
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Enabling Cloud Services at the edge with App Hosting on Catalyst 9000

Sai Zeya
Technical Marketing Engineer
BRKENS-1090

Cisco Webex App

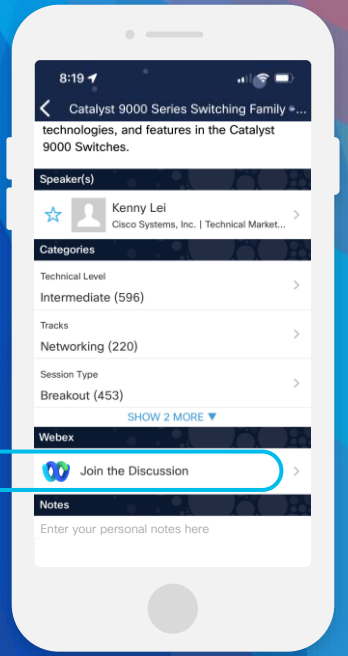
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.



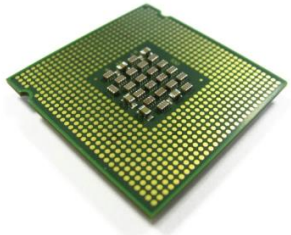
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENS-1090

Agenda

- Introduction
- App Hosting Use Cases
- App Hosting Infra
- App Lifecycle Management
- App Hosting Features
- Conclusion

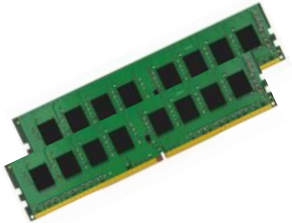
Networking Today …

Catalyst 9000



x86 CPU

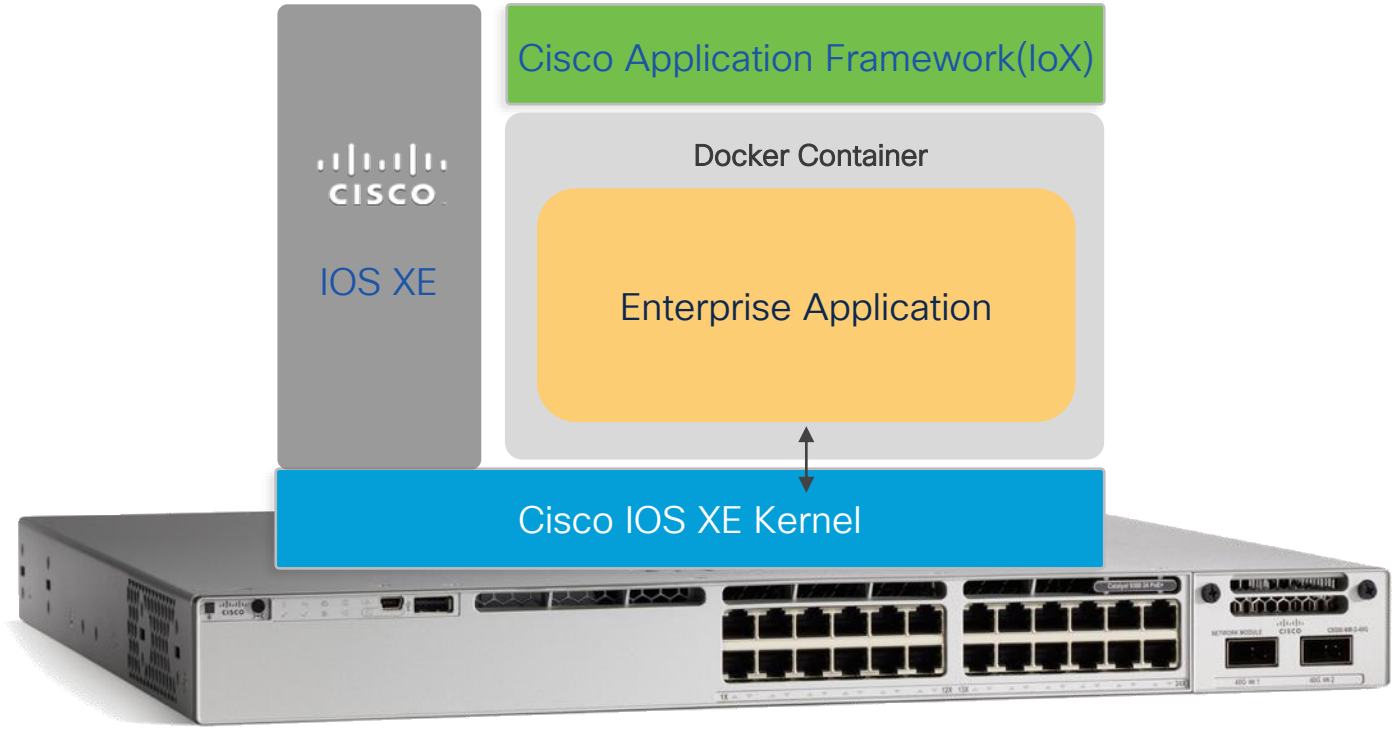
Linux-based OS



Memory/Storage

Enables hosting docker containers and 3rd party apps

Catalyst 9000 Application Hosting Infra



New strategic capabilities with App Hosting on C9K Switches

Existing Hardware

Managed via CLI or DNA-C

Real Time Processing

Lower Latency

Save Bandwidth

IT Operations and Monitoring Tools

Consolidate Physical Infrastructure

ThousandEyes

kibana

WIRESHARK

perfSONAR powered

Security Agents and Functions

Enhance Visibility & Security Enforcement

ipsecclient by codilime

Attivo NETWORKS

TRAPX SECURITY

ASAc

Cloud Gateways with Serverless Edge Compute

Reduce App Latency & Optimize App Traffic

Cybervision

Cisco DNA Spaces

NS1.

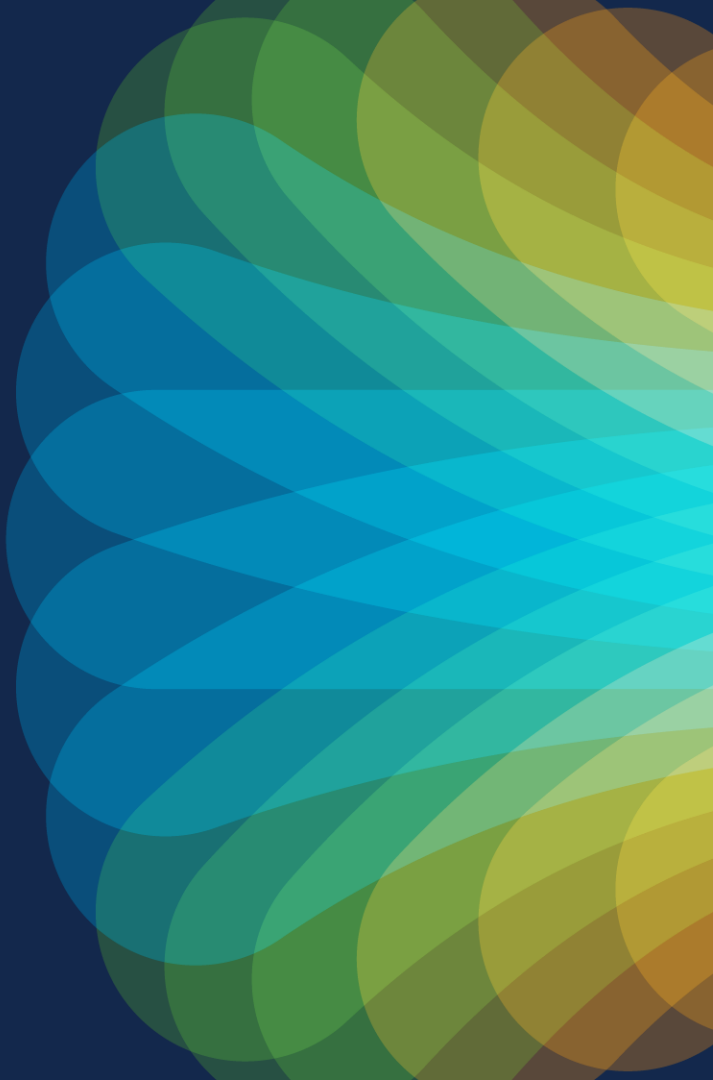
Alleantia

Customer Specific Applications

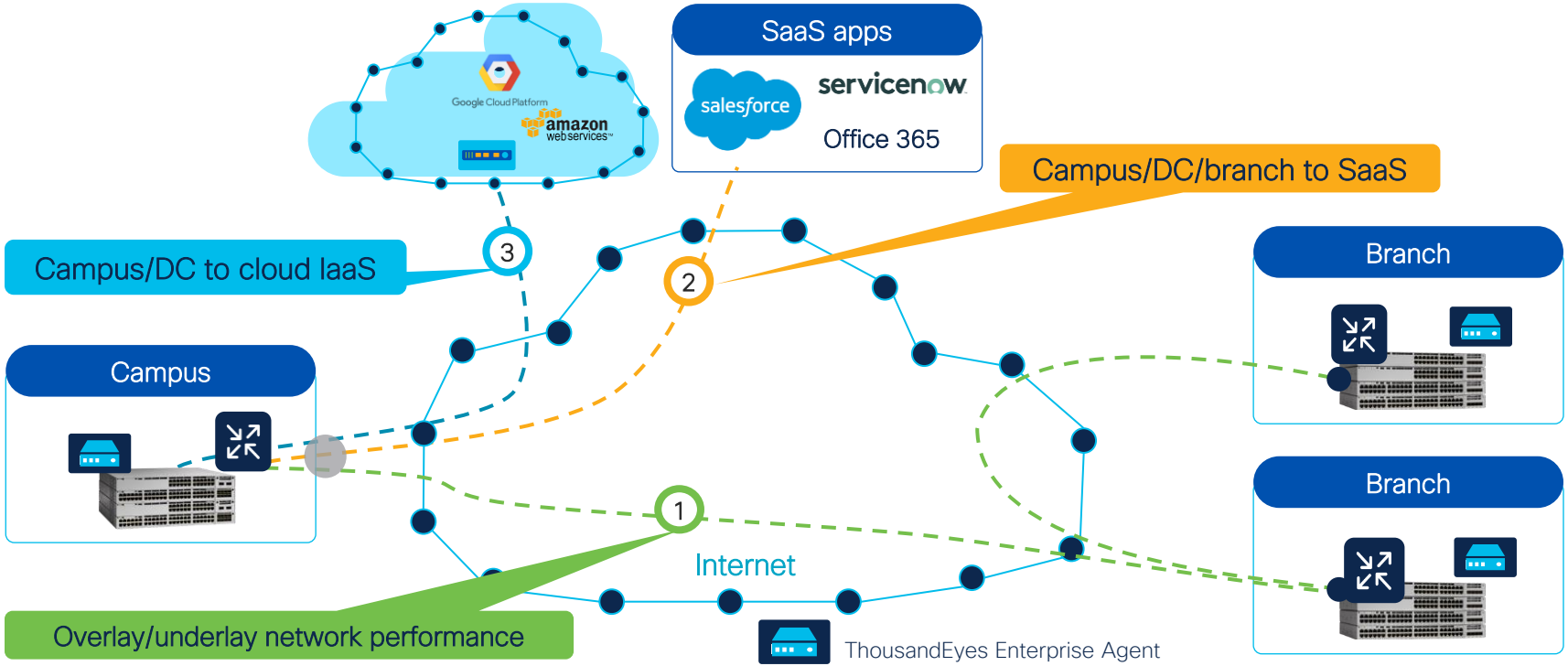
3rd Party App Hosting

Rich ecosystem partnership with 25+ certified apps and 200+ active customer

ThousandEyes



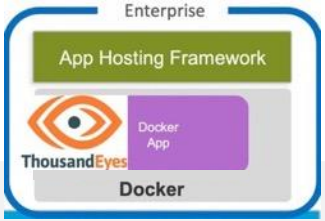
Service Assurance is beyond the enterprise domain
Use cases for ThousandEyes Enterprise Agent



ThousandEyes now included with Cisco DNA licenses

New and existing Catalyst 9000 switches now include ThousandEyes service assurance

App hosting: no extra hardware



- Run ThousandEyes agent natively on flash of 9300/9400 switches
- Out of the box access to ThousandEyes for new switches

DNA subscription benefits

- Includes 22 x ThousandEyes Units for a month
- Pool entitled test capacity to deploy anywhere within your network

Data Visualization

- License to ThousandEyes SaaS-based management platform
- Access to Dashboards, alerts and reporting tools

Campus connectivity | Modern WAN | Application experience

*Choose from a menu of several networking, web and voice tests
Browser-based tests need the use of SSD and consume more ThousandEyes units

Service Assurance from Catalyst 9000

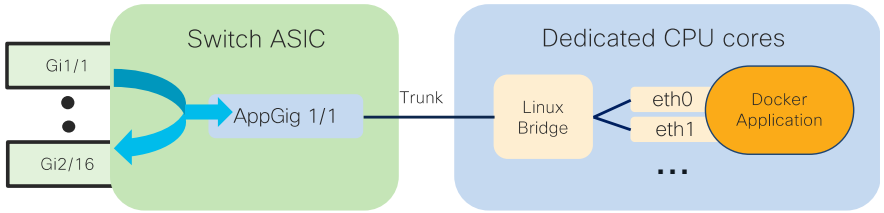
ThousandEyes Enterprise Agent

Agent installed in Flash
Test Included:
- **Web** – HTTP Server, FTP Server
- **DNS** – DNS Server, DNS Trace, DNSSEC
- **Network** – Agent to Agent, Agent to Server
- **Voice** – SIP Server, RTP Stream, Voice Call

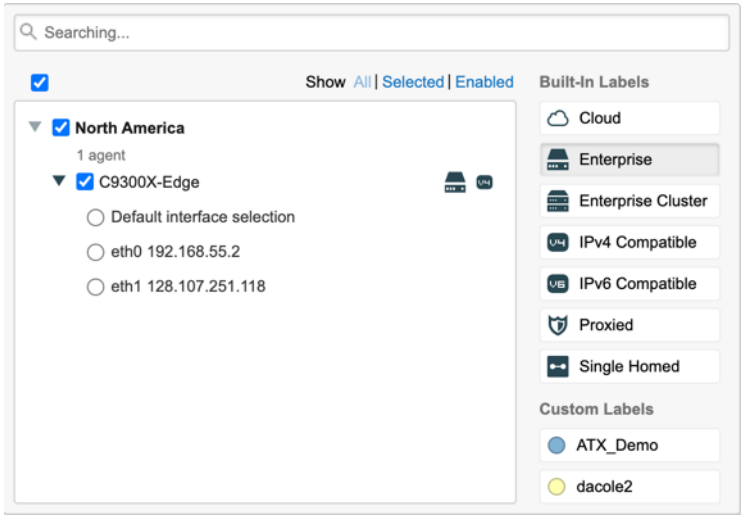
Agent installed in SSD
Test Included:
- **Web** – HTTP Server, FTP Server
- **DNS** – DNS Server, DNS Trace, DNSSEC
- **Network** – Agent to Agent, Agent to Server
- **Voice** – SIP Server, RTP Stream, Voice Call
- **BrowserBot** – Page load & Transaction (IOS-XE 17.6.1 required)

Multiple Interfaces with ThousandEyes

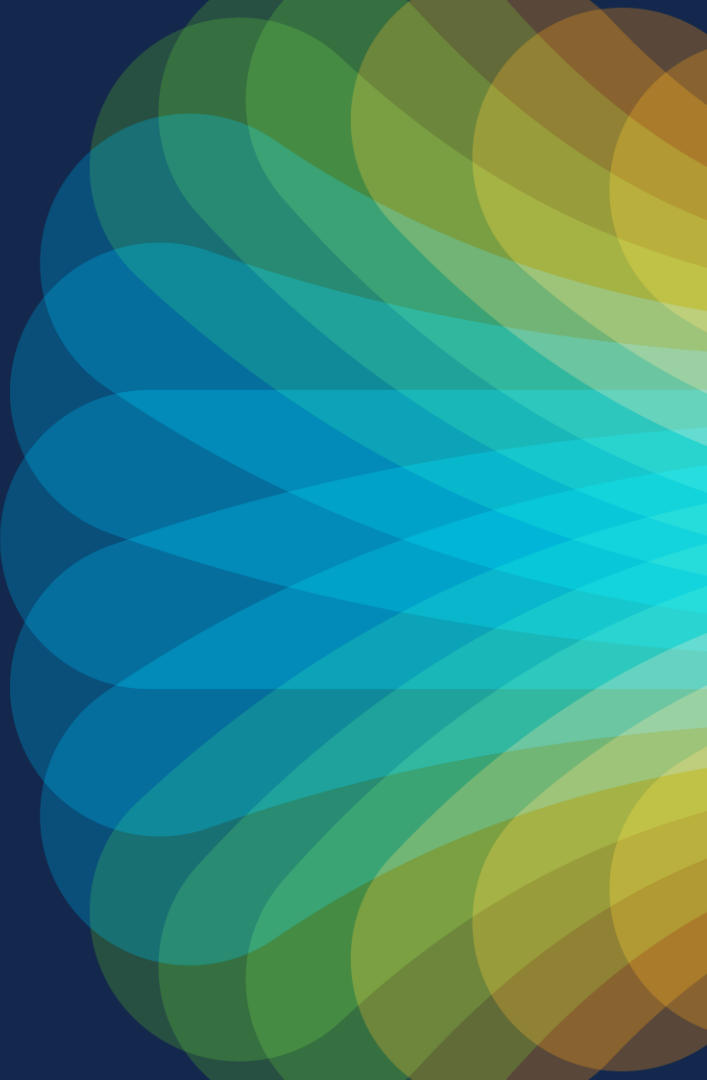
App Traffic View



ThousandEyes Dashboard View

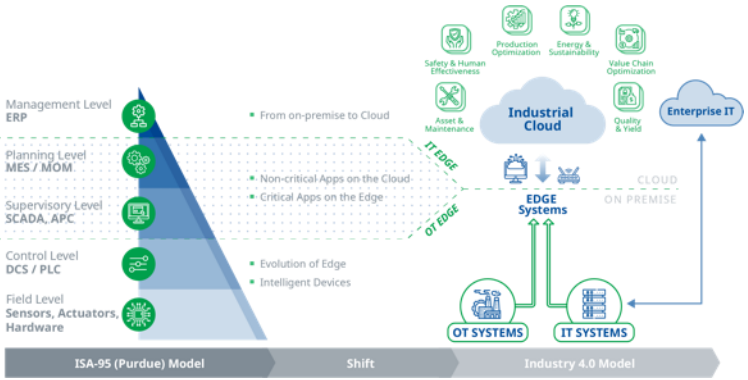


ASAc Firewall



Industry Trends

Driving the need for Distributed Firewall Architectures



Industry 4.0

OT to leverage the power of IT & cloud

Digital Transformation and Smart Manufacturing have **accelerated the convergence of IT & OT** domains in the process industry

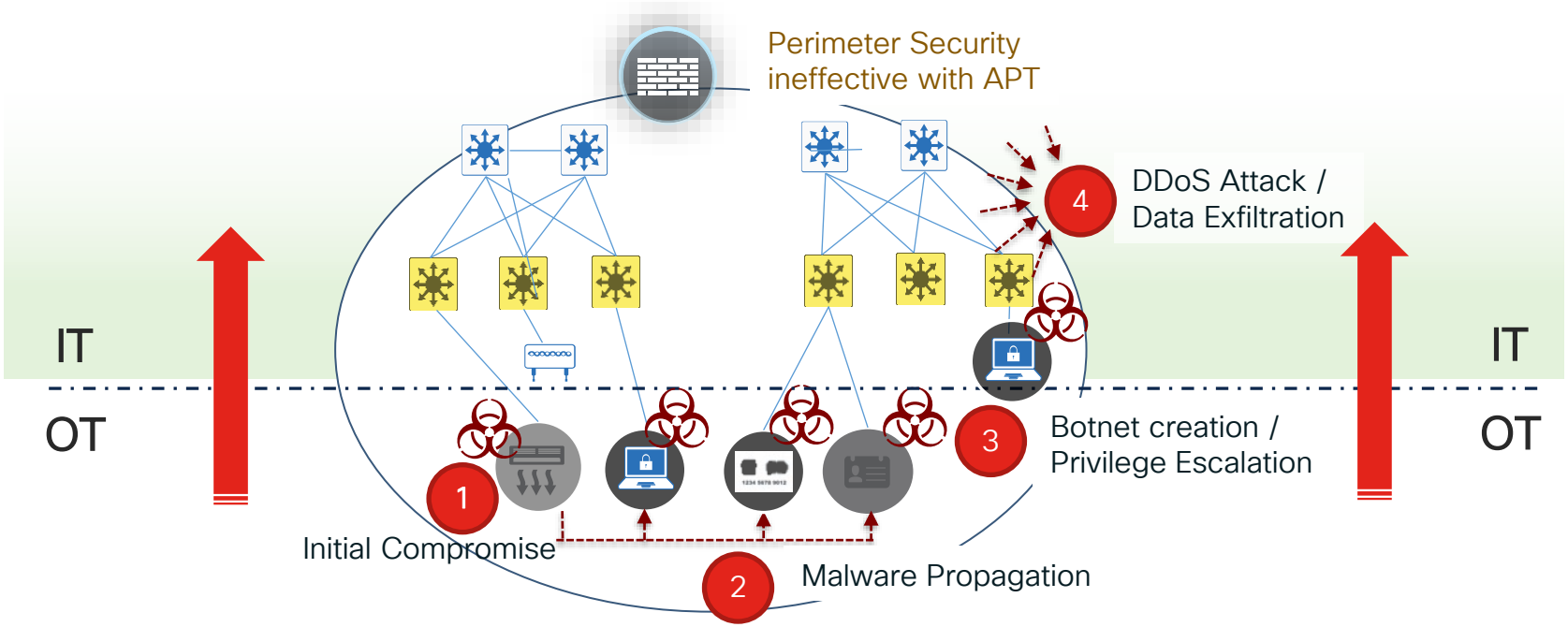
Smart Building / Consumer IoT

Proliferation of IoT

Increased presence of IoT in IT Networks: HVAC, lighting, alarms, and security converge into a **single IT managed network infrastructure** to build smarter and safer workspaces

IT at constant risk due to OT vulnerabilities

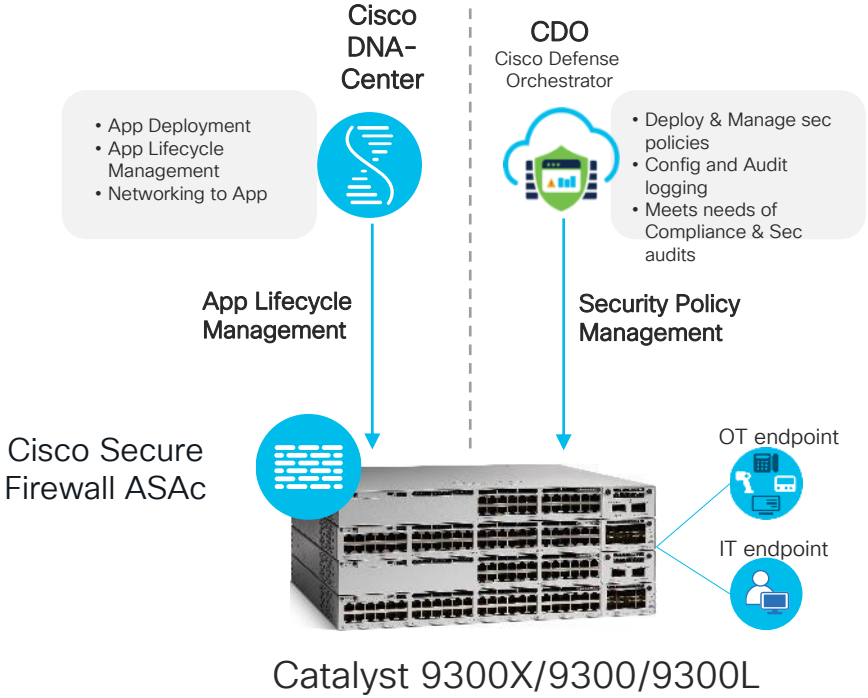
OT Endpoints have Limited security & crypto capabilities, prone to hacks



Need for Stateful Inspection of IOT traffic at the Edge

ASAc Firewall hosted on C9K Switches

Bringing Cisco EN and Security solutions together for improved Operations

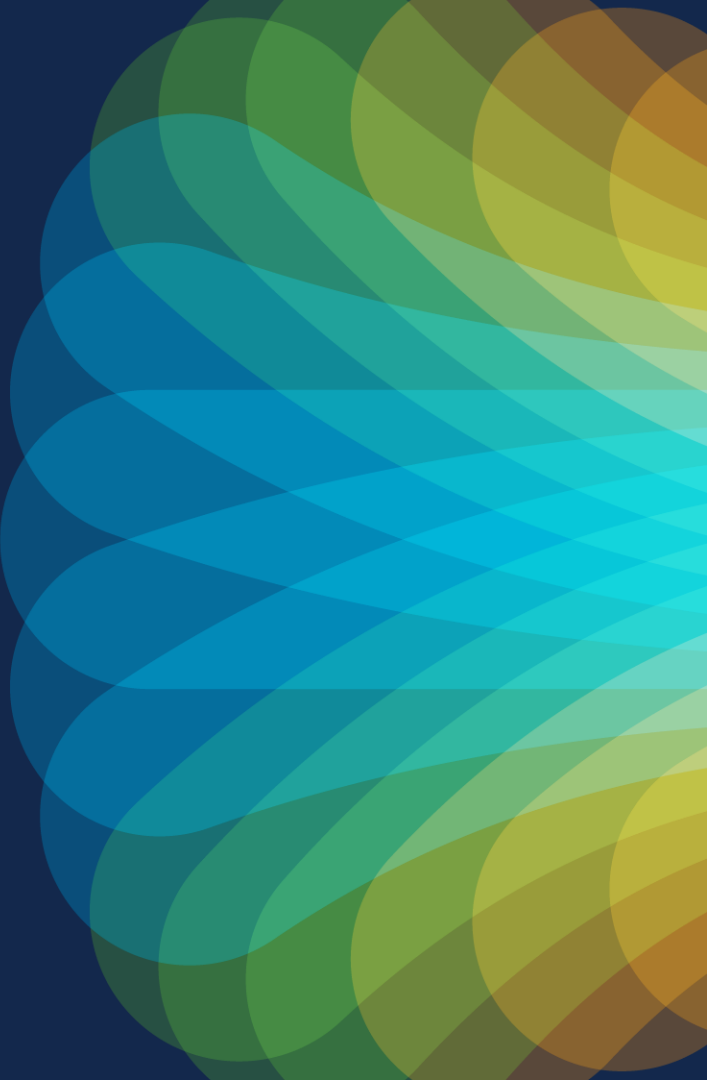


Use Case

- Stateful inspection of OT traffic at the Edge
- No need of Physical Firewall
- No need to change network architecture
- No waste of network bandwidth
- Automation to scale operations

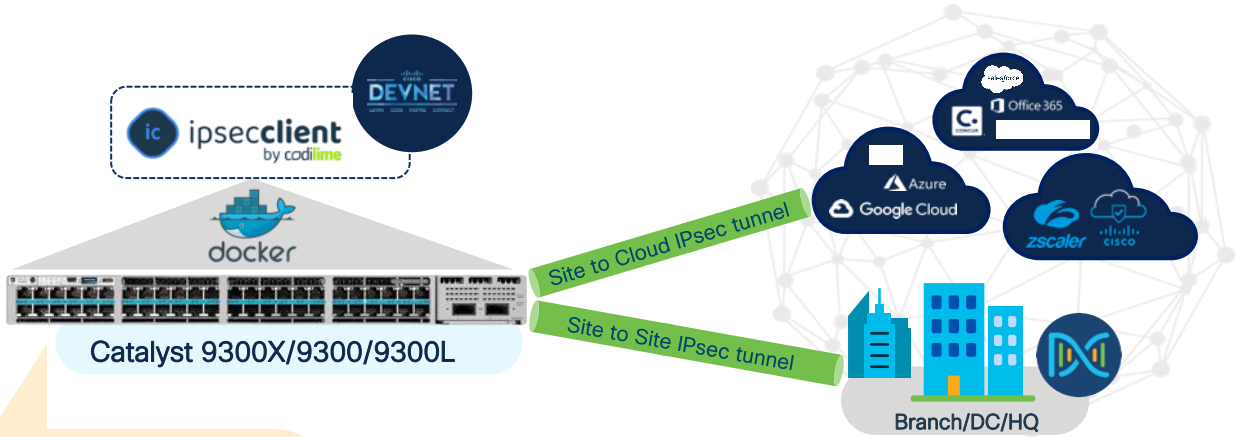
- Powerful Stateful Inspection Firewall
- Separation of SecOps and NetOps
- L3 Firewall (Routed Mode only)
- Support for SGT
- 100M – 300M (IMIX) ASAc Throughput for IT & OT Convergence

Codilime App



Codilime: IPsec delivered via App-Hosting

Cisco IOS® XE 17.10



App Resources

Memory (RAM)	: 409 MB
Disk (SSD)	: 10 MB
CPU	: 1480 units
CPU-percent	: 20 % of 1Core

- IPsec VPN Application hosted on Cat9k
- Runs in Docker container
- Interactive Web UI for IPsec config
- SW IPsec - C9300/9300L
- HW & SW IPsec - C9300X
- Will be available on Cisco DEVNET

Security

- IPsec IKEv2
- Authentication using PSK or x509

Protocol Support

- VRF Aware
- NAT
- NAT-T

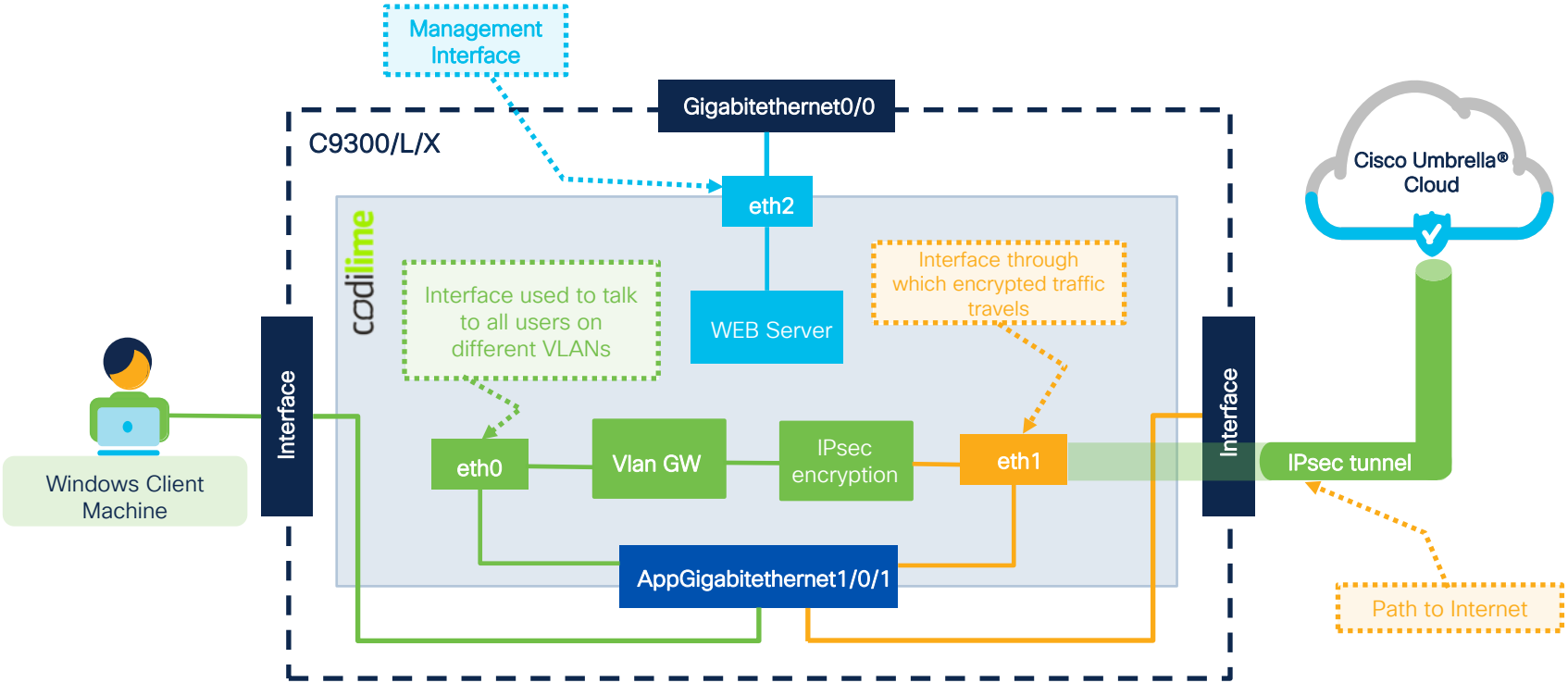
Automation

- YANG model with REST API

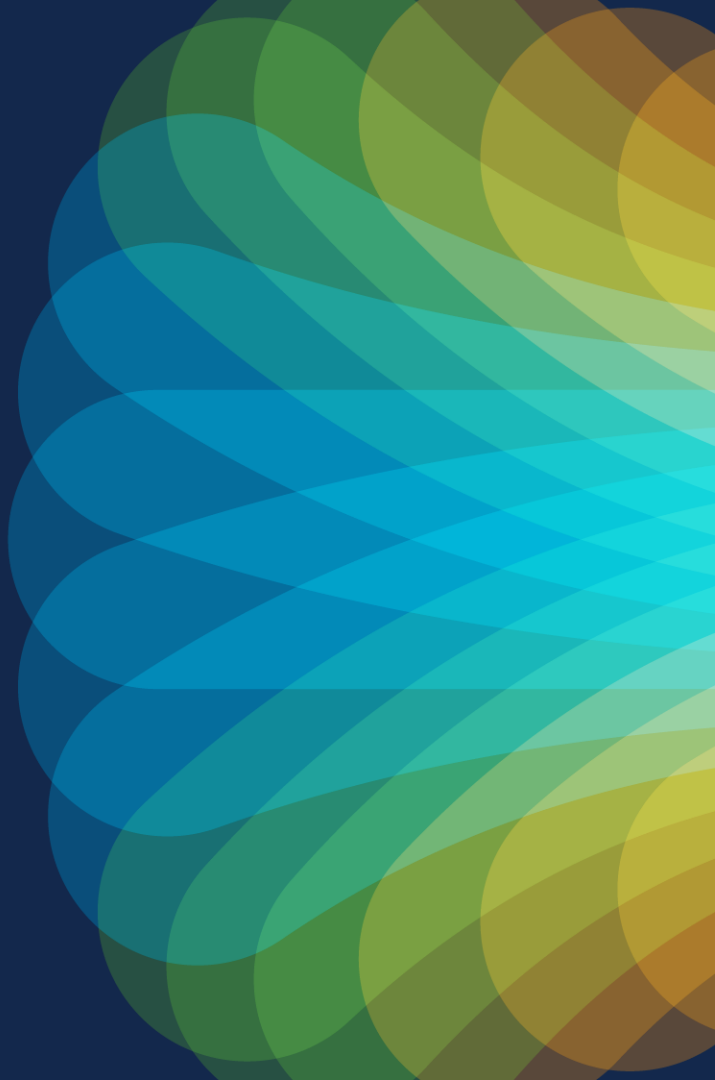
Interoperability

- AWS, GCP, Azure
- Cisco Umbrella, Zscaler
- C8K, ISR/ASR, Juniper

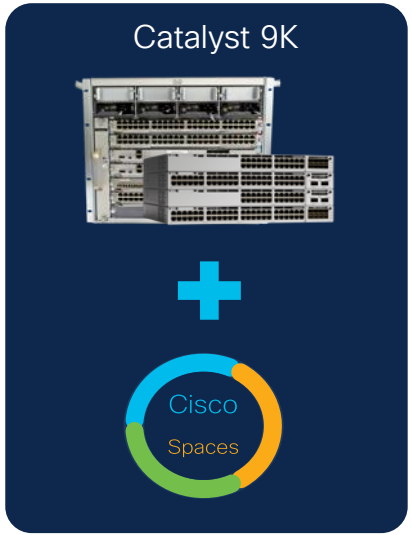
Application Design



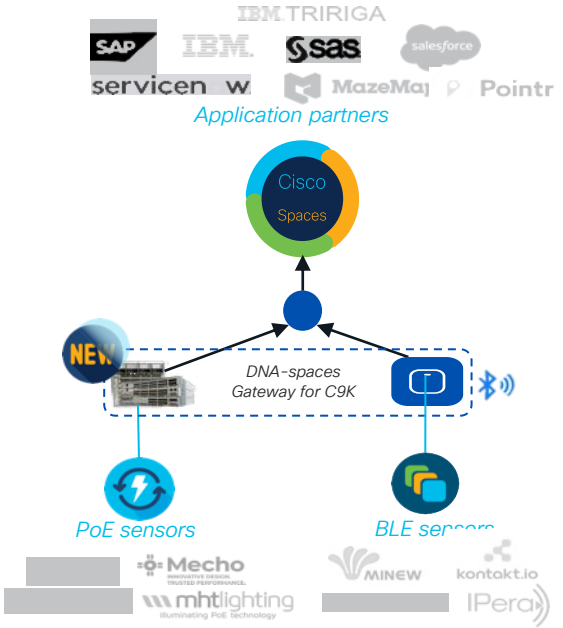
IoT Gateway App



Catalyst 9K expands value for Smart buildings



Next: DNA-spaces gateway for Catalyst 9K will expand outcomes



New use cases

- Sustainable buildings
- Employee health & Safety
- Productivity Improvement
- Building Analytics

Unified Marketplace

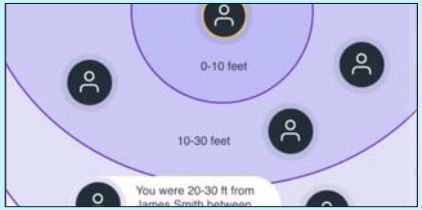
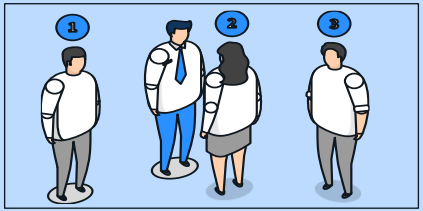
- Largest choice of IoT devices
- Unmatched solution scale
- Cisco validated

Lower TCO

- Automated workflows
- No vendor lock-ins
- Cloud based as-a-service

*Source: Cisco Smart building TCO calculator

Use Cases

User Experience	Safety & Compliance	Real Estate Utilization	Automation & Optimization
Conference Room Booking	Density Triggers	Device/People Counting	Environmental Monitoring & Asset location
GA			
			
Cisco Catalyst 9K			
Cisco Spaces			
PoE lights & Sensors	Cisco Catalyst Wireless LAN Controller	Cisco Catalyst Wireless LAN Controller	POE sensors / HVAC

Indoor IoT Services – Overview

Cisco Spaces cloud

- IoT Market place and Partner Apps.
- Firehose API

Cisco Spaces Connector

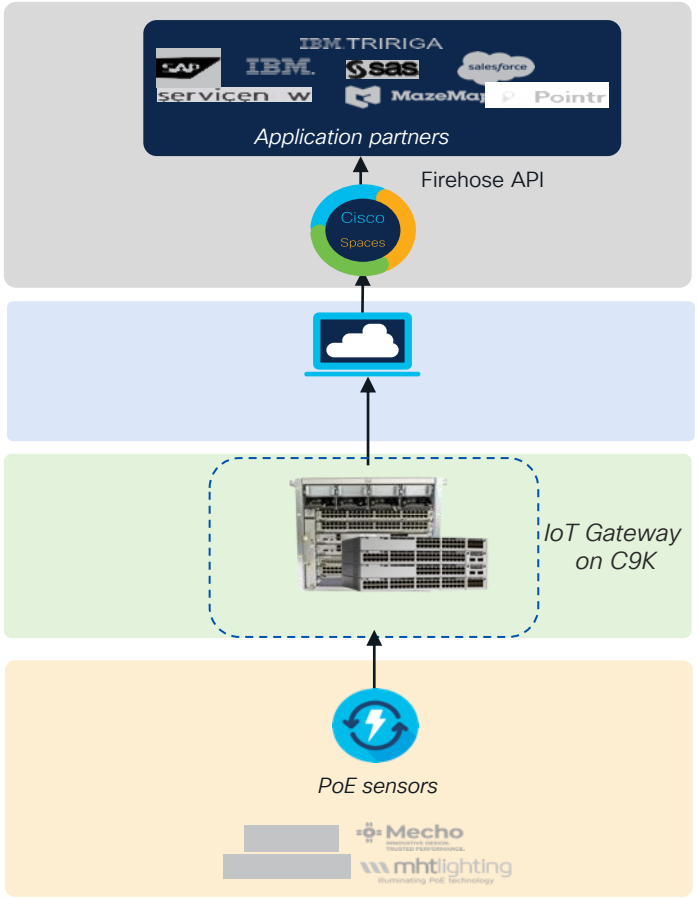
- Interfaces between Cisco Spaces Cloud & on prem devices
- Collects sensor data

Catalyst 9300/9400

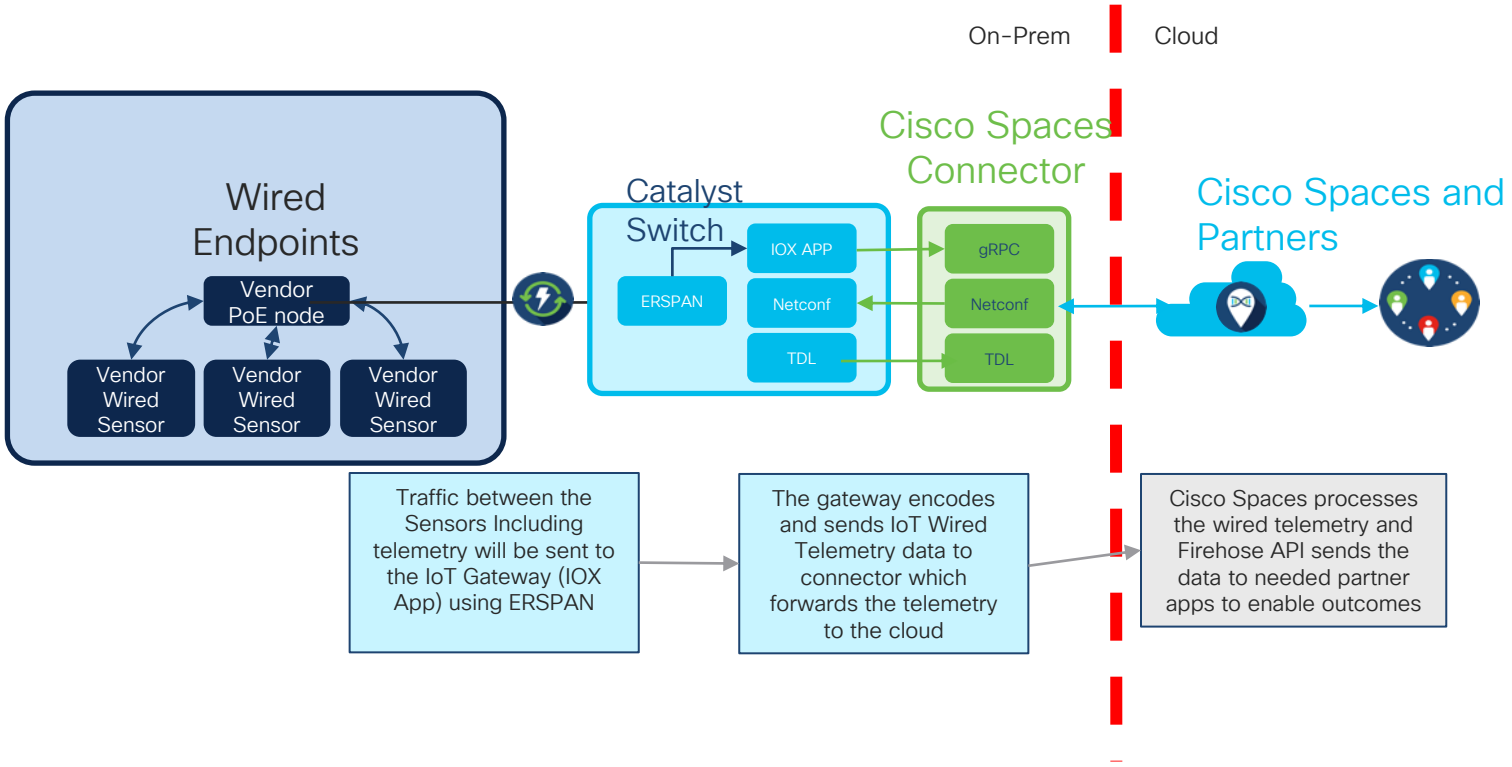
- UPOE/UPOE+ Connectivity
- IoT GW App

PoE Sensors

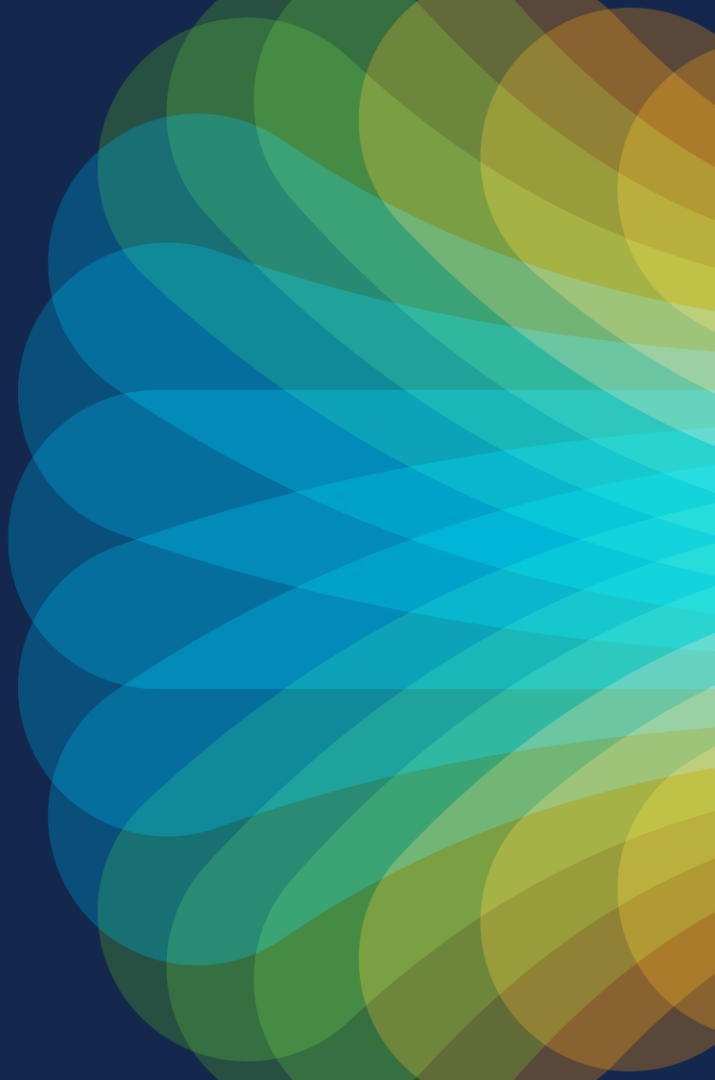
- Wired PoE Sensors
- Powered by UPOE/UPOE+ port on the switch



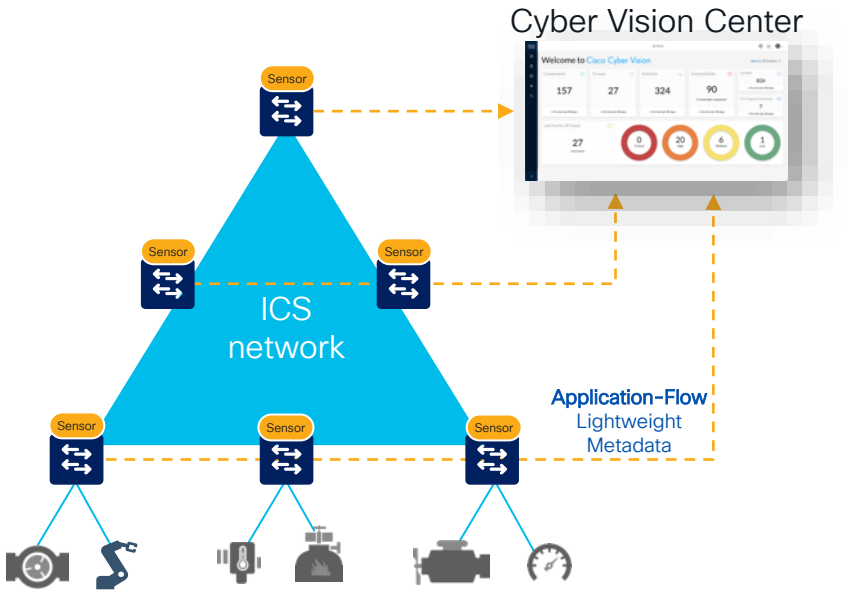
Indoor IoT Services with IoT Gateway App



Cyber Vision App



Cisco Cyber Vision
Visibility & detection built into your network infrastructure



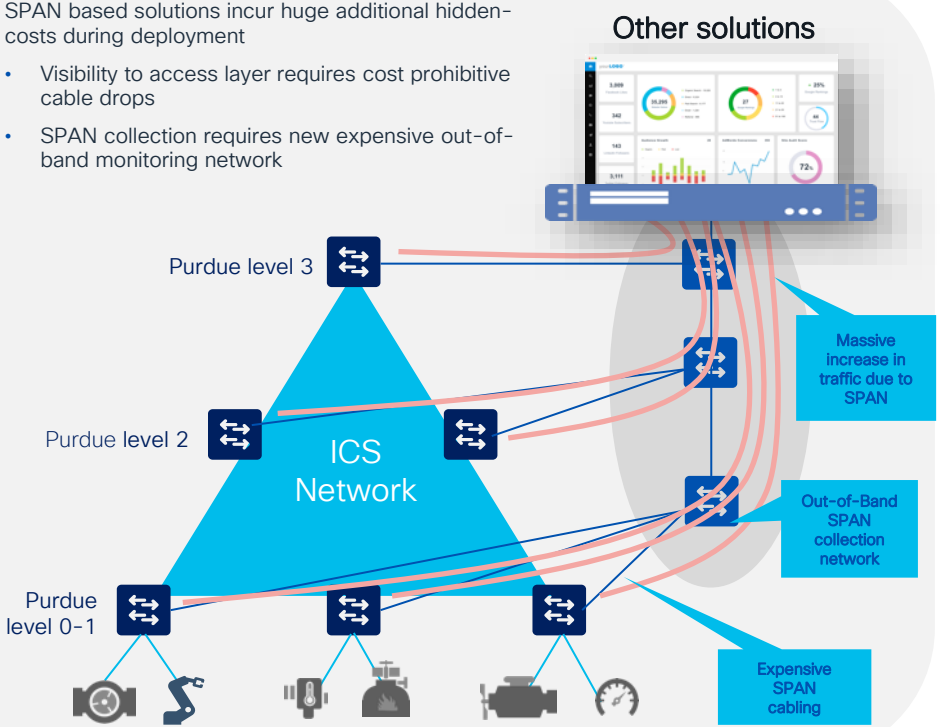
Monitoring at the edge

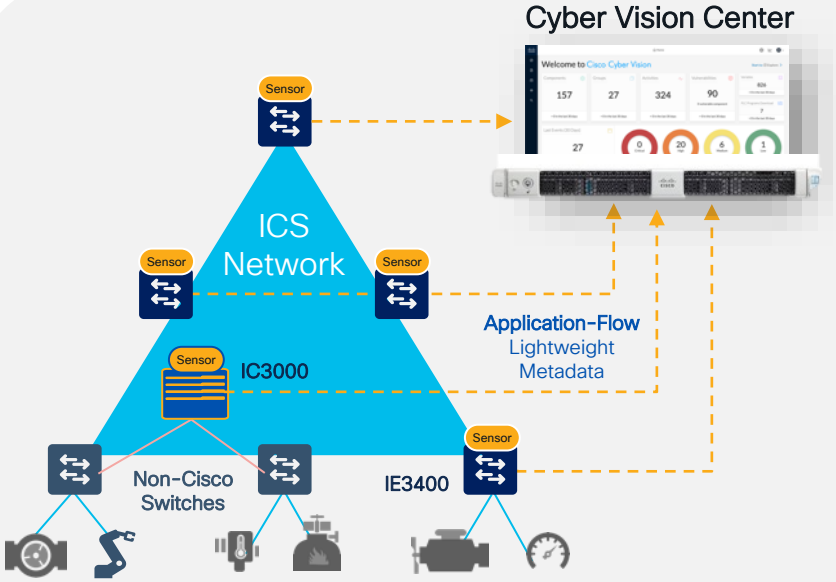
- Cyber Vision Sensors embedded into industrial network equipment
- No additional hardware needed
- No need for an out-of-band monitoring network
- No impact on performance

Cyber Vision architecture

SPAN based solutions incur huge additional hidden-costs during deployment

- Visibility to access layer requires cost prohibitive cable drops
- SPAN collection requires new expensive out-of-band monitoring network



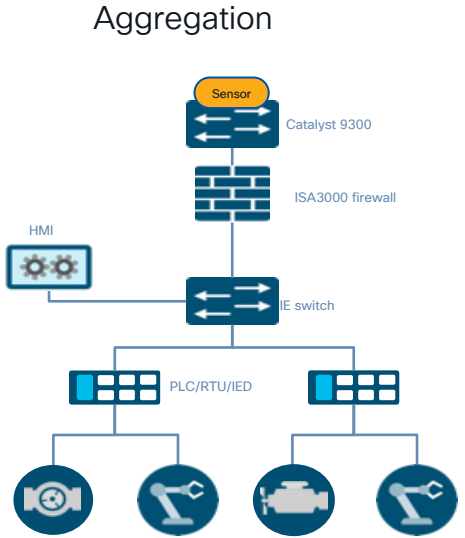


Network-Sensors eliminate the need for SPAN

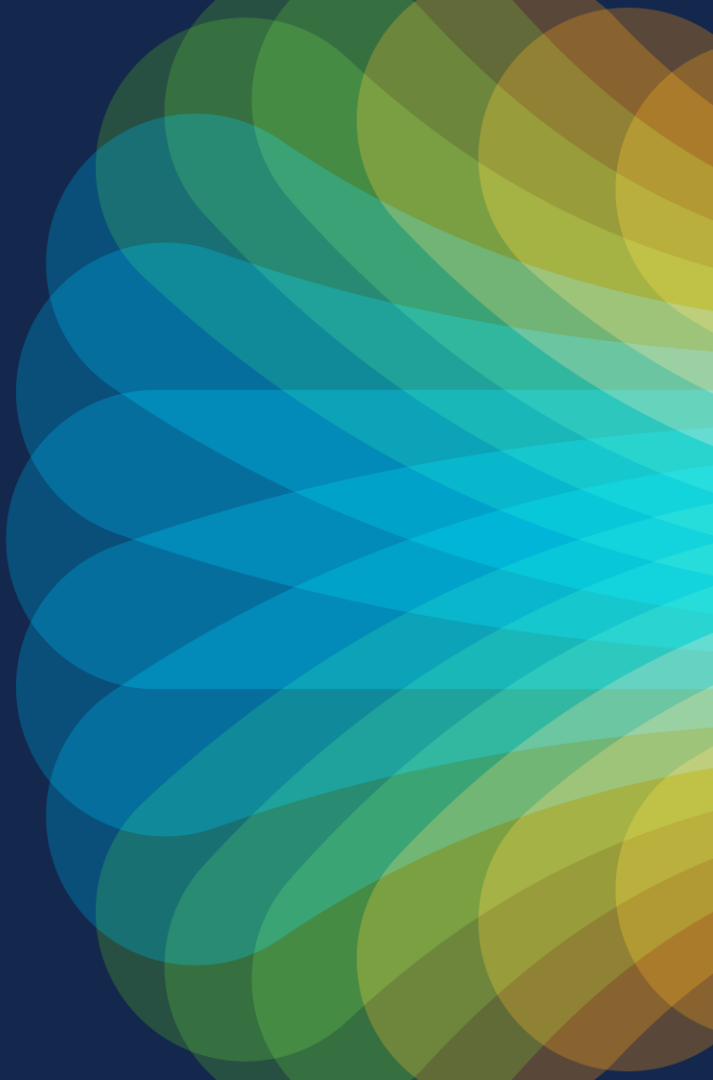
- The application-flow is streamed through existing network enabling lowest TCO
- Hardware-sensor to support brownfield only requires one-hop SPAN

Catalyst 9000 deployment

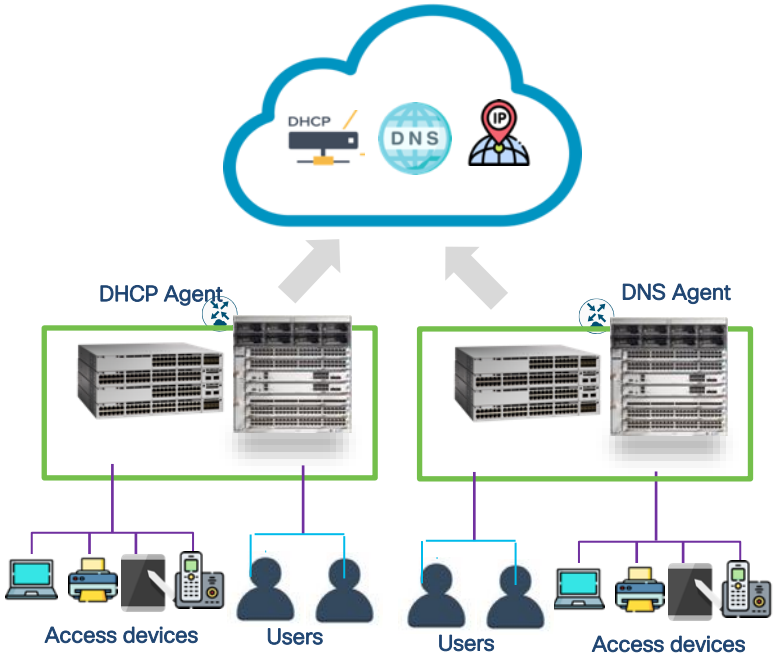
- Leverages ERSPAN to receive traffic from switch
- Supports up to 30000 pps
- Catalyst 9300, 9400 ,9500 and 9600 (must support application hosting)
  - Requires SSD
- Can be deployed as access, aggregation, core or as an out of band span aggregation sensor



DNS, DHCP,& IPAM (DDI)



Making Network Edge more Intelligent



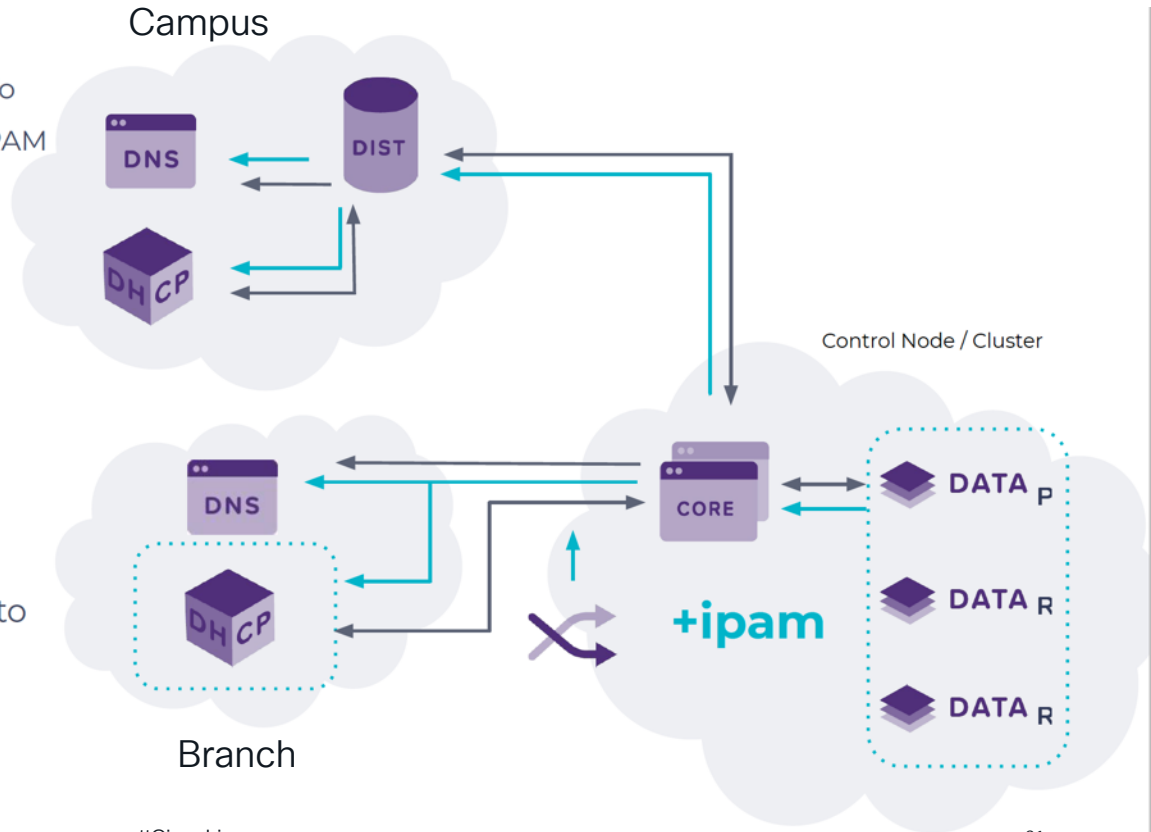
Capabilities

- Distributed model with centralized cloud control
- DevOps Ready Framework
- Granular control over DDI services
- Deployment on Scale with Cisco DNA Center

Scale and reliably deliver DHCP, DNS, and IPAM (DDI) services when you need them

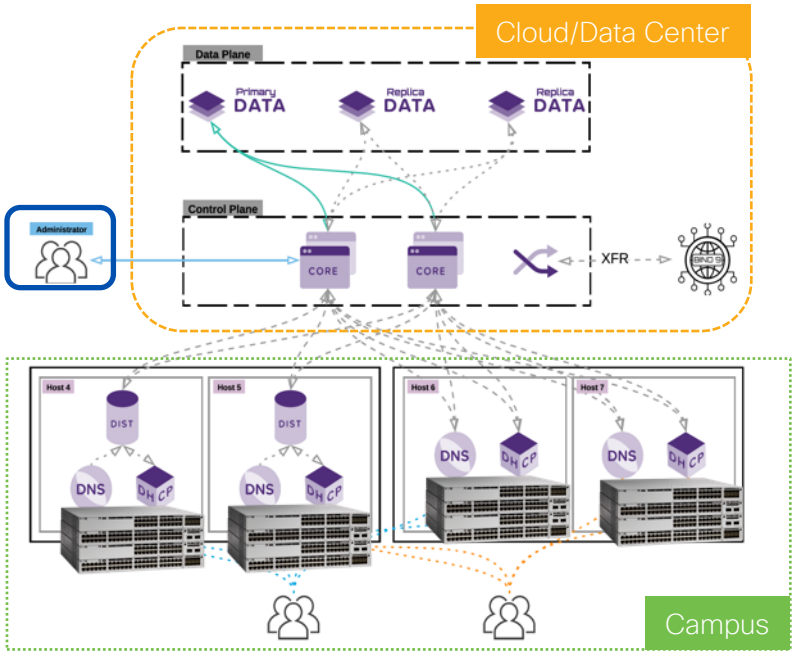
NS1 DDI Architecture

- Containers have six basic roles
  - data: zone, record and IP Address info
  - core: api and web portal including IPAM interfaces
  - xfr: zone transfers
  - dns: NS1's next-gen nameserver and high-speed caching daemon
  - dist: a.k.a. "distribution node" a local copy of the main database at the network edge
  - dhcp: DHCP engine
- Architecture allows for deployment into varied, topologically-complex environments



Catalyst enabled DDI aaService with NS1

Scale and reliably deliver DDI services



Can individually host DNS and DHCP containers in C9300 and C9400

Other DDI Containers can flexibility host on Sever or Cloud.

Resource type	Catalyst 9300/L	Catalyst 9300X	Catalyst 9400
Memory	2GB	8GB	up to 8GB
CPU	1 core (25%)	2 core (25%)	1 core (25%)
Storage	120/240 GB (USB3.0/SSD)	240GB (USB3.0/SSD)	240-960GB (SATA)

NS1 Enterprise DDI Installation Guide

NS1 deployment on C9K

- Flexible Deployments via Cisco DNA-C / CLI / WebUI
- One Container per C9K switch.
- IP reachability is required for Control Services Containers.
- Docker run options:

DNS Container: -v $(APP_DATA):/data -p 3301:3300 -p 53:53/udp -p 53:53/tcp -e CONFIG_PORT= 3301 --core_host=x.x.x.x

DHCP Container: -v $(APP_DATA):/data -p 67:67/udp -e CONFIG_PORT= 3300 --core_host=x.x.x.x --service_def_id=2

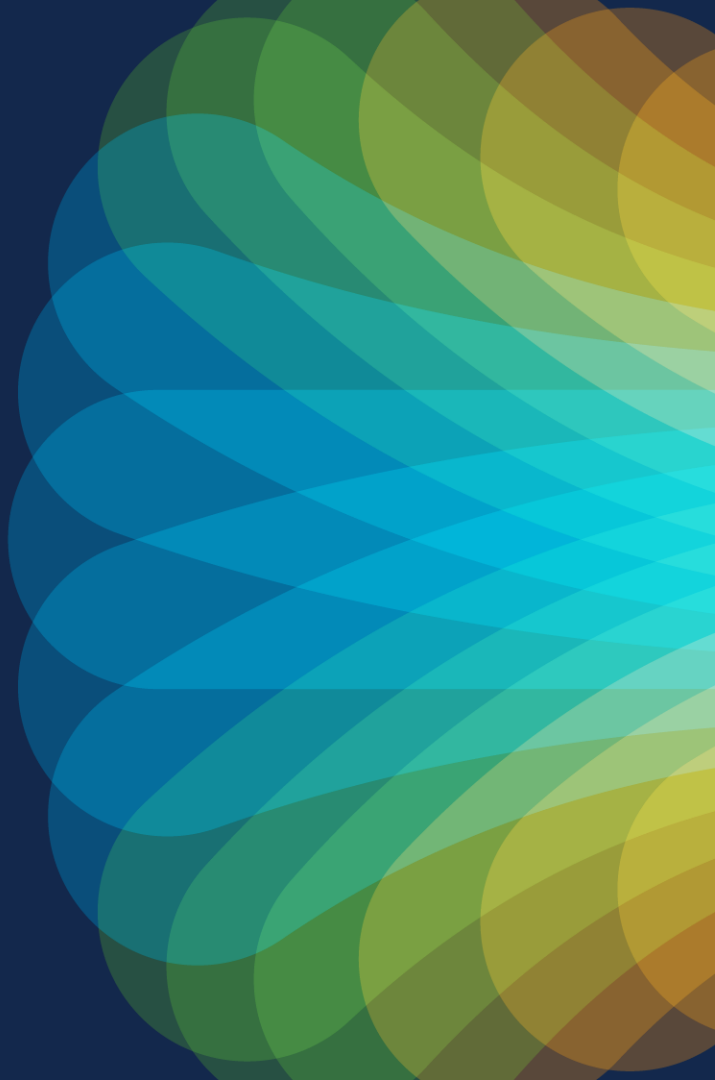
Integrated into the Cisco's Umbrella Architecture
Already on the Global Price List
For More details: https://www.ns1.com/Cisco

Validated Apps- DevNet Eco System Exchange

DevNet Eco System Exchange

- Cisco will not provide any support to third-party apps and open source apps unless specifically called out.
- Such apps, however, will be validated for compatibility on Cisco® Catalyst® 9000 switches.
- DevNet ecosystem will indicate the partners who have worked on Cisco Catalyst 9000 switches.

App Hosting Infra



HW resources for App Hosting

	Resource type	Catalyst 9300	Catalyst 9300-X	Catalyst 9400	Catalyst 9400-X	Catalyst 9500	Catalyst 9500-X	Catalyst 9600	Catalyst 9600-X
Networking	AppGig Port	1x1G	2x10G	1x1G	2x10G	Mgmt Port*	2x10G	Mgmt Port*	Mgmt Port* (2x10G CPU ports)
Resources	Memory	2GB	8GB	8GB	8GB	8GB	8GB	8GB	8GB
	CPU	1 core	2 core	1 core	1 core	1 core	1 core	1 core	1 core
	Storage	240GB (USB3.0/SSD)	240GB (USB3.0/SSD)	480-960GB (SATA)	480-960GB (SATA)	480-960GB (SATA)	480-960GB (SATA)	480-960GB (SATA)	480-960GB (SATA)

* Using loopback with any external ports

Catalyst 9300-X

USB 3.0
240GB

Back panel

Catalyst 9400-X

M2 SATA
480/960GB

Plug into removable SUP

Catalyst 9500-X

M2 SATA
480/960GB

Back panel

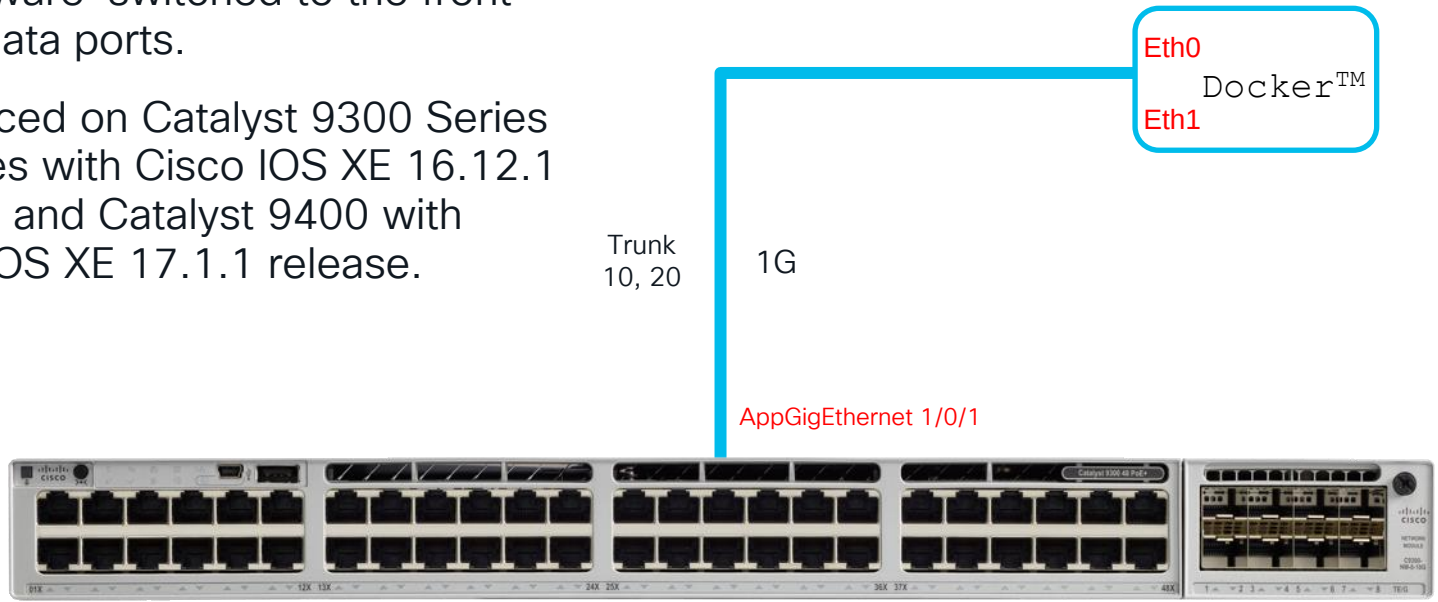
Catalyst 9600-X

M2 SATA
480/960GB

Plug into removable SUP

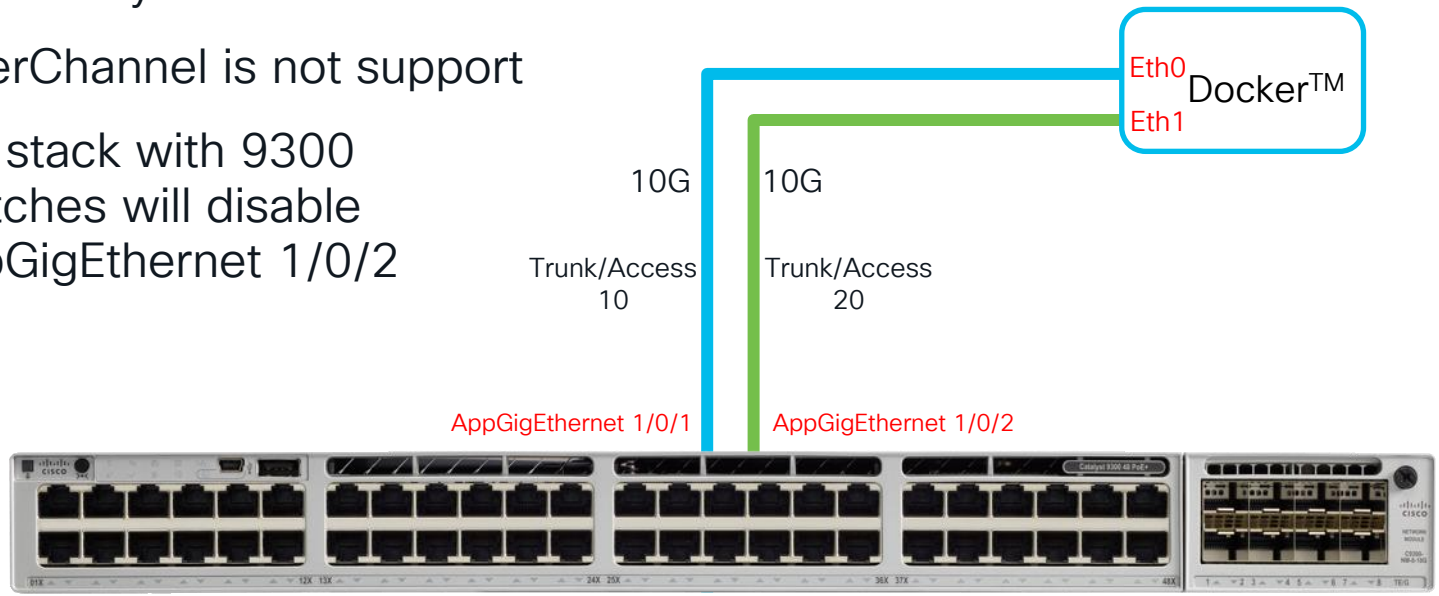
AppGigEthernet Port

- What is AppGigEthernet Port ?
- An internal hardware data port which is hardware-switched to the front-panel data ports.
- Introduced on Catalyst 9300 Series switches with Cisco IOS XE 16.12.1 release and Catalyst 9400 with Cisco IOS XE 17.1.1 release.

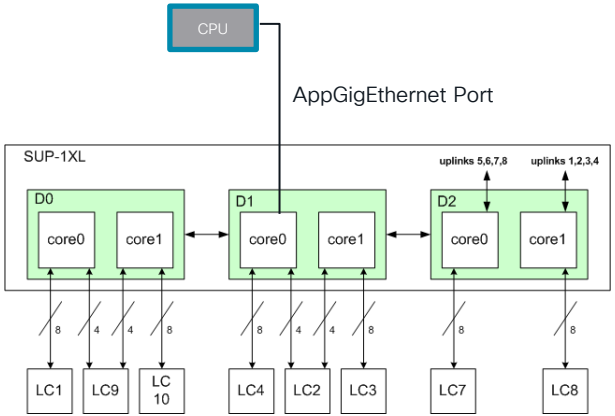


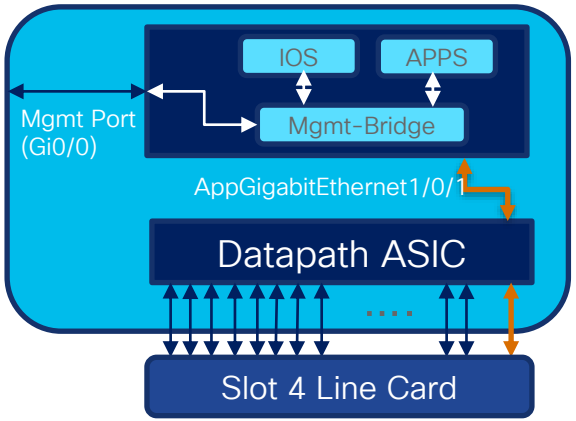
Multiple AppGigEthernet Interface with C9000X

- Use 2x 10G AppGig port individually
- EtherChannel is not support
- Mix stack with 9300 switches will disable AppGigEthernet 1/0/2



Application Hosting support on Catalyst 9410 Sup 1





- No extra physical port available on ASIC1 Core 0 to service the AppGig port (Sup1 Only)
- Enabling AppGig port by disabling Slot 4 port 48.
- 24 ports LC in Slot 4 don't require to disable port.
- Sup 2 don't have this limitation.

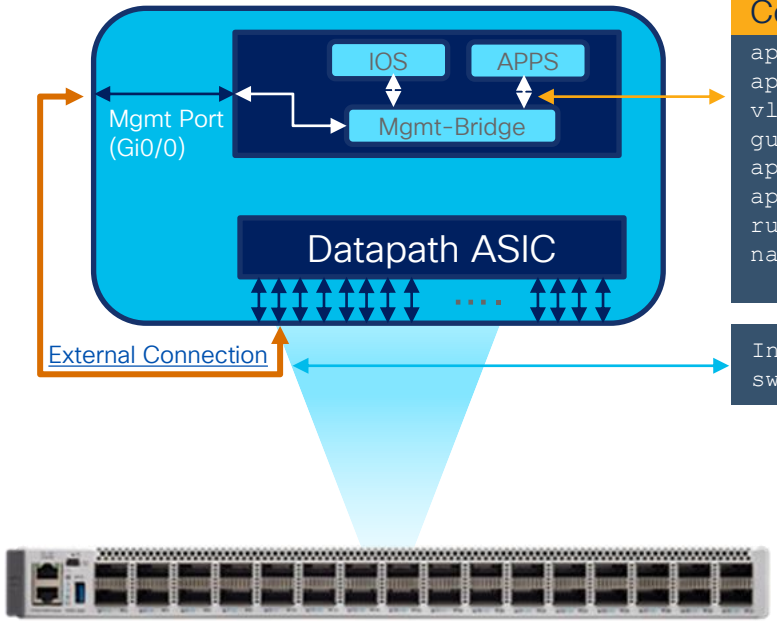
Config

```
Interface AppGigEthernet 1/0/1
enable
```

Application Hosting on C9500H

Using Front Panel Port

IOS-XE 17.5.1



Config

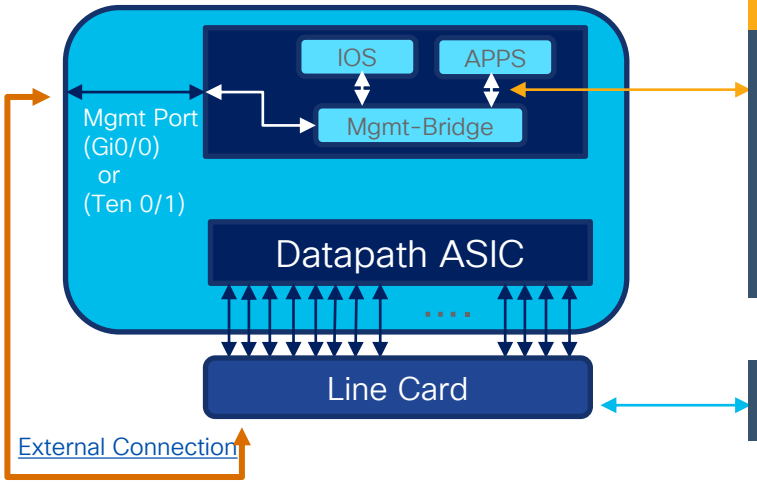
```
app-hosting appid <app_name>
app-vnic AppGigabitEthernet port 0 trunk
vlan 101 guest-interface 0
guest-ipaddress 100.1.1.252 netmask 255.255.255.0
app-default-gateway 100.1.1.251 guest-interface 0
app-resource docker
run-opts 1 "-v $(APP_DATA):/data"
name-server0 25.25.25.25
```

```
Interface HundredGigE1/0/x
switchport mode trunk
```

Application Hosting on C9600

Using Front Panel Port

IOS-XE 17.5.1



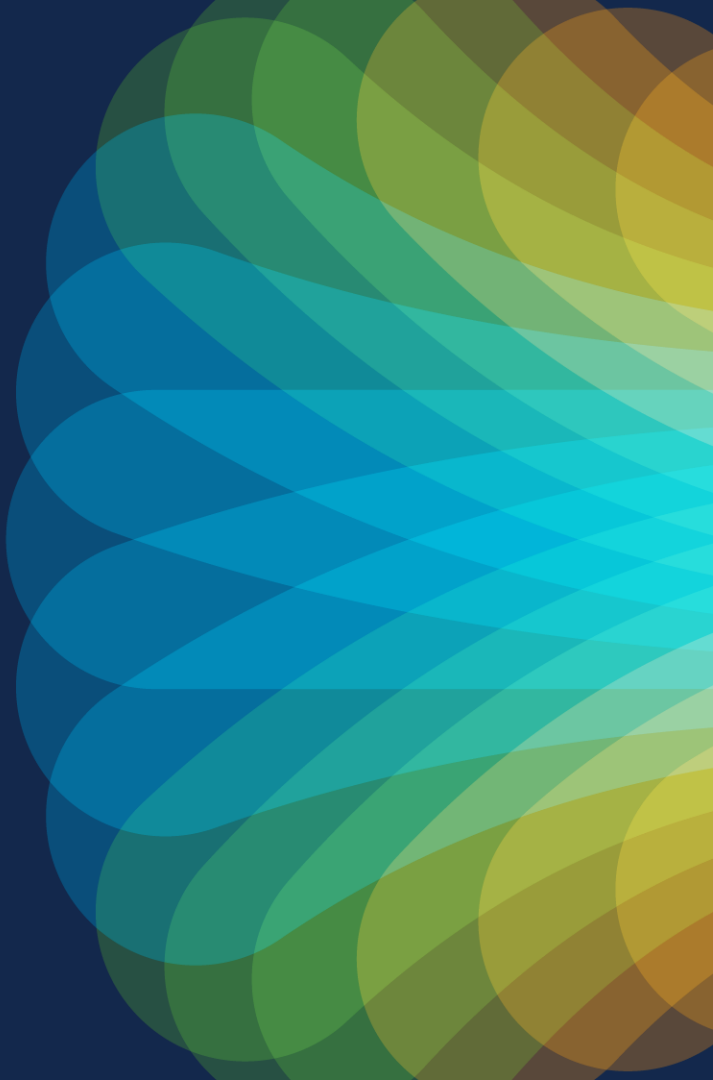
Config

```
app-hosting appid <app_name>
app-vnic AppGigabitEthernet port 0 trunk
vlan 101 guest-interface 0
guest-ipaddress 100.1.1.252 netmask 255.255.255.0
app-default-gateway 100.1.1.251 guest-interface 0
app-resource docker
run-opts 1 "-v $(APP_DATA):/data"
name-server0 25.25.25.25
```

```
Interface HundredGigE1/0/x
switchport mode trunk
```

```
app-vnic AppGigabitEthernet port 0 trunk – for G0/0
app-vnic AppGigabitEthernet port 1 trunk – for Te0/1
```

App Security



IOS XE performance and security protection

- Memory and CPU usage for Apps are bounded using Control groups (cgroups).
- Process and files access for Apps are isolated and restricted (using user namespace)
- Disk usage is isolated using separate storage.

Cgroups HW Resource Sharing

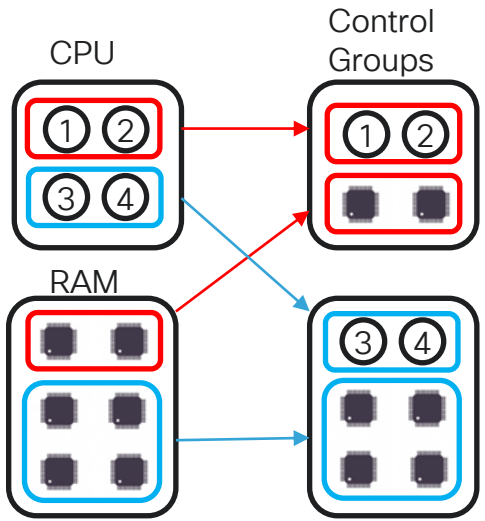
Cgroups limits Application resources for:

- System Memory
- CPU resource

System Memory: defines how much Memory available for Applications.

CPU resource: defines dynamic CPU load sharing among 3 Cgroups.

- Linux OS processes (highest priority)
- IOS-XE Control Plane
- Applications



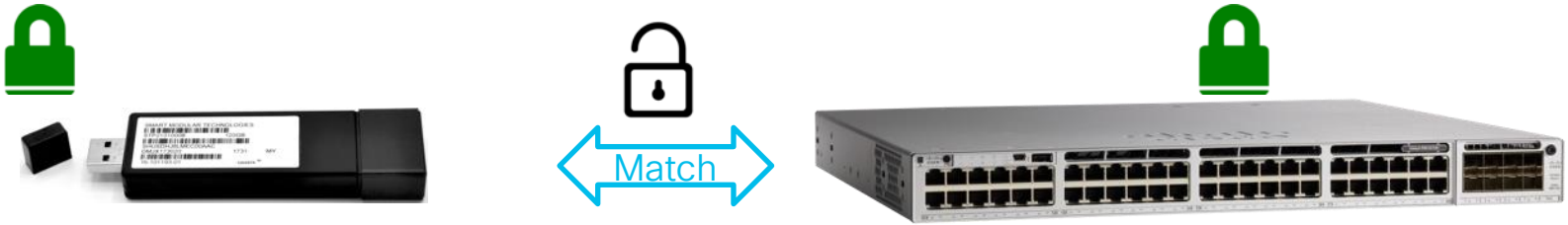
- If one cgroup is idle or under-utilizing allocation, other active cgroup(s) can be used extra CPU resources from that cgroup.
- If fully congested, each cgroup cannot exceed their CPU allocation.

Cisco Application Framework (CAF) validates available HW resources before activating Containers.

Storage Security

SSD offers two layers of security:

- AES-256 Hardware encryption on SSD
- Passcode Authentication on the switch and SSD



- Switch#hw-module switch 1 usbflash1 security ?
  disable disable security on USB3.0
  enable Enable security on USB3.0
  unlock Unlock USB3.0

Switch# conf t
Switch(config)# hw-module switch 1 usbflash1-password
Switch(config)# no hw-module switch 1 usbflash1-password

Application Development Workflow

Docker Workflow –Custom App

1 Dockerfile

```
FROM ubuntu:18.04 as base
RUN apt-get update -yq && apt-get install -yq python
COPY poll-temperature.py /usr/bin/poll-temperature.py
RUN chmod 777 /usr/bin/poll-temperature.py
CMD /usr/bin/poll-temperature.py
```

2 Build Docker Image

```
docker build -t <app> .
```

3 Deploy App

```
docker save myapp > myapp.tar
```

Application File

```
#!/usr/bin/Python
import time
import os
os.makedirs("/var/volatile/log")
f = open('/var/log/poll-temp.log', 'w')
while (1):
s = "%s %s polling temperature ...\n" %
(time.strftime("%d/%m/%Y"), time.strftime("%l:%M:%S"))
f.write(s)
f.flush()
time.sleep(5)
```

App Descriptor (Optional)

Docker Workflow – Docker Hub

1 Pull Docker Image

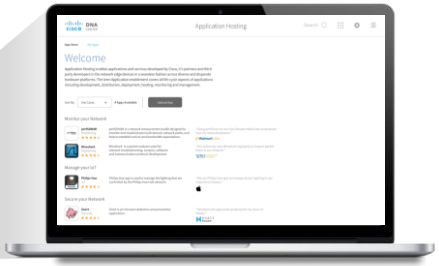
`docker pull <app>`

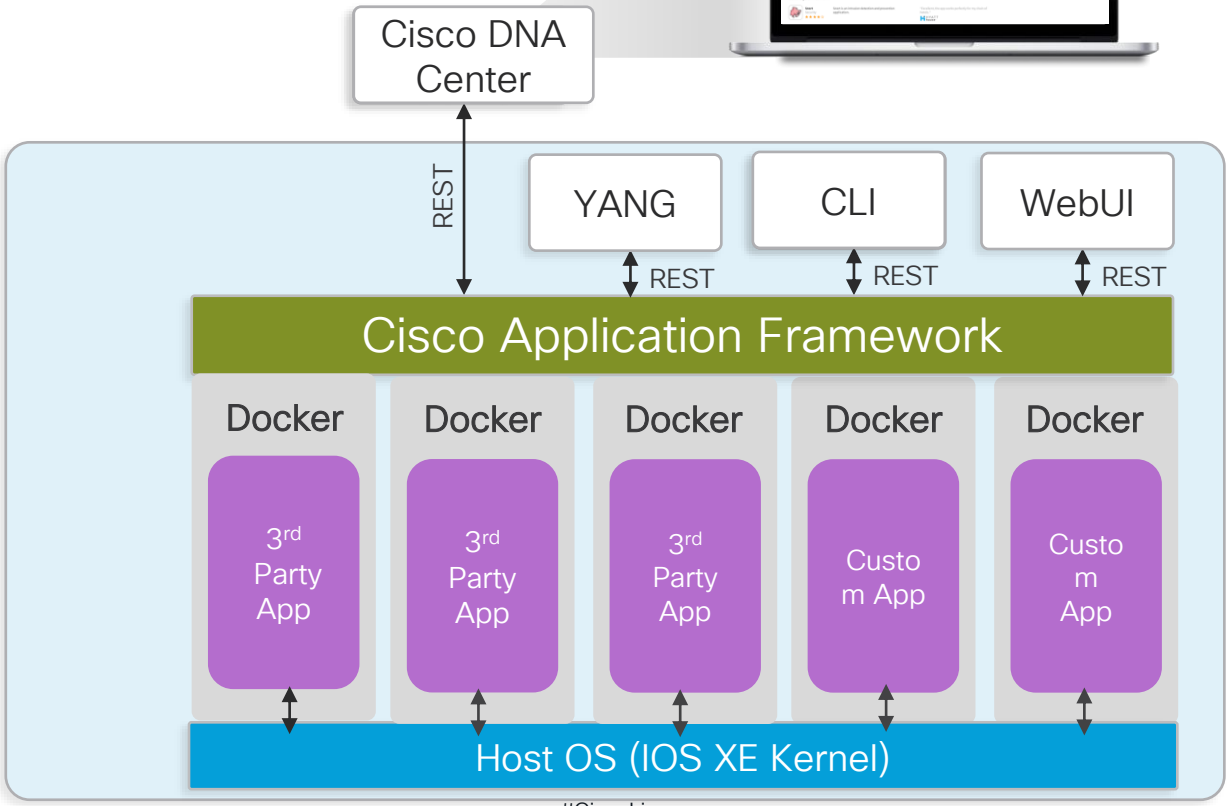
2 Deploy App

`docker save myapp > myapp.tar`

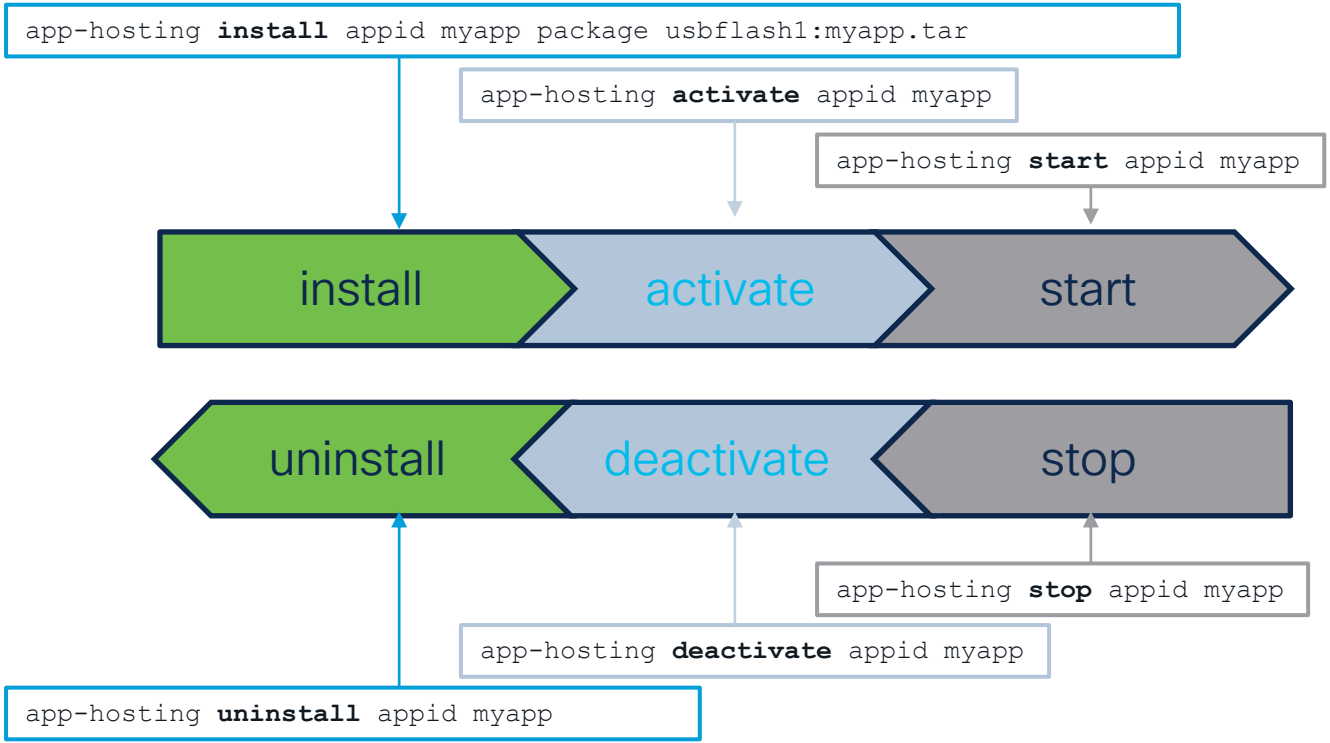
App Lifecycle Management

Application Management





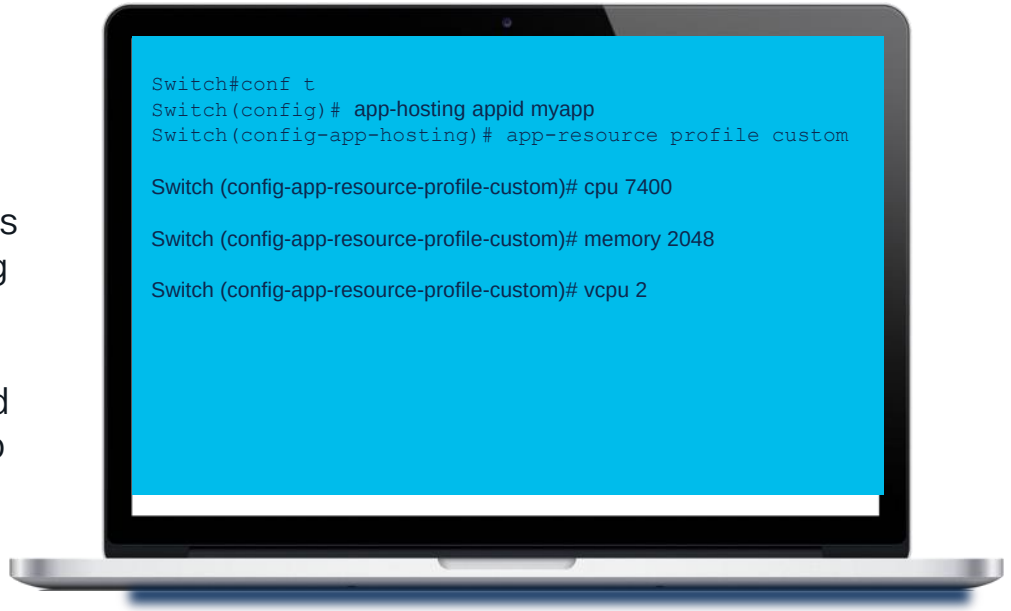
App Lifecycle Management – State Transitions



App Resources Configuration

Reserved resource specified in app package can be overridden by setting a custom resource profile

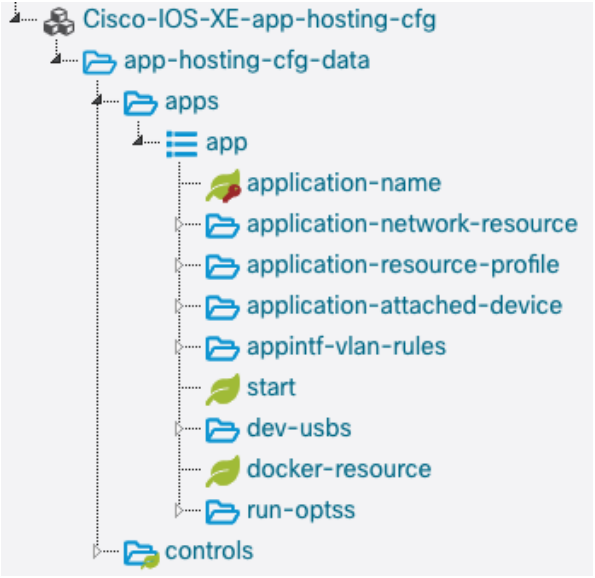
- Only cpu, memory, vcpu resource can be changed
- Application config vnic and resource changes will only take effect by the next “app-hosting activate” command.
- Resource values are application specific, and any adjustments need to ensure that the app can run reliably with the new changes.

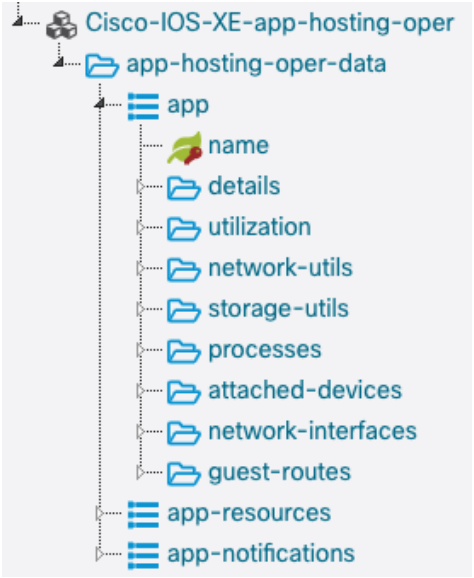


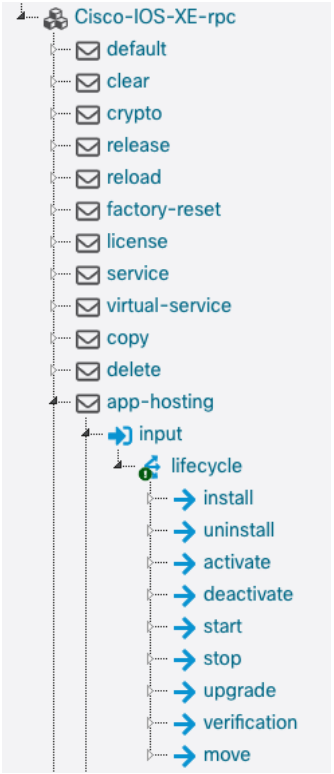
app-resource profile custom

YANG Data Models for Application Hosting

1. Cisco-IOS-XE-app-hosting-cfg.yang
2. Cisco-IOS-XE-app-hosting-oper.yang
3. Cisco-IOS-XE-rpc.yang



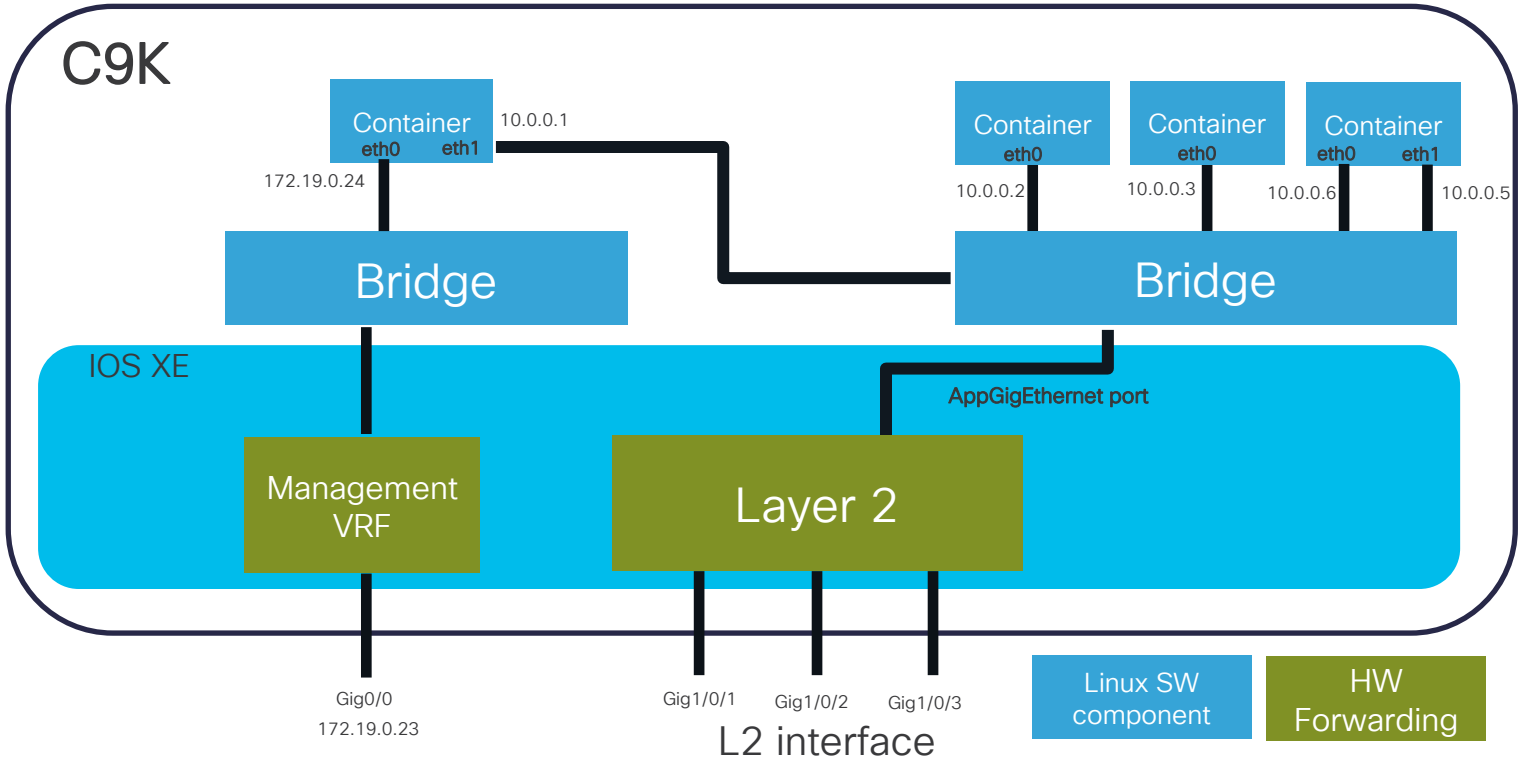




Catalyst 9000 Containers Networking

cisco Live!

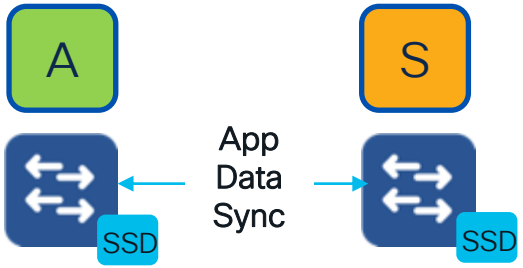
Catalyst 9000 Containers Networking



Application Hosting Features

App Hosting High Availability with Auto-Restart

- Provides cold restartability of application and the underlying app hosting framework
- Retain the last configured operational state of app in the event of system switchover or restart
- 1+1 redundancy mode
- Same storage type (Flash* or SSD) required on both Active and Standby
- Enabled by default



Supported Platforms	Release
9300 StackWise (1+1 mode only)	17.2.1
9400 Dual Sup (Single Chassis & StackWise Virtual)	17.5.1
9500/H StackWise Virtual	17.5.1
9600 Dual Sup (Single Chassis & StackWise Virtual)	17.5.1

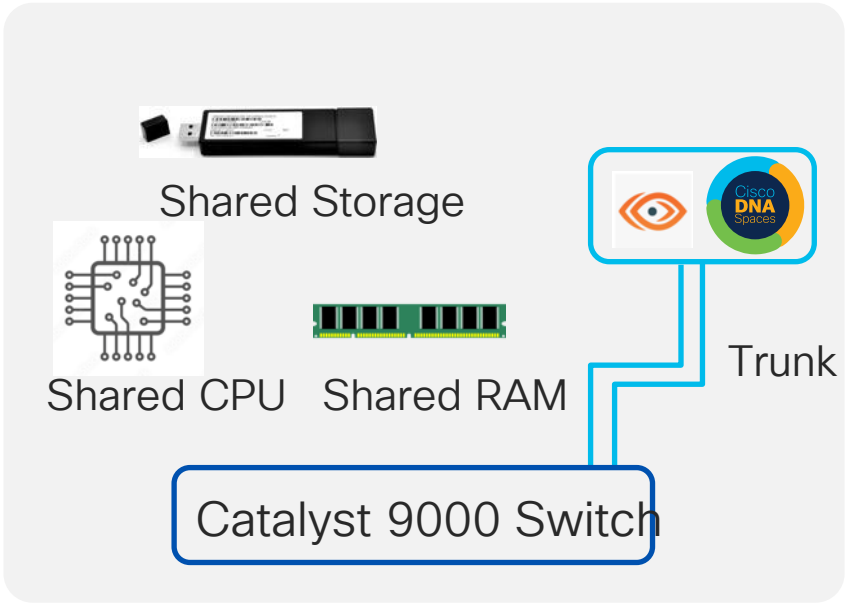
* Flash is only for Cisco Singed app

Multiple Applications Support on Catalyst 9K

17.5.1

Requirements :

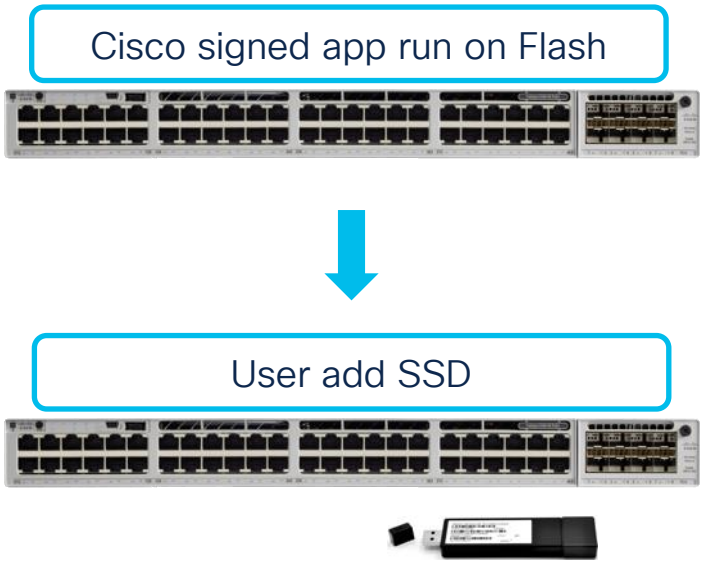
- **Cisco Signed Applications Only**
  (ex. ThousandEyes, IoT Gateway)
- Must use SSD Storage
- Enough HW resources should be available to run all applications
- AppGigabitEthernet ports config must not create a conflict between the apps



HW resource can be customized via DNA-C and CLI

Application Auto Transfer from Flash to SSD

17.6.1



- Help container as the same state as before the media change.
- Transfer all the persistent data and volumes attached to the application.
- Enabled by default
- Application partition from flash will be deleted only transfer is completed.

Transferring ThousandEyes App from Flash to SSD

Transfer Steps

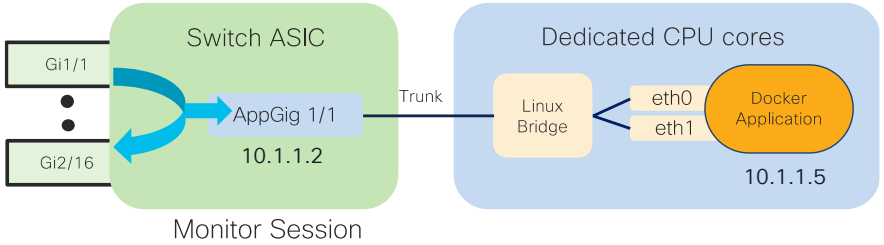
17.6.1

1. Insert SSD
2. Disable iox (no iox) and re-enable iox (iox) (or reboot the system).
3. IOX service will detect new SSD and will start transfer the app data.
   If SSD has application partition already, it will be deleted before transfer.
   If transfer failed for any reason, an error log will be shown on console and IOx service will not be started.
4. IOX service will start once transfer is completed and delete application partition from flash.

17.10.1

ERSPAN on AppGigabit Port

Some application required to get copy traffic from the switch for processing.
i.e Application required IDS/IPS capability (Cisco Cyber Vision App)



ERSPAN Source – physical interface

```
Switch(config)#monitor session 2 type  erspan-source
Switch(config-mon-erspan-src)#source interface g 1/0/3
Switch(config-mon-erspan-src)#no shut
Switch(config-mon-erspan-src)#destination
Switch(config-mon-erspan-src-dst)#ip address 10.1.1.5
Switch(config-mon-erspan-src-dst)#origin ip address 10.1.1.2
Switch(config-mon-erspan-src-dst)#erspan-id 5
```

App Port Configuration (L3 Port)

```
Switch(config)#int ap 1/0/1
Switch(config-if)#no sw
Switch(config-if)#ip address 10.1.1.2 255.255.255.0
```

ERSPAN Source – vlan interface

```
Switch(config)#monitor session 2 type  erspan-source
Switch(config-mon-erspan-src)#source interface vlan 10
Switch(config-mon-erspan-src)#no shut
Switch(config-mon-erspan-src)#destination
Switch(config-mon-erspan-src-dst)#ip address 10.1.1.5
Switch(config-mon-erspan-src-dst)#origin ip address 10.1.1.1
Switch(config-mon-erspan-src-dst)#erspan-id 5
```

App Port Configuration (L2 Port)

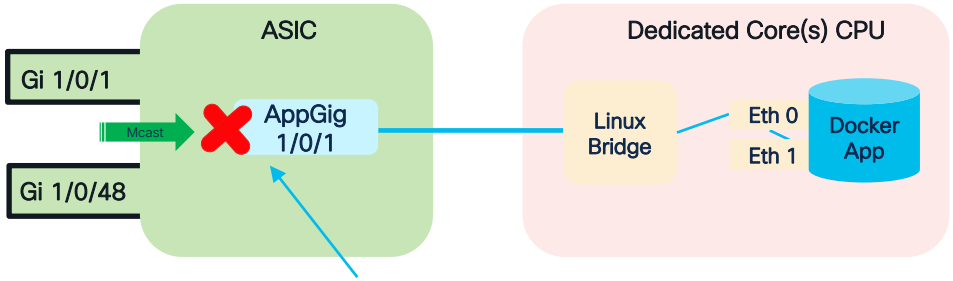
```
Switch(config)#int ap 1/0/1
Switch(config-if)# switchport mode  trunk
Switch (config-if)#exit
```

17.11.1

Multicast support in AppGig interface

By Default, C9K switch don't allow the multicast packets to be forwarded on AppGig Port.

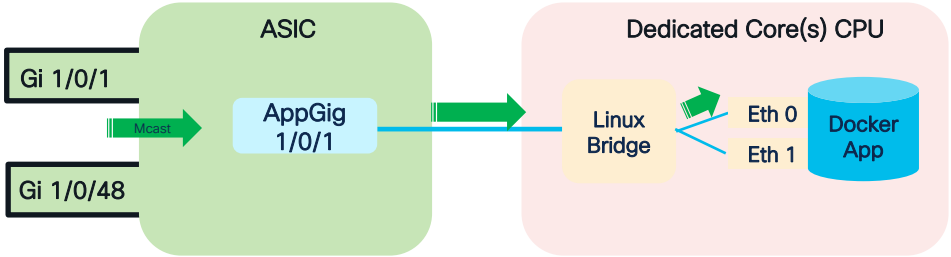
Avoiding unnecessary traffic to be forwarded to the application.



17.11.1

App Hosting Configuration for Multicast

Multicast Traffic is required for certain applications to function properly.




```
app-hosting appid Media_App
 app-vnic AppGigabitEthernet trunk
  vlan 10 guest-interface 0
   guest-ipaddress 192.168.13.2 netmask 255.255.255.0
   mirroring
   multicast
 app-default-gateway 192.168.13.1 guest-interface 0
```

Per application interface

Allow Multicast Traffic

Allowing multicast traffic to an application based on application's configuration

Additional resources

Get hands on and explore more about Application Hosting on DevNet

https://developer.cisco.com/app-hosting/

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

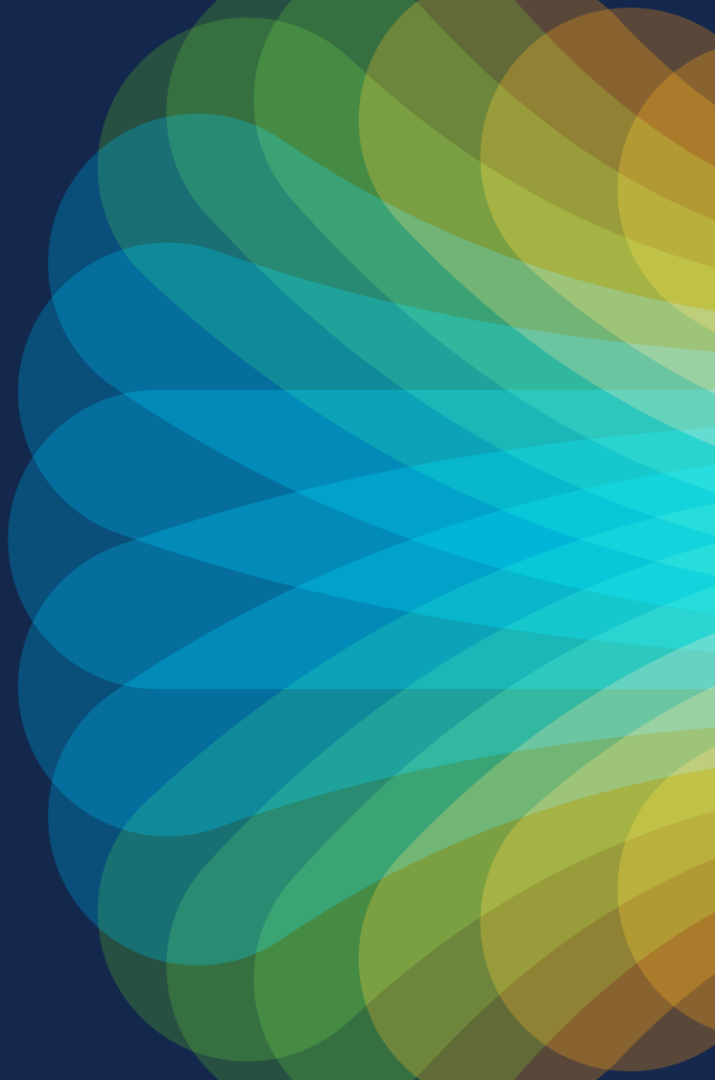
These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you



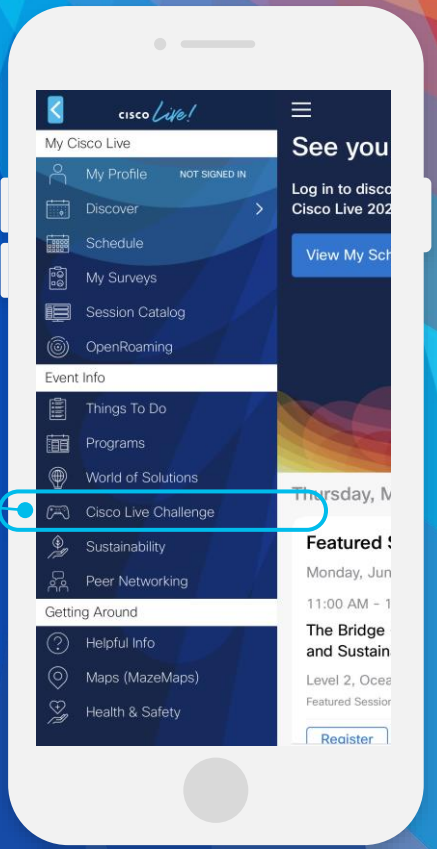
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:




cisco Live!
Let's go
#CiscoLive