思科在 OpenStack 的雲端技術創新及貢獻

How Cisco ACI flexibly supports Neutron ML2 and GBP for advanced application deployment

July 18th, 2017 Taipei

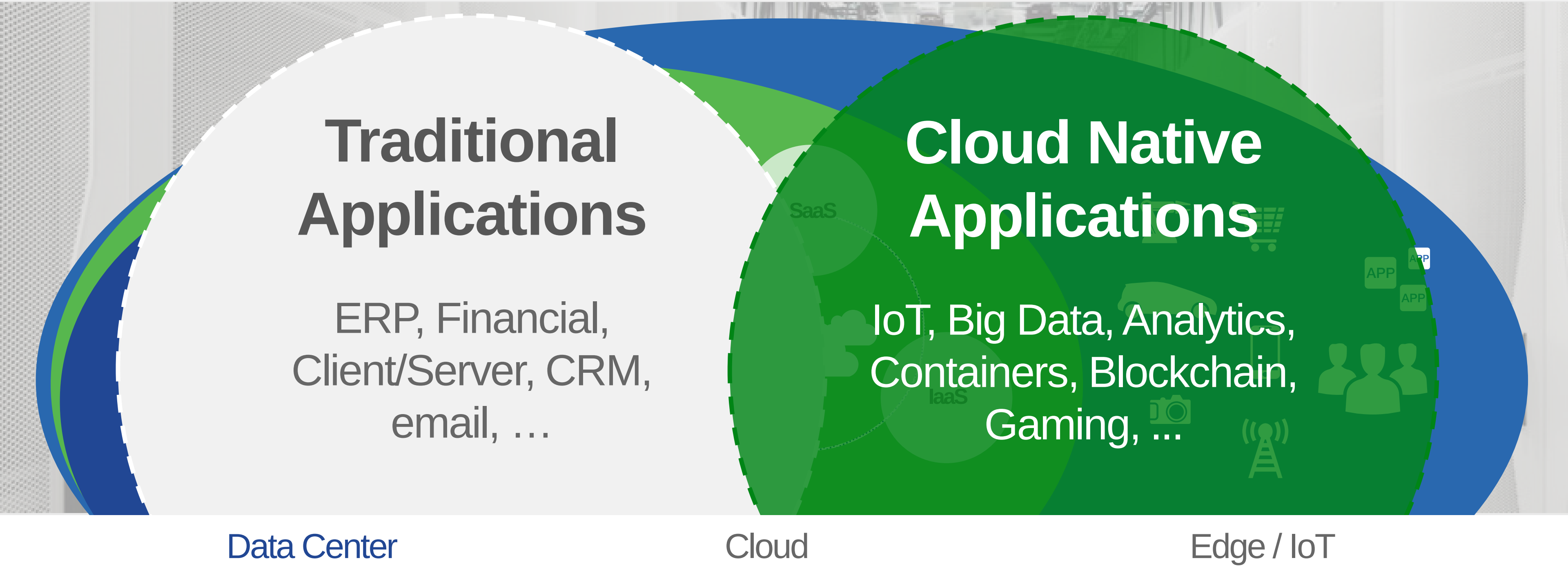
Philip Wong, Technical Solution Architecture, Cisco Greater China

Kent Wu, Technical Leader, Openstack and ACI Integration Team, Cisco

Legal Disclaimer

Many of the products and features described herein remain in varying stages of development and will be offered on a when-and-if-available basis. This roadmap is subject to change at the sole discretion of Cisco Systems, and Cisco Systems will have no liability for delay in the delivery or failure to deliver any of the products or features set forth in this document.

Applications in the Connected World



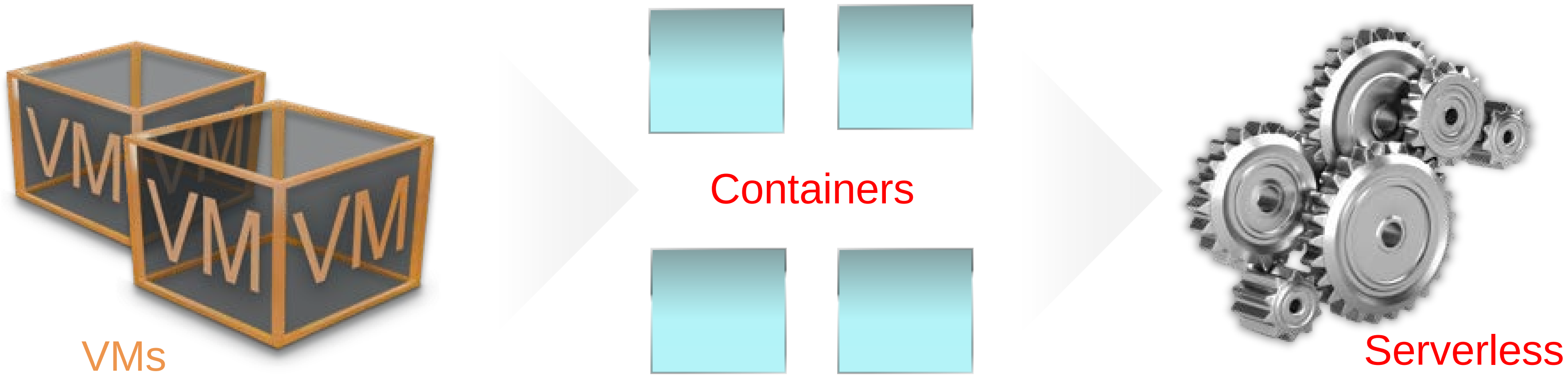
Traditional Applications

ERP, Financial, Client/Server, CRM, email, …

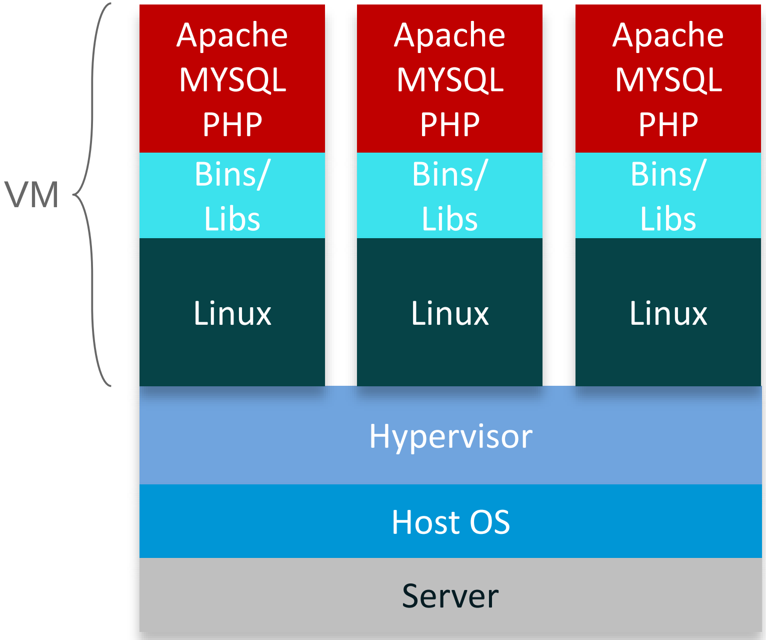
Cloud Native Applications

IoT, Big Data, Analytics, Containers, Blockchain, Gaming, ...

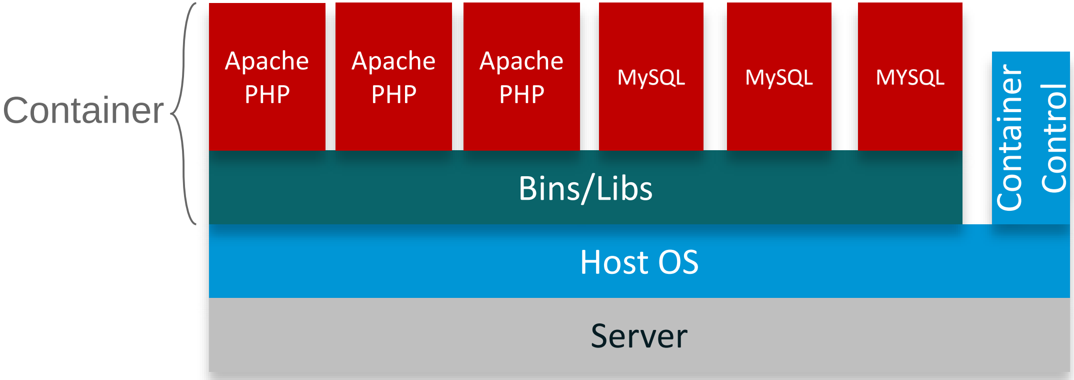
Application Evolution is Driving Infrastructure Transformation



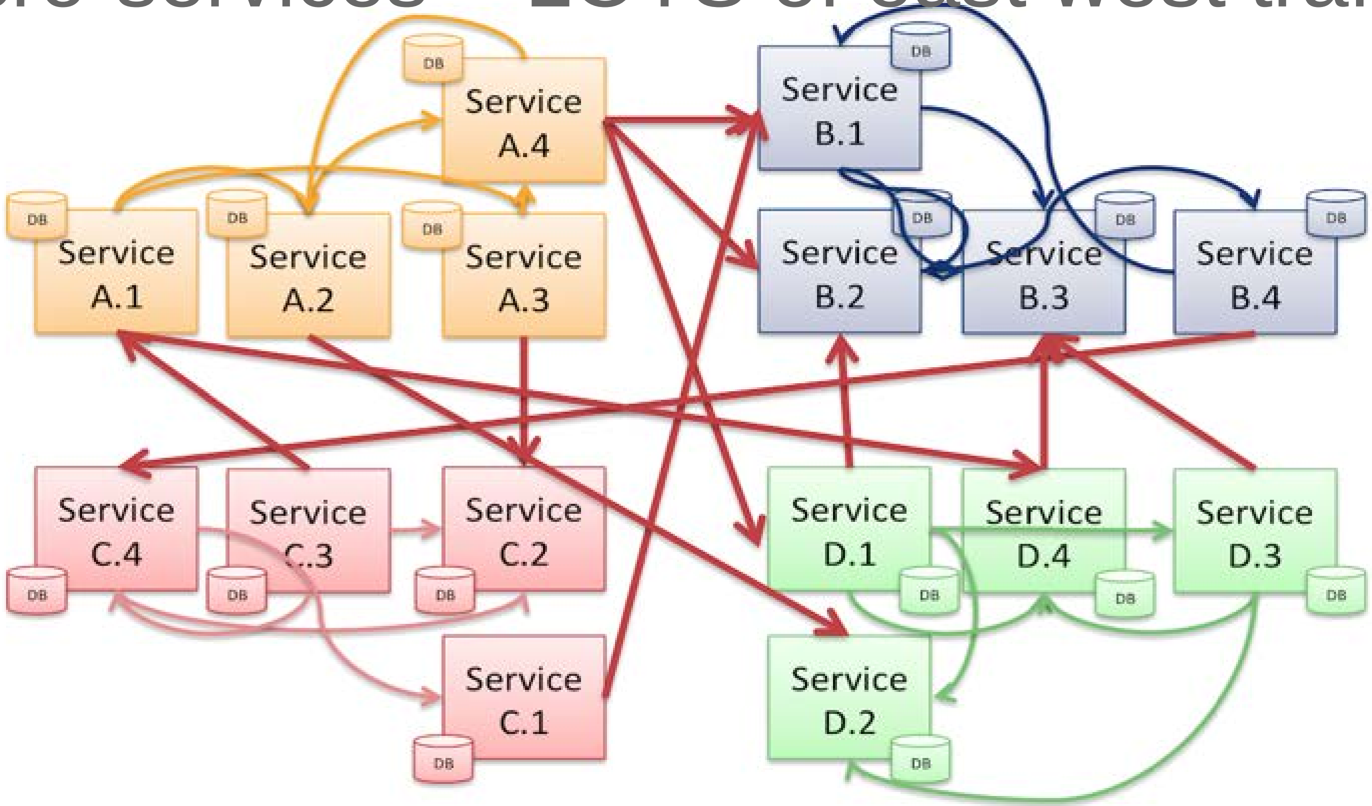
The trend of “containerizing” applications



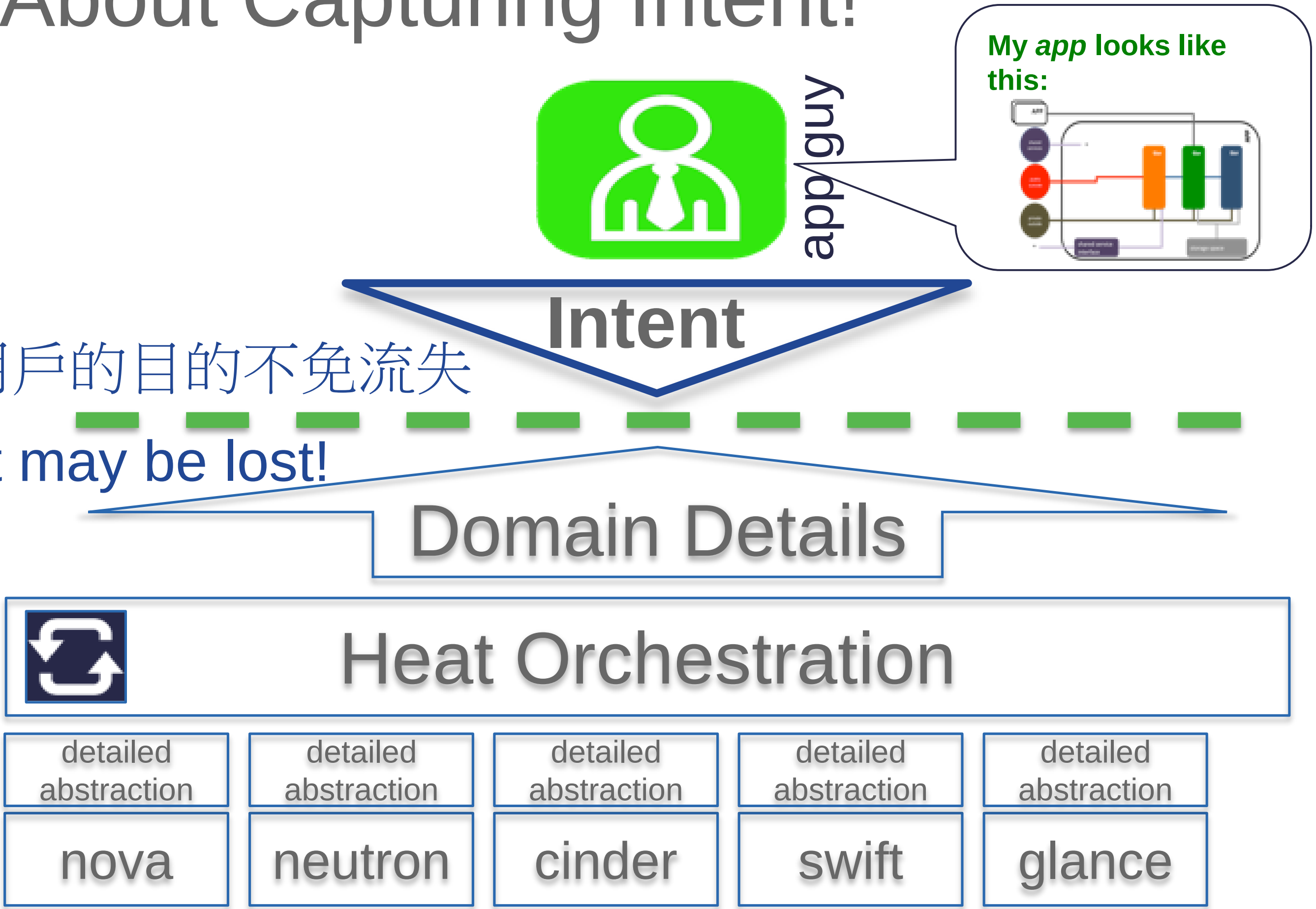
Containers are isolated but share OS and where appropriate bins/libraries



Micro-services = LOTS of east west traffic



Its All About Capturing Intent!



My *app* looks like this:

app guy

Intent

轉換過程用戶的目的不免流失

User intent may be lost!

Domain Details

Heat Orchestration

detailed abstraction	detailed abstraction	detailed abstraction	detailed abstraction	detailed abstraction
nova	neutron	cinder	swift	glance

傳統的數據中心網絡部署

網絡語言

ACL, VLAN, QOS, SVI

Network architect/engineers perform configurations on the network equipment (CLI, GUI)

翻譯

網絡分區
安全定義
負載均衡

System/Network team translates the requirements into infrastructural specifications

應用溝通需求

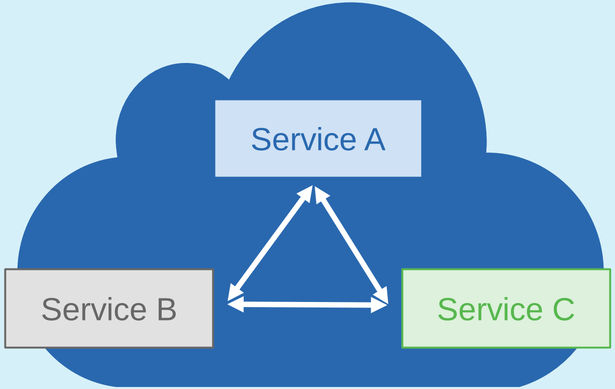
Web界面
應用程序
認證系統
数据库

Application owners provide the network requirements of application environment

應用速度慢——應用問題？網絡問題？——如何快速排错？

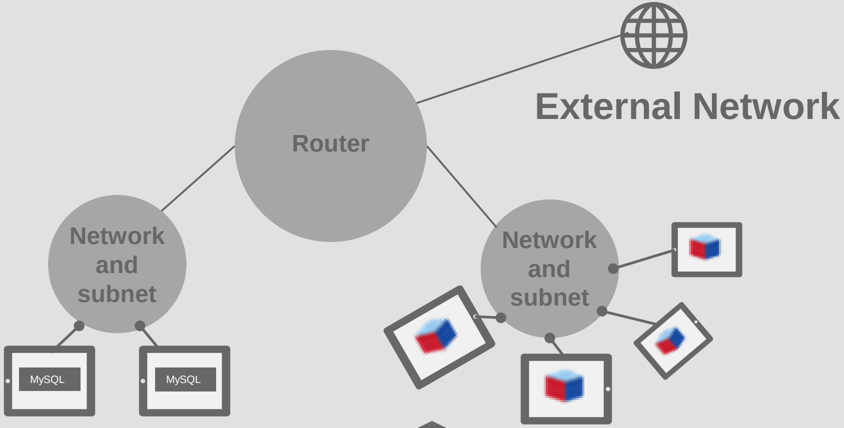
What may be further enhanced with OpenStack Networking Today?

Cloud Application Model



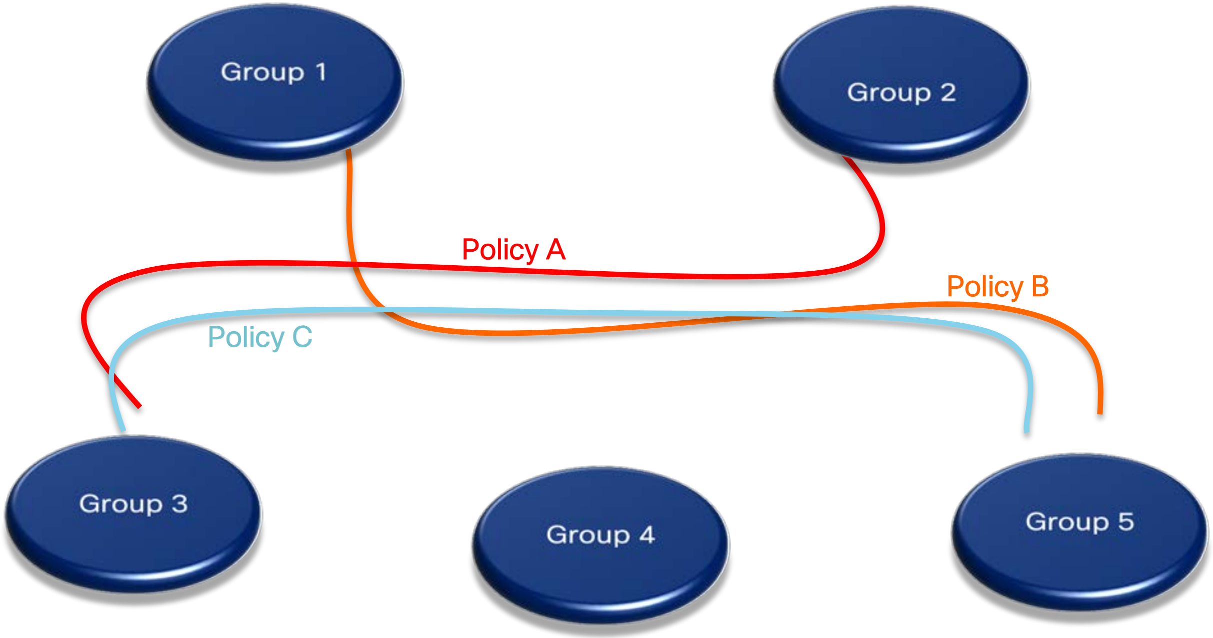
- No broadcast or multicast
- Resilient and fault tolerant
- Scalable tiers
- Built around loosely coupled services
- Does not care about IP addresses

Neutron Model



- Layer 2 and broadcast is the base API
- Network, routers, and subnets
- Based on existing networking models
- No concept of dependency mapping or intent

What we need is a policy-based networking model

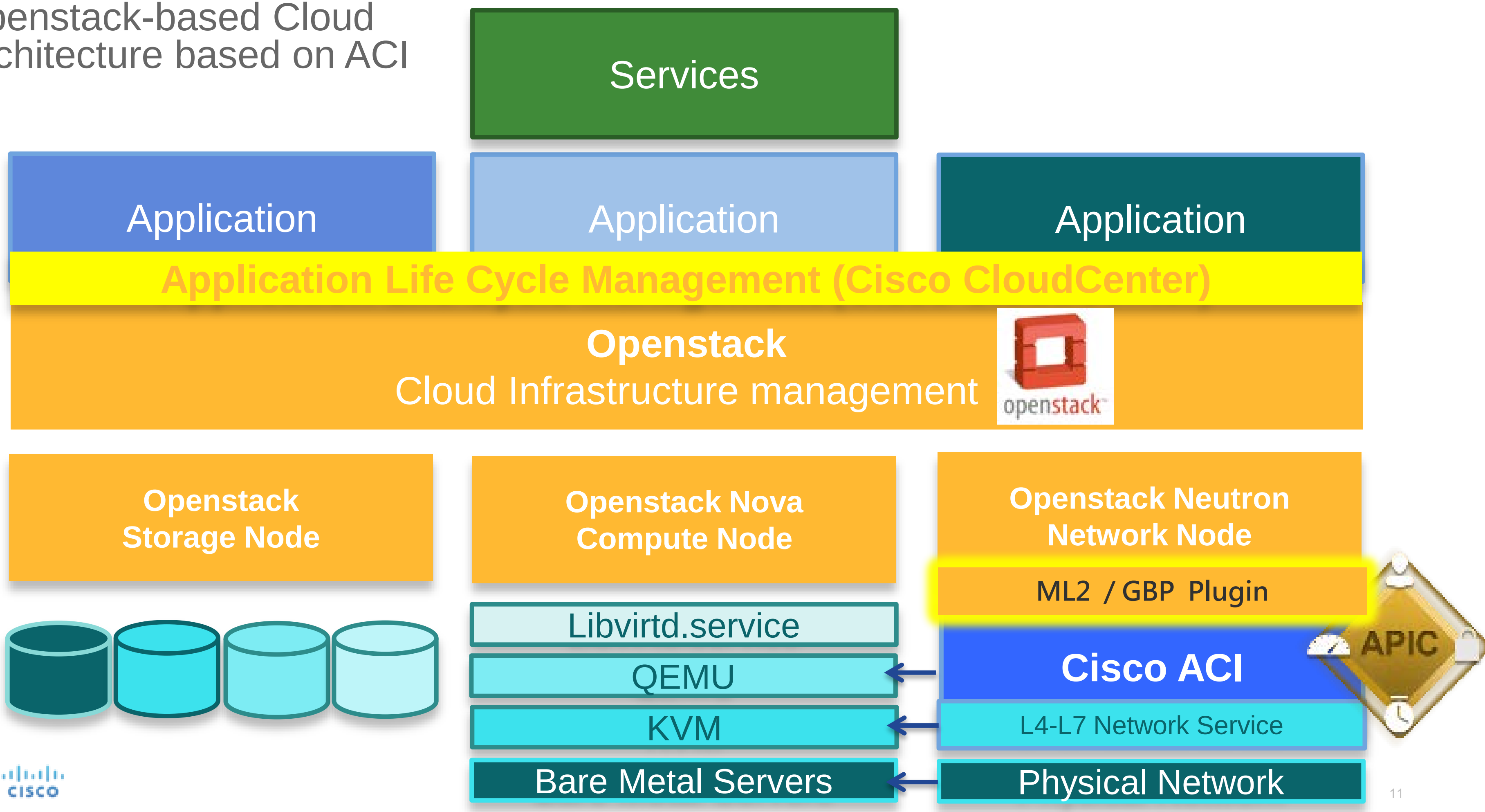


App A
Group 2,3,5
Policy A
Policy C

App B
Group 1,5
Policy B

Applications are defined by policies governing groups' interaction

Openstack-based Cloud Architecture based on ACI



Services

Application

Application

Application

Application Life Cycle Management (Cisco CloudCenter)

Openstack

Cloud Infrastructure management

openstack

Openstack Storage Node

Openstack Nova Compute Node

Openstack Neutron Network Node

ML2 / GBP Plugin

Libvirtd.service

QEMU

KVM

Bare Metal Servers

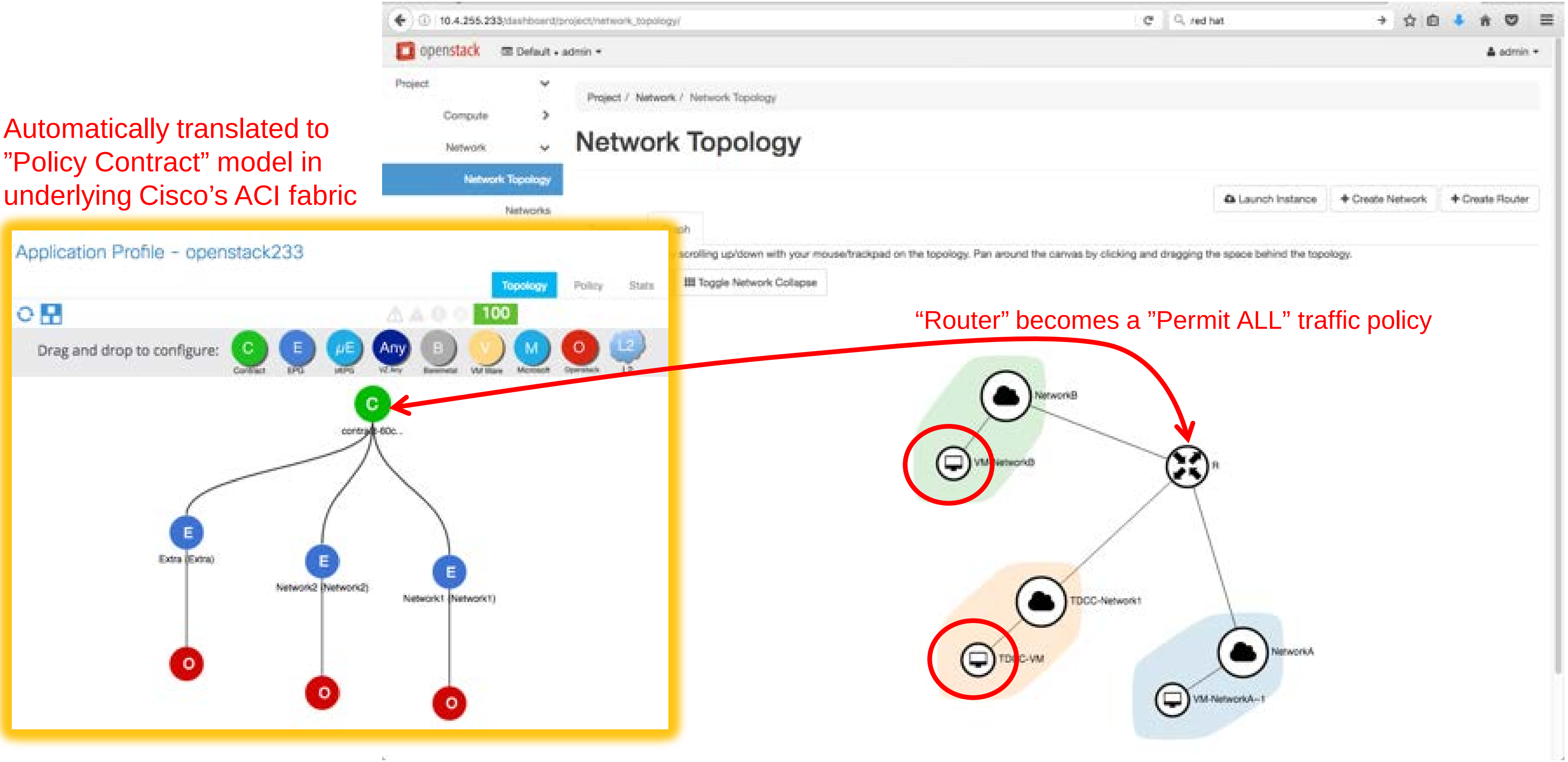
Cisco ACI

APIC

L4-L7 Network Service

Physical Network

ML2 – Traditional Networking Model



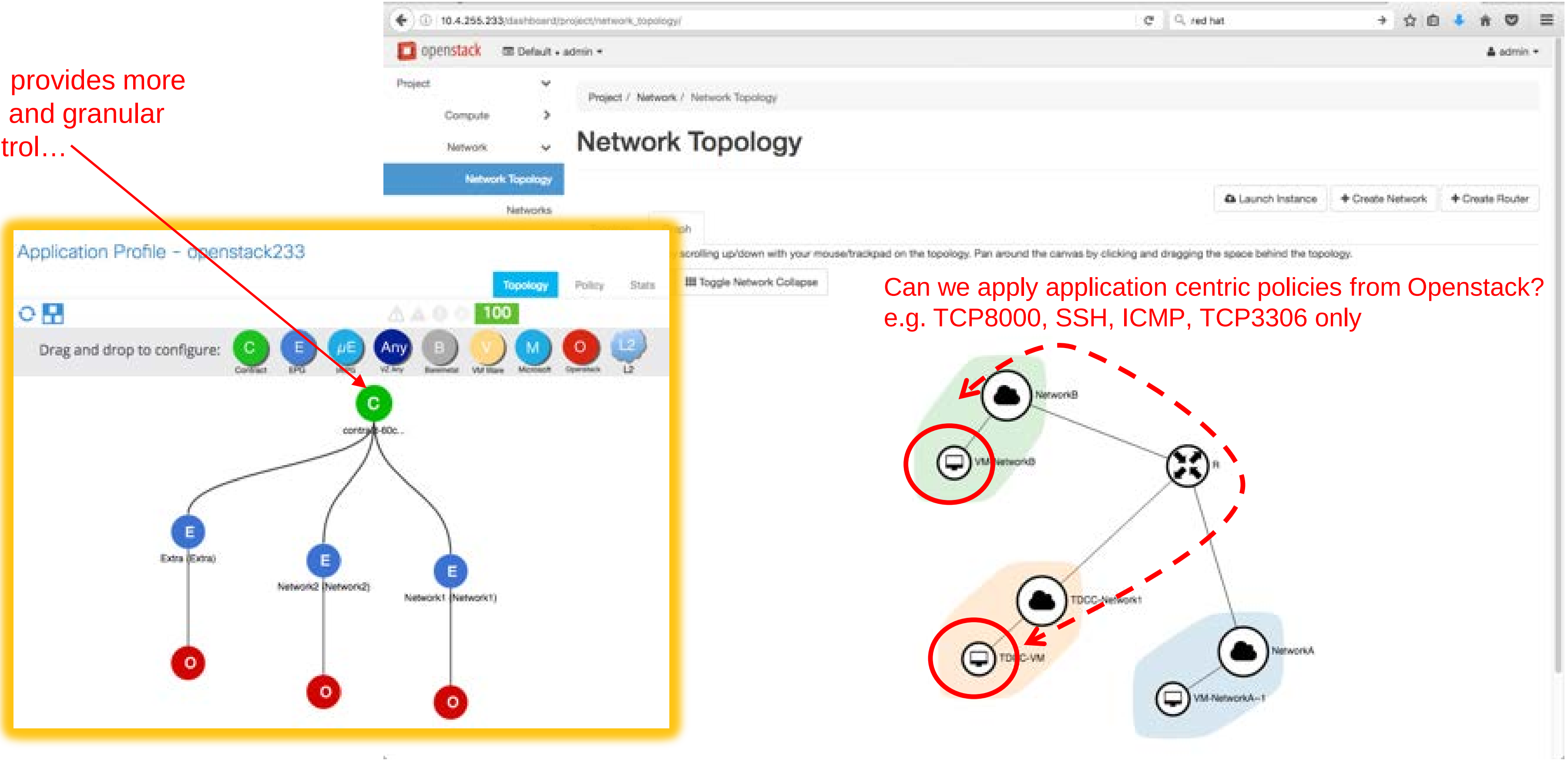
Automatically translated to ”Policy Contract” model in underlying Cisco’s ACI fabric

“Router” becomes a ”Permit ALL” traffic policy

...scrolling up/down with your mouse/trackpad on the topology. Pan around the canvas by clicking and dragging the space behind the topology.

ML2 – Traditional Networking Model

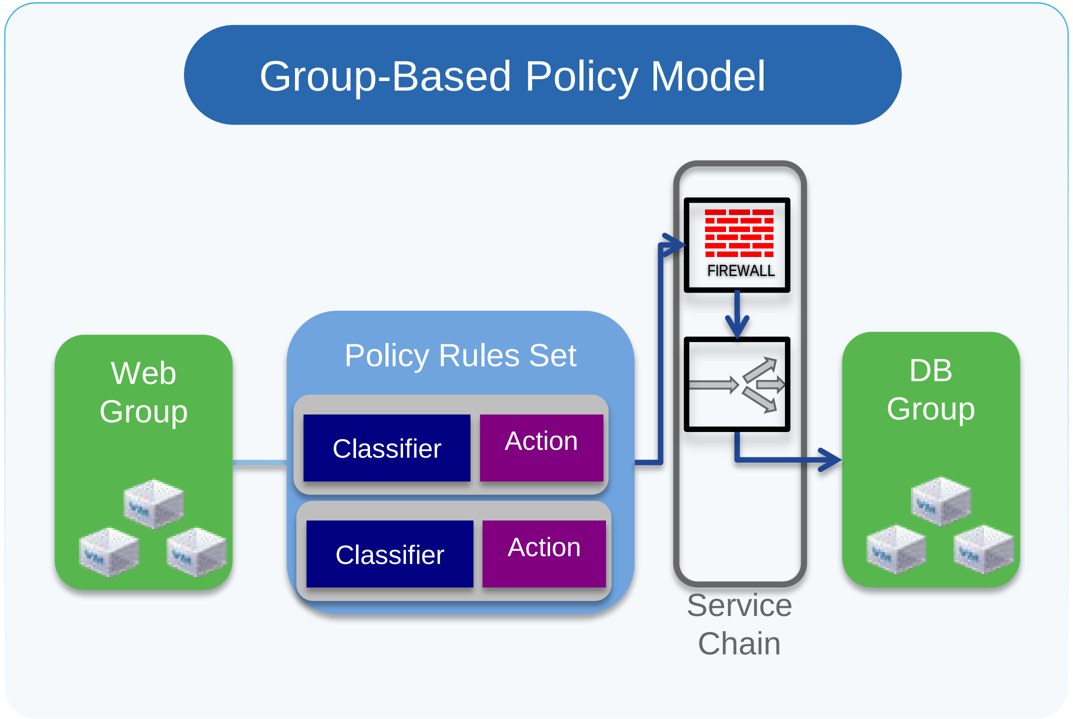
ACI provides more fine and granular control…



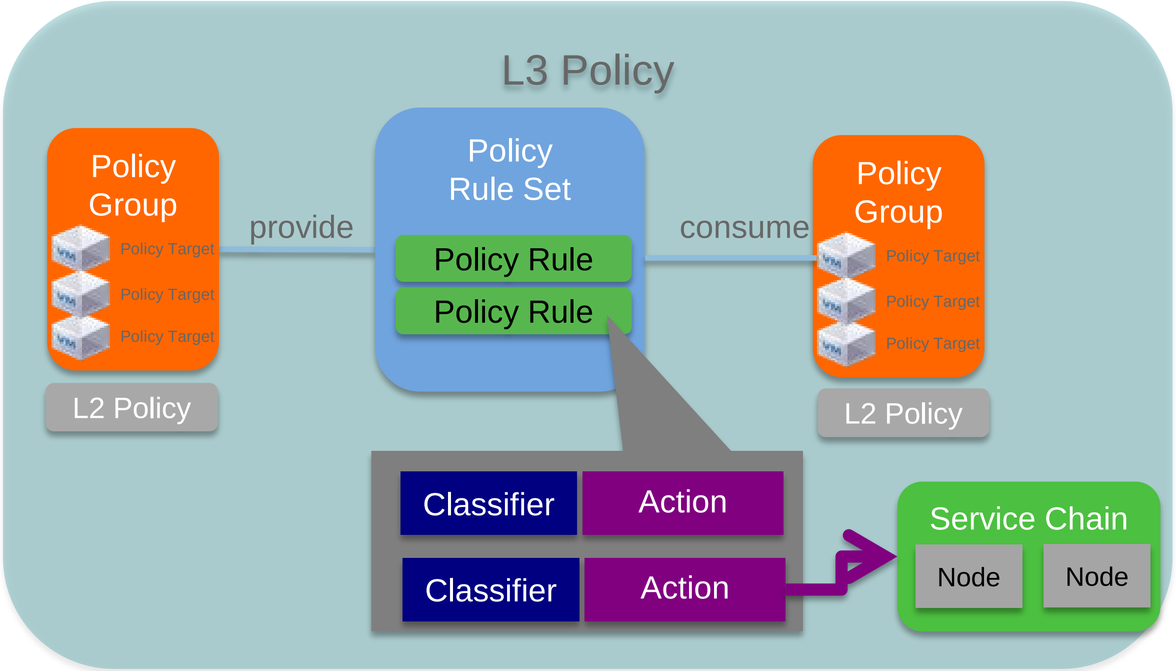
Can we apply application centric policies from Openstack?
e.g. TCP8000, SSH, ICMP, TCP3306 only

Group-Based Policy for OpenStack

- A 100% open source, Apache-licensed
- Interface for capturing application intent, including network service requirements
- Model inspired by APIC but available for any hardware / software platform
- Networking today, plans to cover compute, storage
- Growing number of contributors and ecosystem partners



Group-Based Policy Model



Policy Group: Set of endpoints with the same properties. Often a tier of an application.

Policy RuleSet: Set of Classifier / Actions describing how Policy Groups communicate.

Policy Classifier: Traffic filter including protocol, port and direction.

Policy Action: Behavior to take as a result of a match. Supported actions include “allow” and “redirect”

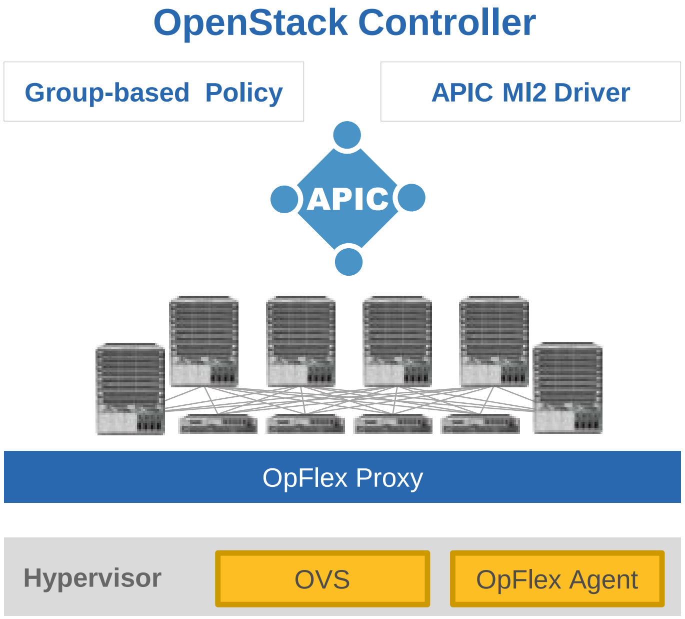
Service Chains: Set of ordered network services between Groups.

L2 Policy: Specifies the boundaries of a switching domain. Broadcast is an optional parameter

L3 Policy: An isolated address space containing L2 Policies / Subnets

ACI + OpenStack – With OpFlex Support

Full Policy Based Network Automation Extended to the Linux Hypervisor



OpFlex for OVS

- Open Source OpFlex agent extends ACI into Linux hypervisor
- OpFlex Proxy exposes new open API in ACI fabric

OpenStack Feature Highlights

- Fully distributed Neutron network functions, including NAT
- Integrated, centrally managed overlay and underlay fabric
- Operational visibility integrating OpenStack, Linux, and APIC
- Choice of virtual network (standard Neutron ML2) or Group-based Policy driven networking

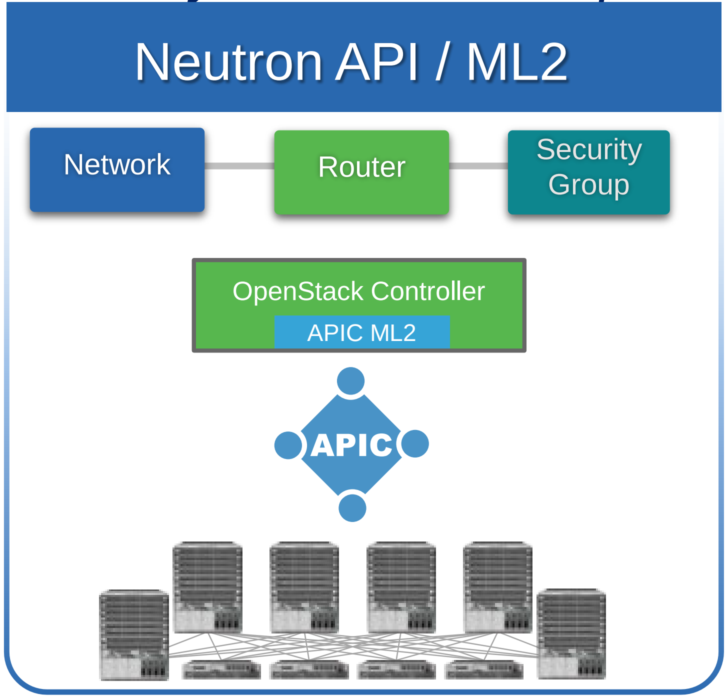
Available Now!

Solutions with Major OpenStack Distributions

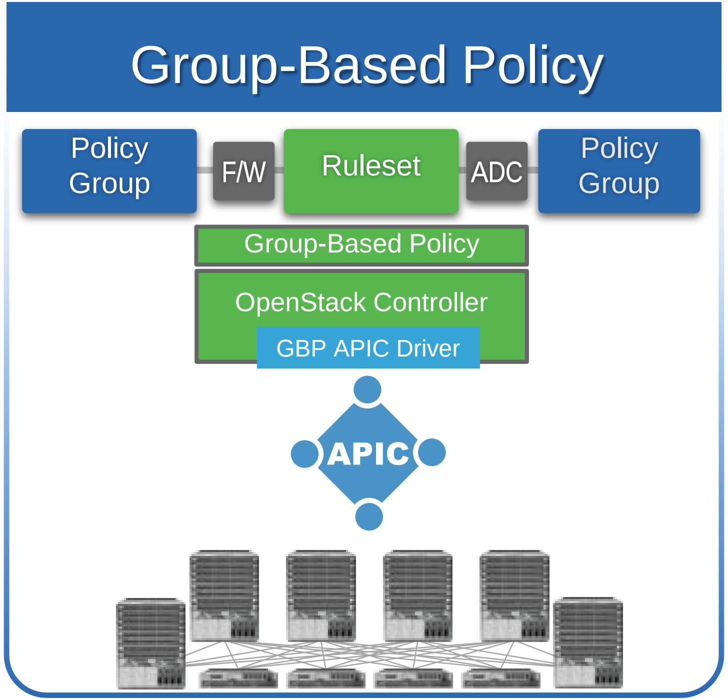
redhat CANONICAL MIRANTIS

Two OpenStack Plugin Options

Previously an "Either-Or" option; NOW with Unified Mode for BOTH



Plugin performs conversion from Neutron to APIC policy model



Group-Based Policy native drivers interfaces directly with APIC policy model

*** Only one model is supported in a given OpenStack deployment**

Benefits of OpenStack on ACI

Distributed, Scalable Virtual Networking

- Fully distributed L2, anycast gateway, DHCP, metadata
- Distributed NAT / Floating IP
- Choice of Group Policy or Neutron API

Hardware Performance

- Automatic VXLAN tunnels at top-of-rack
- No wasted CPU cycles for tunneling

Operations and Telemetry

- Troubleshooting across physical and virtual environments
- Health scores, atomic counters, capacity planning per tenant network

Integrated Overlay and Underlay

- Fully managed underlay network through APIC controller
- Ability to connect physical servers and multiple hypervisors to overlay networks

Service Chaining

- Support for L3 or L2 service insertion and chaining
- Device package ecosystem for 3rd party devices or Group-Based Policy service chaining

Secure Multi-tenancy

- Virtual network isolation is maintained even when a hypervisor is compromised

cisco

TOMORROW starts here.

cisco

思科 LINE@ & FB 好康雙重享

加入思科LINE & FB按個讚，科技趣味多

請掃描我
當個 LINE 友吧

LINE @cisco.tw

思科台灣 Facebook 按個 👍

思科台灣

歡迎成為【數位轉型馬拉松】一份子，

讓我們一起向成功邁進！

好友限定

1. 專屬活動
2. 科技時事一把抓
3. 好康不斷線

CISCO

SuperCloud

思科超級雲客戶體驗中心

數位轉型新視野

零距離的專家互動，實機情境模擬

限額體驗
立即申請

立即申請