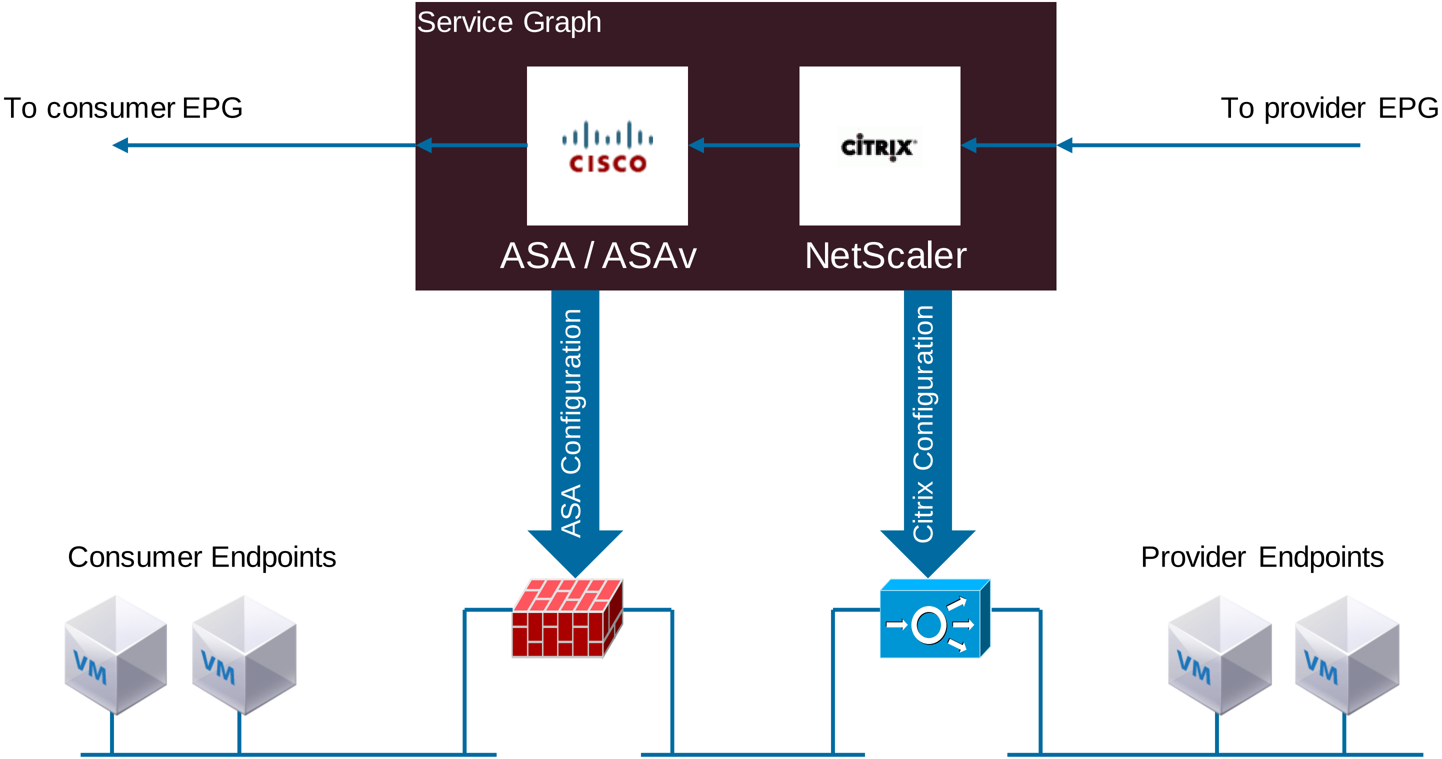
Service Graph



Service Graph – Data Plane

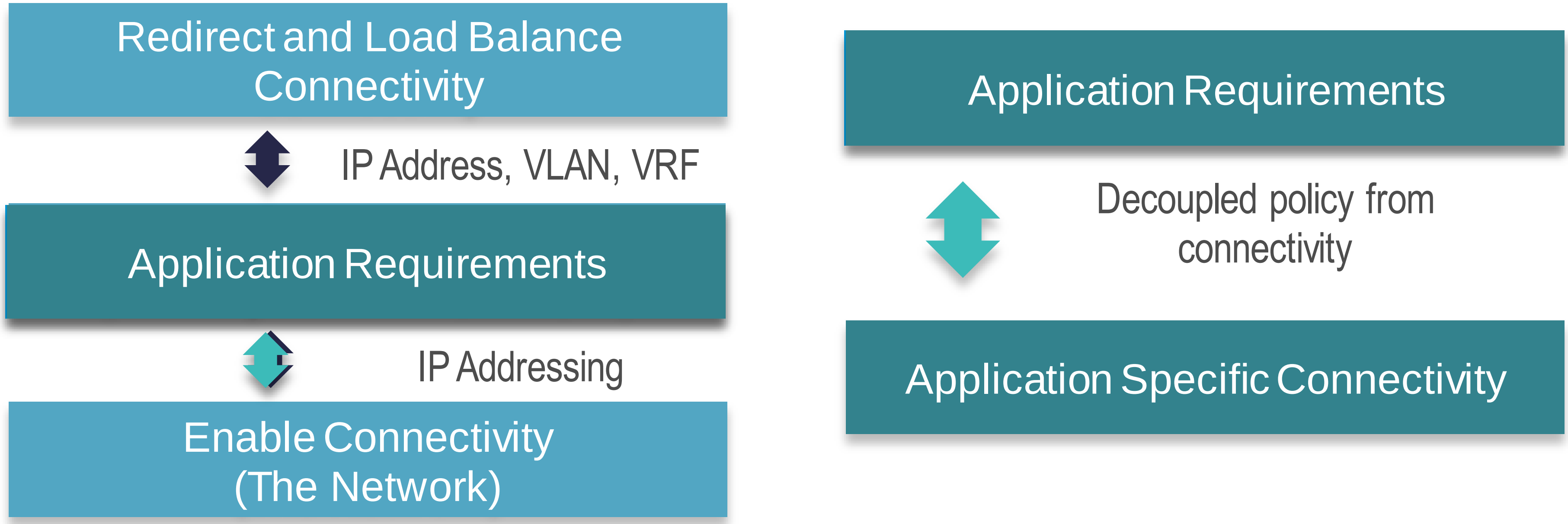


Service Graph – Configuration Plane



Conclusion

Abstraction



Redirect and Load Balance Connectivity

IP Address, VLAN, VRF

Application Requirements

IP Addressing

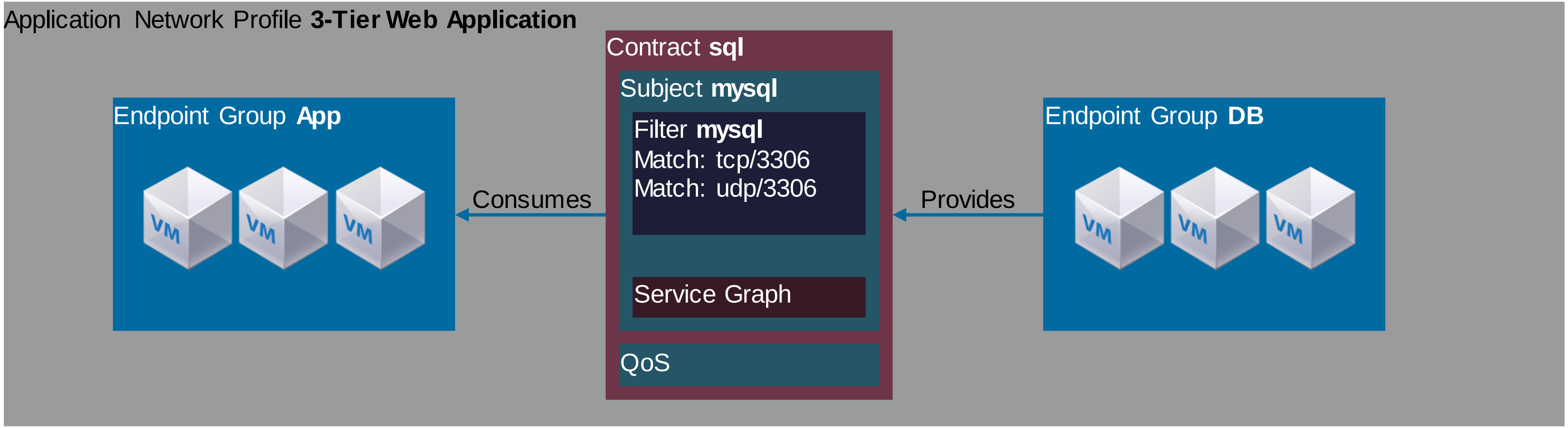
Enable Connectivity (The Network)

Application Requirements

Decoupled policy from connectivity

Application Specific Connectivity

Extensibility



Application Network Profile **3-Tier Web Application**

Endpoint Group **App**

Consumes

Contract **sql**

Subject **mysql**

Filter **mysql**
Match: tcp/3306
Match: udp/3306

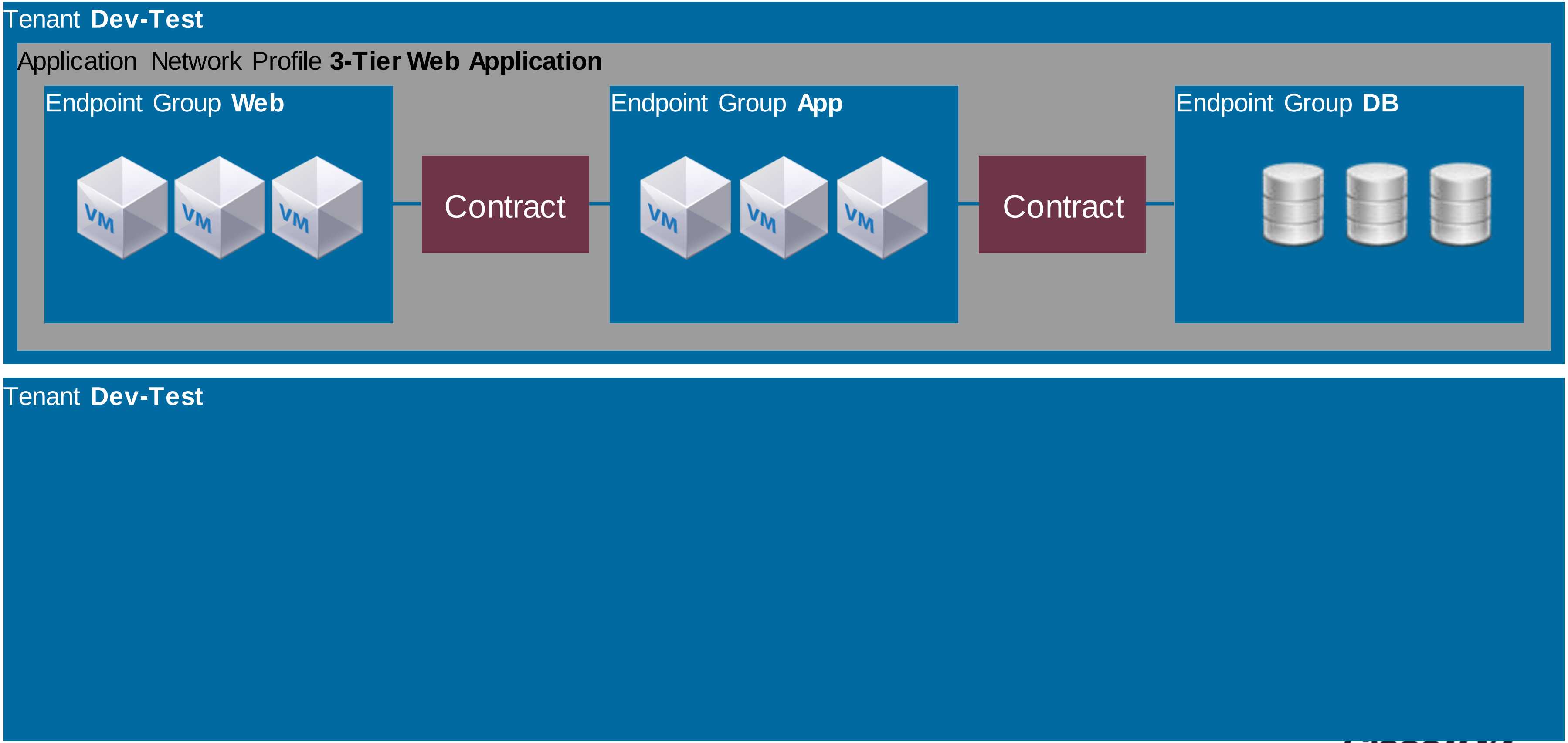
Service Graph

QoS

Provides

Endpoint Group **DB**

Reuse



Tenant **Dev-Test**

Application Network Profile **3-Tier Web Application**

Endpoint Group **Web**

Contract

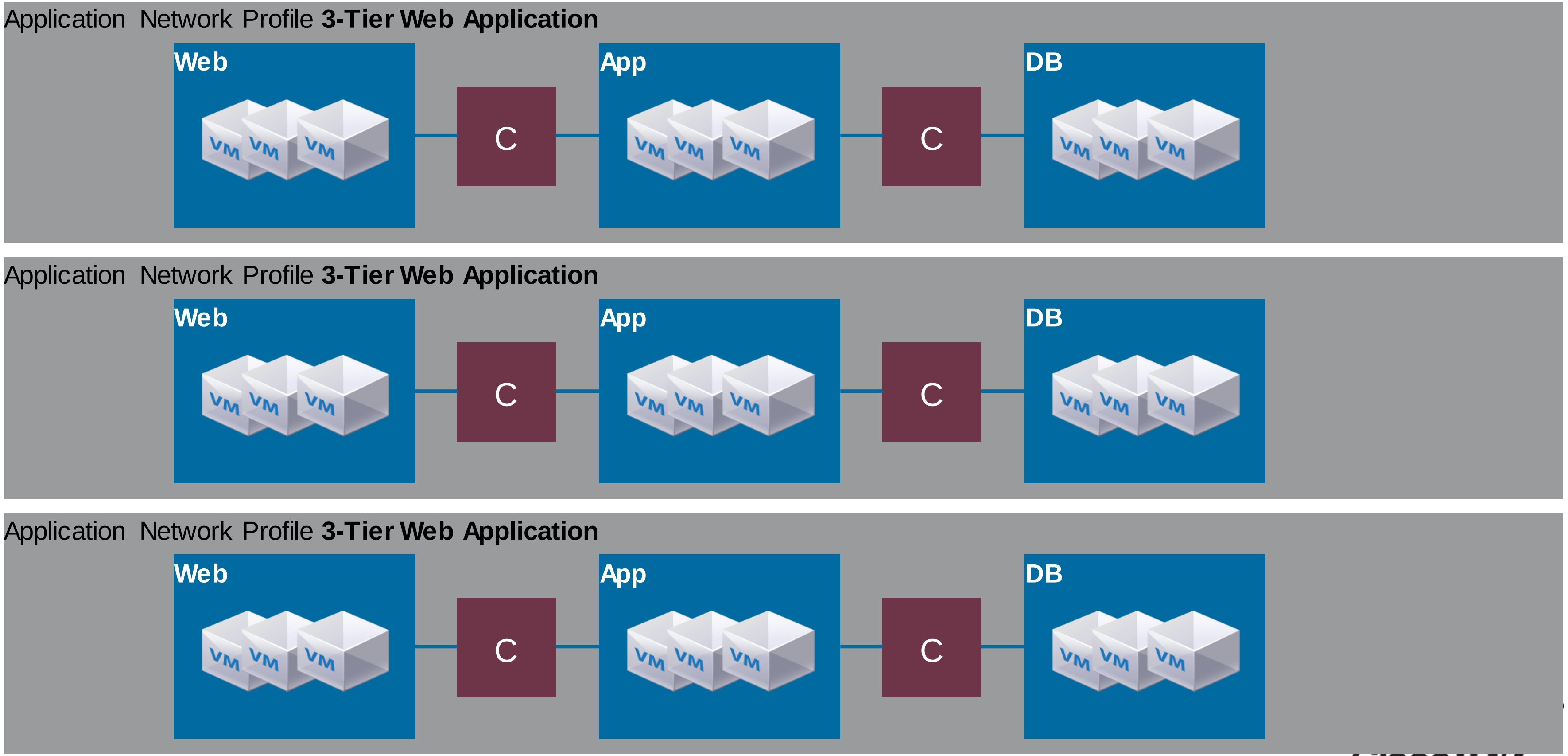
Endpoint Group **App**

Contract

Endpoint Group **DB**

Tenant **Dev-Test**

Consistency



Application Network Profile **3-Tier Web Application**

Web C **App** C **DB**

Application Network Profile **3-Tier Web Application**

Web C **App** C **DB**

Application Network Profile **3-Tier Web Application**

Web C **App** C **DB**

Summary

- Traditional networking approaches
  - not agile enough
  - not cost effective
- Declarative, policy driven approach required:
  - Abstracted
  - Extensible
  - Reusable logical components
  - Consistency

Q & A

Complete Your Online Session Evaluation

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

Complete your Overall Event Survey and 5 Session Evaluations.

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

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

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

Thank you.

cisco