cisco Live!

TURN IT UP

#CiscoLive

The bridge to possible

Catalyst 9000 IOS-XE Innovations

Dimitar Hristov, Senior Technical Marketing Engineer

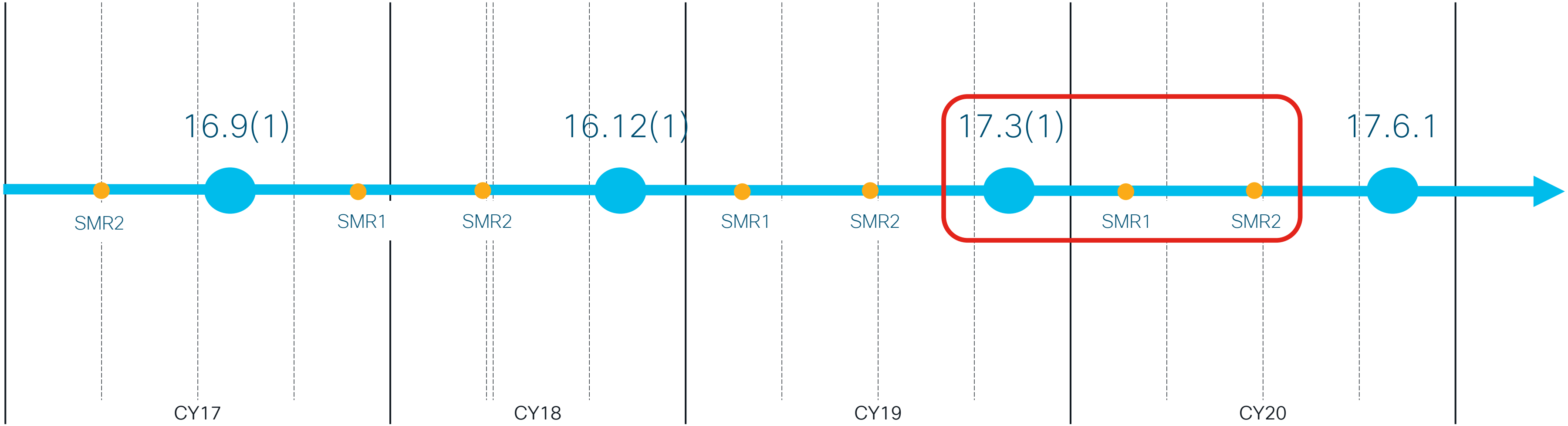
BRKENS-2004

Agenda

- Introduction
- Latest Innovations
  - Assurance
  - Zero Trust
  - Custom SDM Templates
  - SD-AVC with ETA
  - High Availability
  - Smart Licensing
- Conclusion

IOS XE Release Schedule

3 Releases Annually (every 4 months)

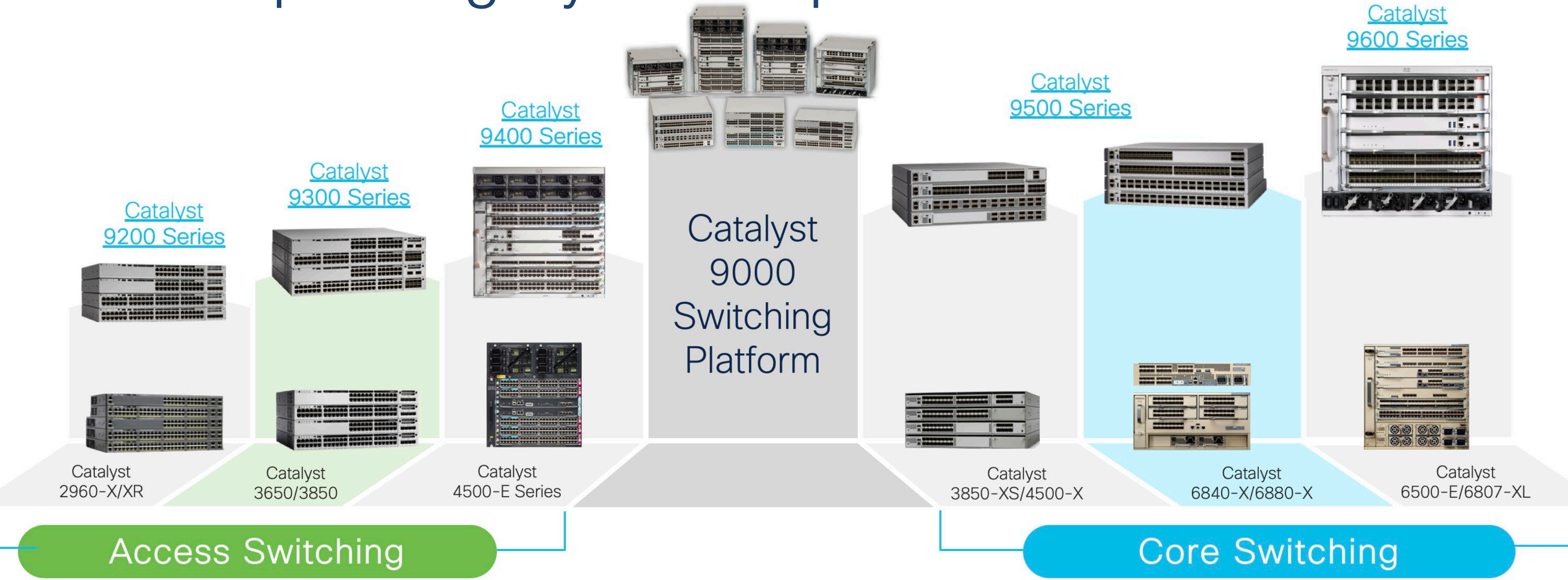


● Extended Maintenance Release ("EMR") – **36 months support.** Recommended for wide-scale production deployments – Supports patches (SMU) and ISSU*

● Standard Maintenance Release ("SMR") – **12 months support**

*Subject to change based of technical limitations

One Operating System: Open IOS-XE



Catalyst 9200 Series

Catalyst 9300 Series

Catalyst 9400 Series

Catalyst 9000 Switching Platform

Catalyst 9500 Series

Catalyst 9600 Series

Catalyst 2960-X/XR

Catalyst 3650/3850

Catalyst 4500-E Series

Catalyst 3850-XS/4500-X

Catalyst 6840-X/6880-X

Catalyst 6500-E/6807-XL

Access Switching

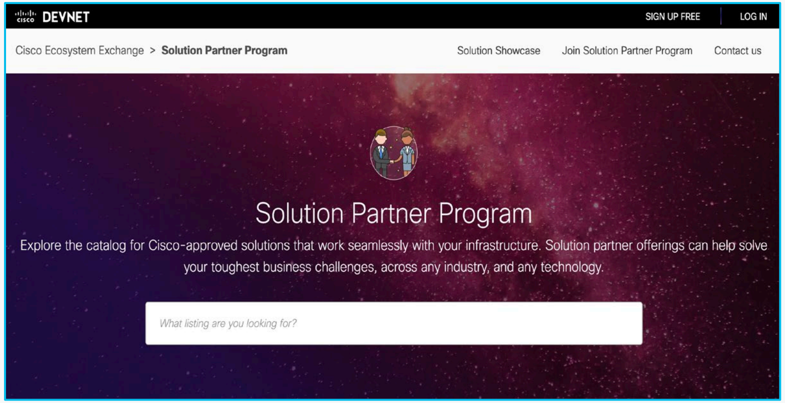
Core Switching

Open IOS-XE 17.5.1

Latest Innovations

Assurance

Catalyst 9Ks enable Industry Leading Network Visibility and Control at Scale



DEVNET

SIGN UP FREE | LOG IN

Cisco Ecosystem Exchange > **Solution Partner Program**

Solution Showcase | Join Solution Partner Program | Contact us

Solution Partner Program

Explore the catalog for Cisco-approved solutions that work seamlessly with your infrastructure. Solution partner offerings can help solve your toughest business challenges, across any industry, and any technology.

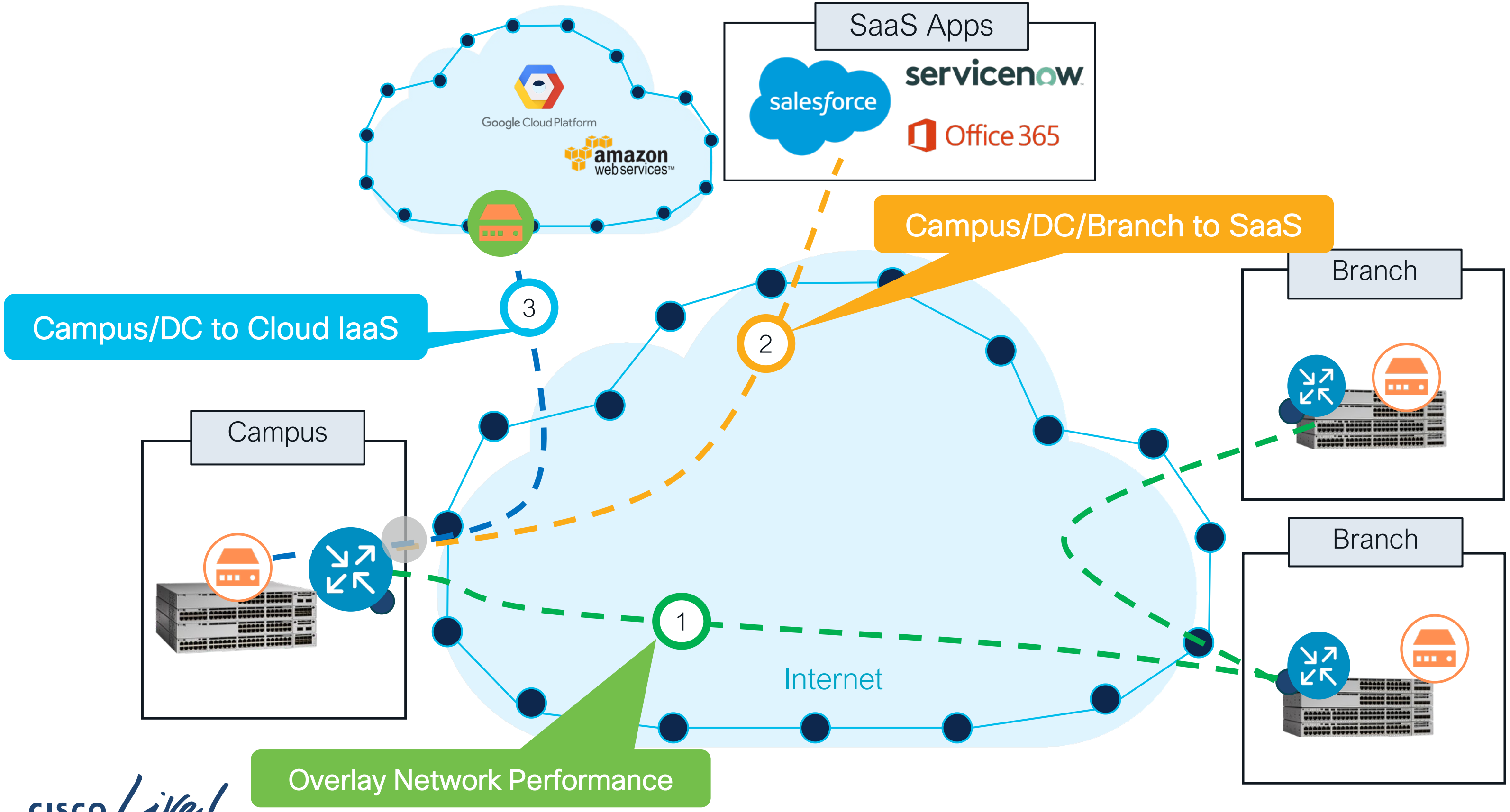
What listing are you looking for?

Thousand Eyes

Improved Service Assurance

Service Assurance is beyond the Enterprise Domain

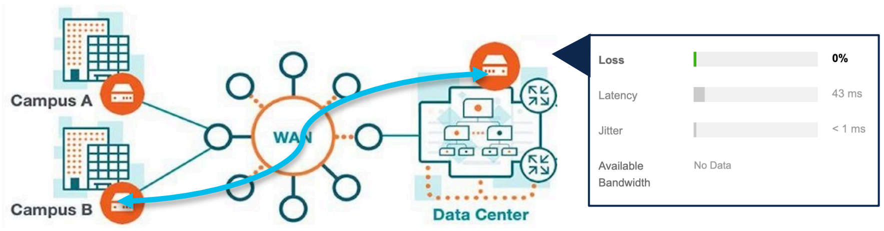
Use cases for ThousandEyes Enterprise Agent



Agent to Agent/Server

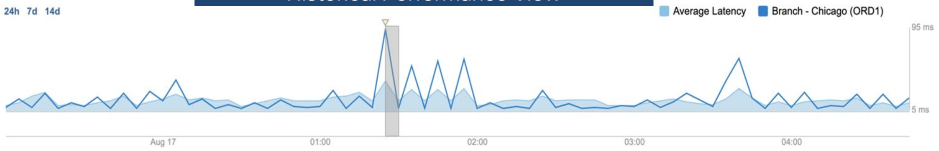
Troubleshooting SaaS & Monitoring Campus Performance

- Identifying **poor user experience**
  - Did traffic handoff to SaaS app optimally?
  - Was there an outage within Enterprise, WAN or SaaS backbone?
- **Full path visibility** to identify and resolve issues
- Active monitoring for **Latency, Loss, Bandwidth, Jitter**

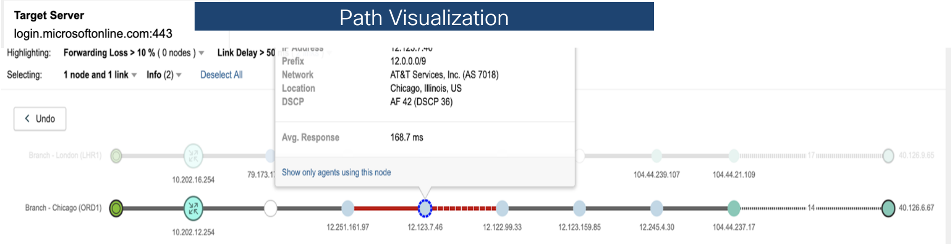


Loss		0%
Latency		43 ms
Jitter		< 1 ms
Available Bandwidth	No Data	

Historical Performance View



Path Visualization


Target Server
login.microsoftonline.com:443

Highlighting: Forwarding Loss > 10 % (0 nodes) Link Delay > 50

Selecting: 1 node and 1 link Info (2) Deselect All

IP Address	12.123.7.46
Prefix	12.0.0.0/9
Network	AT&T Services, Inc. (AS 7018)
Location	Chicago, Illinois, US
DSCP	AF 42 (DSCP 36)
Avg. Response	168.7 ms

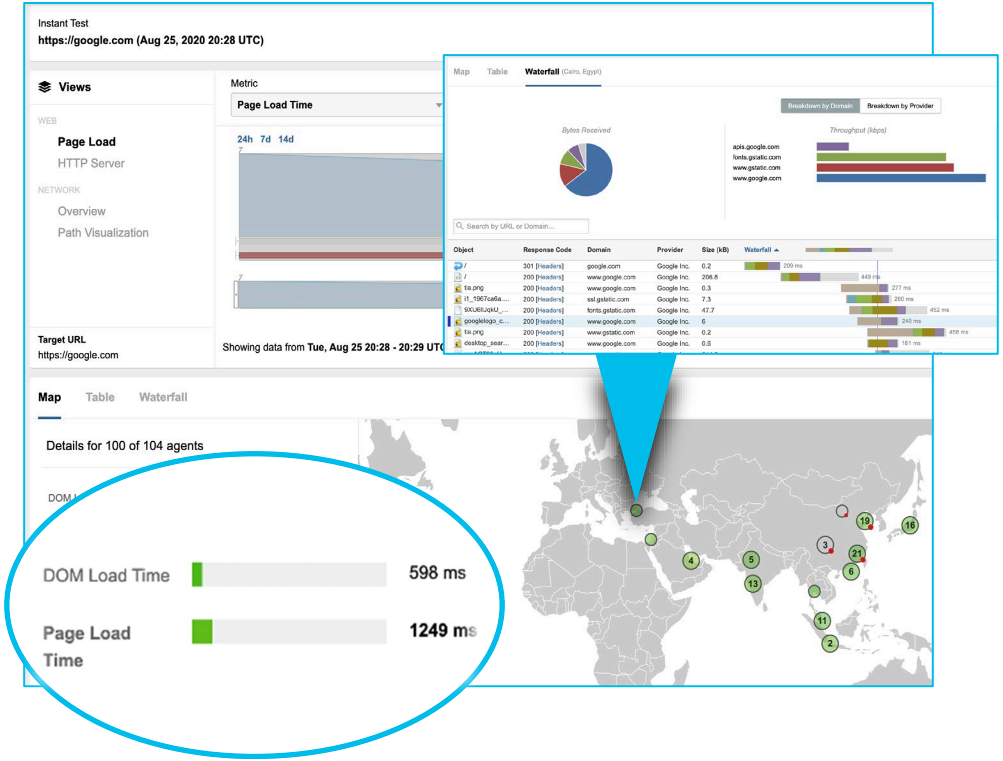
Show only agents using this node

Hop-by-hop picture of performance with Proactive Customizable Alerts

DNS and Web Performance Monitoring

DNS and Web

- **DNS Tests** – Server, Trace, DNSSEC
- In-depth metrics regarding the **in-browser user experience** with waterfall chart
- Identify objects preventing or **prolonging page load** completion
- **HTTP Server Performance**
  - Availability
  - Response Time
  - Throughput



Instant Test
https://google.com (Aug 25, 2020 20:28 UTC)

Views
WEB
Page Load
HTTP Server
NETWORK
Overview
Path Visualization

Metric
Page Load Time

24h 7d 14d

Target URL
https://google.com

Showing data from **Tue, Aug 25 20:28 - 20:29 UTC**

Map | Table | Waterfall

Details for 100 of 104 agents

DOM Load Time 598 ms

Page Load Time 1249 ms

Map | Table | **Waterfall** (Cairo, Egypt)

Breakdown by Domain | Breakdown by Provider

Bytes Received

Throughput (kbps)

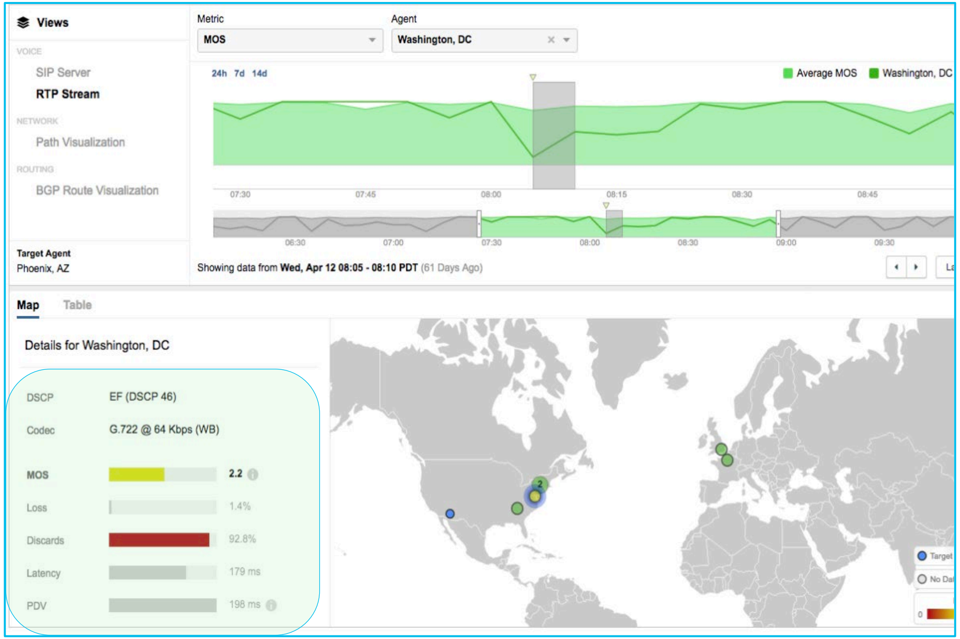
apis.google.com
fonts.gstatic.com
www.gstatic.com
www.google.com

Search by URL or Domain...

Object	Response Code	Domain	Provider	Size (kB)	Waterfall ▲
/	301 [Headers]	google.com	Google Inc.	0.2	209 ms
/	200 [Headers]	www.google.com	Google Inc.	206.8	449 ms
tia.png	200 [Headers]	www.google.com	Google Inc.	0.3	277 ms
i1_1967ca6a....	200 [Headers]	ssl.gstatic.com	Google Inc.	7.3	260 ms
9XU6IlJqkU_...	200 [Headers]	fonts.gstatic.com	Google Inc.	47.7	452 ms
googlelogo_c...	200 [Headers]	www.google.com	Google Inc.	6	240 ms
tia.png	200 [Headers]	www.gstatic.com	Google Inc.	0.2	458 ms
desktop_sear...	200 [Headers]	www.google.com	Google Inc.	0.6	181 ms

Troubleshooting VOIP

- VoIP packets are **extremely susceptible** to underlying network conditions that traditional VoIP monitors can't detect
- **Simulate VoIP calls** between Enterprise Agents in branch office
- Measure **SIP and RTP server availability.**



Target Agent
Phoenix, AZ

Metric: MOS

Agent: Washington, DC

Showing data from **Wed, Apr 12 08:05 - 08:10 PDT** (61 Days Ago)

Details for Washington, DC

DSCP EF (DSCP 46)

Codec G.722 @ 64 Kbps (WB)

MOS 2.2

Loss 1.4%

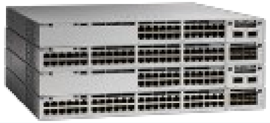
Discards 92.8%

Latency 179 ms

PDV 198 ms

Platform Support for ThousandEyes Agent

For Your Reference



Catalyst 9300
Catalyst 9300L

w/ IOS 17.3.3

Catalyst 9400

w/ IOS 17.5.1

	HW Specification
Type	Light Weight Docker
CPU	1-2 vCPU
RAM	1-2 GB
Flash Storage	1 GB App Data

ThousandEyes Agent preload on Flash

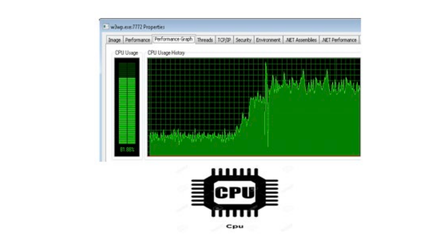
Automated Issue Resolution with Machine Reasoning Engine

DNAC 2.1.2

Power Supply Failure

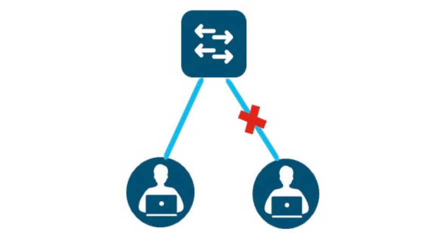
- Power starvation
- Power supply with no input power
- Power supply missing

High CPU Utilization



- Broadcast of a lot of data traffic on network causes excessive use of CPU resources

Interface Flap

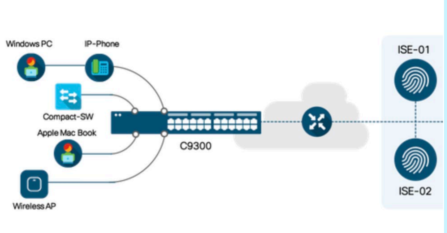


- Flap errors/ CRC Errors
- Interface connectivity loss
- Faulty optics

New

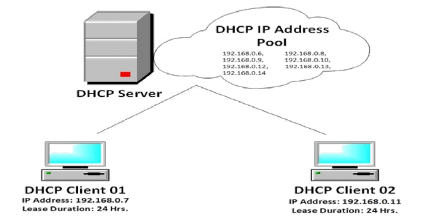
DNAC

Authentication Failure



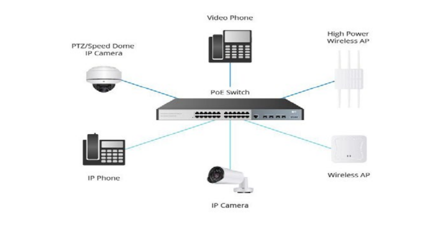
- Dot1x/MAB configuration methods missing
- Credential failure
- Ping to ISE failure

DHCP Reachability Failure



- Mac Address not present in IPDT
- Discover packets has not been punted
- Multiple logical routes b/w DHCP server & clients

POE Power Overdraw



- IEEE non-compliant powered device request power more than the standard
- PoE Imax errors

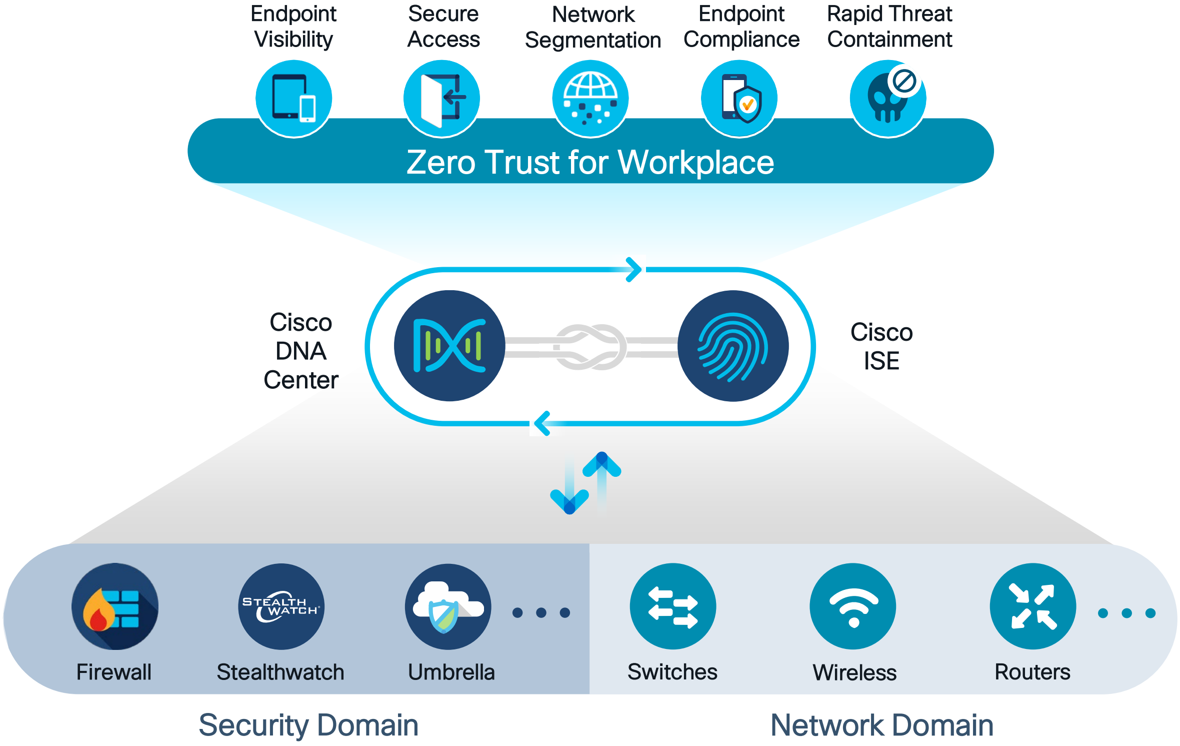
Zero-Trust

Zero-Trust for Workplace Framework

Simplicity: Simplify security operations through automation

Efficacy: Strengthen workplace defenses with security integrations

Efficiency: Increase efficiency of security services by leveraging network context



Catalyst 9K - Cloud Security Services enabled switch

Secure Access

- Isolate Peer Endpoints
- URL Based Access Control
- Intelligent Device Classification

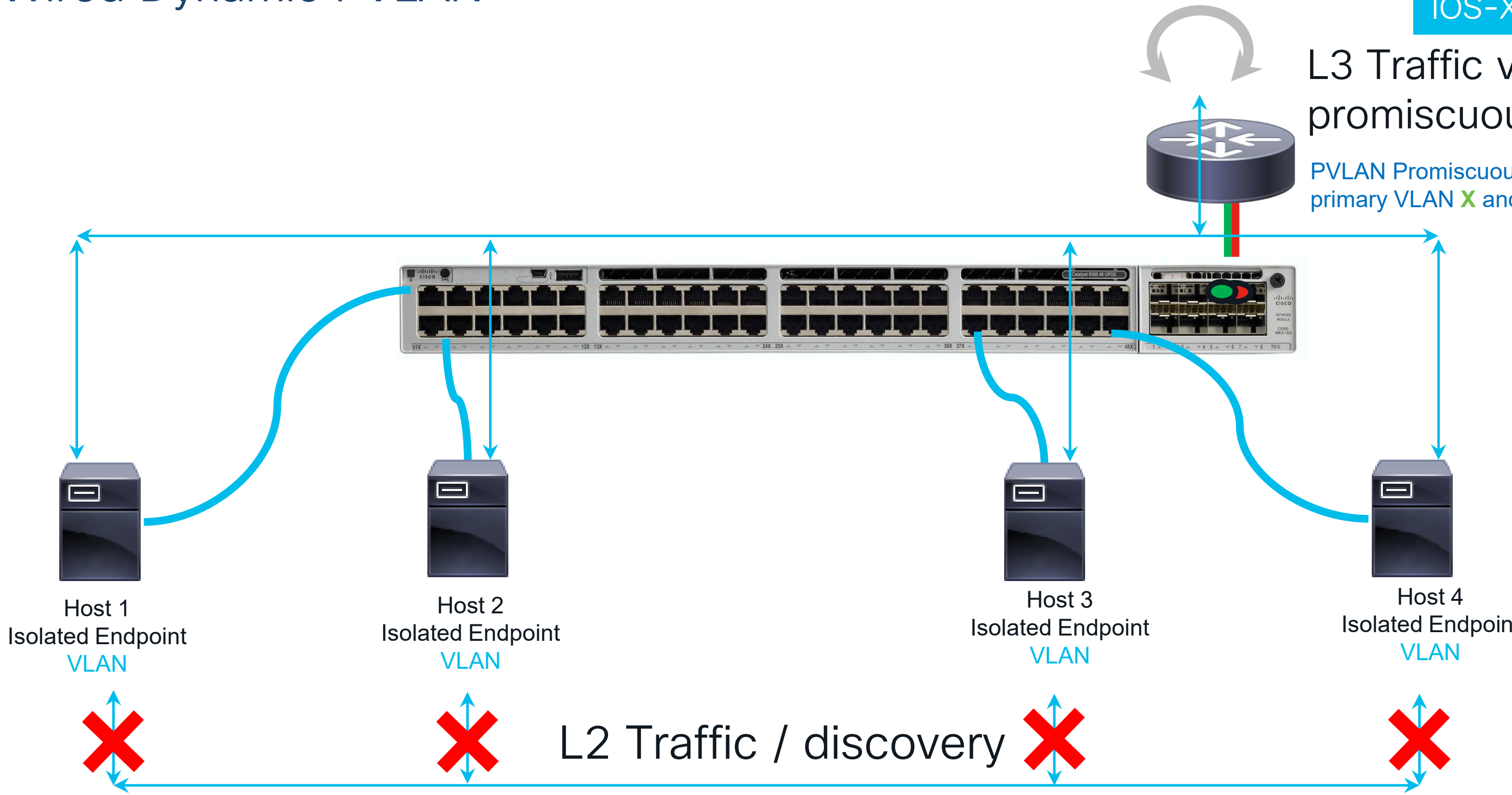
Cloud Security Services

- Secure RADIUS over Public Networks
- DNS based threat protection
- Detect anomalies in traffic with limited resources

Isolate Peer Endpoints – Zero Trust at Access

Wired Dynamic PVLAN

IOS-XE 17.5.1 EFT



L3 Traffic via promiscuous only

PVLAN Promiscuous Trunk carrying primary VLAN X and Y

Host 1
Isolated Endpoint
VLAN

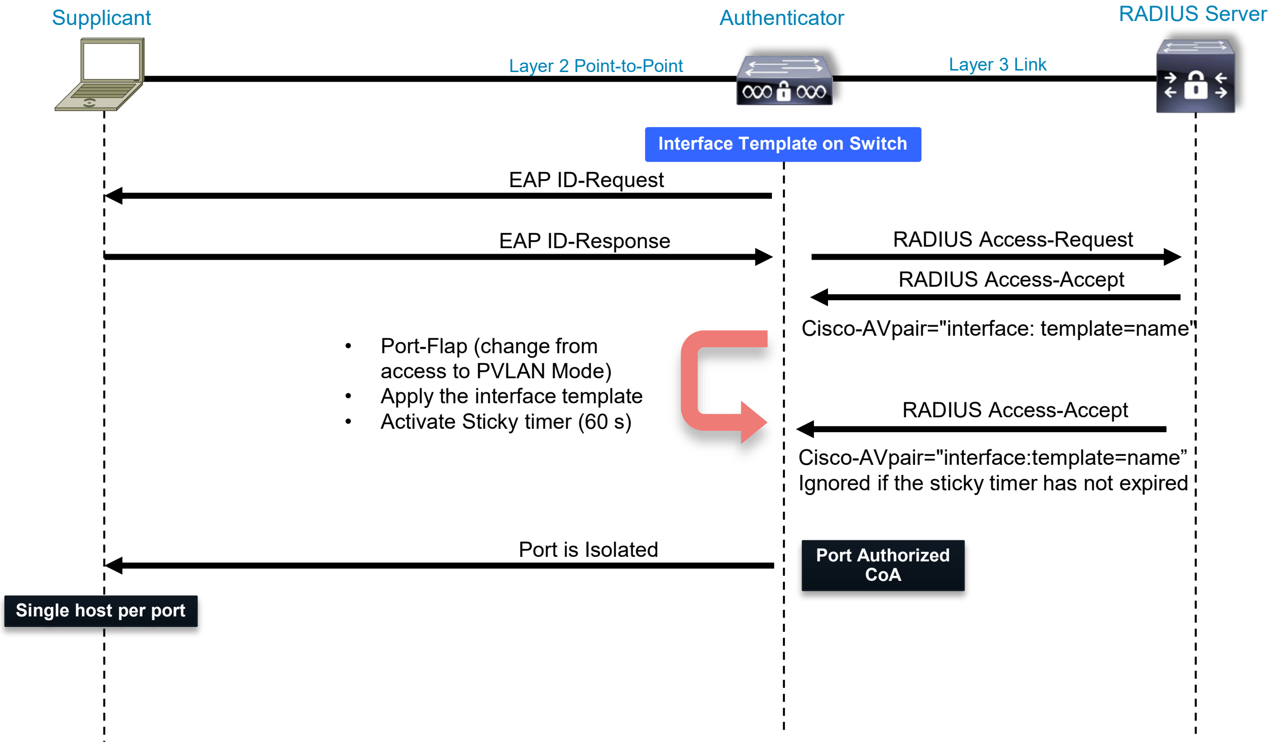
Host 2
Isolated Endpoint
VLAN

Host 3
Isolated Endpoint
VLAN

Host 4
Isolated Endpoint
VLAN

L2 Traffic / discovery

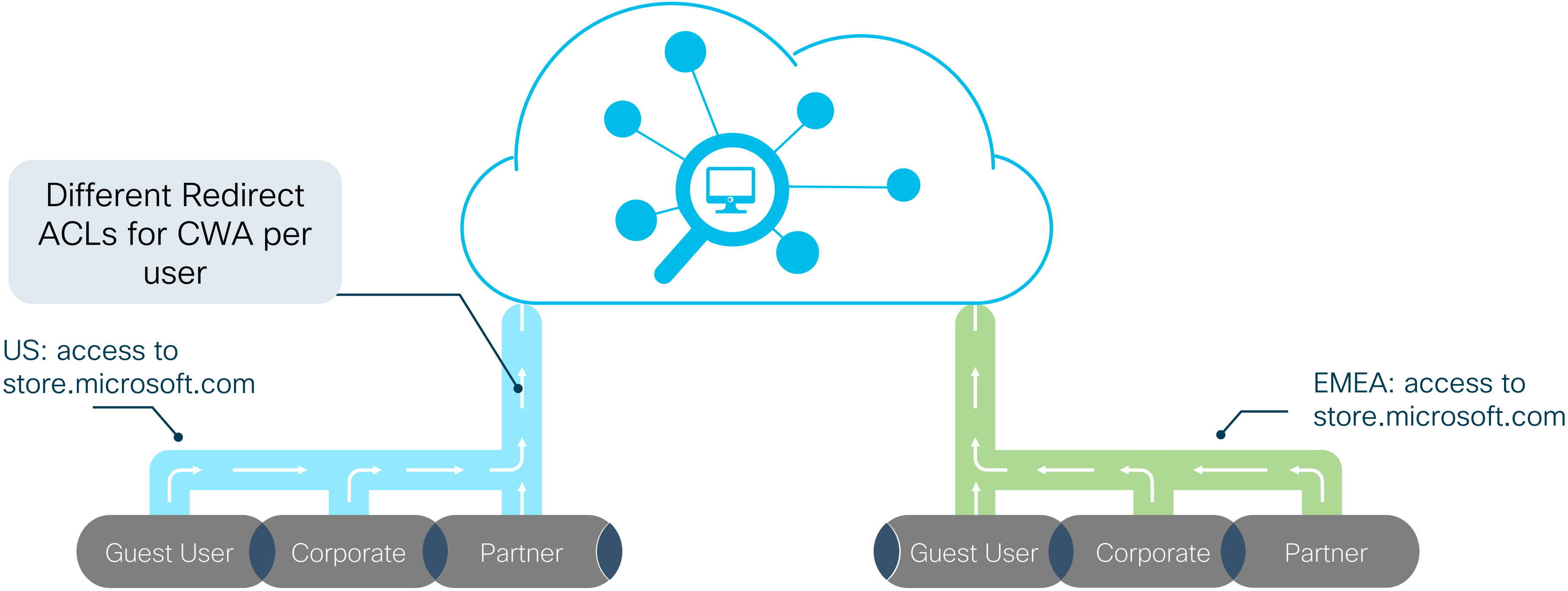
How does Wired Dynamic PVLAN work?



- Port-Flap (change from access to PVLAN Mode)
- Apply the interface template
- Activate Sticky timer (60 s)

IP Based Access Management is complex due to SaaS/Cloud

Simplified URL based access control needed



Different Redirect ACLs for CWA per user

US: access to store.microsoft.com

EMEA: access to store.microsoft.com

FQDN Redirect ACL for CWA

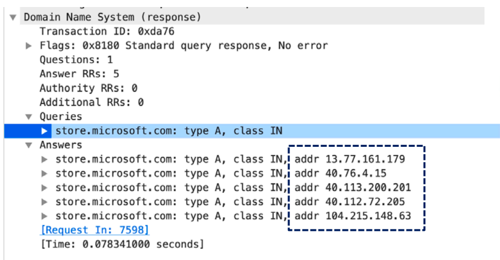
Simplified Redirect ACL Configurations

IOS-XE 17.4.1

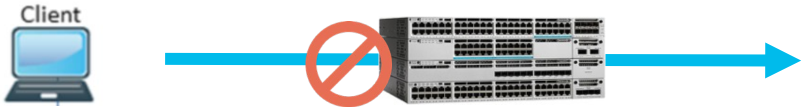
```
ip access-list redirect-CWA
   290 deny ip any host 40.126.0.69
   300 deny ip any host 40.126.0.65
   310 deny ip any host 40.126.0.67
   320 deny ip any host 20.190.134.98
   330 permit ip any host 40.126.6.65
   340 permit ip any host 20.190.134.96
   350 permit ip any host 40.126.6.0
   ….
```

Traditional IP based ACLs

DNS for store.microsoft.com



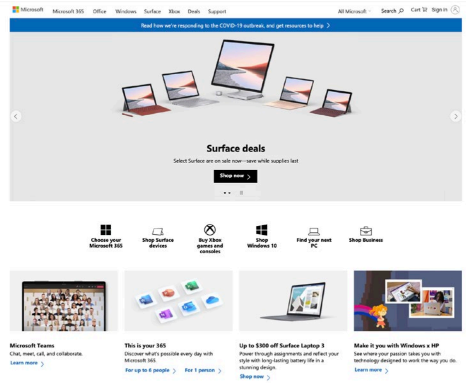
```
▼ Domain Name System (response)
    Transaction ID: 0xda76
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 5
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ store.microsoft.com: type A, class IN
  ▼ Answers
    ▶ store.microsoft.com: type A, class IN, addr 13.77.161.179
    ▶ store.microsoft.com: type A, class IN, addr 40.76.4.15
    ▶ store.microsoft.com: type A, class IN, addr 40.113.200.201
    ▶ store.microsoft.com: type A, class IN, addr 40.112.72.205
    ▶ store.microsoft.com: type A, class IN, addr 104.215.148.63
    [Request In: 7598]
    [Time: 0.078341000 seconds]
```



NEW FQDN Based ACLs

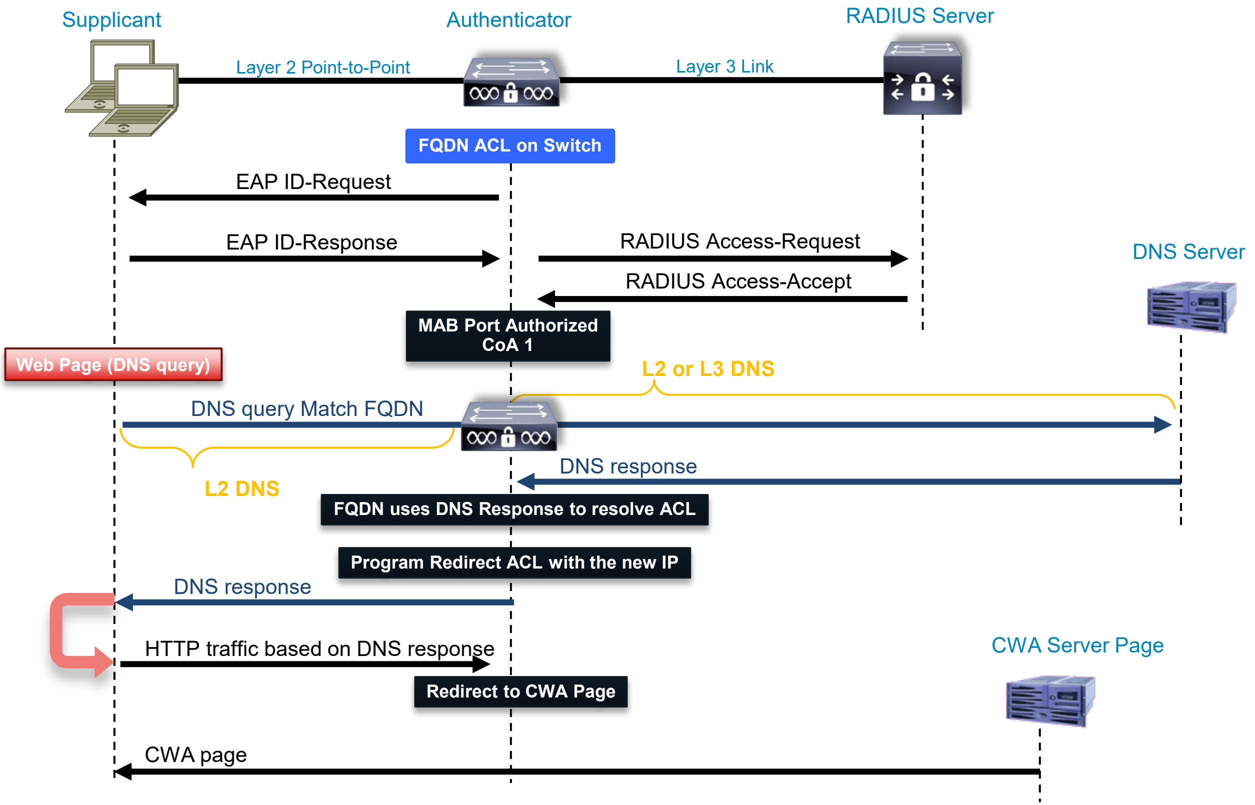
```
ip access-list fqdn redirect-CWA
  10 deny ip any host dynamic store.microsoft.com
  20 deny ip any host dynamic office.microsoft.com
  30 permit ip any host dynamic guests.microsoft.com
```

store.microsoft.com



- Configure Redirect ACL entry with the domain name instead of IP
- The IP address is dynamically learned from DNS response and programmed in the hardware
- No configuration changes needed when IP changed under the domain name

How it works in 17.5(1)?



Supplicant

Authenticator

RADIUS Server

Layer 2 Point-to-Point

Layer 3 Link

FQDN ACL on Switch

EAP ID-Request

EAP ID-Response

RADIUS Access-Request

RADIUS Access-Accept

DNS Server

MAB Port Authorized
CoA 1

Web Page (DNS query)

L2 or L3 DNS

DNS query Match FQDN

DNS response

L2 DNS

FQDN uses DNS Response to resolve ACL

Program Redirect ACL with the new IP

DNS response

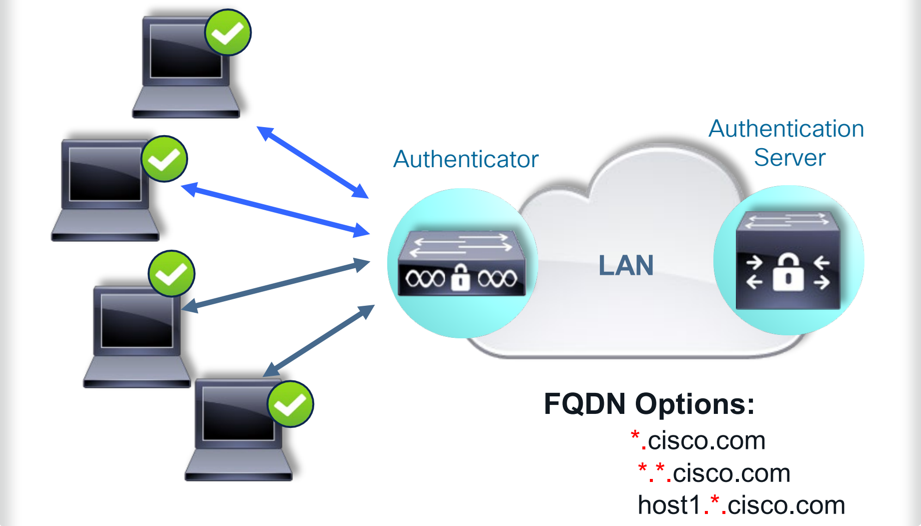
HTTP traffic based on DNS response

CWA Server Page

Redirect to CWA Page

CWA page

FQDN extensions in 17.5(1) ...

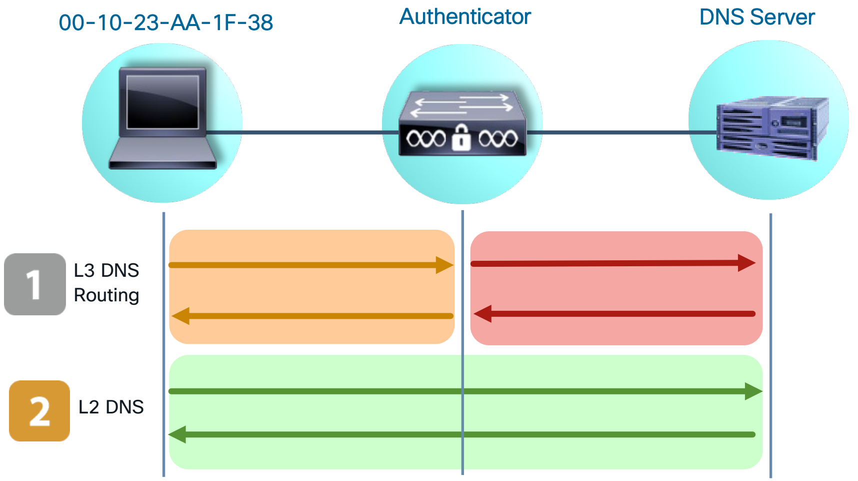


FQDN Options:

*.cisco.com

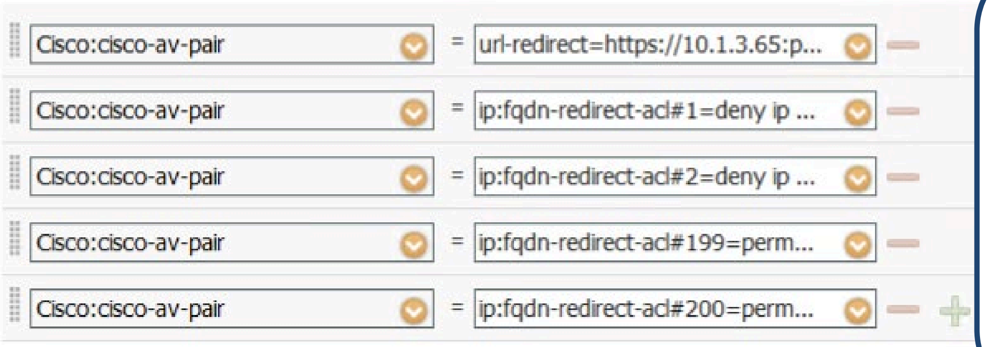
..cisco.com

host1.*.cisco.com



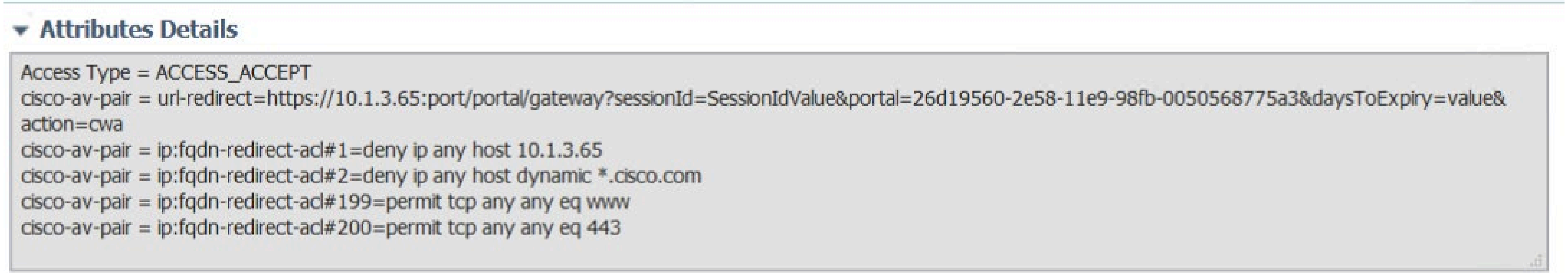
Wildcard maks "*" to match multiple hosts = | L3 DNS Queries

Support for AV-PAIRs



```
Cisco:cisco-av-pair = url-redirect=https://10.1.3.65:p...
Cisco:cisco-av-pair = ip:fqdn-redirect-acl#1=deny ip ...
Cisco:cisco-av-pair = ip:fqdn-redirect-acl#2=deny ip ...
Cisco:cisco-av-pair = ip:fqdn-redirect-acl#199=perm...
Cisco:cisco-av-pair = ip:fqdn-redirect-acl#200=perm...
```

- Central Redirect ACL Management
- Support on any RADIUS
- Per User Session
- Higher TCAM consumption



Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect=https://10.1.3.65:port/portal/gateway?sessionId=SessionIdValue&portal=26d19560-2e58-11e9-98fb-005056875a3&daysToExpiry=value&
action=cwa
cisco-av-pair = ip:fqdn-redirect-acl#1=deny ip any host 10.1.3.65
cisco-av-pair = ip:fqdn-redirect-acl#2=deny ip any host dynamic *.cisco.com
cisco-av-pair = ip:fqdn-redirect-acl#199=permit tcp any any eq www
cisco-av-pair = ip:fqdn-redirect-acl#200=permit tcp any any eq 443
```

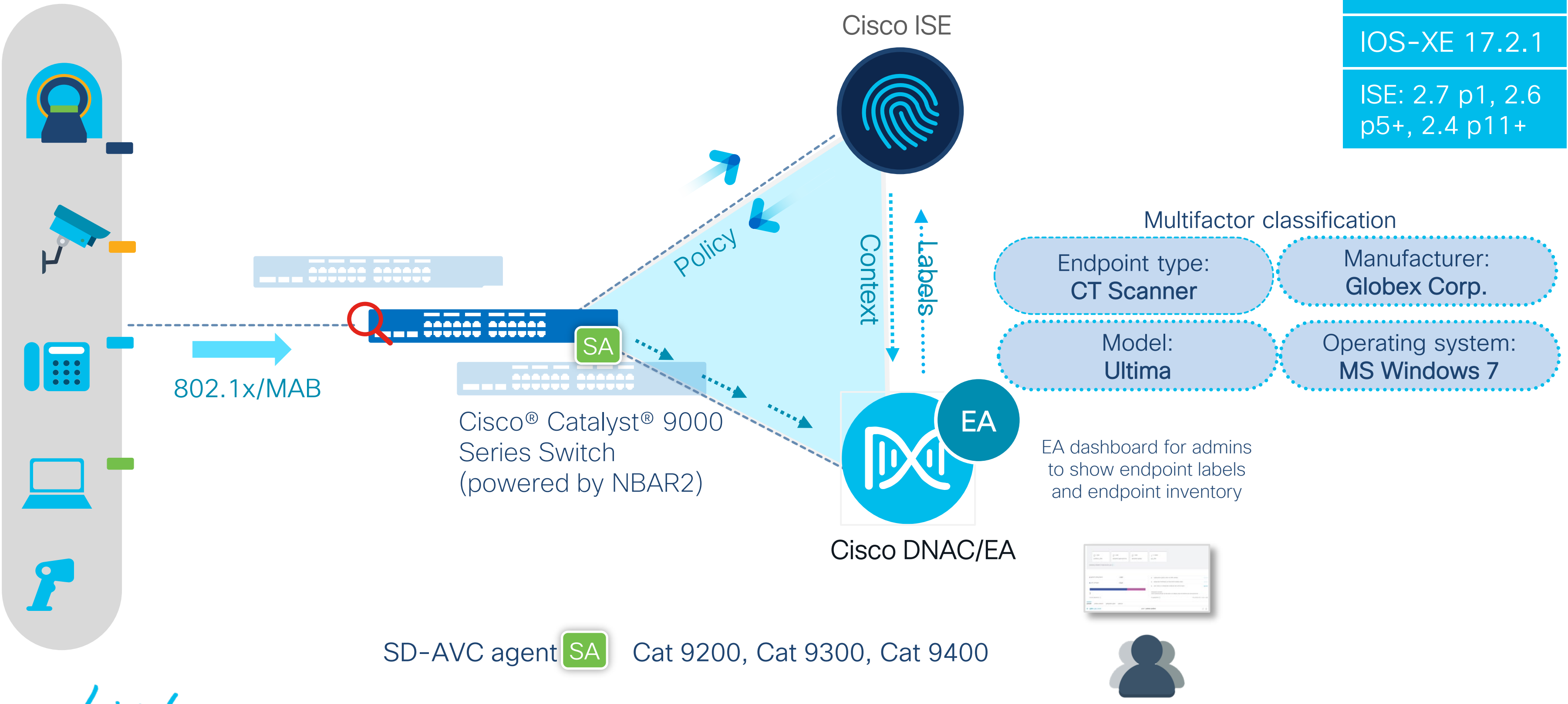
AI Endpoint Analytics

Identify Endpoints, Enforce Policies, and Stop Threats

DNAC 2.1.1.3

IOS-XE 17.2.1

ISE: 2.7 p1, 2.6 p5+, 2.4 p11+



Multifactor classification

Endpoint type: **CT Scanner**	Manufacturer: **Globex Corp.**
Model: **Ultima**	Operating system: **MS Windows 7**

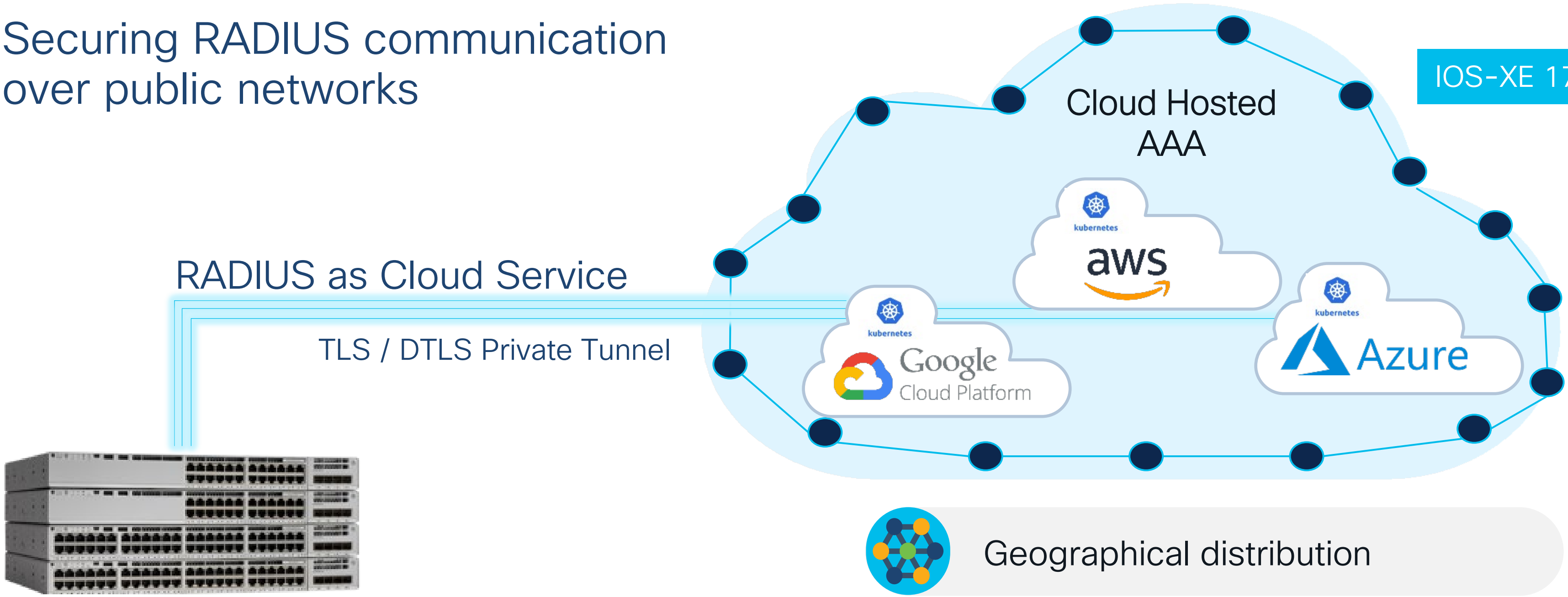
EA dashboard for admins to show endpoint labels and endpoint inventory

SD-AVC agent SA Cat 9200, Cat 9300, Cat 9400

RadSec

Securing RADIUS communication over public networks

IOS-XE 17.4.1



Cisco® Catalyst® 9000 Series Switches
Open IOS-XE 17.4.1

- Geographical distribution
- Cloud redundancy and availability
- Data at transit Encrypted

Umbrella Integration with Catalyst 9200/9300

Network Enforced DNS Security

Hosts can not bypass DNS Security

Trace Source of Anomaly

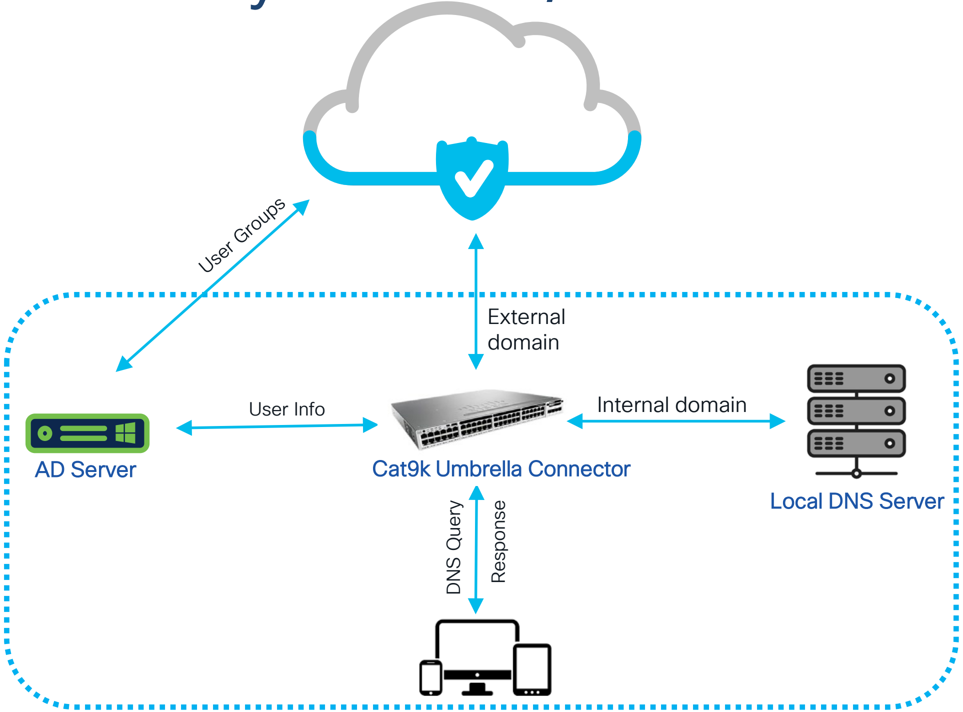
Switch shares User and device login information
Switch shares Local IP address

Granular DNS policies

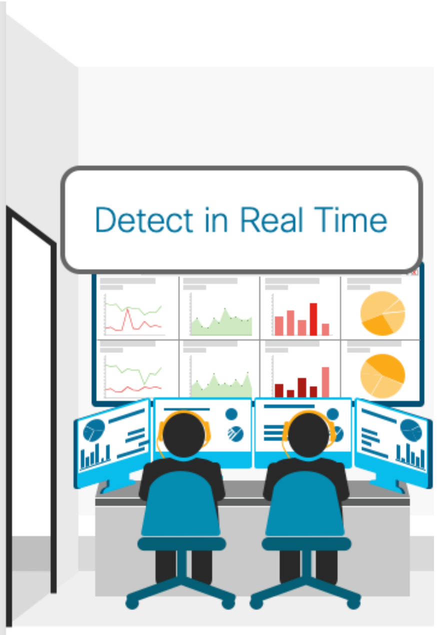
Tag based polices – Static interface config
AD Group based policies – Dynamic

Split Domain

local domain DNS queries to internal DNS Server
External domain DNS queries to Umbrella Cloud



Why need Switch to Stealthwatch Cloud?



Usecase: Lateral Movement and Data exfiltration

Usecase: The careless employee compromised credentials

Usecase: The unskilled employee with privileged access

Usecase: The angry employee malicious insider

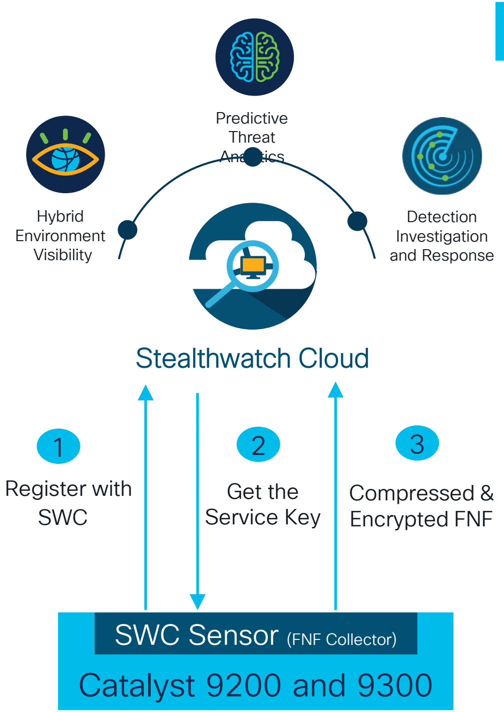
Usecase: The victimized employee compromised credentials

Native Stealthwatch Cloud Sensor on C9K

Add Advanced Cloud Security to your network

IOS-XE 17.5.1

- Easy Registration
- Simplified FNF configuration
- No additional devices/VMs - Inbuilt FNF Collector
- Consumes less WAN Bandwidth – ZIP Compressed FNF records
- Secure communication – HTTPS encrypted FNF traffic

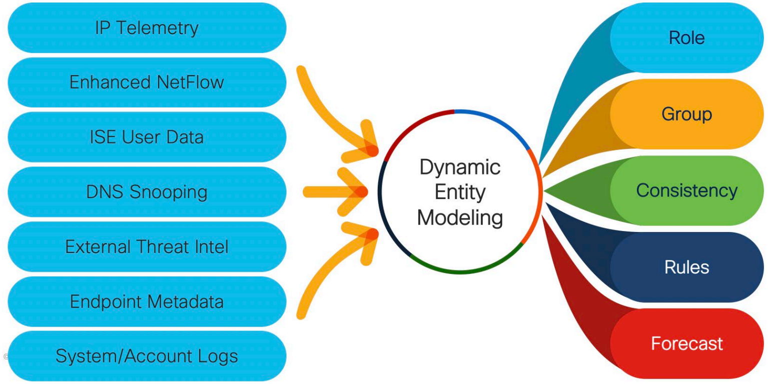


Discounted SWC licenses with DNA-Premier

Dynamic entity modeling for High Alert Fidelity

95% Stealthwatch Cloud alerts rated as “helpful” by customers

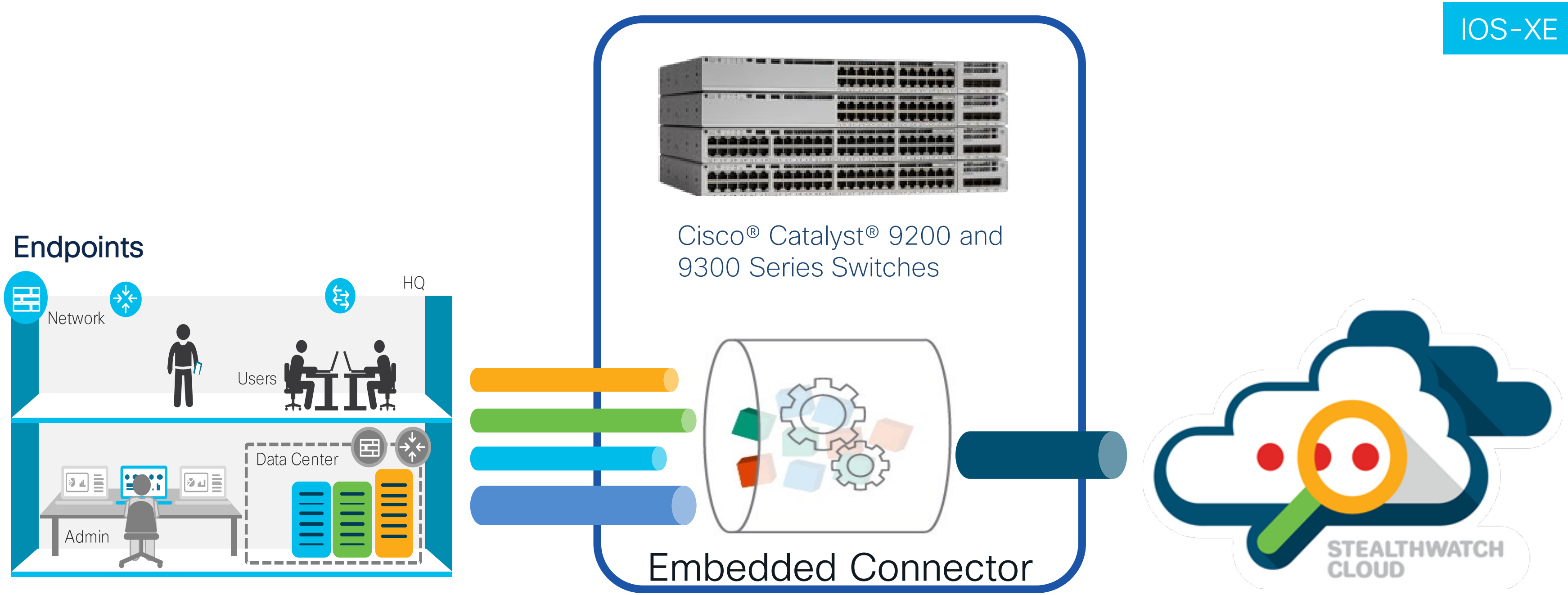
Machine Learning based Analytics



- Excessive failed access attempts
- DDoS and amplification attacks
- Potential data exfiltration
- Geographically unusual remote access
- Connection to a suspicious destination
- Custom segmentation and configuration policies

Stealthwatch Cloud Sensor on Cat 9K

IOS-XE 17.5.1



Available on Cisco Catalyst 9200 and 9300 Switches

Custom SDM Templates

C9K provides most flexible design and HA options

Platform

- ✓ Modularity
- ✓ Speed
- ✓ Power
- ✓ POE
- ✓ Wireless
- ✓ ASIC Customization
- ✓ Scale

Design Options

- ✓ SDA
- ✓ BGP-EVPN
- ✓ MPLS

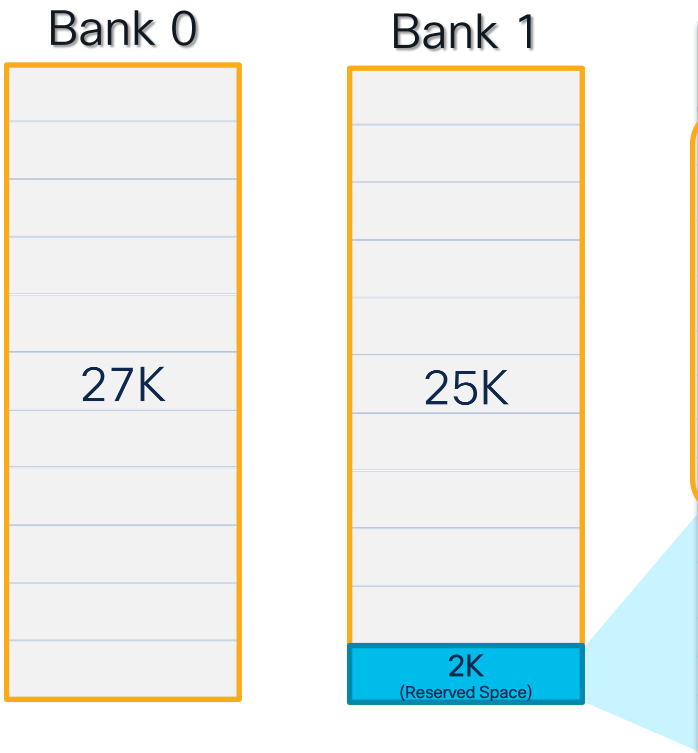
High Availability

- ✓ StackWise
- ✓ StackWise Virtual
- ✓ NSF/SSO
- ✓ ISSU
- ✓ GIR
- ✓ NSR/IPFRR
- ✓ Quad SUP RPR
- ✓ xFSU

Mix-Match to build the best Infra for your needs

ACL Scale Considerations

IOS-XE 17.4.1



ACL Features

Feature	Scale Values (Min – Max)	Default Value	Step Size	Customizable
Ingress ACL	4K – 26K, **27K**	4K	2K	Y
Egress ACL	4K – 26K, **27K**	4K	2K	Y
Ingress QoS	1K, 2K - **16K**	1K	2K	Y
Egress QoS	1K, 2K - **16K**	1K	2K	Y
PBR/NAT	1K, 2K - **16K**	1K	2K	Y
LISP	1K - **2K**	1K	1K	Y
Tunnels	1K - **3K**	1K	1K	Y
NFL ACL	1K – **2K**	1K	1K	Y
Ingress SPAN	NA	0.5K	NA	N
Egress SPAN	NA	0.5K	NA	N
CPP	NA	0.5K	NA	N
Sec. Assoc	NA	0.5K	NA	N
Macsec SPD	NA	0.25K	NA	N

Customized Scale on Catalyst 9500H/9600

Custom SDM Templates for Deployment Flexibility

UADP 3.0

IOS-XE 17.4.1

Custom Template FIB IOS-XE 17.3

New

Custom Template TCAM IOS-XE 17.4

Feature		Distribution	Core (default)	NAT
Routes (IPv4/IPv6)		114K/114K	212K/212K	212K/212K
Multicast routes (IPv4/IPv6)		16K/16K	32K/32K	32K/32K
MAC address table		82K	32K	32K
IGMP/MLD snooping		2K	2K	2K
Flexible NetFlow (Ingress)		49K/ASIC	32K/ASIC	32K/ASIC
Flexible NetFlow (Egress)		49K/ASIC	32K/ASIC	32K/ASIC
SGT label		32K	32K	32K
Security ACL	Ingress	12K		12K
	Egress	15K		8K
QOS ACL	Ingress	8K		4K
	Egress	8K		4K
NetFlow ACL	Ingress	1K		1K
	Egress	1K		1K
SPAN	Ingress	0.5K		0.5K
	Egress	0.5K		0.5K
PBR/NAT		3K		15.5K
CPP		1K		1K
Tunnel termination and MACsec		3K		2K
LISP		1K		1K

🟦 Higher scale

✕ Customizable resources

ACL Scale Customization - Allocation Examples

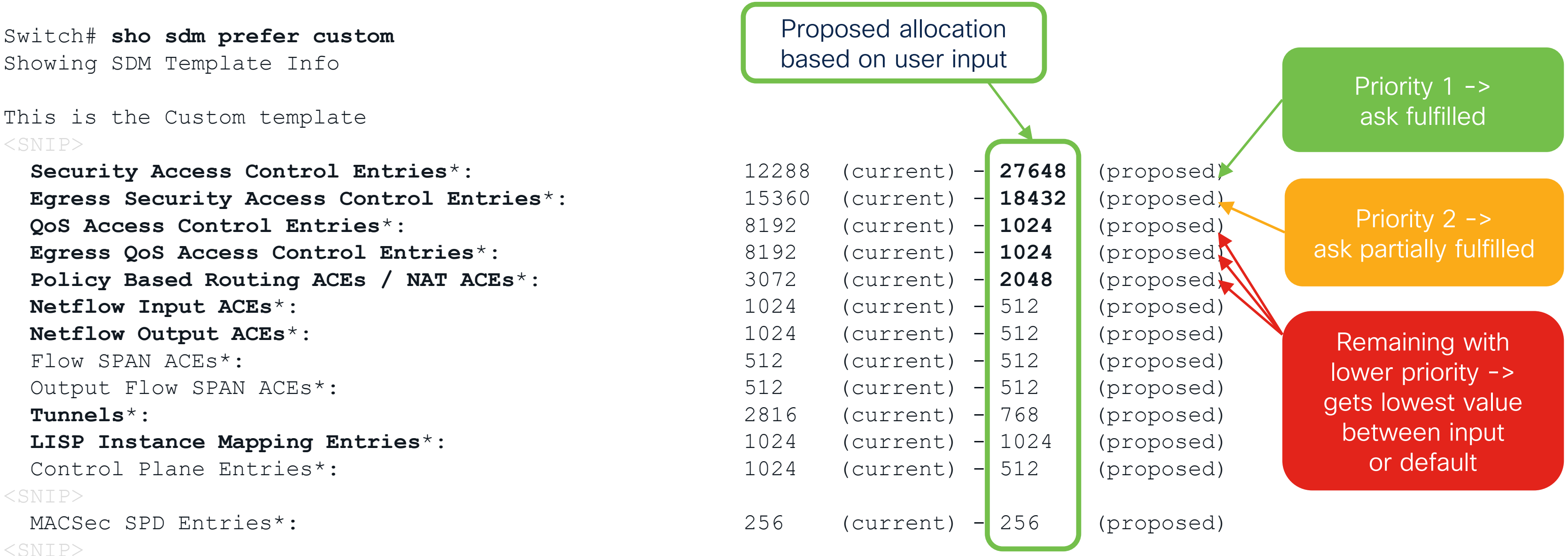
IOS-XE 17.4.1

	Customer 1 **Security focus**	Customer 2 **QoS focus**	Customer 3 **NAT focus**
Security - Input	**27K**	6K	12K
Security - Output	**18K**	6K	8K
QoS - Input	1K	**16K**	6K
QoS - Output	1K	**16K**	4K
PBR/NAT	2K	3K	**16K**
LISP	1K	2K	2K
Tunnels	1K	2K	1K
Netflow ACL	1K	1K	1K
Total Resources *	**54K**		

* 2K entries are reserved for System

1K - 1024
16K - 16384

ACL Customization – view proposed allocation



```
Switch# sho sdm prefer custom
Showing SDM Template Info

This is the Custom template
<SNIP>
  Security Access Control Entries*:                       12288   (current) - 27648  (proposed)
  Egress Security Access Control Entries*:                15360   (current) - 18432  (proposed)
  QoS Access Control Entries*:                            8192    (current) - 1024   (proposed)
  Egress QoS Access Control Entries*:                     8192    (current) - 1024   (proposed)
  Policy Based Routing ACEs / NAT ACEs*:                  3072    (current) - 2048   (proposed)
  Netflow Input ACEs*:                                    1024    (current) - 512    (proposed)
  Netflow Output ACEs*:                                   1024    (current) - 512    (proposed)
  Flow SPAN ACEs*:                                        512     (current) - 512    (proposed)
  Output Flow SPAN ACEs*:                                 512     (current) - 512    (proposed)
  Tunnels*:                                               2816    (current) - 768    (proposed)
  LISP Instance Mapping Entries*:                         1024    (current) - 1024   (proposed)
  Control Plane Entries*:                                 1024    (current) - 512    (proposed)
<SNIP>
  MACSec SPD Entries*:                                    256     (current) - 256    (proposed)
<SNIP>

(*) values can be modified by sdm cli
The proposed values will take effect post reload.

Switch#
```

Proposed allocation based on user input

Priority 1 -> ask fulfilled

Priority 2 -> ask partially fulfilled

Remaining with lower priority -> gets lowest value between input or default

Input:
- ACL Ing (1): 27K
- ACL Egr (2): 20K
- PBR/NAT (3): 3K
- QOS Ing (4): 4K
- QOS Egr (5): 4K

Total Input: 58K

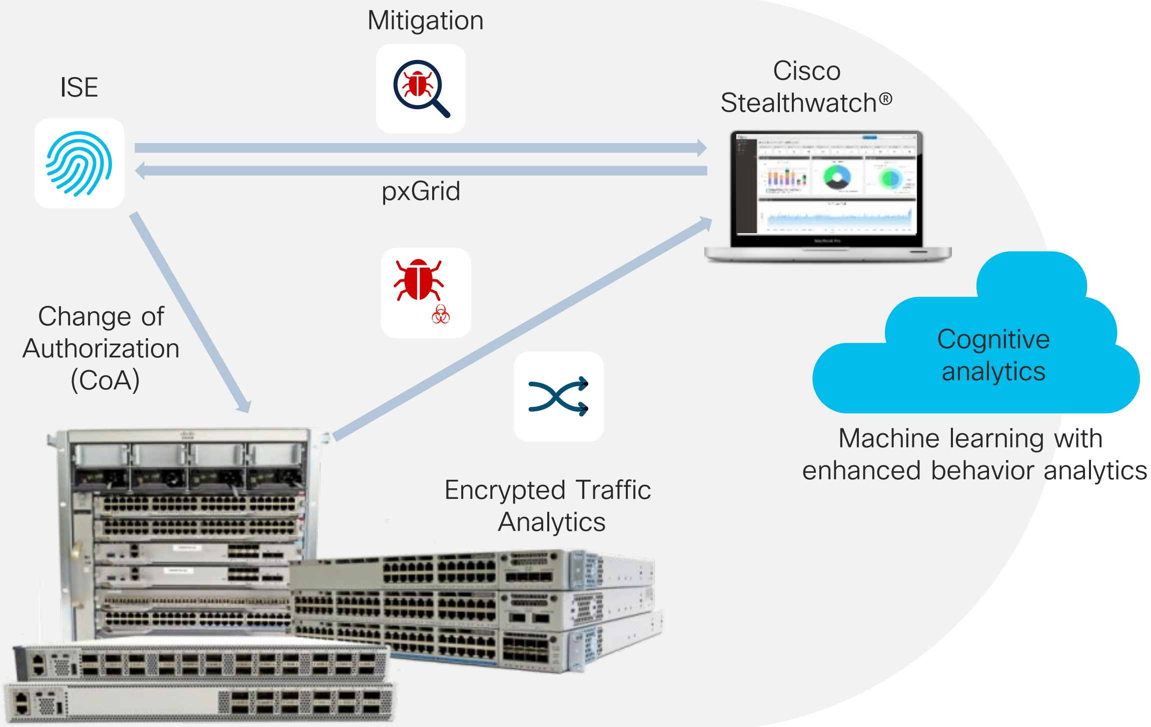
Proposed:

ACL Ing (1):	27K	NFL-In:	512
ACL Egr (2):	18K	NFL-Out:	512
PBR/NAT (3):	2K	LISP:	1K
QOS Ing (4):	1K	Tunnels:	768
QOS Egr (5):	1K		

AVC/NBAR2 and ETA on same port

Cisco Catalyst 9300 / 9400 switches enable Encrypted Traffic Analytics (ETA)

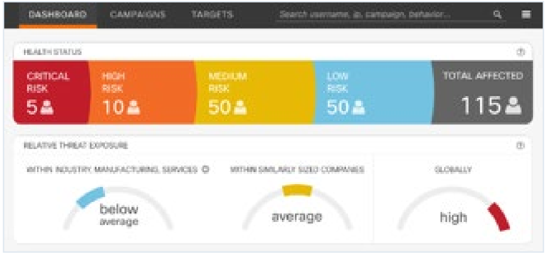
Rapidly mitigate malware and vulnerabilities in encrypted traffic



Machine learning with enhanced behavior analytics

Threat Grid

Talos



cognitive.cisco.com

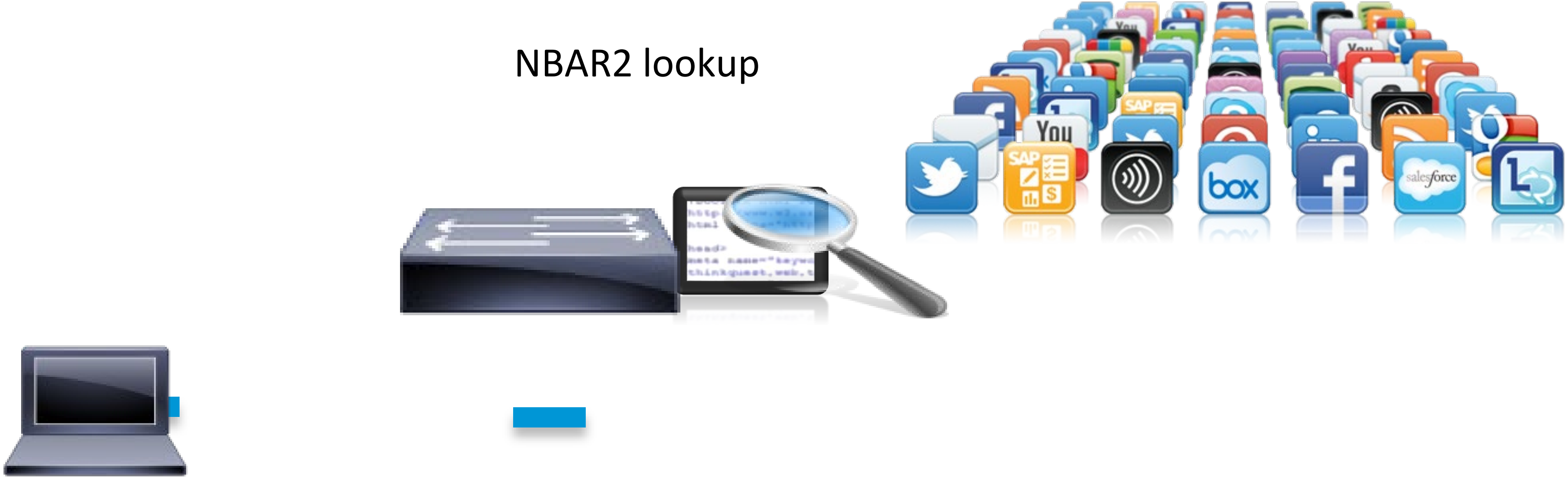
Analytics indicating malware in encrypted traffic at 99%+ efficacy

Mitigation using ISE and network

ERSPAN to send traffic for deeper analysis

Not available on Catalyst 9200 Series switches

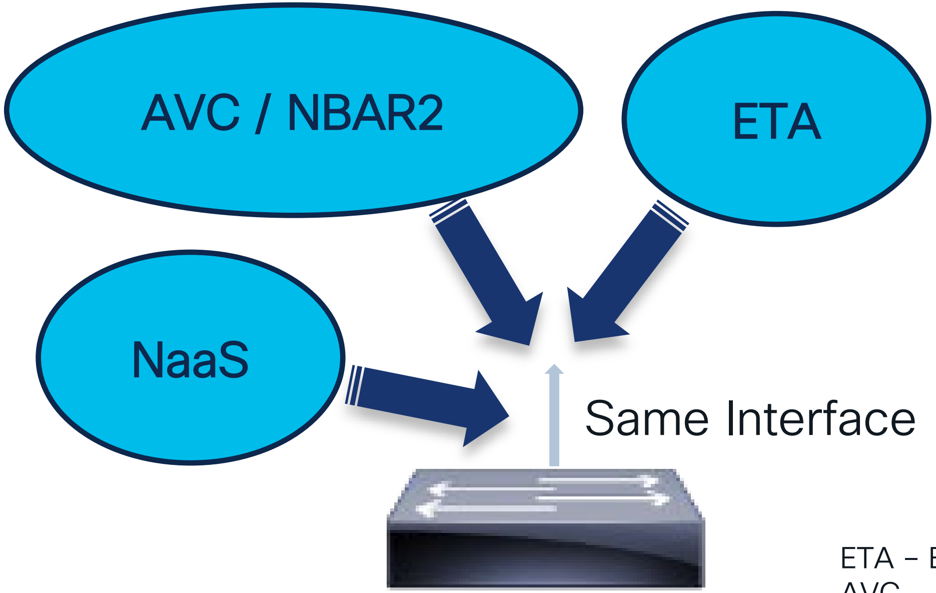
NBAR2 on Catalyst 9200/9300/9400 – How is it done?



- Original packets of a flow are hardware-switched to destination
- Copies of the initial few packets of a flow to CPU
- The software interacts with the NBAR2 module and detect the Application.

Network Based Application Recognition 2 (NBAR2)

IOS-XE 17.5.1



ETA – Encrypted Traffic Analytics
AVC – Application Visibility and Control
NBAR2 – Network Based Application Recognition
NaaS – Network as a Service

High Availability

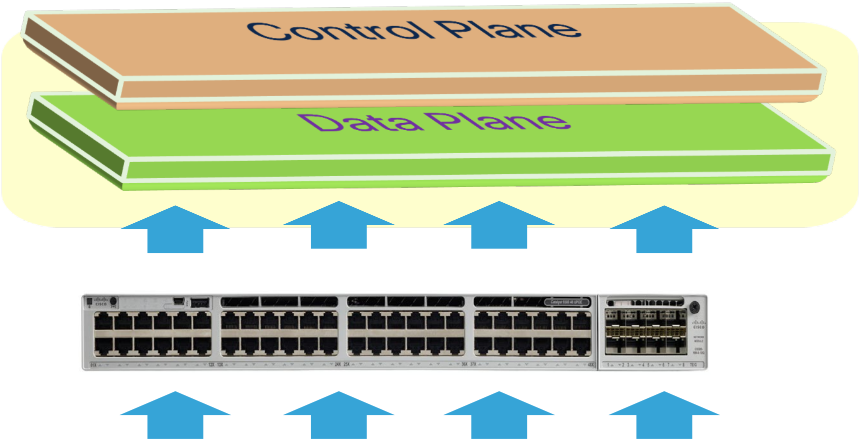
xFSU

xFSU on Catalyst 9300 - GA with 17.3.2

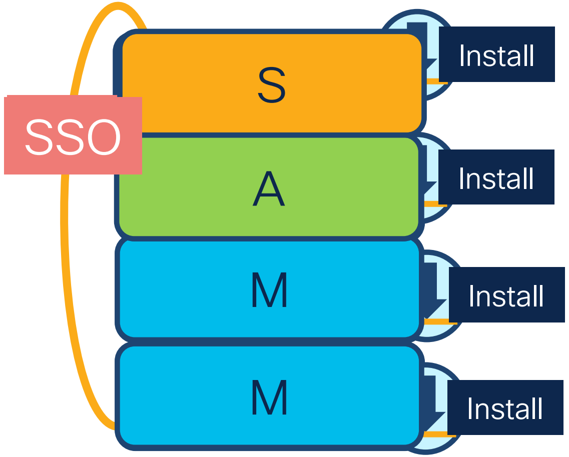
IOS-XE 17.3.2

Reload Only and Software Upgrade Options

- ➢ Step 1 : Control Plane Update
- ➢ Step 2 : Data Plane Update



- ➢ Step 1 : Standby and Members Upgrade
- ➢ Step 2 : Active Only



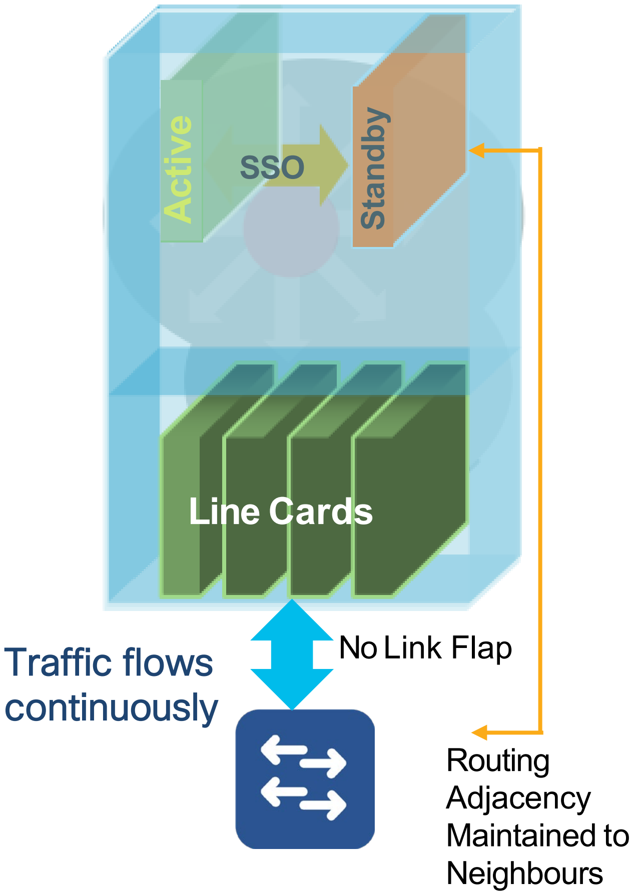
Traffic Impact during the complete upgrade is less than 30 seconds

Non-Stop Routing (NSR)

Non-Stop Routing

- Non-stop routing feature:
  - Synching all unicast routing information to Standby
  - Standby device will take over immediately from Active state with neighbor not knowing about the failures
  - NSF-aware peer devices not needed but **recommended**
  - Self-Contained Routing HA Solution

No disruption to the routing protocol interaction with other routers.


Active
SSO
Standby
Line Cards
Traffic flows continuously
No Link Flap
Routing Adjacency Maintained to Neighbours

NSR vs NSF

Non-Stop Routing (NSR)	Non-Stop Forwarding (NSF)
No support from peer switches needed	**Support** from peer switches required
Routing Sessions are **not terminated**	Routing Sessions are **terminated** and **reestablished**
Self contained solution	**Requires routing protocol extension**
NSR is enabled only on the **local device**	NSF needs to be enabled on **all devices** participating in routing
Unicast **Routing Control Plane** and **forwarding information are synced**	Only Unicast **Forwarding is synced**

NSR/GR Difference and Similarity

Non-Stop Routing (NSR)

- NSR is disabled by default
- NSR is supported only on Catalyst 9400, 9500H and 9600
- OSPFv2 and OSPFv3 are supported
- Can coexist with Graceful Restart configuration (Cisco NSF or IETF GR)

```
router ospf 1
        nsr
```

```
router ospfv3 1
        nsr
```

Non-Stop Forwarding (NSF)

- NSF is disabled by default
- Peer need to support Graceful Restart
- BGP, OSPFv2 and EIGRP are supported
- Can coexist with Graceful Restart configuration (Cisco NSF or IETF GR)

```
router ospf 1
        nsf
```

```
router eigrp 1
        nsf
```

```
router bgp 1
        graceful-restart
```

Smart Licensing

Smart Licensing Enhancements

Eliminating Day 0 deployment friction, Simplifying licensing workflow

1 Purchase

- Licenses applied to devices on purchase
- One-time reporting done by manufacturing for new direct orders

2 Use

- Devices work out of the box
- No initial registration process/eval mode
- License state always “In-Use”

3 Report

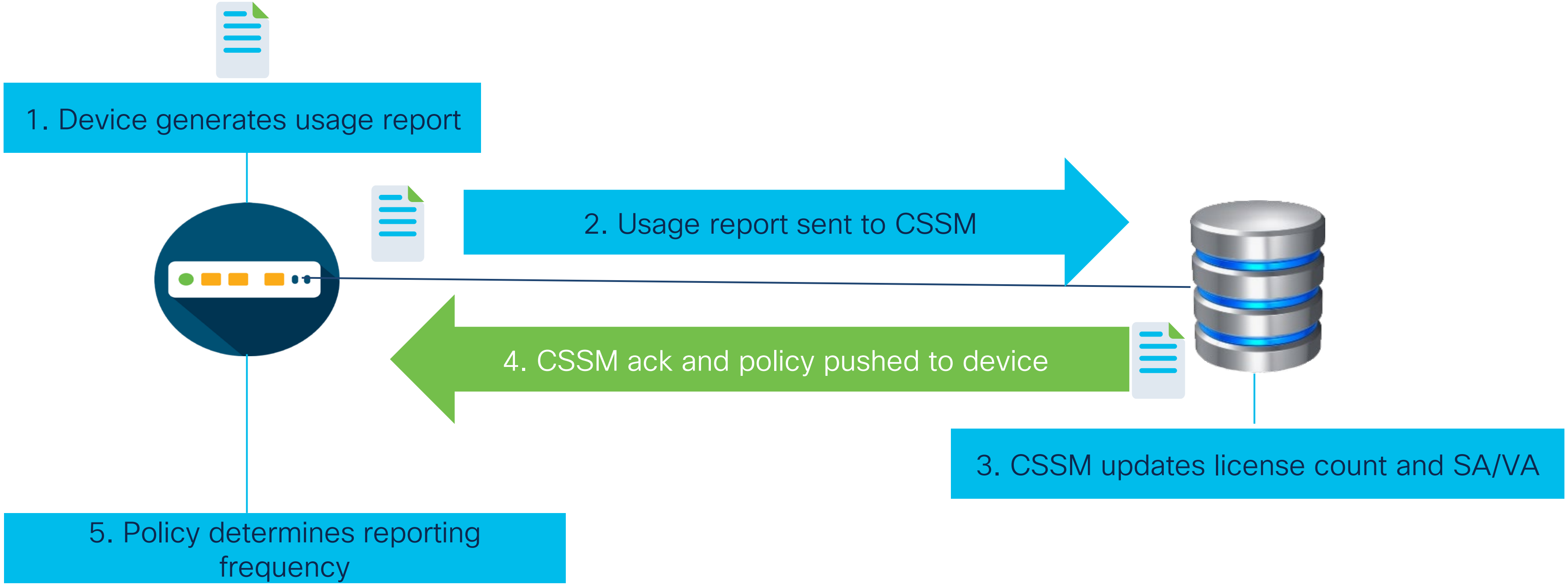
- Device generates usage reports which are sent to the CSSM
- Online and offline reporting options
- One-time reporting for perpetual license, Periodic reporting for subscription licenses

4 Billing and renewals

- SW purchased in advance
- Subscription renewal dates based on an EA or transactional

Catalyst 9000 platform support starting IOS-XE 17.3.2 and 17.4.1

SLP Flow



1. Device generates usage report

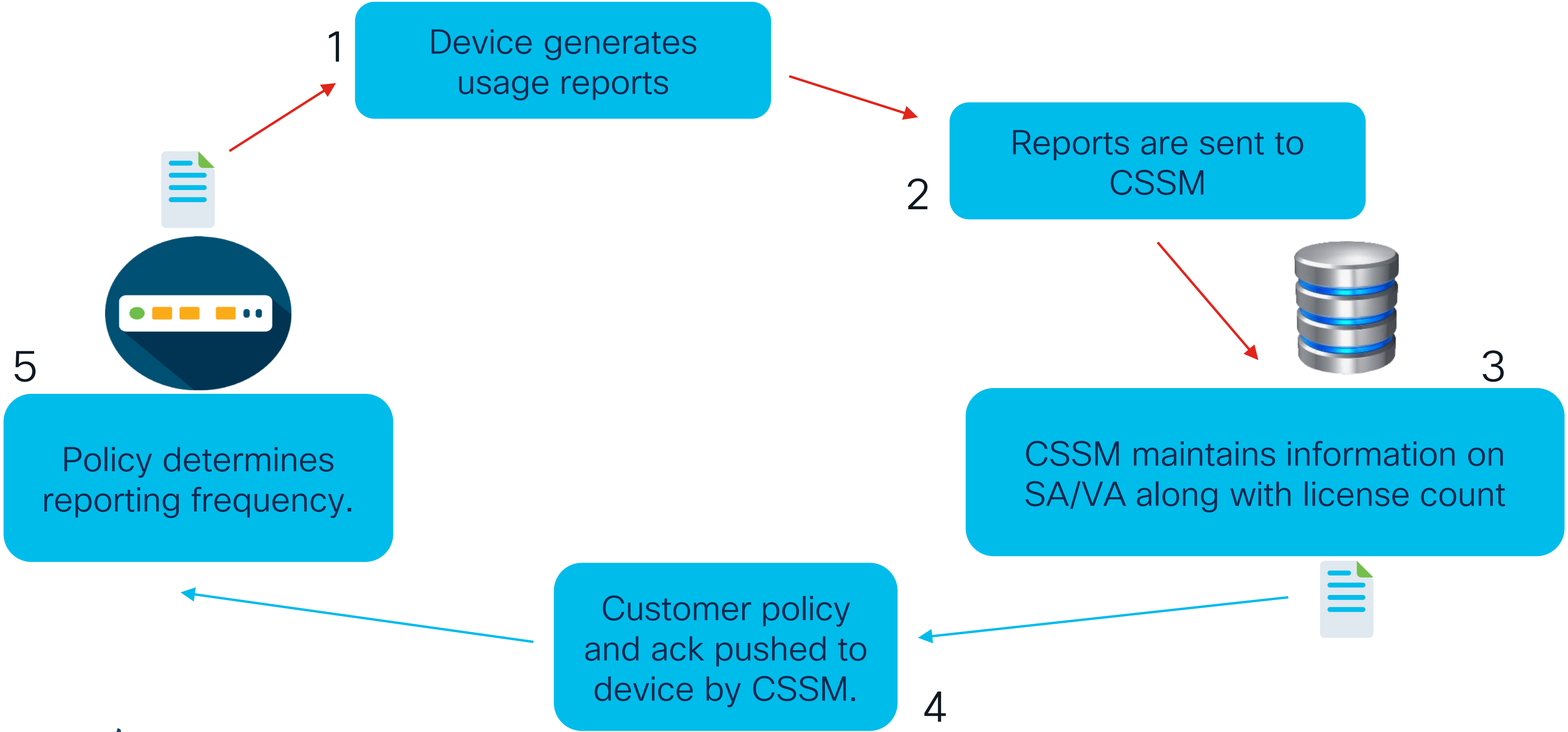
2. Usage report sent to CSSM

3. CSSM updates license count and SA/VA

4. CSSM ack and policy pushed to device

5. Policy determines reporting frequency

SLP Flow



1 Device generates usage reports

2 Reports are sent to CSSM

3 CSSM maintains information on SA/VA along with license count

4 Customer policy and ack pushed to device by CSSM.

5 Policy determines reporting frequency.

SL vs SLP

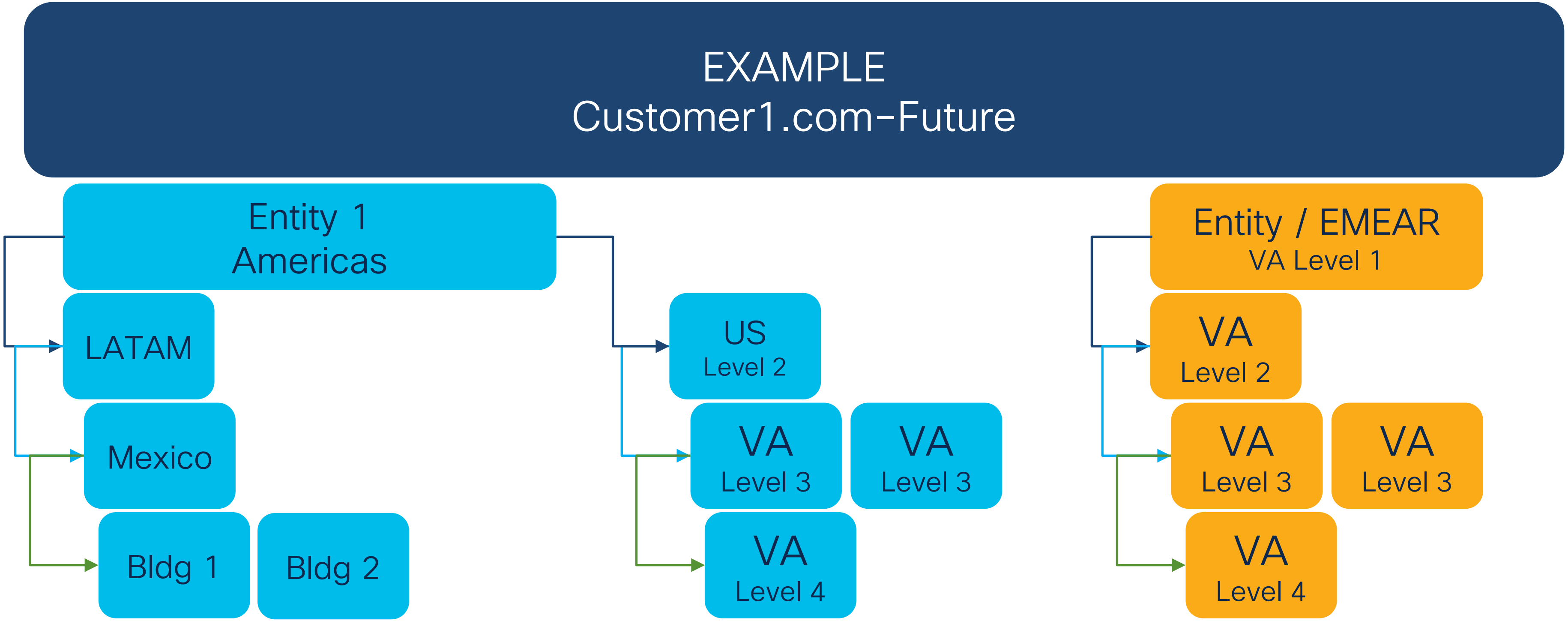
Features	SL	SLP
License states	Eval, Unregistered, Registered	In-use
License reservation	Yes	Not applicable*
Factory SLR	Yes (feature on request)	Check Factory license reporting
Custom reporting frequency	No	Yes
Eval mode	Yes	No
Factory license reporting	No	Yes (default behaviour)
Perpetual license	Reporting needed	No reporting needed.

*Device honors SLR by older install. Refer to section “Upgrade scena

SA Tree / Nested Structure

Reconciliation and Reporting Options

For Your Reference



EXAMPLE
Customer1.com–Future

Entity 1
Americas

LATAM

Mexico

Bldg 1

Bldg 2

US
Level 2

VA
Level 3

VA
Level 3

VA
Level 4

Entity / EMEAR
VA Level 1

VA
Level 2

VA
Level 3

VA
Level 3

VA
Level 4

Key Takeaways

- Use software value with **Zero-Trust**
- C9K **Architectural Flexibility**
- Benefit with **mGig and UPOE+ models**
- **Assurance is better than a believe**
- Integrate with Cloud

C9K - Unmatched Value with Each Port

The bridge to possible

Thank you

cisco Live!

TURN
IT
UP

#CiscoLive