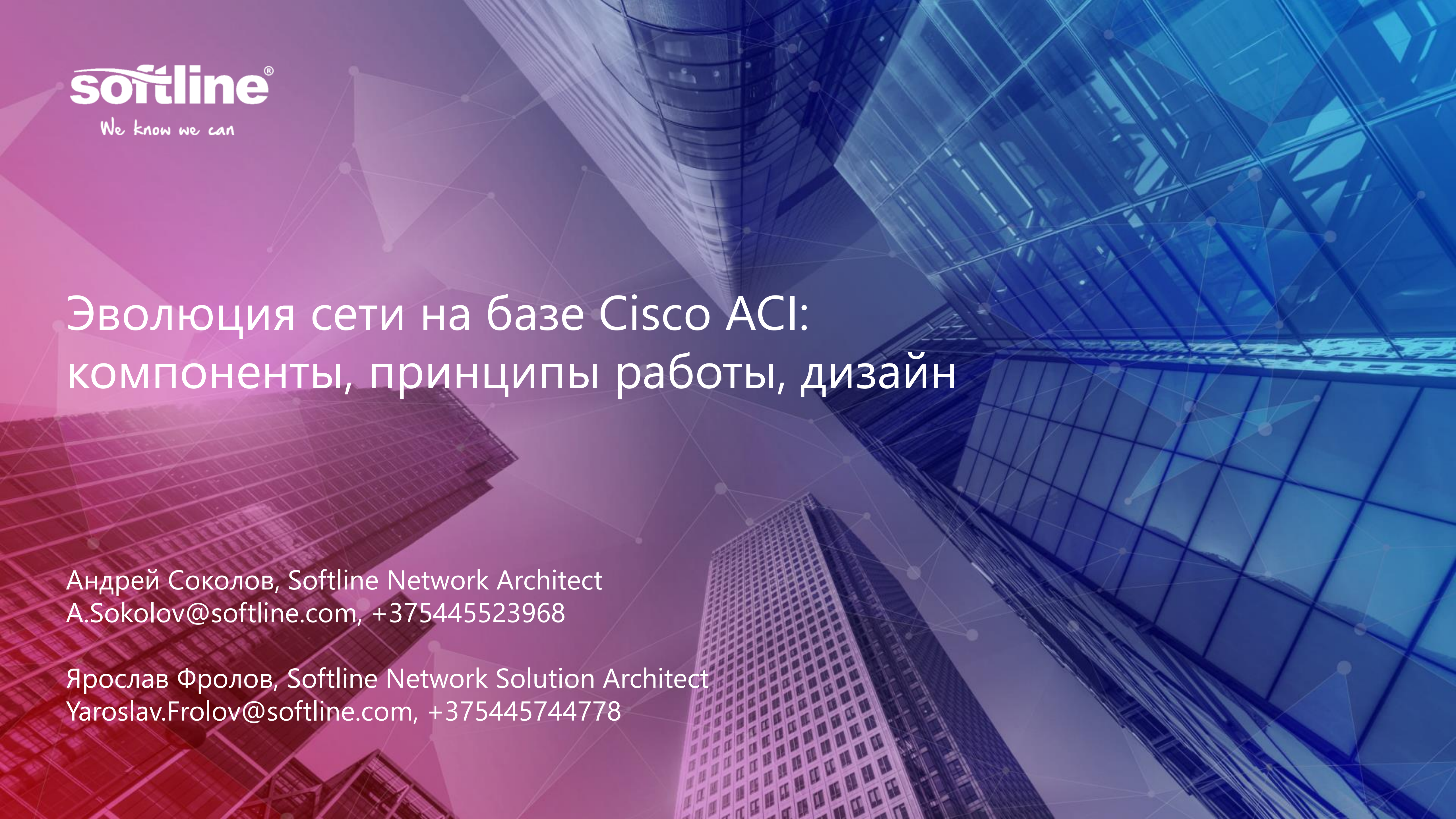


softline®

We know we can

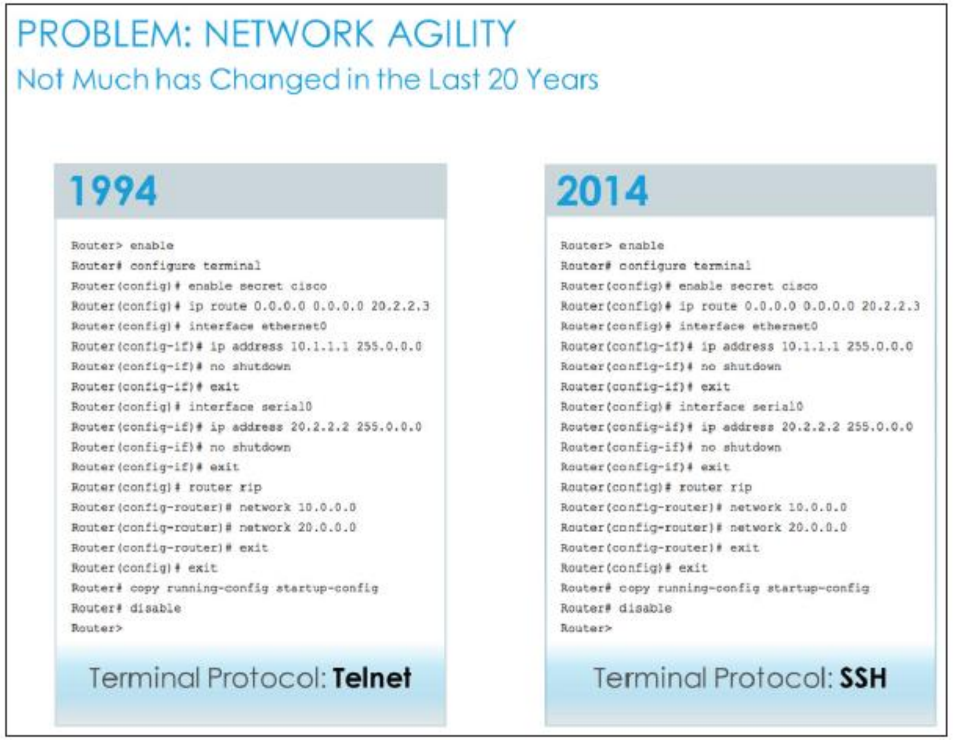
Эволюция сети на базе Cisco ACI: компоненты, принципы работы, дизайн

Андрей Соколов, Softline Network Architect
A.Sokolov@softline.com, +375445523968

Ярослав Фролов, Softline Network Solution Architect
Yaroslav.Frolov@softline.com, +375445744778

SDN Architecture

- Software defined networking (SDN) is a network architecture that has been developed to virtualize the network. SDN can virtualize the control plane. SDN moves the control plane from each network device to a central network intelligence and policy-making entity called the SDN controller.



PROBLEM: NETWORK AGILITY

Not Much has Changed in the Last 20 Years

1994

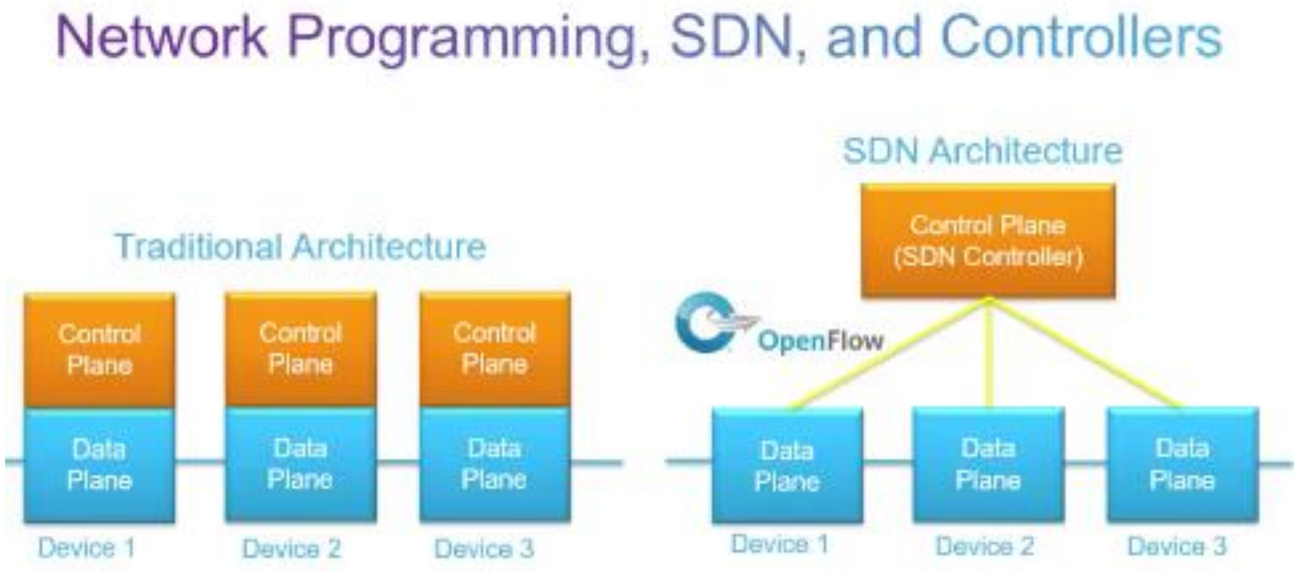
```
Router> enable
Router# configure terminal
Router(config)# enable secret cisco
Router(config)# ip route 0.0.0.0 0.0.0.0 20.2.2.3
Router(config)# interface ethernet0
Router(config-if)# ip address 10.1.1.1 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface serial0
Router(config-if)# ip address 20.2.2.2 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# network 20.0.0.0
Router(config-router)# exit
Router(config)# exit
Router# copy running-config startup-config
Router# disable
Router>
```

Terminal Protocol: **Telnet**

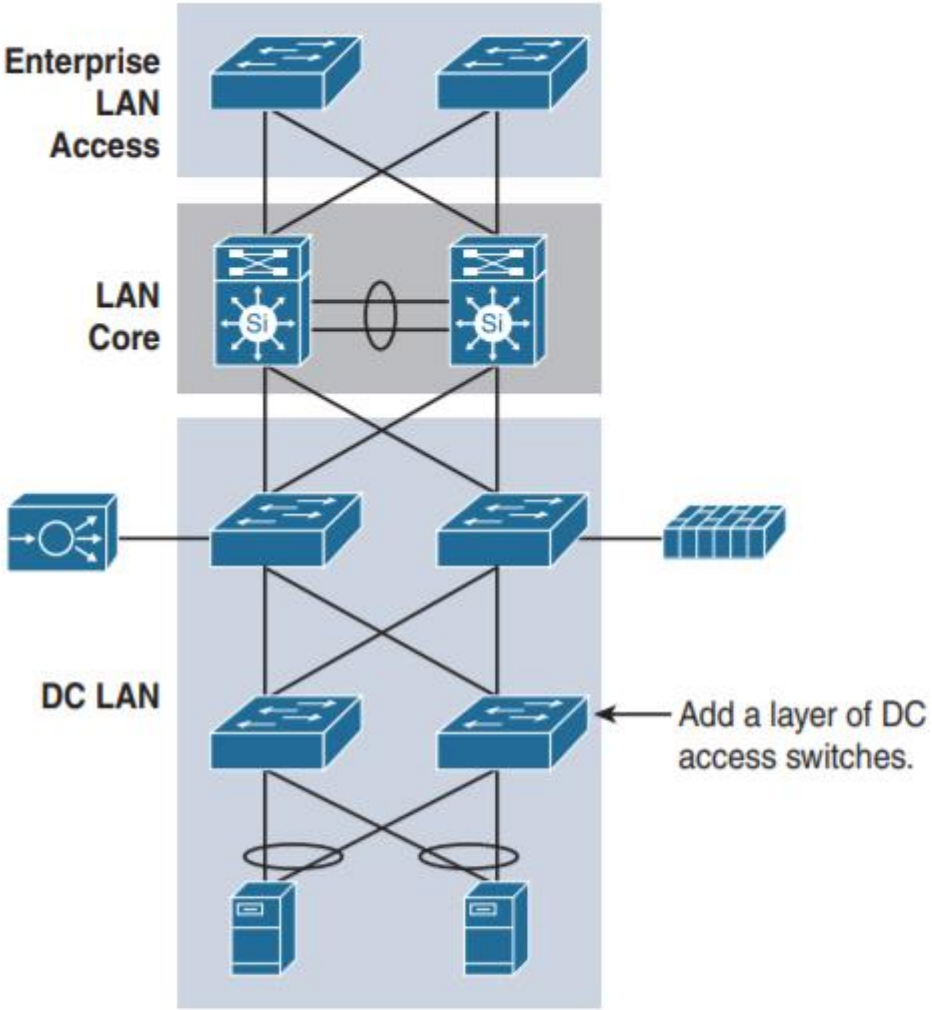
2014

```
Router> enable
Router# configure terminal
Router(config)# enable secret cisco
Router(config)# ip route 0.0.0.0 0.0.0.0 20.2.2.3
Router(config)# interface ethernet0
Router(config-if)# ip address 10.1.1.1 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface serial0
Router(config-if)# ip address 20.2.2.2 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# network 20.0.0.0
Router(config-router)# exit
Router(config)# exit
Router# copy running-config startup-config
Router# disable
Router>
```

Terminal Protocol: **SSH**



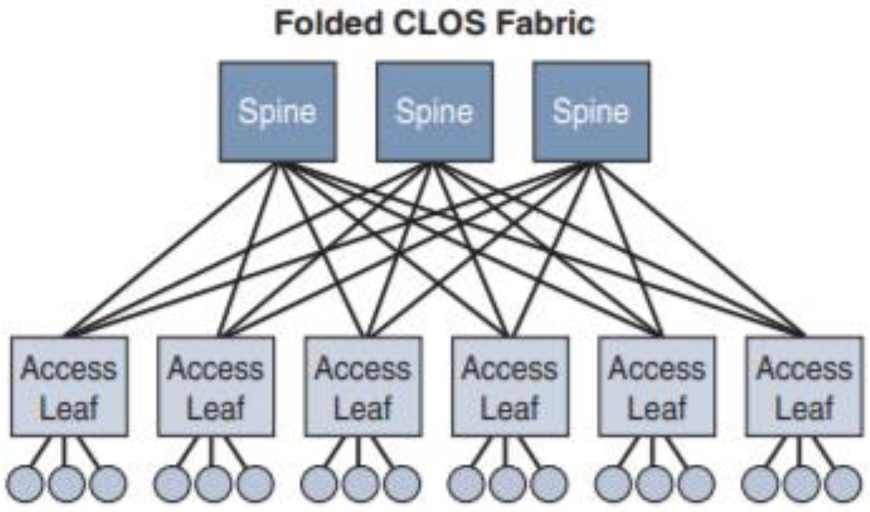
Three-Tier Data Center Network Architecture



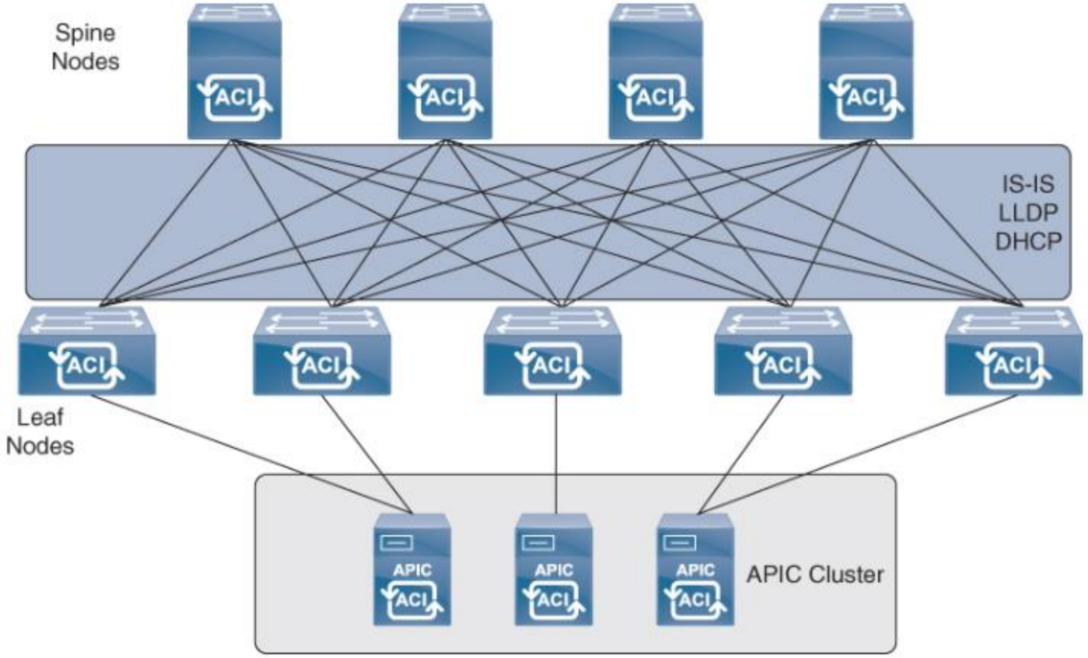
- The access layer increases the number of available ports, but more important, it reduces the number of required cables. Servers are now connected to the nearest access switch.
- The access switches are connected northbound to aggregation switches with a pair of copper or optical cables.
- The aggregation switches are also connected in the same manner to core switches, but with this architecture, the data center can have multiple pairs of aggregation switches connected to a pair of core switches to support large-scale data center networks.
- With this architecture, the services and appliances are connected to the aggregation switches.

Spine-Leaf Data Center Design

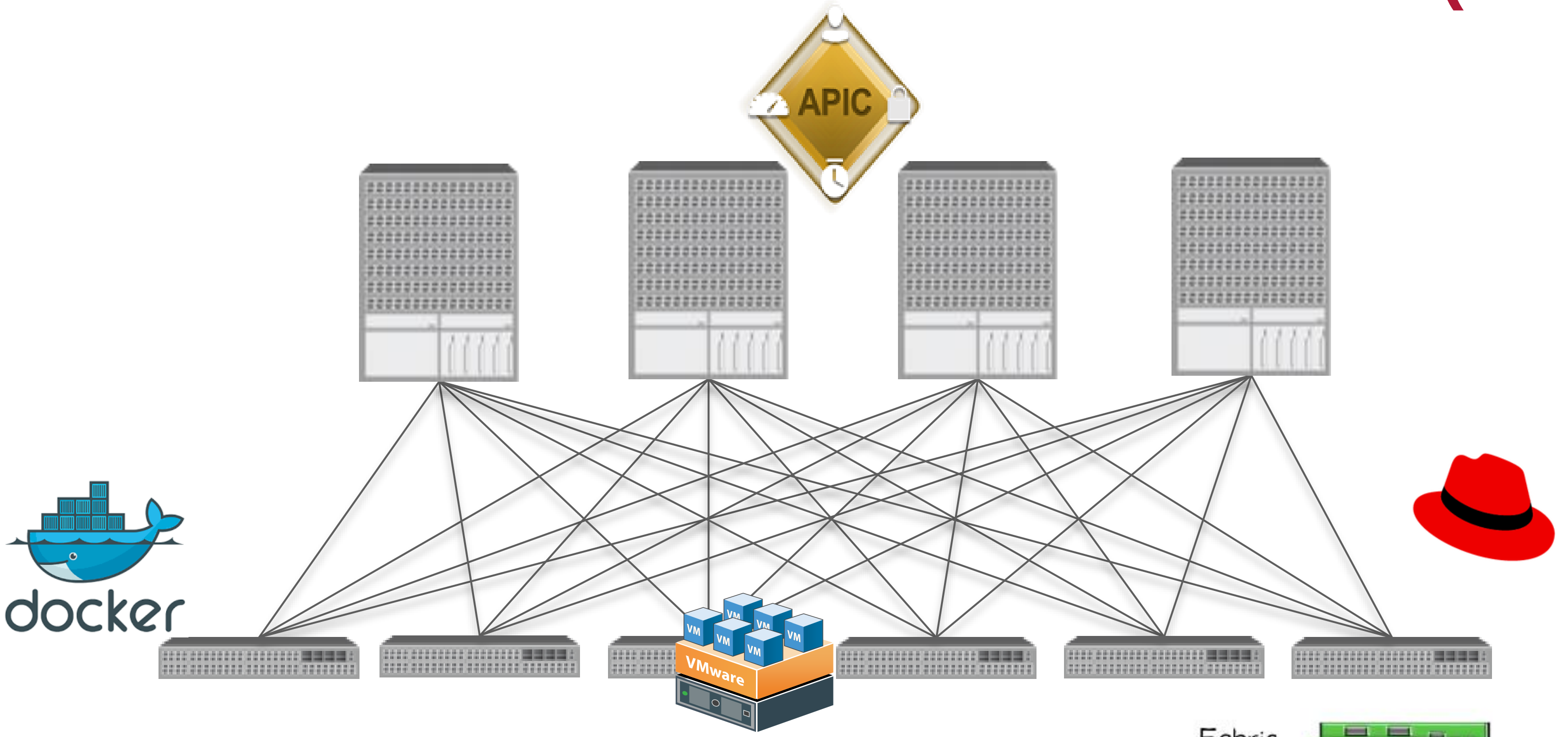
Traditional CLOS DC

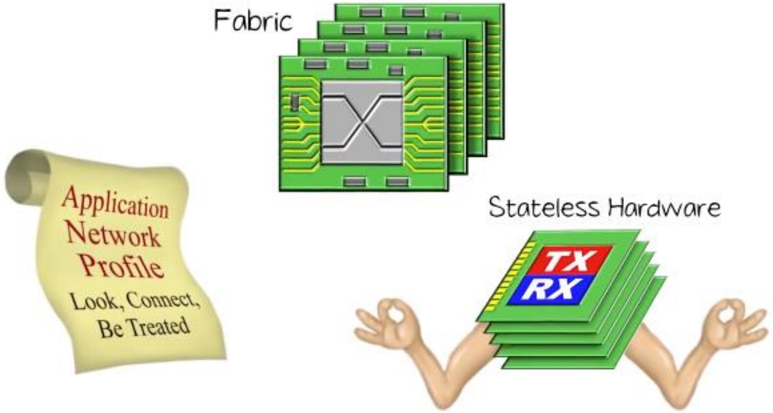


Cisco ACI Fabric



CISCO APPLICATION CENTRIC INFRASTRUCTURE (ACI) OVERVIEW

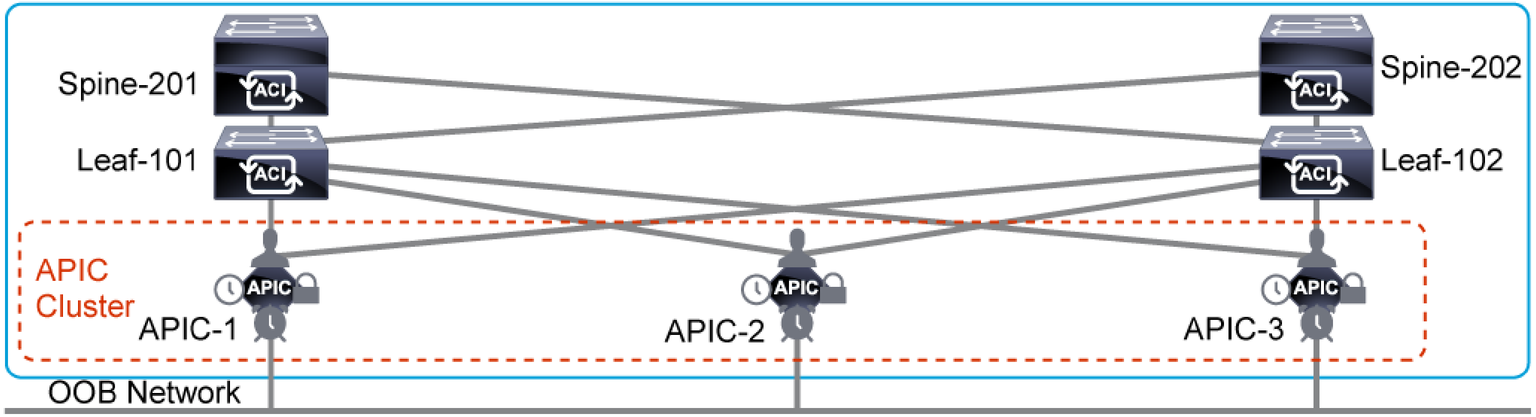


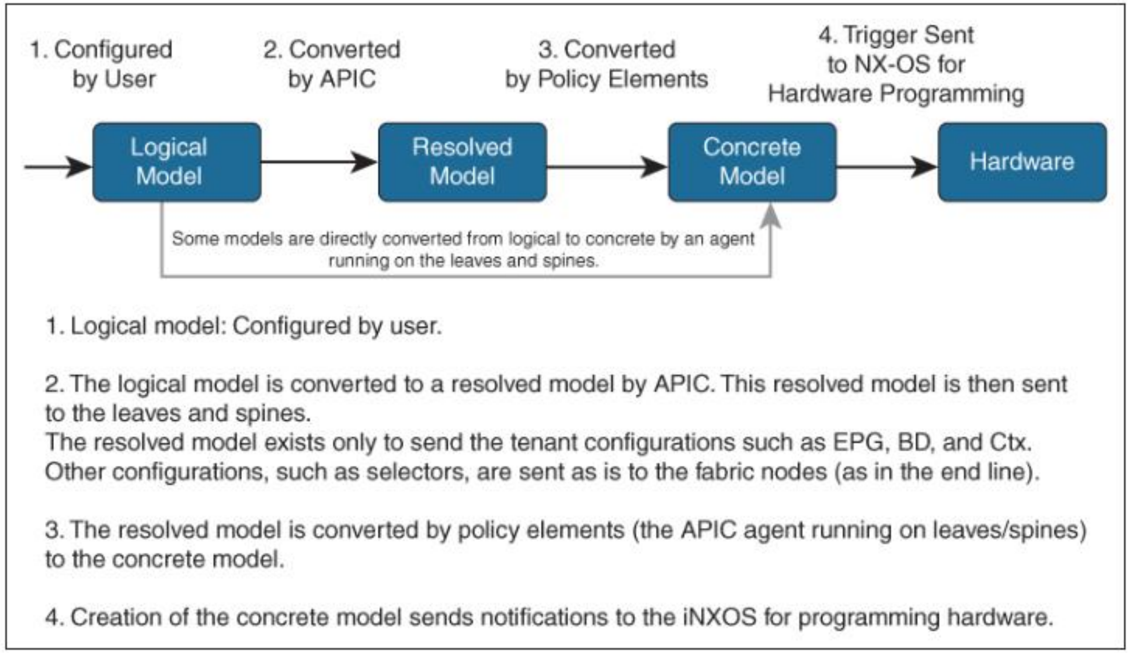


Cisco ACI benefits include the following:

- Centralized policy-defined automation management
- Real-time visibility and application health score
- Open and comprehensive end-to-end security

Cisco Application Policy Infrastructure Controller





Some models are directly converted from logical to concrete by an agent running on the leaves and spines.

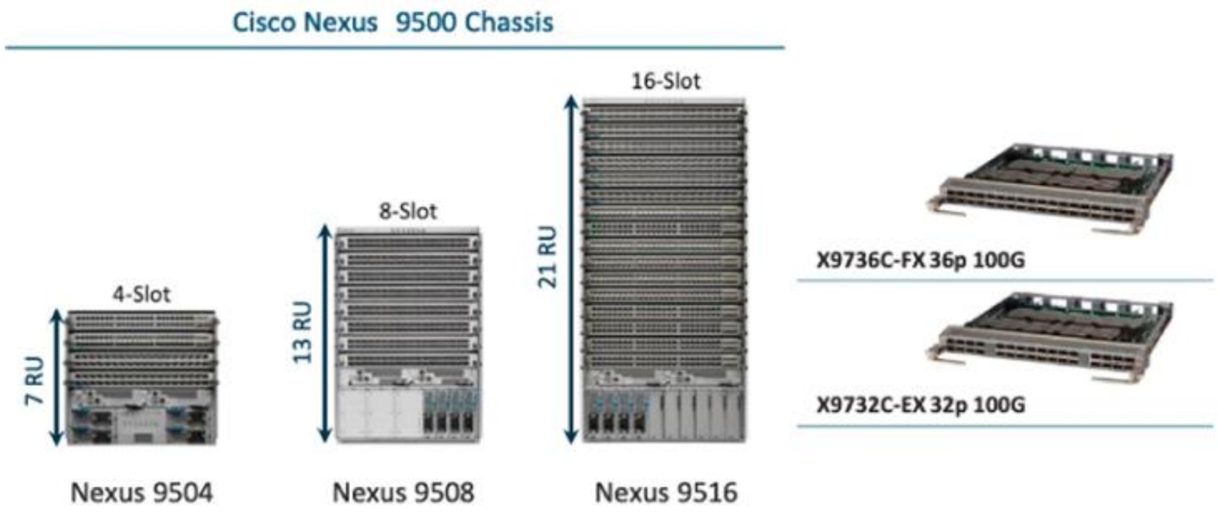
1. Logical model: Configured by user.

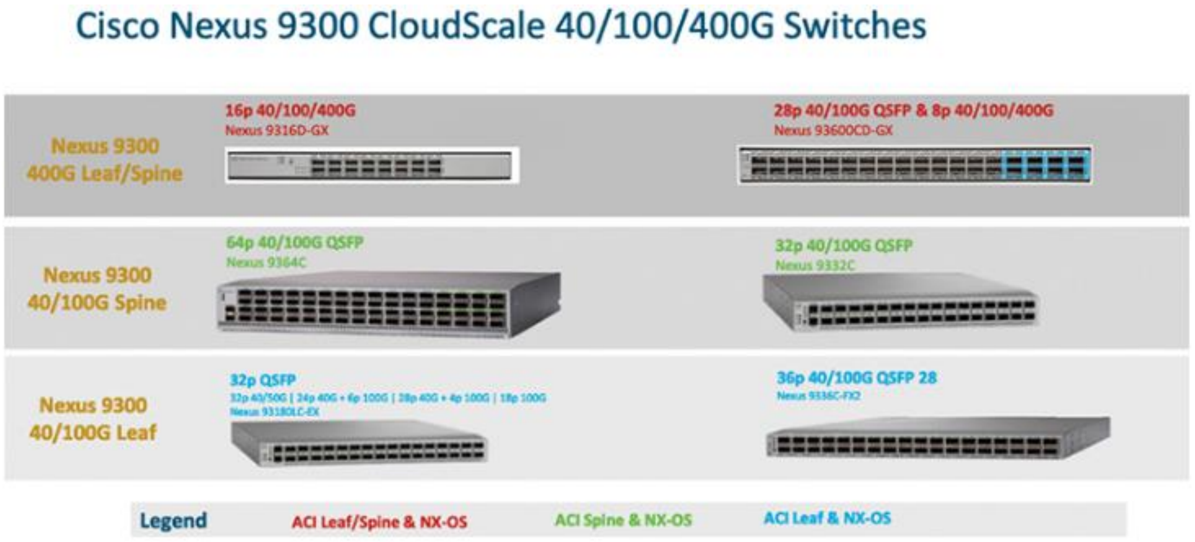
2. The logical model is converted to a resolved model by APIC. This resolved model is then sent to the leaves and spines.
The resolved model exists only to send the tenant configurations such as EPG, BD, and Ctx.
Other configurations, such as selectors, are sent as is to the fabric nodes (as in the end line).

3. The resolved model is converted by policy elements (the APIC agent running on leaves/spines) to the concrete model.

4. Creation of the concrete model sends notifications to the iNXOS for programming hardware.

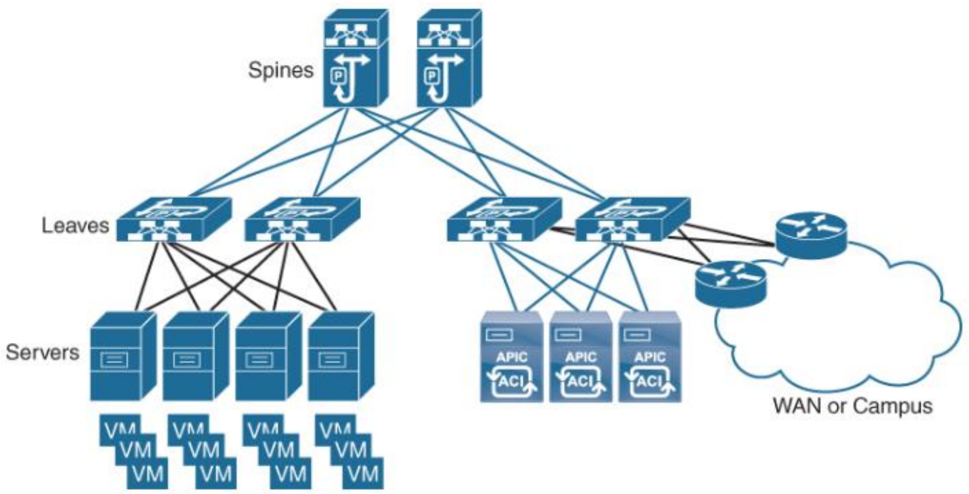
Cisco Nexus 9000 Series Spine and Leaf Switches for Cisco ACI



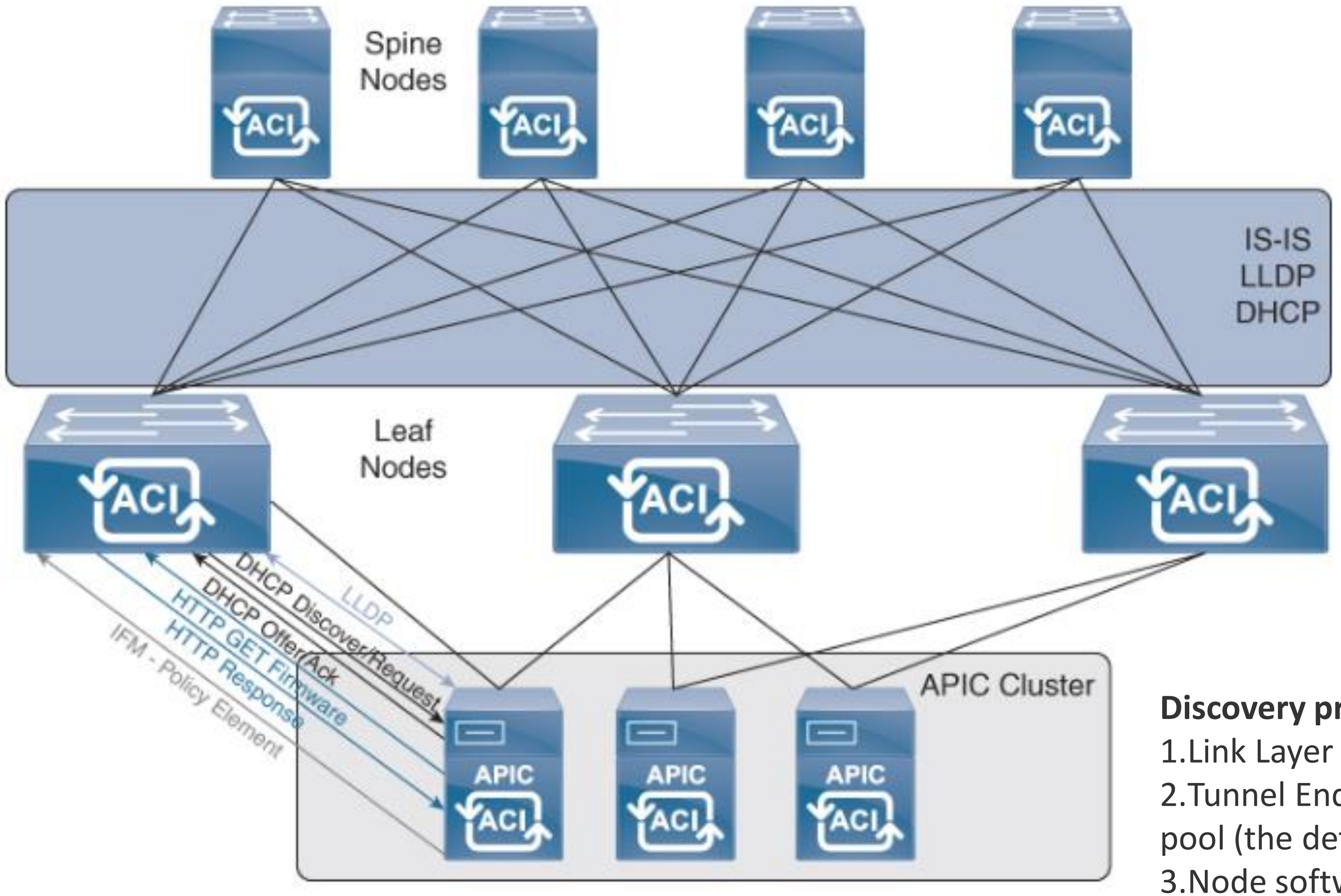


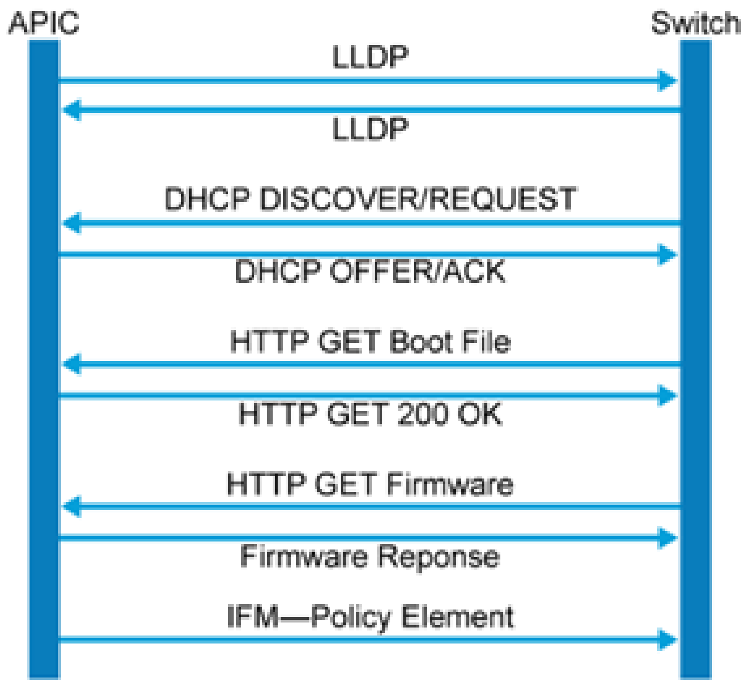
Cisco Nexus 9000 product family consists of:

- Cisco Nexus 9500 Series modular chassis
  - 4 slot, 8 slot, 16 slot
- Cisco Nexus 9300 Series ToR and spine switches
  - Cisco ACI spine and leaf varieties
- Cisco Nexus 9500 Series line cards
  - Cisco Nexus 9700 Series for Cisco ACI spine
  - Cisco Nexus 9500 Series for Cisco ACI leaf
- Cisco Nexus 9600 and 9400 Series line cards not for Cisco ACI



Cisco ACI Initial Setup & Discovery





Discovery process:

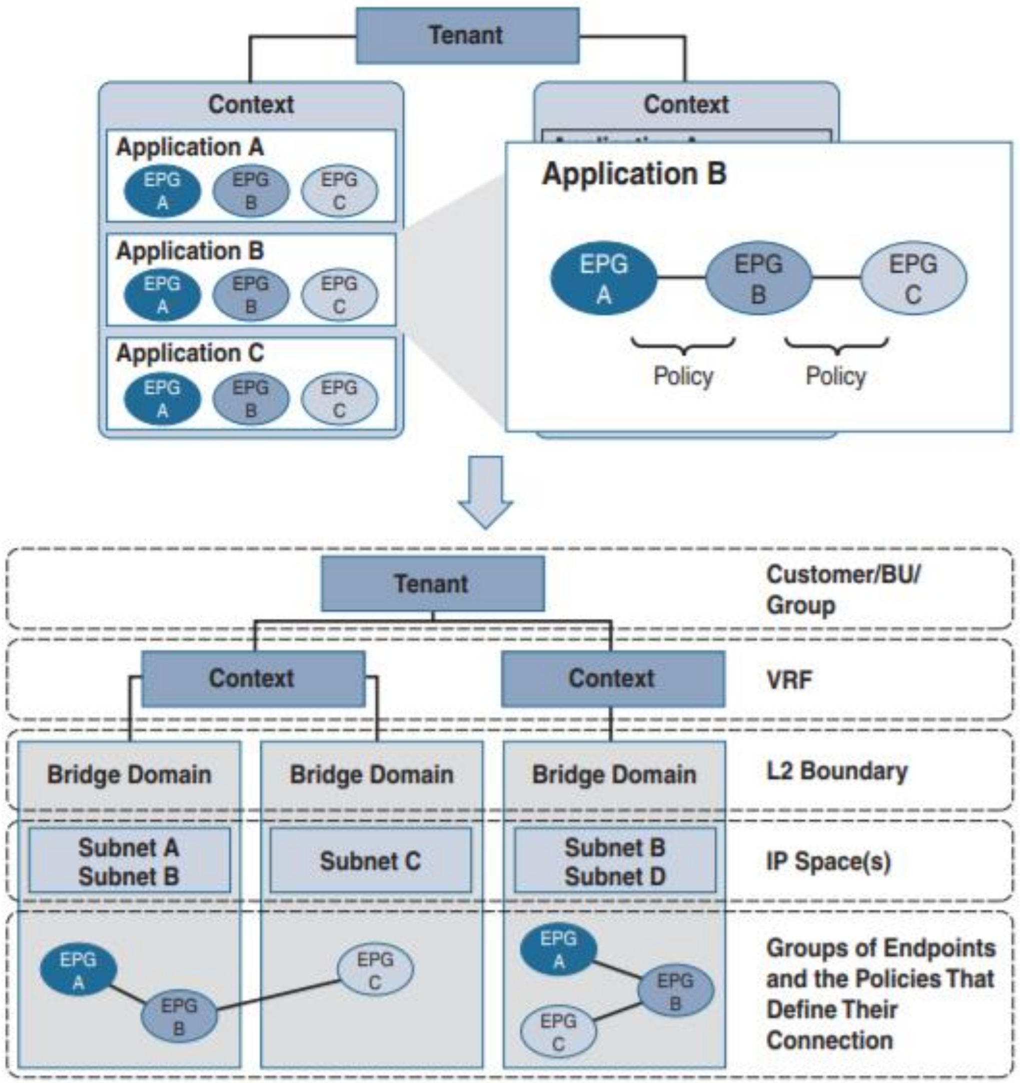
1.Link Layer Discovery Protocol (LLDP) Neighbor Discovery

2.Tunnel End Point (TEP) IP address assignment to the node from the TEP address pool (the default TEP pool is 10.0.0.0/16)

3.Node software upgraded if necessary, downloading the new software from APIC repository

4.Policy Element IFM setup

Cisco ACI Policy model



Tenant

Context

Application A

EPG A

EPG B

EPG C

Application B

EPG A

EPG B

EPG C

Application C

EPG A

EPG B

EPG C

Context

Application B

EPG A

EPG B

EPG C

Policy

Policy

Tenant

Customer/BU/ Group

Context

Context

VRF

Bridge Domain

Bridge Domain

Bridge Domain

L2 Boundary

Subnet A Subnet B

Subnet C

Subnet B Subnet D

IP Space(s)

EPG A

EPG B

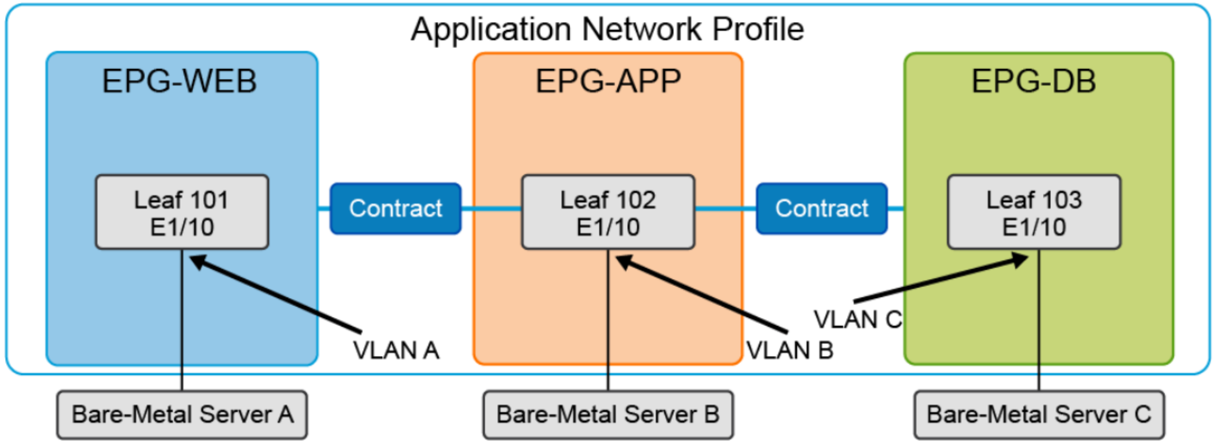
EPG C

EPG A

EPG B

EPG C

Groups of Endpoints and the Policies That Define Their Connection



Application Network Profile

EPG-WEB

EPG-APP

EPG-DB

Leaf 101 E1/10

Contract

Leaf 102 E1/10

Contract

Leaf 103 E1/10

VLAN A

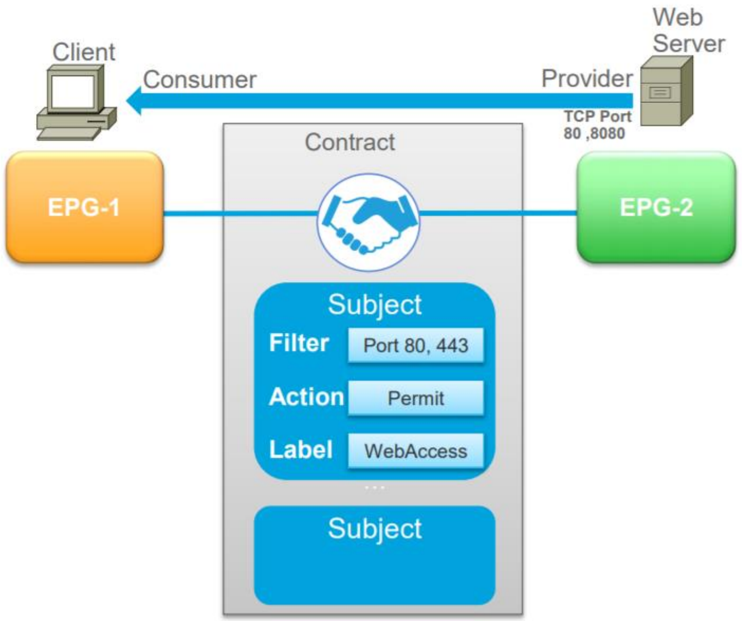
VLAN B

VLAN C

Bare-Metal Server A

Bare-Metal Server B

Bare-Metal Server C



Client

Consumer

Web Server

Provider

TCP Port 80 ,8080

Contract

EPG-1

EPG-2

Subject

Filter Port 80, 443

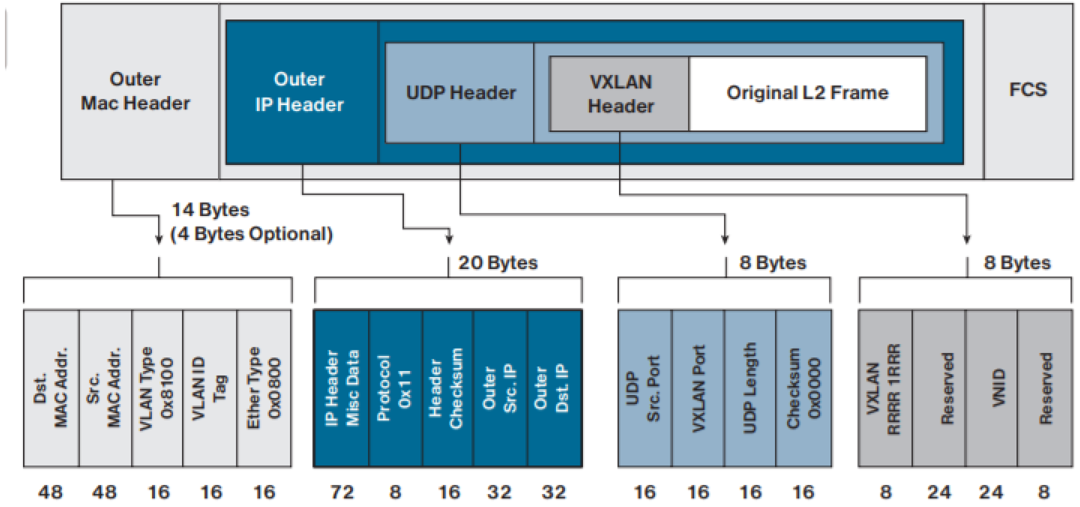
Action Permit

Label WebAccess

Subject

ACI VXLAN

Traditional VXLAN encapsulation



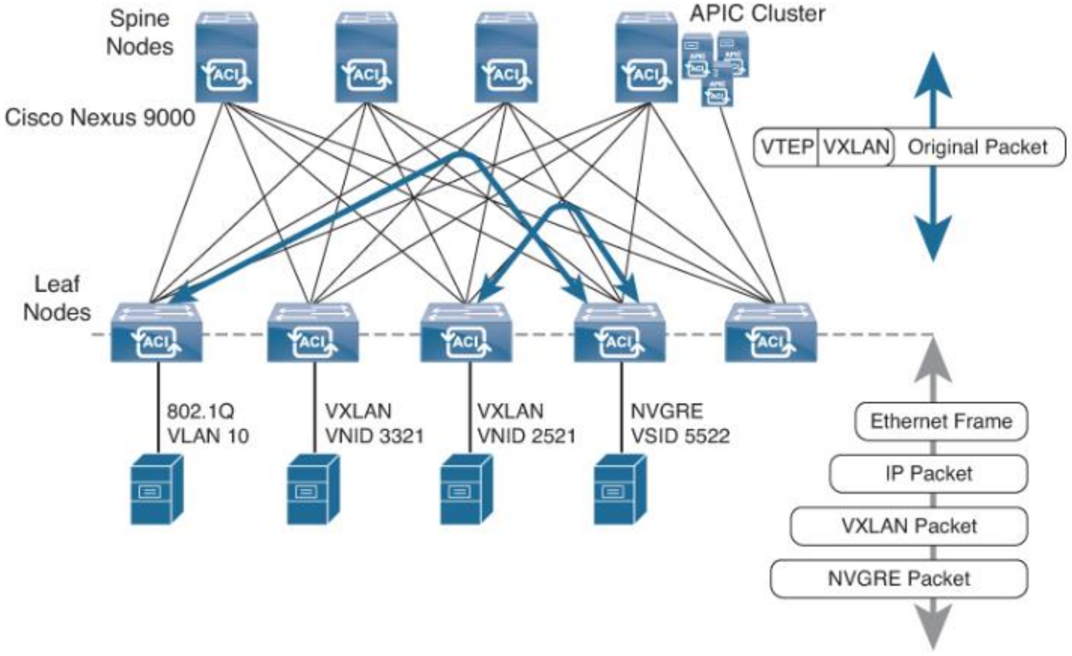
Dst. MAC Addr.	Src. MAC Addr.	VLAN Type 0x8100	VLAN ID Tag	Ether Type 0x0800
48	48	16	16	16

IP Header Misc Data	Protocol 0x11	Header Checksum	Outer Src. IP	Outer Dst. IP
72	8	16	32	32

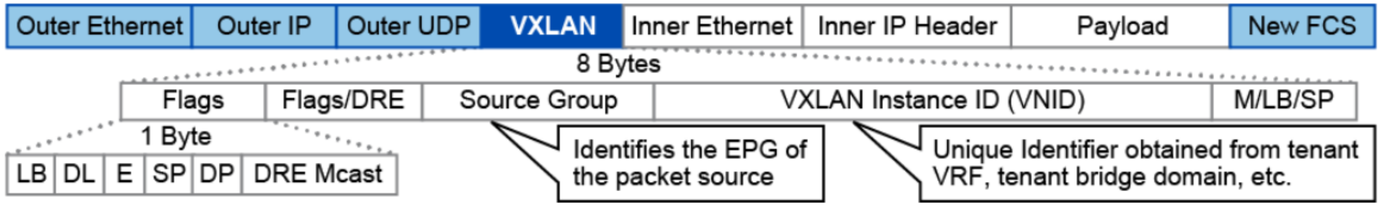
UDP Src. Port	VXLAN Port	UDP Length	Checksum 0x0000
16	16	16	16

VXLAN RRRR 1RRR	Reserved	VNID	Reserved
8	24	24	8

ACI Encapsulation Normalization



Cisco ACI VXLAN encapsulation



Outer Ethernet	Outer IP	Outer UDP	VXLAN	Inner Ethernet	Inner IP Header	Payload	New FCS

8 Bytes

Flags	Flags/DRE	Source Group	VXLAN Instance ID (VNID)	M/LB/SP

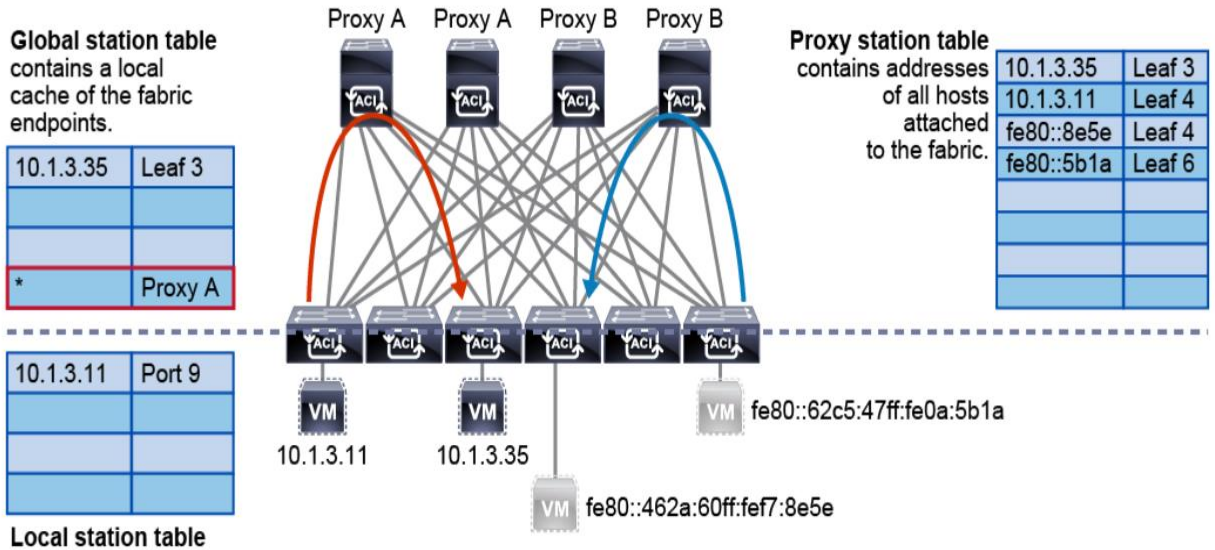
1 Byte

LB	DL	E	SP	DP	DRE Mcast

Identifies the EPG of the packet source

Unique Identifier obtained from tenant VRF, tenant bridge domain, etc.

Forwarding Mechanisms



Global station table contains a local cache of the fabric endpoints.

10.1.3.35	Leaf 3
*	Proxy A

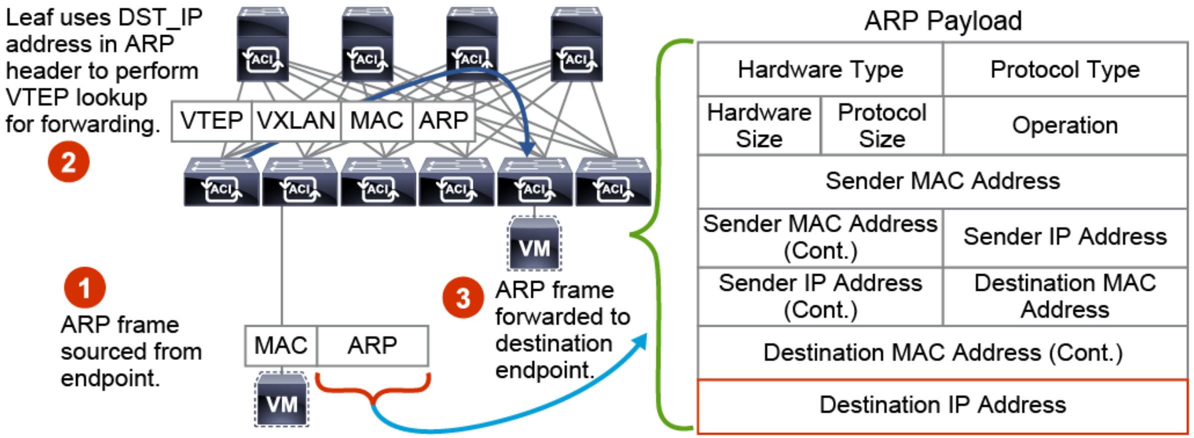
Proxy station table contains addresses of all hosts attached to the fabric.

10.1.3.35	Leaf 3
10.1.3.11	Leaf 4
fe80::8e5e	Leaf 4
fe80::5b1a	Leaf 6

10.1.3.11	Port 9

Local station table contains addresses of all hosts attached directly to the leaf.

Inline hardware mapping database can contain more than 1,000,000 hosts.



Leaf uses DST_IP address in ARP header to perform VTEP lookup for forwarding.

VTEP	VXLAN	MAC	ARP

ARP frame sourced from endpoint.

MAC	ARP

ARP frame forwarded to destination endpoint.

ARP Payload

<table>
<tr><td colspan="2">Hardware Type</td><td>Protocol Type</td></tr>
<tr><td>Hardware Size</td><td>Protocol Size</td><td>Operation</td></tr>
<tr><td colspan="3">Sender MAC Address</td></tr>
<tr><td colspan="2">Sender MAC Address (Cont.)</td><td>Sender IP Address</td></tr>
<tr><td colspan="2">Sender IP Address (Cont.)</td><td>Destination MAC Address</td></tr>
<tr><td colspan="3">Destination MAC Address (Cont.)</td></tr>
<tr><td colspan="3">Destination IP Address</td></tr>
</table>

ARP handling in Cisco ACI is summarized in these rules:

- Cisco ACI does not flood ARP packets by default
- Leaf sends ARP packets to destination IP identified in ARP payload

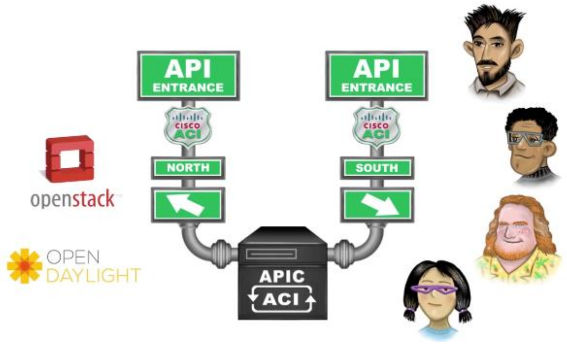
- Fabric learns IP and MAC addresses of endpoints (ARP, DHCP)
- Council of Oracles Protocol, also known as COOP, sends the mappings to the spine proxy
- Forwarding of IP packets based on destination IP address
  - Packets routed if destination MAC address is router-mac
  - Otherwise packets are bridged (no TTL decrement or MAC rewrite)
- Forwarding of non-IP packets based on MAC address

The Council of Oracles Protocol, which is known as COOP, running in the fabric ensures the following:

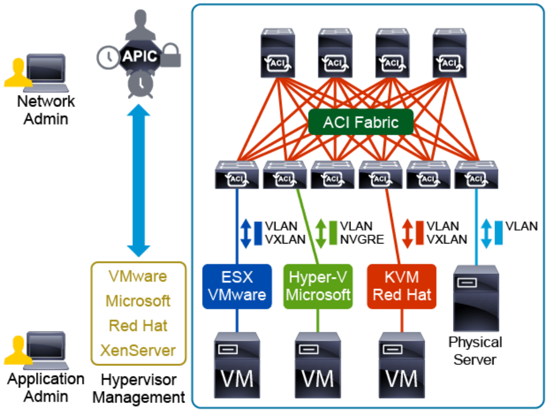
- All spines maintain a consistent copy of endpoint address and location information.
- All spines maintain the endpoint identity to the location mapping database.

Additional Capabilities

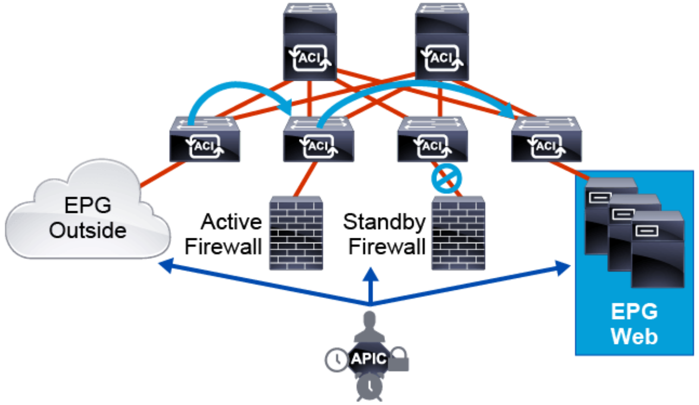
Orchestration with OpenStack



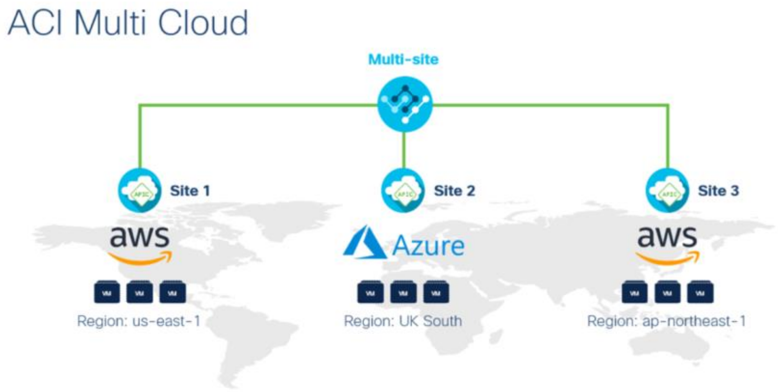
Virtual Domain Integration



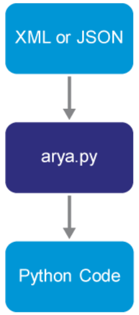
Service Insertion



Public Cloud Integration



Programmability



XML or JSON

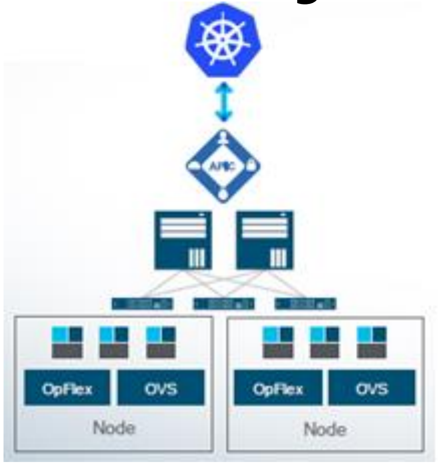
arya.py

Python Code

```
{"fvTenant":{"attributes":{"dn":"uni/tn-Cisco","name":"Cisco","rn":"tn-Cisco",
"status":"created"},"children":[{"fvBD":{"attributes":{"dn":"uni/tn-Cisco/
BD-CiscoBd","mac":"00:22:BD:F8:19:FF","name":"CiscoBd","rn":"BD-CiscoBd","status":
"created"},"children":[{"fvRsCtx":{"attributes":{"tnFvCtxName":"CiscoNetwork",
"status":"created,modified"},"children":[]}},{"fvSubnet":{"attributes":{"dn":"uni/
tn-Cisco/BD-CiscoBd/subnet-[10.0.0.1/8]","ip":"10.0.0.1/8","rn":"subnet-
[10.0.0.1/8]","status":"created"},"children":[]}}]}},{"fvCtx":{"attributes":{"dn":
"uni/tn-Cisco/ctx-CiscoNetwork","name":"CiscoNetwork","rn":"ctx-CiscoNetwork",
"status":"created"},"children":[]}}]}}
```

```
fvTenant = cobra.model.fv.Tenant(topMo, name='Cisco')fvTenant = cobra.model.fv.Ctx
(fvTenant, name='CiscoNetwork')fvBD = cobra.model.fv.BD(fvTenant, mac='00:22:BD:F8:
19:FF',name='CiscoBd')fvRsCtx = cobra.model.fv.RsCtx(fvBD, tnFvCtxName=fvCtx.name)
fvSubnet = cobra.model.fv.Cubnet(fvBD, ip='10.0.0.1/8')
```

Containers Integration



Summary

Create the best network with Cisco ACI

- Central management, automation and monitoring (reduced deployment time, increased productivity of IT staff)

- Reduction of time to control the security system (whitelist principle)

- Application-oriented infrastructure (policy application with flexibility and depending on the components required)

- Integration with third-party ecosystems (Vmware ESX, Microsoft Hyper-V, KVM Red Hat, Docker/ Kubernetes)

- Cisco Nexus 9000 series as the basis of transport system (scaling, performance, fault tolerance)

Demo: ACI simulator

Time to get hands a bit dirty! ;)

GO GLOBAL

GO CLOUD

GO INNOVATIVE

Digital Transformation and Cybersecurity Solution Service Provider