



Possibilities

#CiscoLive

Introduction to Cisco Catalyst 9800 Wireless Controller

Aparajita Sood, Technical Marketing Engineer
DGTL-BRKEWN-2670



#CiscoLive



Agenda

Why Catalyst 9800 ?

Platform Support | Software Interoperability | IRCM

Cisco Catalyst 9800 Wireless Controller Appliances

Cisco Catalyst 9800 Wireless Controller Public and Private Cloud

Cisco Catalyst 9800 Series Wireless Controller for SDA

Embedded Wireless Controller on Catalyst 9100

Differentiators

Resiliency

Security

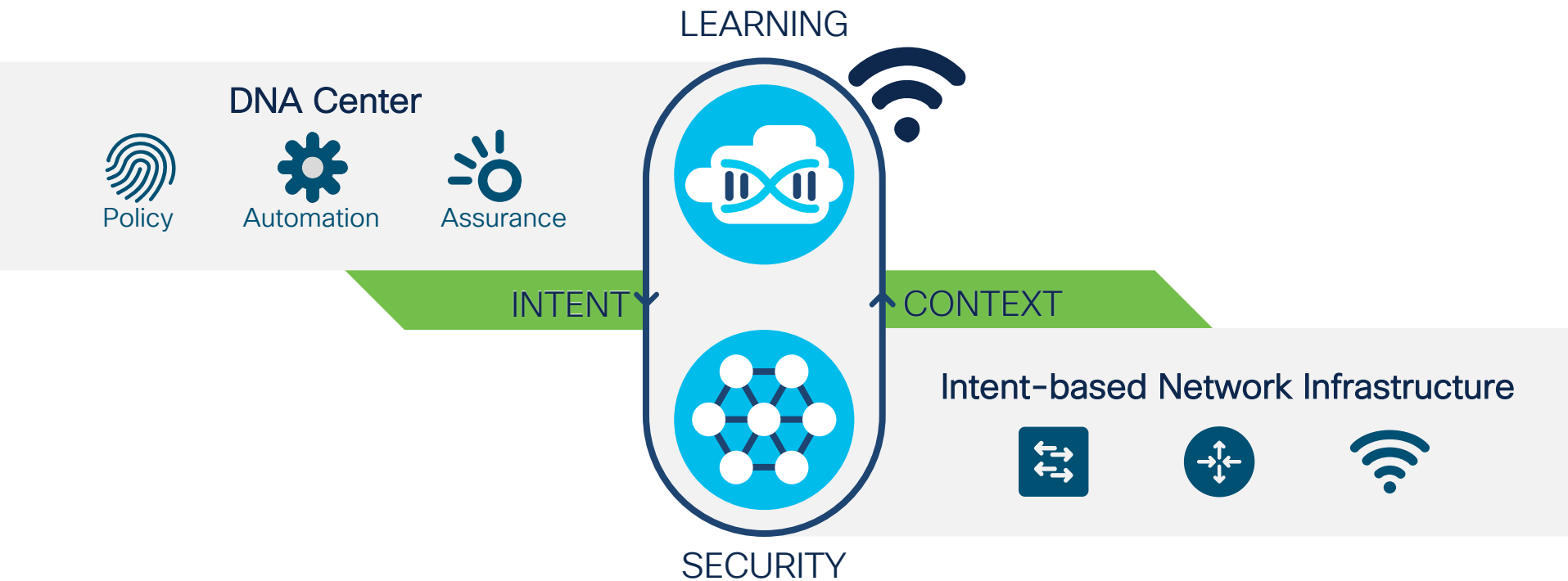
Intelligence

Adoption

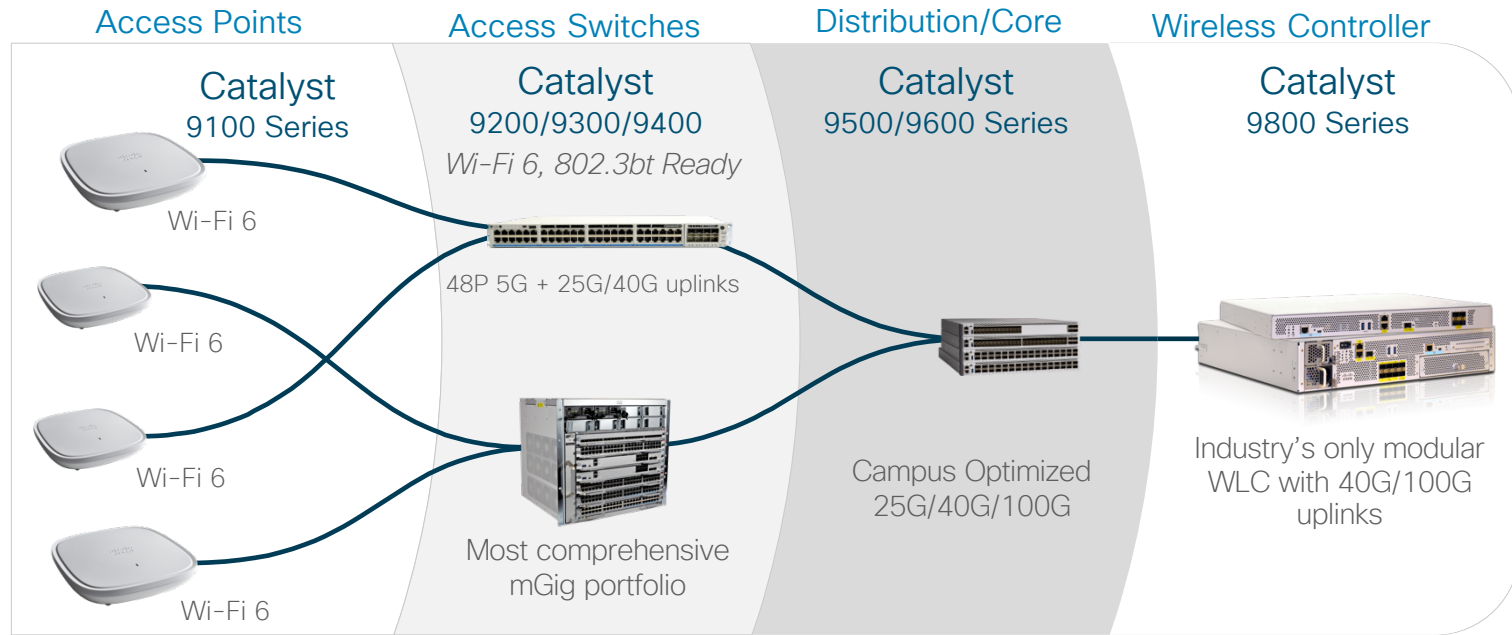
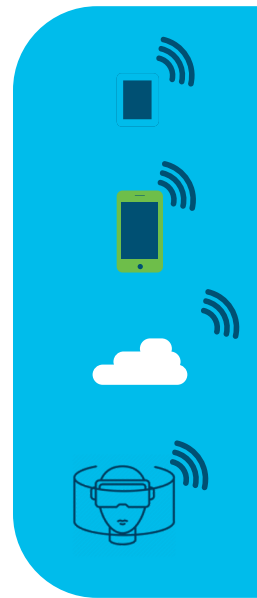
New Configuration Model

Migration Strategies

Intent-Based Networking (IBN) strategy



Best Access Experience for IT and IoT starts with the Catalyst Access Network



← Fully Integrated End to End →

Built for intent-based networking



Automation



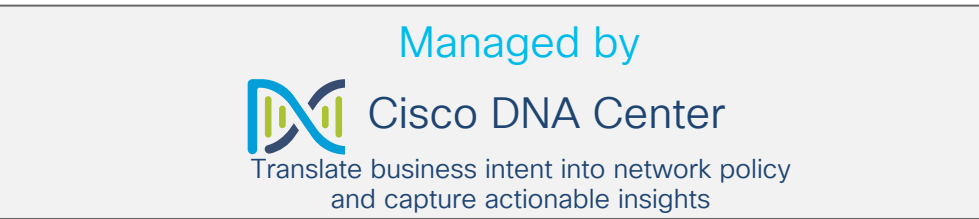
Security



Analytics

Cisco's Next Gen Wireless Stack is Ready for Scale Deployments

Enabling next-generation mobility powered for Wi-Fi 6



Resilient



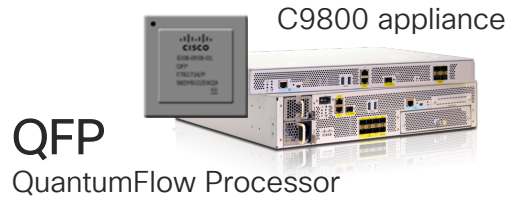
Secure



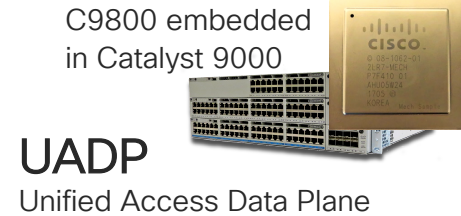
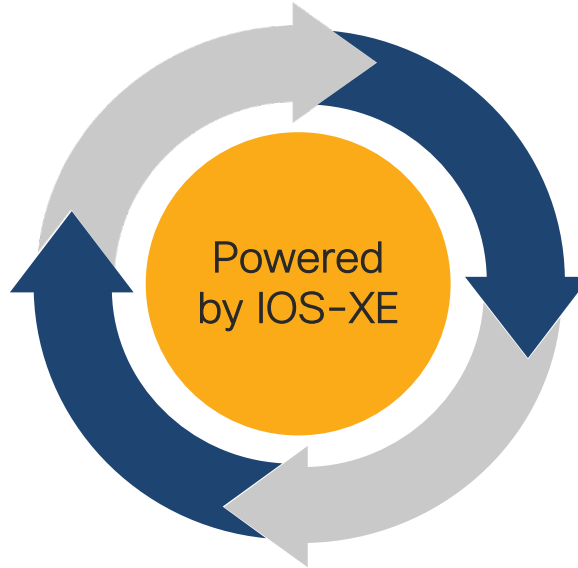
Intelligent

Cisco Catalyst 9800 – Next Gen Wireless

IBN starts from a strong Hardware Architecture Foundation



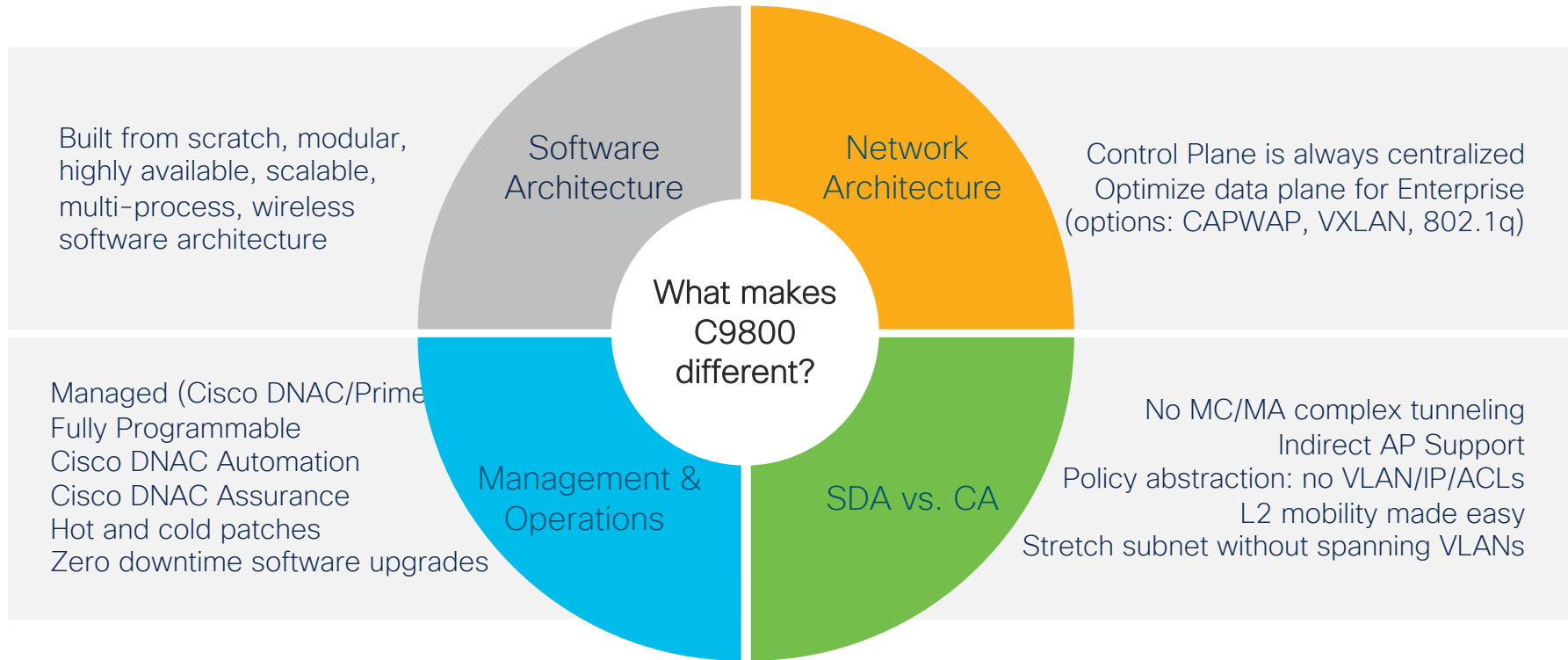
- Advanced, Multi-Core, Feature-Rich
- **Fully Programmable**
- Scalable
- Advanced on-chip QoS
- Secure
- **Extensible Architecture**



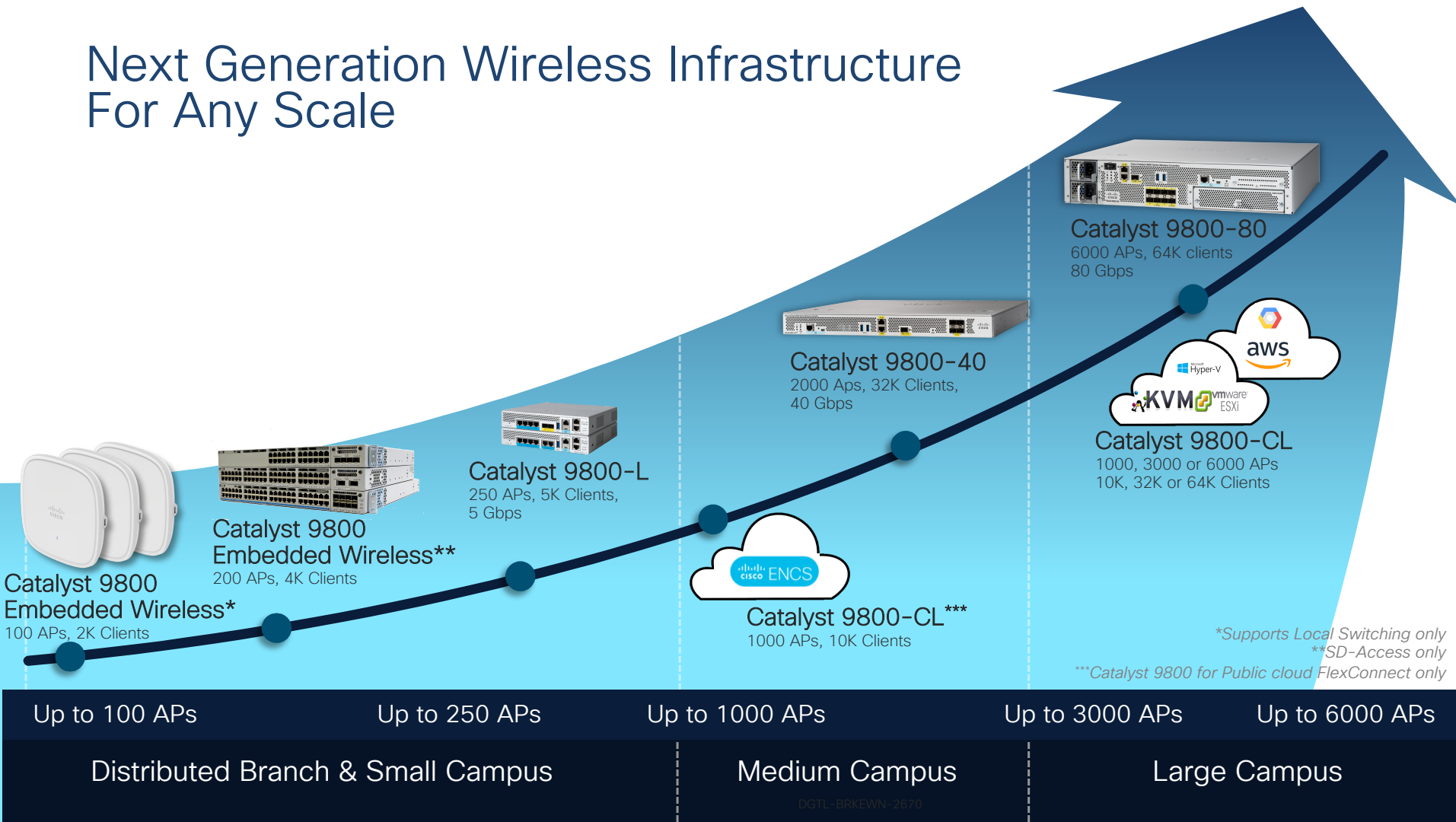
- Flexible, Programmable, High-Performance
- Fully Programmable
- Scalable
- Advanced on-chip QoS
- Secure
- **Extensible Architecture**

100% Cisco-developed Flexible Silicon – Unlocking the Power of DNA at Hardware Speeds

Cisco Catalyst 9800 – Next Gen Wireless Architecture



Next Generation Wireless Infrastructure For Any Scale



Cisco Catalyst 9100 Series Access Points

Ideal for small to medium-sized deployments



Mission critical



Best in Class

Coming soon



9105AX

- 2x2 + 2x2
- MU-MIMO, OFDMA
- Spectrum intelligence
- IoT ready
- 1x 2.5 mGig (WP)
- TWT



9115AX | 9117AX

- 4x4 + 4x4 | 8x8 + 4x4
- MU-MIMO, OFDMA
- Spectrum intelligence
- 1 x 2.5 mGig | 1 x 5 mGig
- TWT



Powered by
Cisco RF ASIC

9120AX

- 4x4 + 4x4
- Cisco RF ASIC for Next Gen CleanAir
- Dual 5GHz, Next Gen HDX
- IoT ready
- 1 x 2.5 mGig
- TWT



Powered by
Cisco RF ASIC

9130AX

- 8x8 + 4x4; 4x4 + 4x4 + 4x4
- Tri-radio: Dual 5GHz + 2.4GHz
- Cisco RF ASIC for Next gen CleanAir
- Full iCap with data packets
- Dual 5GHz, Next Gen HDX
- IoT ready
- Smart Antennas supporting up to 8x8
- 1 x 5 mGig
- First 8x8 AP with external antennas
- TWT

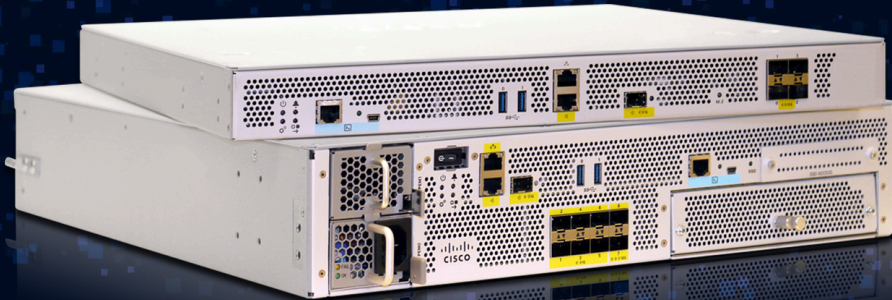
Bluetooth 5

USB

Integrated or External Antenna

Cisco DNA Assurance with iCAP

Cisco Catalyst 9800 Wireless Controller Appliances



Unprecedented throughput with C9800 appliances

99%+

Accuracy with
Encrypted Traffic Analytics
and Stealthwatch integration



Always-on:
High availability and
seamless software
updates

2x

Throughput option now
available with C9800-80
going up to 80 Gbps

CISCO *Live!*



Catalyst 9800 Series Wireless
Controller Appliances
C9800-40 and C9800-80



Open standards based
programmability with
model-driven telemetry



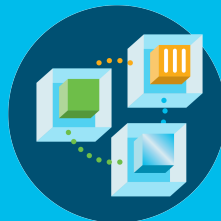
Industry's 1st
100GE uplink



Investment
protection with
modular uplinks



Scale options for
your campus



Programmable multi-
core network processor

C9800-80-K9

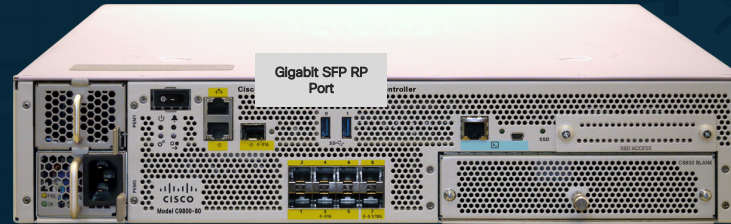
Front Panel

EXTERNAL INTERFACES

- RJ-45 Console Port
- Mini USB Console Port
- 2 External USB Ports
- RJ-45 Ethernet Management Port (SP)
- RJ-45 Ethernet Redundancy port (RP)
- SFP Gigabit Ethernet Port
- BUILT-IN-6x10GE/2x1GE or 10GE
- C9800 Modules

LEDs

- Power Status LED
 - Alarm LED
 - High availability LED
 - USB console LED
 - 10/100/1000 RJ45 Link LED
 - 10/100/1000 RJ45 Activity LED
 - SSD Activity LED
 - System Status LED
-
- Power Supply (PEM 0)
 - Power Supply (PEM 1)
 - Power Switch



Dimensions of C9800-80-K9: 17.3" (439.42 mm) wide, 3.5" (88.9 mm) tall (2RU), and 22.0" (558.8 mm) deep

(Compared to
30.8 " for 8540)

C9800-40-K9

Front Panel

EXTERNAL INTERFACES

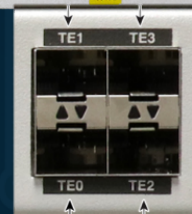
- RJ-45 Console Port
- Mini USB Console Port
- 2 External USB Ports
- RJ-45 Ethernet Management Port (SP)
- RJ-45 Ethernet Redundancy port (RP)
- SFP Gigabit RP Port
- 4 x 10GE/1GE SFP and SFP+ ports

LEDs

- Power Status LED
- Alarm LED
- High availability LED
- USB console LED
- 10/100/1000 RJ45 Link LED
- 10/100/1000 RJ45 Activity LED
- SSD Activity LED
- System Status LED



Gigabit SFP
RP Port



Dimensions : 17.3" (439 mm) wide, 1.75" (44.4 mm) tall (1RU), and 18.3" (464 mm) deep*

C9800-40-K9

AIR-CT-5508-K9

AIR-CT-5520-K9



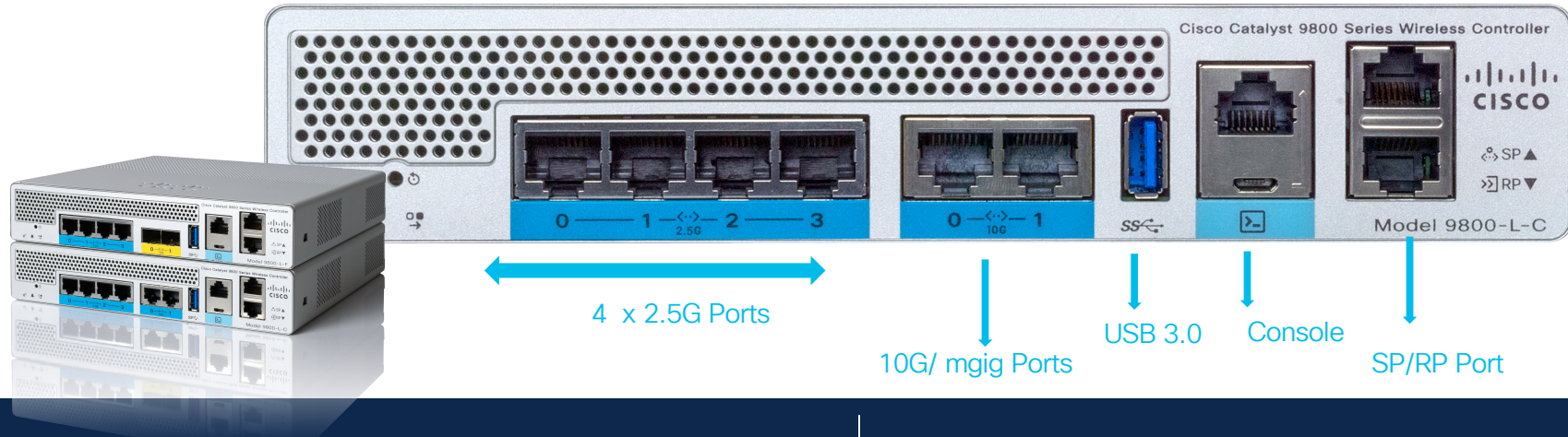
*compared to 30.98" (786 mm) in 5520

C9800- L: Industry's first fixed Wireless Controller with Seamless software Updates

Up to 250 APs

Up to 5,000 Clients

5 Gbps



Fully programmable multi-core network processor

Support for Netflow, AVC and ETA

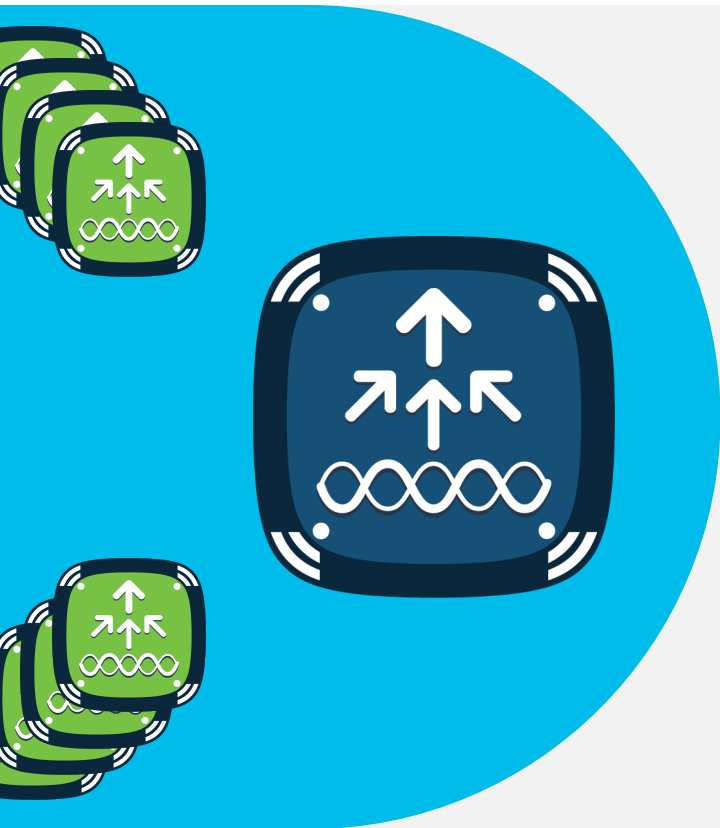


Embedded Wireless Controller (EWC) on Catalyst 9100 APs

Simplicity without compromise

Embedded Wireless Controller on Catalyst 9100

Ready for Enterprise deployments



Runs C9800 **IOS-XE**
Wireless Controller on
Catalyst Access Points

Modern OS, scalable,
open and programmable,
supports telemetry



Supports Advanced
Enterprise Feature Set

HA, SMU, aWIPS,
Umbrella, NetFlow, ICAP



Flexible Management
Options

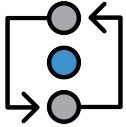
Use Mobile App, WebUI
and DNA-C to Deploy,
Manage and Monitor



Investment Protection

Migrate Access Points to
controller for more than
100 Access Points

Embedded Wireless Controller ready Branch Deployments



Redundancy with Active & Standby
Controllers running simultaneously on
two Access Points

<10seconds

Active to Standby switchover in
a few seconds



SMU(patching) support for both
Controller and Access Point



aWIPS*, Rogue detection,
identification and **mitigation**



Walled Garden & DNS
Blocking¹



Cisco
Umbrella

Cloud Delivered Enterprise
Security with Cisco Umbrella*



Simplified WebUI for
Monitoring, Provisioning and
Day-N Operations



DNA Center

PnP, Automation and
Assurance



Open standards based
programmability with NETCONF,
YANG

* IOS-XE 17.1 #CiscoLive



Resilient



Secure



Intelligent & IT Simplicity

Embedded Wireless Controller Catalyst 9100 Access Points

Ideal for single or multi-site small to medium Enterprise deployments



C9115AX-EWC

- 50 Access Point, 1000 Clients
- 4x4 + 4x4
- MU-MIMO, OFDMA
- Spectrum intelligence
- Bluetooth 5
- 1 x 2.5 mGig
- USB
- Integrated or External antenna



C9117AX-EWC

- 50 Access Point, 1000 Clients
- 8x8 + 4x4
- MU-MIMO, OFDMA (only DL)
- Spectrum intelligence
- Bluetooth 5
- 1 x 5 mGig
- USB
- Integrated Antenna only

Mission Critical
Best suited for High Density Enterprise Branch Deployments



Powered by Cisco RF ASIC

C9120AX-EWC

- 100 Access Point, 2000 Clients
- 4x4 + 4x4
- MU-MIMO, OFDMA
- Cisco RF ASIC
- Dual 5GHz, HDX
- RF signature capture
- 1 x 2.5 mGig
- Integrated or External antenna



Powered by Cisco RF ASIC

C9130AX-EWC

- 100 Access Point, 2000 Clients
- 8x8 + 4x4 or 4x4 + 4x4 + 4x4
- Tri-radio (Dual 5GHz + 2.4GHz), HDX
- Cisco RF ASIC
- RF signature capture
- Decrypted data packet iCAP
- 1 x 5 mGig
- 8 port Smart Antennas

Software Feature Parity
across APs

Supports up to 100 APs,
2000 Clients

Supports Wave 2 APs as
client serving

Cisco DNA Assurance with
iCAP

What about 802.11ac Wave 2 Access Points?

Supports client serving mode

Ideal for small to medium-sized deployments

Mission critical

Indoor



1815W



1815L, 1815M



1832



1842



1852

Outdoor



1540



2802



3802



4800



1560

ALL 11ac Wave 2 Access Points can connect to Embedded Wireless Controller

Someone said
Cloud??



Some definitions first...



PRIVATE

- ❑ Customer has unique access to dedicated DC virtualized or physical resources
- ❑ The resources are onPrem DC or hosted by a Colo provider
- ❑ WLC as a Virtual Machine



PUBLIC

- ❑ Customer doesn't own the infrastructure (computing, storage, networking).
- ❑ WLC is consumed as Infrastructure as a Service (IaaS)



HYBRID

- ❑ Simply the reality...
- ❑ Customer will have both Private and Public cloud deployments for some time

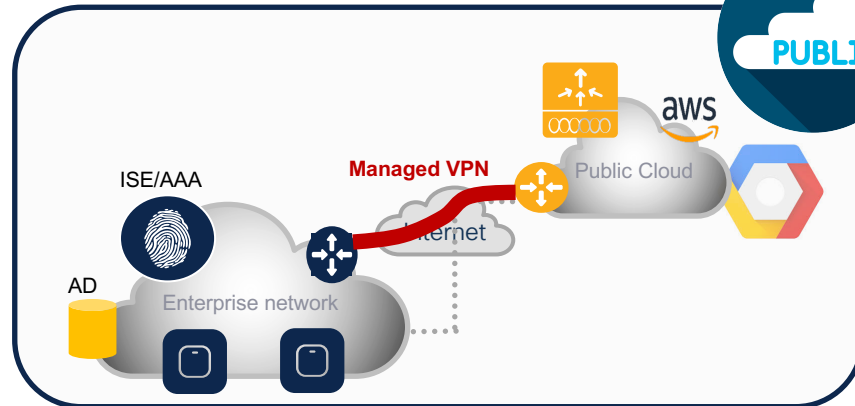
Catalyst 9800 Wireless Controller for Cloud



Hypervisors: ESXi, KVM, NFVIS on ENCS

Cisco DNA Center 1.3
Wi-Fi 6, W1 & W2 802.11ac APs

All deployments mode: Centralized, SDA,
FlexConnect, Mesh



Amazon AWS with Managed VPN

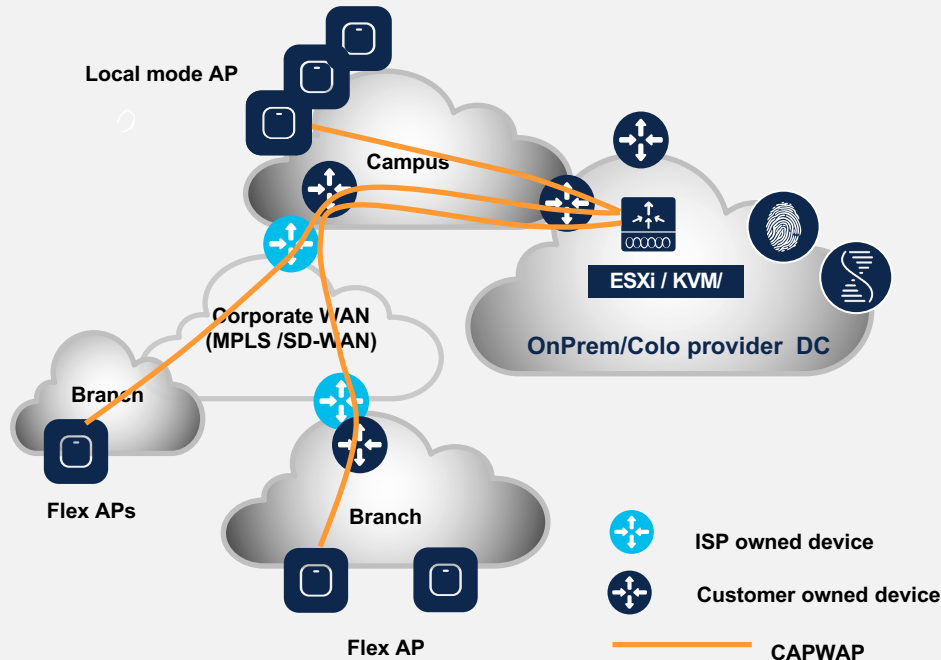
6000 APs / 64000 Clients

FlexConnect local switching only

Private Cloud



Catalyst 9800 Private Cloud deployment



■ Key benefits:

- Deploy wireless controller where you want it, how you want it
- All AP modes supported
- Feature parity with appliance (only exception is GuestShell)

■ Support

- VMware ESXi , KVM, ENCS and Hyper-V(starting 17.1)
- Wi-Fi 6, Wave2 and Wave1 APs
- Centrally switched traffic <= 1.5 Gbps
- ESXi vCenter or KVM Virt-Mgr for VM provisioning
- Automated VM bootstrap flow (ESXi vCenter only)

High throughput templates for C9800-CL(Private)



- IOS-XE 17.3 release introduces high throughput templates to the C9800-CL private cloud instances
- High throughput templates require 3 additional CPU cores for each template type
- List of all templates supported in 17.3 and their hardware requirements

Model Configuration	Small (Low throughput)	Medium (Low throughput)	Large (Low throughput)	Small (High throughput)	Medium (High throughput)	Large (High throughput)
Minimum Number of vCPUs	4	6	10	7	9	13
Minimum CPU Allocation (MHz)	4,000	6,000	10,000	4,000	6,000	10,000
Minimum Memory (GB)	8	16	32	8	16	32
Required Storage (GB)	16	16	16	16	16	16
Virtual NICs (vNIC)	2/(3)*	2/(3)*	2/(3)*	2/(3)*	2/(3)*	2/(3)*
(*) 3rd NIC is for High Availability						

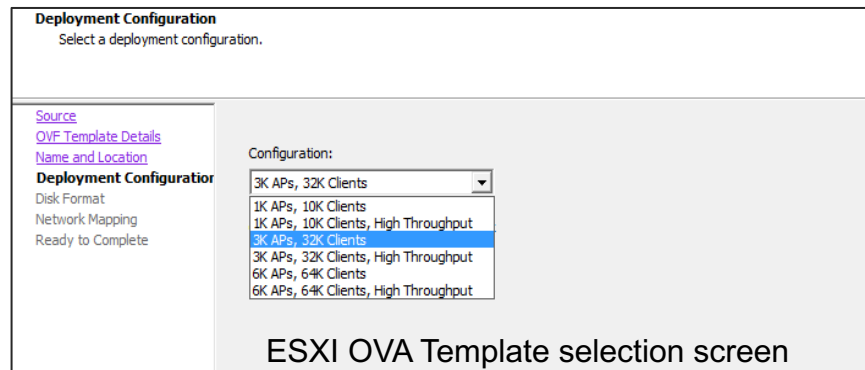
CP and DP Core Split

The list below shows the split of the cores between Control Plane (CP) functions and Data Plane (DP)/Packet Processing across all the templates

Template/ Throughput	APs	Clients	vCPUs	vCPUs Allocated for CP	vCPUs Allocated for DP	RAM Size (in GB)
Small Low	1K	10K	4	2	2	8
Small High	1K	10K	7	2	5	8
Medium Low	3K	32K	6	4	2	16
Medium High	3K	32K	9	4	5	16
Large Low	6K	64K	10	8	2	32
Large High	6K	64K	13	8	5	32

Installation/Configuration Options

- Deploying through the 17.3 based OVA will now show all the 6 supported templates
- In KVM or ISO installation if user can set invalid values for vCPU, and RAM. The template will be selected by the software automatically during bootup.
- Resource rules for template are shown below



VM Template	Throughput	RAM (in GB)	vCPUs
Large	High	>=32	>=13
Large	Low	>=32	>=10
Medium	High	>=16 and <32	>=9
Medium	Low	>=16 and <32	>=6
Small	High	>=8 and <16	>=7
Small	Low	>=8 and <16	>=4

HA, Backward and forward Compatibility

- The HA pair will not form if the throughput settings do not match on the two WLC instances forming the pair
- When the instance running 17.3 boots with or is downgraded to the previous release of software the VM template for that release will be chosen on boot up .
- Resource rules for template for Pre 17.3 releases is shown below

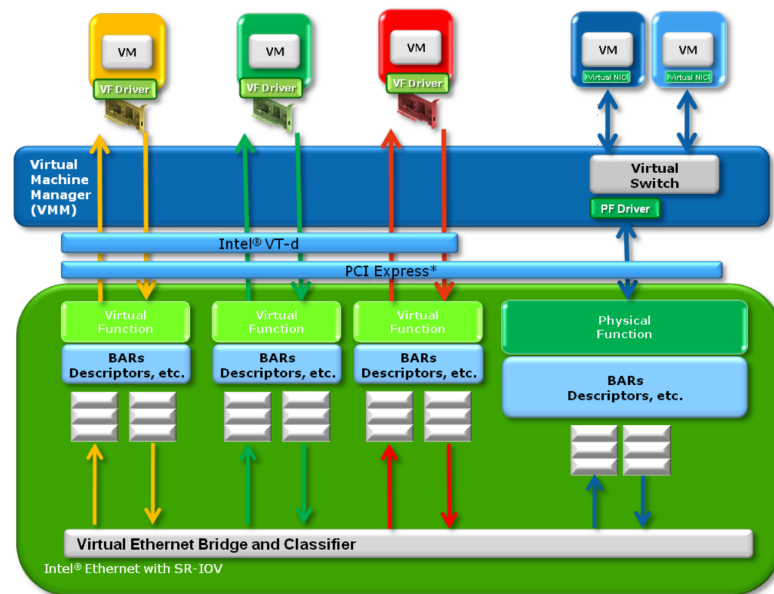
VM Template	RAM (in GB)	vCPUs
Large	≥ 32	≥ 10
Medium	≥ 16	≥ 6
Small	≥ 8	≥ 4

Hard disk Requirement update

- Starting 17.3 the Disk Size recommended for all C9800-CL would be atleast 16 GB
- This is applicable for all hypervisors (ESXI , KVM & Hyper-V) and public cloud (AWS & GCP).
- For the instances created before 17.3 release the recommended disk size is 8GB . They will continue to work fine even after upgrade to 17.3 but for enhanced logging and to features like ISSU it is recommended to have a disk size of 16GB.
- (ESXI from 17.2 requires 16GB)

SR-IOV (single root input/output virtualization)

- SR-IOV provides the ability to partition a single physical PCI resource into virtual PCI functions which can then be injected into a VM. These Network VFs (Virtual Functions) of SR-IOV improves north-south network performance by allowing traffic to bypass the host machine's network stack.
- Each virtual machine is directly assigned and given access to the physical resources (VFs) by the hypervisor (VMM)
- VMM tells it has a VF attached and indicates the HW registers for VFs to the nic driver in the Virtual Machine



SR-IOV Support on C9800-CL

- SR-IOV is supported on C9800-CL only on ESXI and KVM Hypervisors
- It is not supported on Hyper-V as of 17.3
- Features such as vMotion, DRS, Snapshots, NIC Teaming are not supported with SR-IOV on C9800-CL

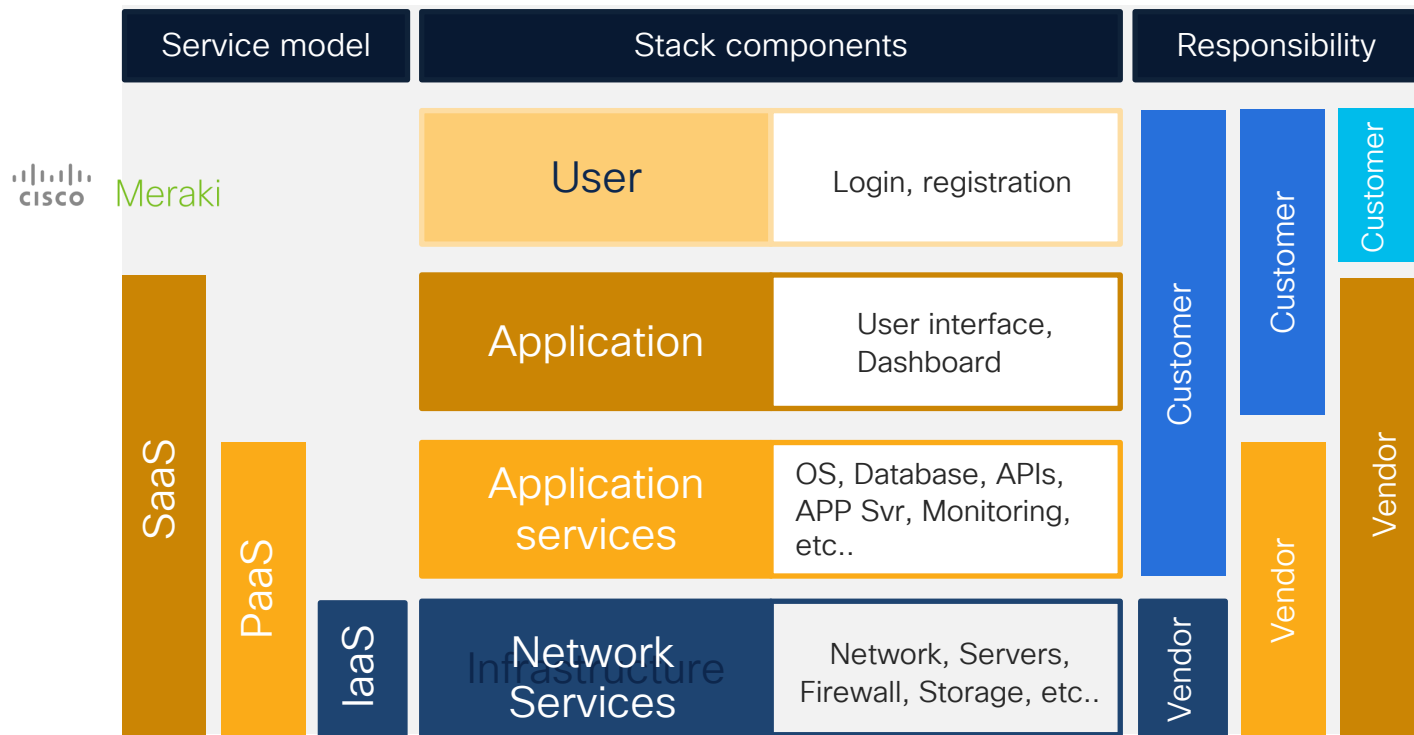
Verified and Recommended Software versions

Hypervisor Version	NIC	Driver Version	Firmware
VMWare Version 6.5	Intel x710	I40en 1.10.6 Plugin version 1.4.1	7.10
VMWare Version 6.5	Ciscoized x710	I40en 1.8.6 Plugin version 1.4.1	7.0 7.0 firmware and 1.8.6 driver has trust mode persistence issue across VM reload. Issue will be fixed in subsequent firmware and driver versions.

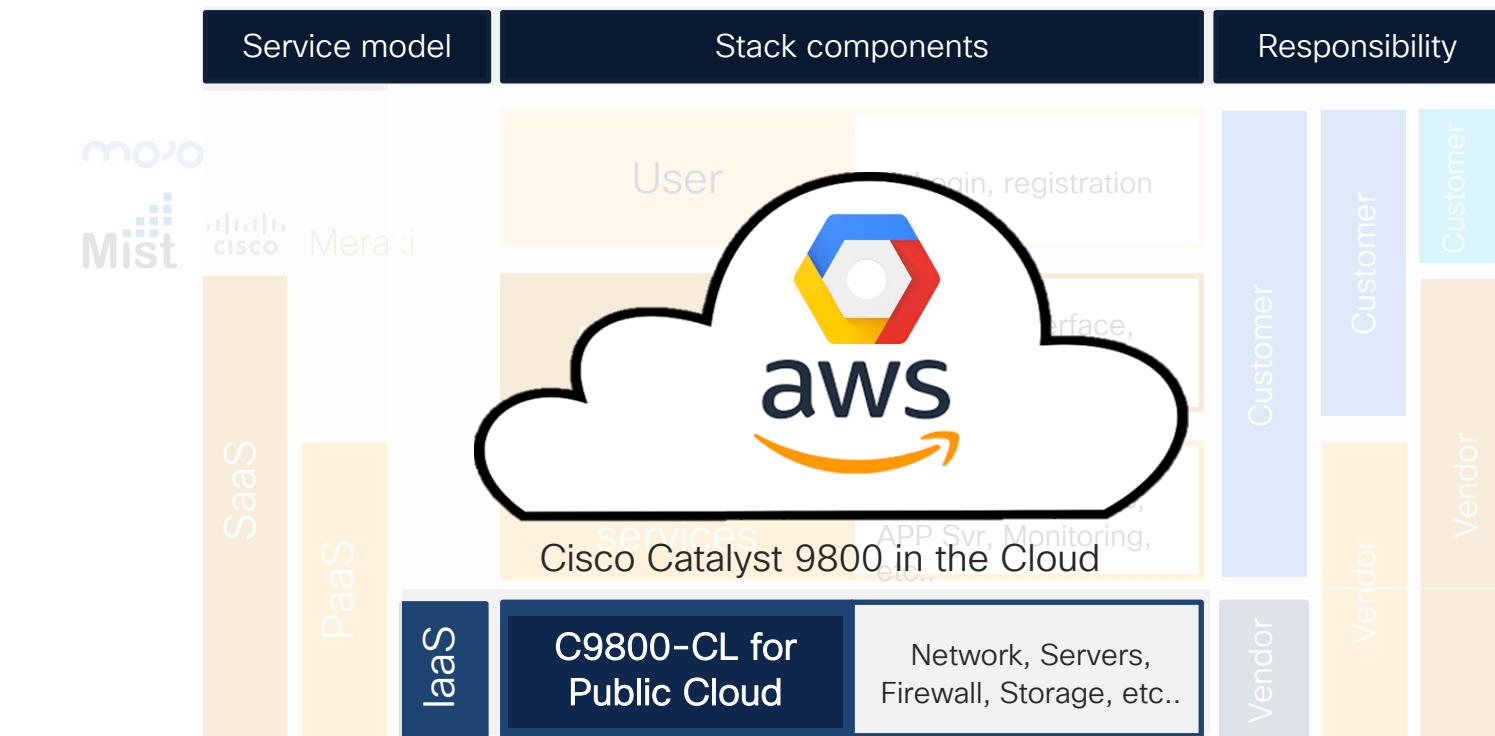
Hypervisor Version	NIC	Driver Version	Firmware
KVM RedHat Version 7.5	Intel x710	I40e 2.10.19.82	7.10
KVM RedHat Version 7.4	Ciscoized x710	I40e 2.10.19.82	7.0

Public Cloud

Public Cloud deployment models



Pioneering IaaS Public Cloud Play : 9800-CL



C9800-CL Support for Google Cloud Platform – IOS XE 17.1



Addition of Google Cloud Platform (GCP) to the C9800 Public Cloud Offering

*Support for C9800 on AWS was introduced
during C9800 FCS*

The screenshot shows the Google Cloud Platform console interface. At the top, there's a blue header with the Google Cloud Platform logo, a search icon, and a dropdown menu showing 'eWLC'. Below the header, the main content area displays the 'Cisco Catalyst 9800-CL Wireless Controller for Cloud' page. On the left, there's a circular icon with the Cisco logo. To the right of the icon, the title 'Cisco Catalyst 9800-CL Wireless Controller for Cloud' is followed by 'Cisco Systems' and 'Estimated costs: \$87.68/month + BYOL license fee'. Below this, there's a 'Deploy and Manage Enterprise-Class Wireless Services' section with a blue 'LAUNCH' button. The page is divided into two columns. The left column contains metadata: 'Runs on' (Google Compute Engine), 'Type' (Virtual machines, Single VM, BYOL), 'Last updated' (2/17/20, 11:47 AM), 'Category' (Networking), 'Version' (16.12.1), and 'Operating system' (IOSXE 16.12.1). The right column contains an 'Overview' section with a detailed description of the controller's capabilities, including BYOL support, high-speed always-on and secure wireless services, and deployment scenarios. A 'Learn more' link is provided at the bottom of the overview. Below the overview, there's an 'About Cisco Systems' section with a brief description of Cisco's role in the IT industry.

Advantages of C9800-CL in Public Cloud

\$0

The C9800-CL Wireless
Controller price

7 minutes

Time taken to deploy
C9800-CL for AWS

Up to 50%

Cost Savings seen by a large
enterprise by deploying
C9800-CL for Private Cloud

**VMware®
VMotion**

No more planned /
unplanned outages



AWS GovCloud

Host the Catalyst 9800 Series
controller in AWS' FedRAMP
certified GovCloud



Agility – simple
to deploy



Scale based on
network size

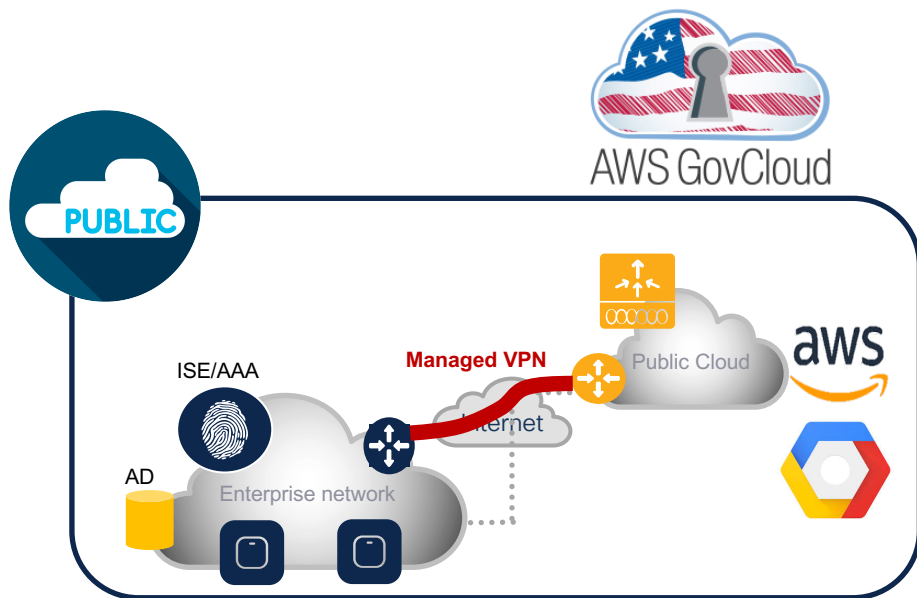


Global Footprint



Cost Effective

Catalyst 9800 Wireless Controller for Cloud



Amazon AWS with Managed VPN

3,000 APs / 32,000 Clients

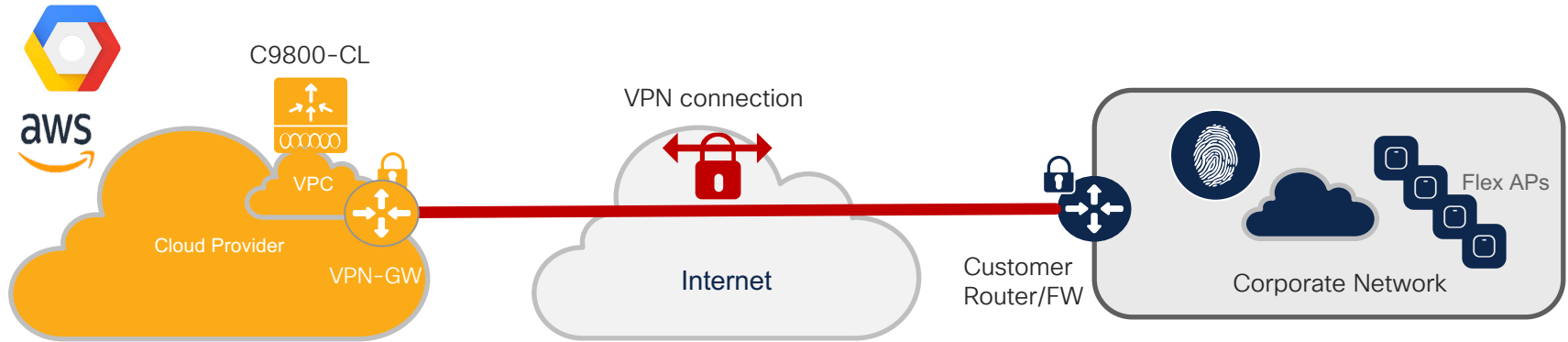
FlexConnect local switching only

ISE and AD typically on Prem

N+1 high availability

Smart License Management &
DNA subscription based AP licenses

Public Cloud – Managed VPN



C9800-CL Public Cloud Profile Specs

Parameters	Small	Medium	Large
vCPUs	4	6	10
RAM (in GB)	8	16	32
Disk (in GB)*	8	8	8
# of NIC	1	1	1
AP Count	1,000	3,000	6,000
Client Count	10,000	32,000	64,000
Deployment Mode	Cisco FlexConnect (Local Switching only)	Cisco FlexConnect (Local Switching only)	Cisco FlexConnect (Local Switching only)
Cloud Providers	AWS, GCP	AWS, GCP	AWS, GCP

* Recommended is 16 GB starting IOS XE 17.3.1

C9800-CL Public Cloud Profile Specs

Parameters	Small	Medium	Large
Max WLANs	4096	4096	4096
Max Site Tags	1,000	3,000	6,000
Max APs per Site	100	100	100
Max RF Profiles	2,000	6,000	12,000
Max Policy Profiles	1,000	1,000	1,000
Max Flex Profiles	1,000	3,000	6,000
High Availability	N+1	N+1	N+1
Guest Anchor	Not Supported	Not Supported	Not Supported

The background is a dark blue field filled with numerous small, semi-transparent squares and dots in various colors including light blue, green, yellow, orange, and red. These elements are scattered across the frame, with a higher concentration of yellow and orange squares on the right side, creating a sense of depth and movement.

Cisco Catalyst 9800 Wireless Controller for SD-Access

SD-Access Everywhere

Optimized for Distributed Branches

Small and Medium Campus

Medium and Large Campus

On Switch



- Cisco IOS® XE Software
- Cat 9300
 - 200 AP, 4k Clients
- SD-Access wireless with Cat9800 Software Package
- Indirect AP Support
- Optimized for Mobility
- Centralize Control Plane
- Always on Fabric with robust HA

On Private Cloud



- Cisco IOS® XE Software
- C9800-CL
 - 1k AP, 10k Clients
 - 3k AP, 32k Clients
 - 6k AP, 64k Clients^
- Scale on demand
- Optimized for mobility
- Designed for IoT
- Always on Fabric with robust HA

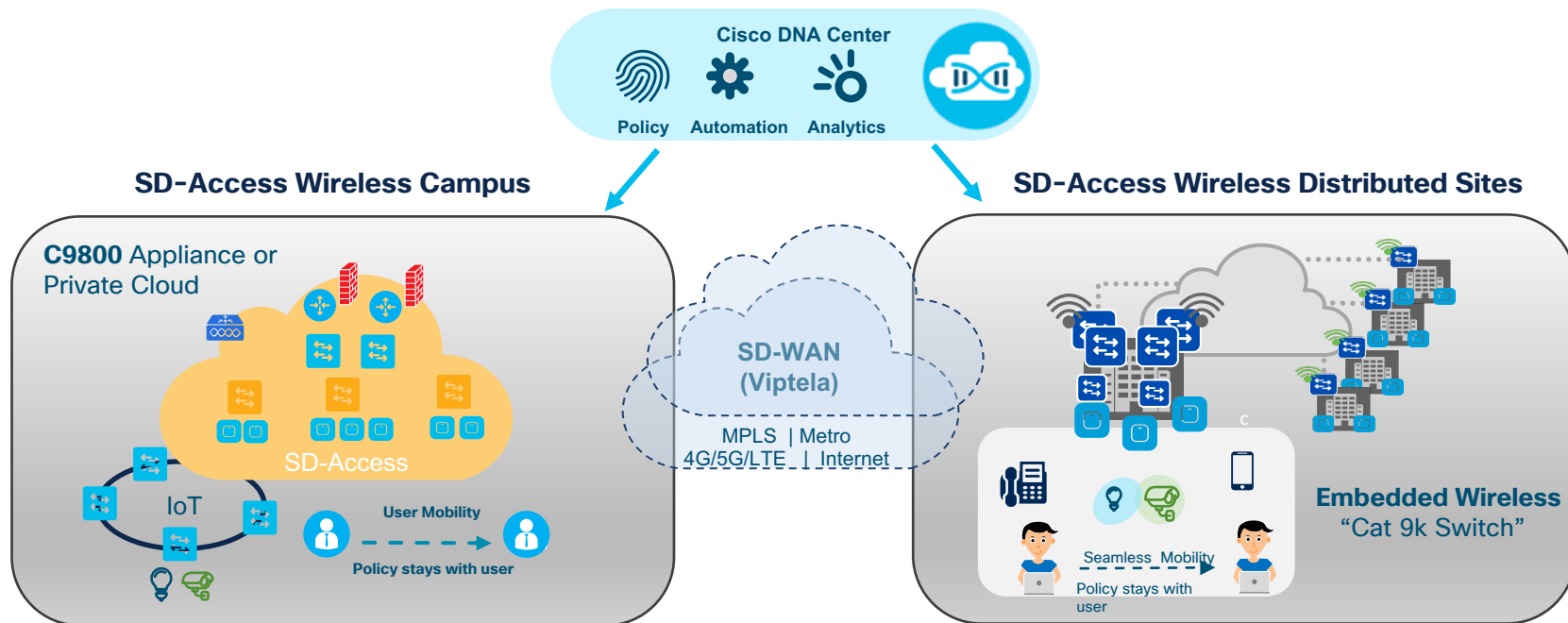
On Appliance



- Cisco IOS® XE Software
- C9800-40-K9
 - 2k APs, 32k Clients
- C9800-80-K9
 - 6k APs, 64k Clients
- Optimized for mobility
- Designed for IoT
- Always on Fabric with robust HA

Catalyst 9800 SD-Access Wireless

Introducing SD-Access Multi-Site Wireless Solution



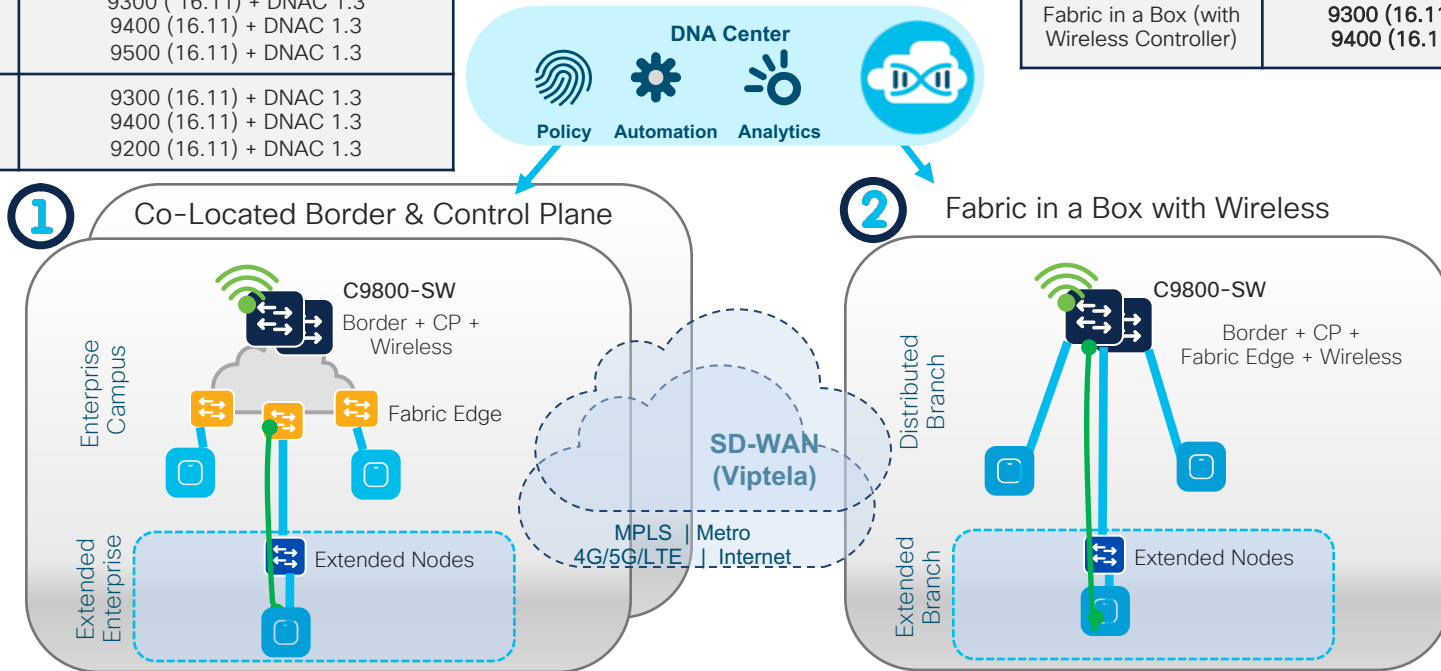
Highly Secure and Optimized Solution for Campus and Distributed Sites

Catalyst 9800 SD-Access Embedded Wireless

DNAC 1.3

Function	Catalyst
Co-located Border and Control + Wireless Controller	9300 (16.11) + DNAC 1.3 9400 (16.11) + DNAC 1.3 9500 (16.11) + DNAC 1.3
Fabric Edge	9300 (16.11) + DNAC 1.3 9400 (16.11) + DNAC 1.3 9200 (16.11) + DNAC 1.3

Function	Catalyst
Fabric in a Box (with Wireless Controller)	9300 (16.11) + DNAC 1.3 9400 (16.11) + DNAC 1.3



SDA Compatibility Matrix: <https://www.cisco.com/c/en/us/solutions/enterprise-networks/software-defined-access/compatibility-matrix.html>

Highly Secure and Optimized Solution for Branch and Small Campus

Cisco Recommended Releases

Catalyst 9800 and 3504/5520/8540 AireOS Wireless Controllers

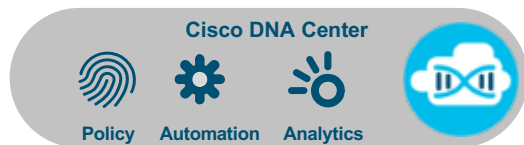
Access Points	IOS-XE	AireOS	DNA-C	Prime	CMX	ISE
C9115AX, C9117AX, C9120AX, 9130AX	16.12.2s	8.10.105.0	1.3.2	3.7MR1	10.6.2	2.2 2.4 2.6
Wave 2	16.12.2s	8.5.161.0	1.3.2	3.7MR1	10.6.2	2.2 2.4 2.6
Wave 2 4800 APs	16.12.2s	8.8.125.0	1.3.2	3.7MR1	10.6.2	2.2 2.4 2.6

Embedded Wireless on C9K Switches

Embedded Wireless on C9K Switches

New

Multi Site Wireless for SDA



Multi Site Secure Wireless Branches SDA Deployment



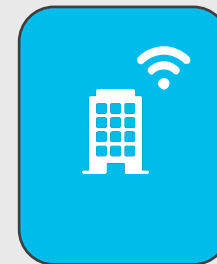
Embedded Wireless
CAT9K Switch (SDA)

Single Site Wireless for Non-SDA



Web UI

Single Site Secure Wireless Deployment

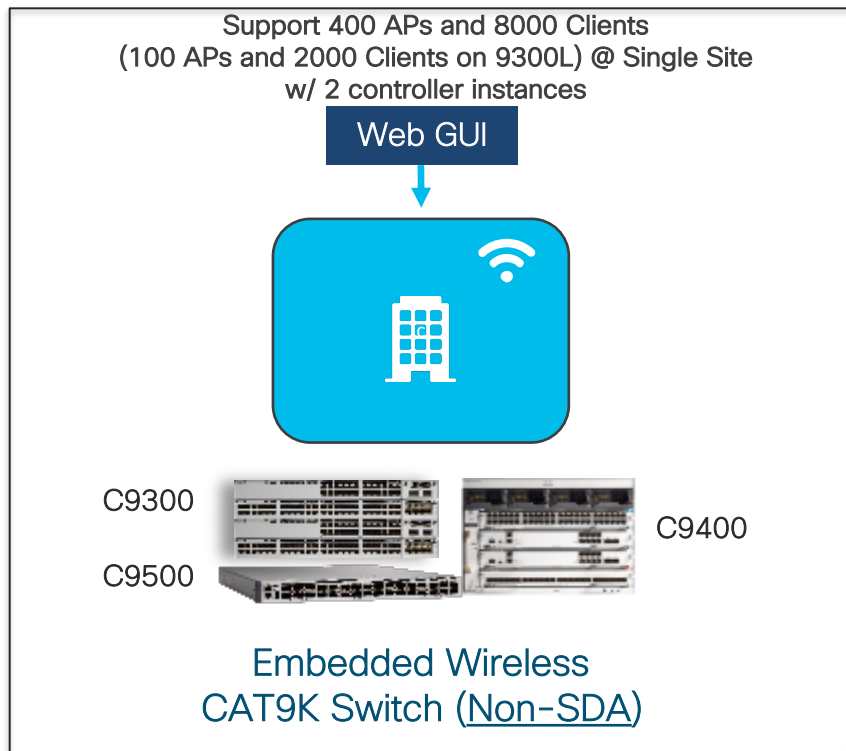


Embedded Wireless
CAT9K Switch (Non-SDA)

Embedded Wireless on C9k Switches (Non-SDA)

Single Site Secure Wireless Deployment

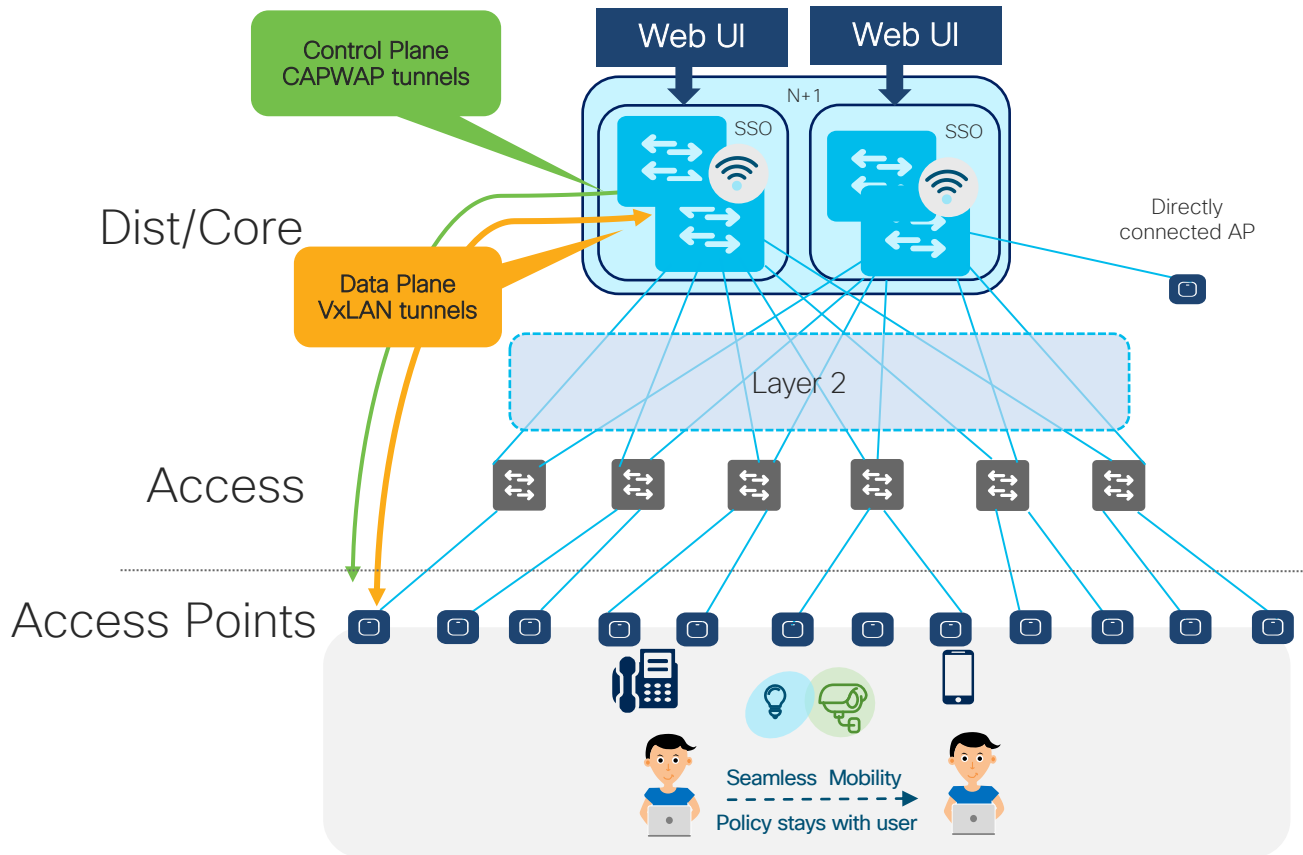
IOS-XE 17.3



- Support 9300L/9300/9400/9500 Catalyst switches
- Designed for Single Site deployment
- Configuration via C9K Web UI only
- Support 200 AP and 4000 clients per switch or switch stack (50 AP and 1000 Clients with 9300L)
- Max 2 embedded controller instances (N+1 mode) on separate Catalyst 9000 series switches
- DNA Advantage License

Switch Model	AP Scale	Client Scale
9300L	50	1000
9300 9400 9500 9500H	200	4000

Embedded Wireless on C9K Switches (Non-SDA)



High Availability (SSO)

- Embedded 9800 runs on Active switch in a stack
- Cannot run more than one instance on one stack
- SSO within stack



All 11ax APs

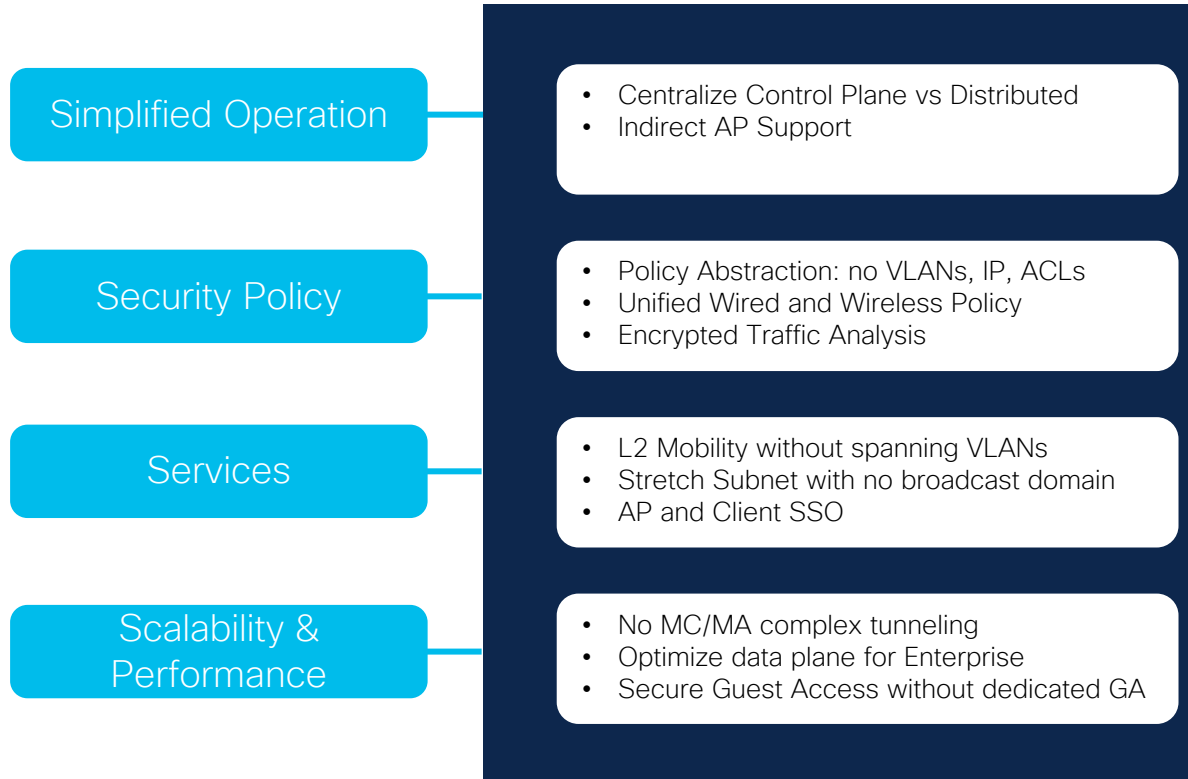


Wave 2 APs (1800, 2800, 3800, 4800)



Outdoor Wave 2 APs (1540, 1560)
Local Mode Only

Embedded Wireless on C9K Switches (Non-SDA) vs CA



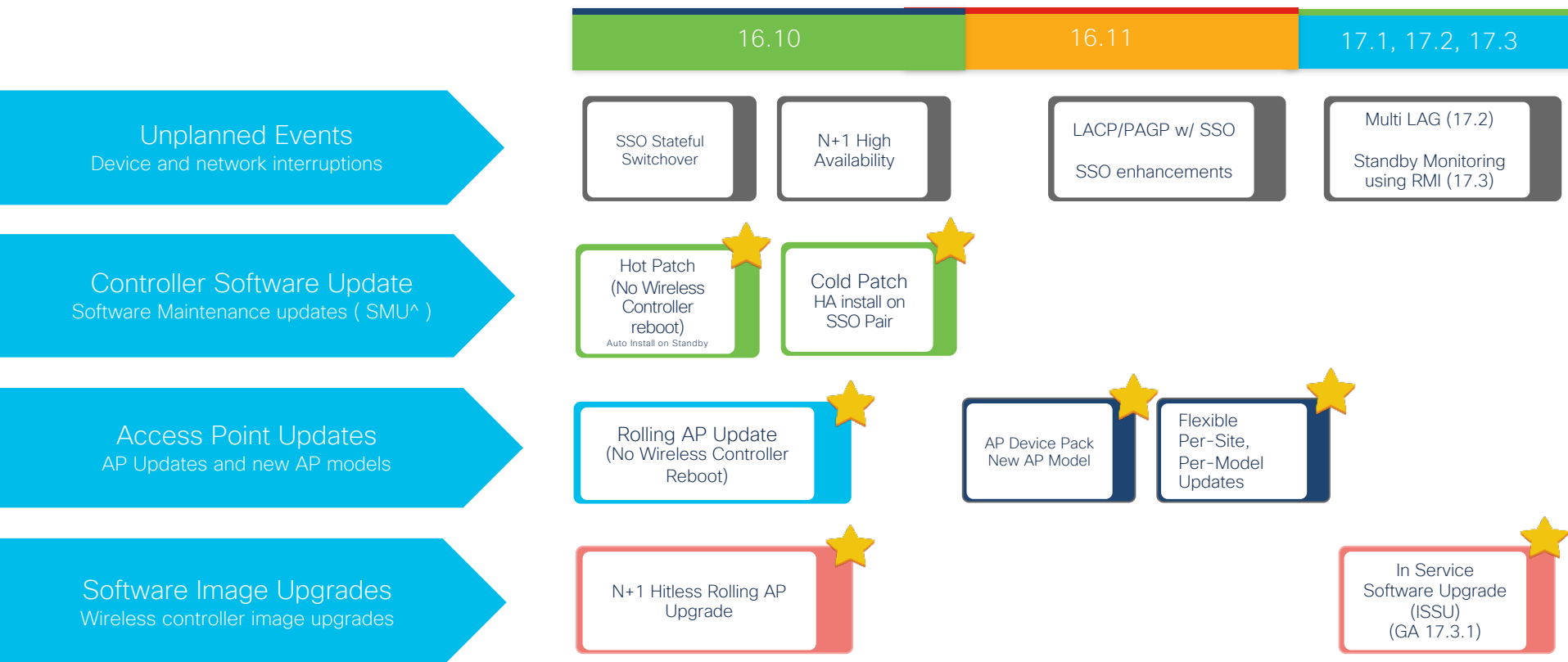
Embedded Wireless on C9K Switches (Non-SDA) : Features Supported

Full Stack Health Visibility	Security and Authentication	Services	RF and Radio	Resiliency
<ul style="list-style-type: none"> WebUI Programmability (Netconf+Yang) 	<ul style="list-style-type: none"> WPA-PSK 802.1x(WPA2/AES) 802.1x (WPA2/TKIP) WPA3 Identity PSK MutiPSK on Single SSID Internal Webauth External Webauth Central Webauth DNS Pre-auth ACL 802.11r 802.11k 802.11v BSS transition 802.11v DMS PMF (802.11w) TACACS Radius server per WLAN Backup Radius Servers CCKM User idle timeout per WLAN 	<ul style="list-style-type: none"> AVC-Mark, Drop, RL AAA override-VNID AAA override: QoS AAA Override – Session timeout AAA override of AVC profile AAA override BW contract QoS Local Profiling RADIUS Profiling Per User Bandwidth Contract Per-SSID Bandwidth Contract Multicast CAC,WMM Policy Adaptive 11r Fastlane MAB MAC Authentication Rogue Detection Passive Clients BYoD, NAC RADIUS, CWA,LWA 	<ul style="list-style-type: none"> RRM-DCA,TPC,CHDM FRA Band Select Load Balancing RF Profiles XOR Optimized Roaming RX-SOP DFS DBS Off-channel Scanning Off-channel scan defer ClientLink A-MSDU/A-MPDU aggregation config per priority ATF UL OFDMA DL OFDMA UL MU MIMO DL MU MIMO TWT BSS Coloring 	<ul style="list-style-type: none"> High availability :SSO High availability : N+1 Hot/Cold Patching AP Service Pack(APSP) AP Device Pack (APDP)
AP Modes				
<ul style="list-style-type: none"> Local switching with Central Auth Monitor Mode 				
Infrastructure				Segmentation
<ul style="list-style-type: none"> Pre-image Download Client IPv6 FIPS Certification* DHCP Option 82 				<ul style="list-style-type: none"> Up to 4 segments No SGT based Segmentation

Resiliency

High Availability

Reducing downtime for Upgrades and Unplanned Events





For your
reference

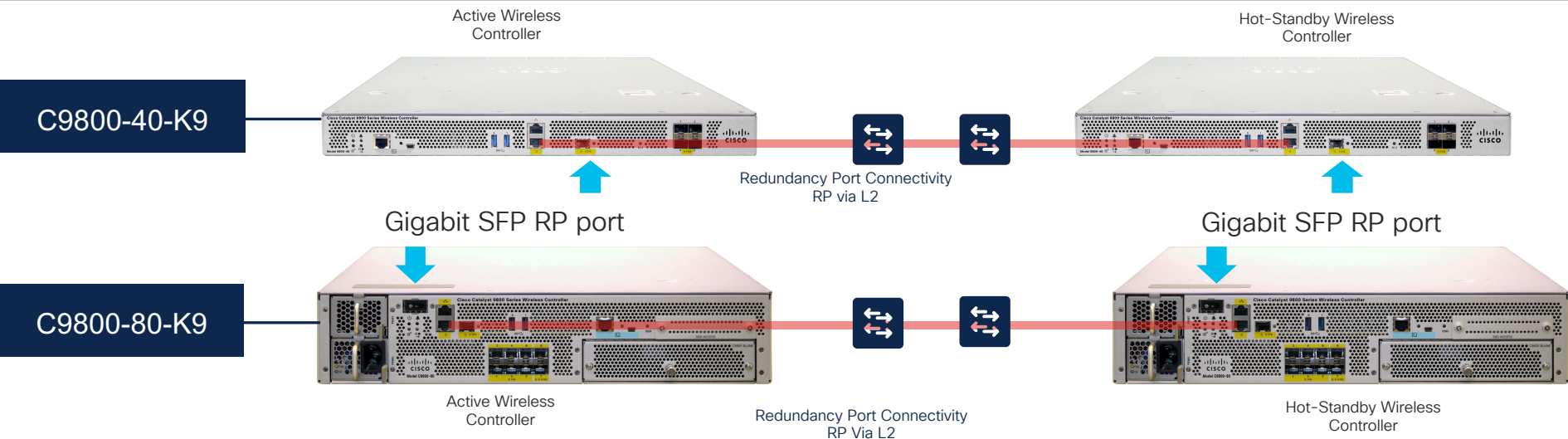
Resiliency Feature Matrix

Functionality		EWC on AP	Embedded controller on 9K	9800-L	9800-40	9800-80	9800-CL PVT Cloud	9800-CL Public Cloud
Unplanned Events	SSO	No	Supported	Supported	Supported	Supported	Supported	No
	SMU	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Infrastructure updates	APSP	Supported	Supported	Supported	Supported	Supported	Supported	Supported
	APSP Per-site	No	Supported	Supported	Supported	Supported	Supported	Supported
	APDP	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Image Upgrade	ISSU	No	No	Supported	Supported	Supported	Supported	No
	N+1 Rolling AP Upgrade	Supported	Supported	Supported	Supported	Supported	Supported	Supported

High Availability – Stateful Switch Over (SSO)

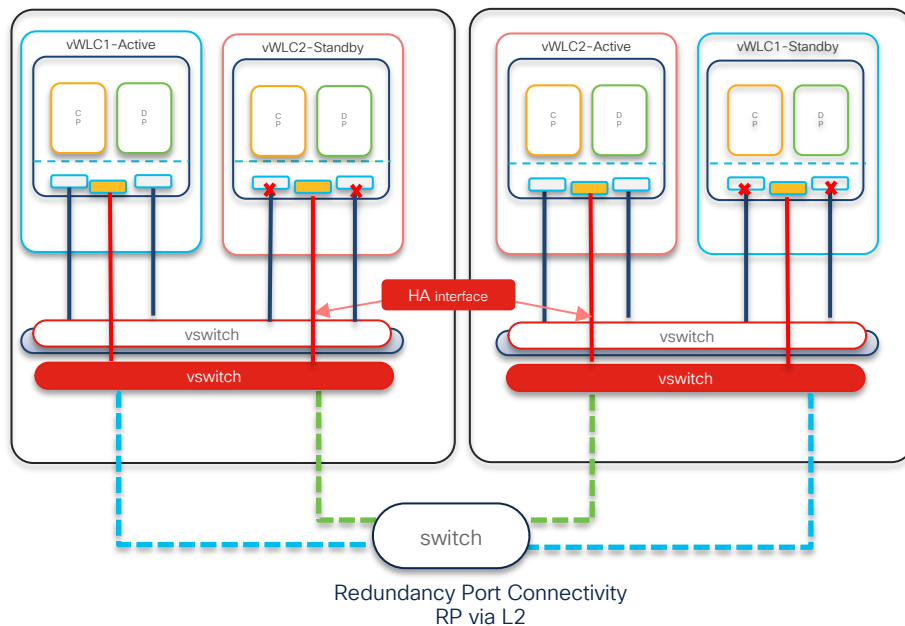
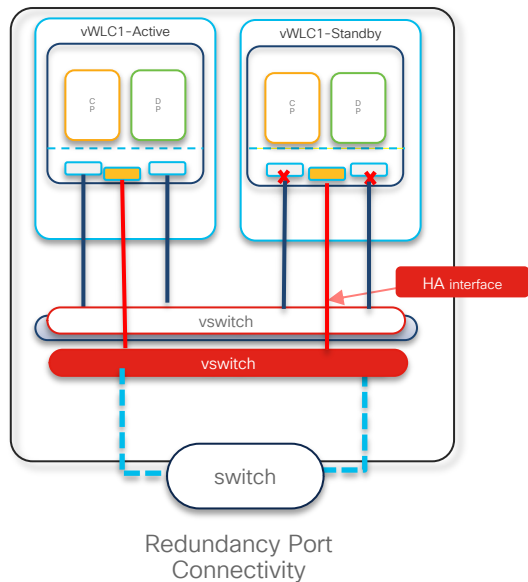
A direct physical connection between Active and Standby Redundant Ports or Layer 2 connectivity is required to provide stateful redundancy within or across datacenters

Sub-second failover and zero SSID outage



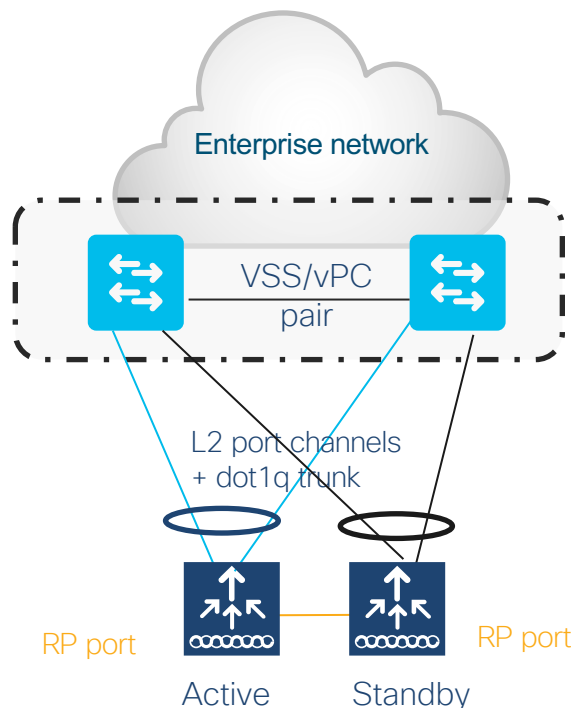
High Availability – Stateful Switch Over (SSO)

C9800-CL-K9



Single VSS switch (or stack/VSL pair/modular switch)

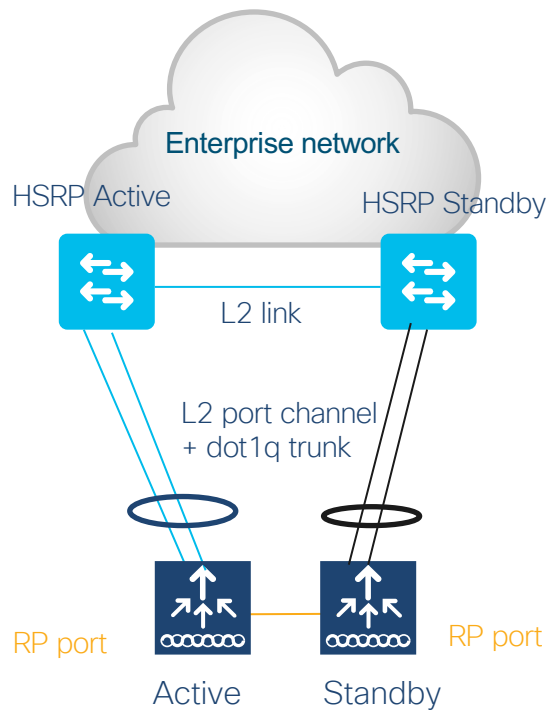
SSO HA pair



- For SSO HA, connect the Standby in the same way (same ports)
- Single L2 port-channel on each box. Ports connected to Active and ports connected to Standby must be put in different port-channel
- Enable dot1q to carry multiple VLANs
- IMPORTANT: **only LAG with mode ON is supported**
- IMPORTANT: **spread the uplinks across the VSS pair and connect the RP back to back (no L2 network in between)**
- Make sure that switch can scale in terms of ARP and MAC table entries
- **This is the recommended topology**

Dual Distribution switches with HSRP (17.1 and higher)

SSO HA pair



- For SSO HA, connect the Standby in the same way
- Single L2 port-channel on each box. Ports connected to Active and ports connected to Standby must be put in different port-channel
- Port-channel PagP and LACP supported
- Enable dot1q to carry multiple VLANs
- Make sure that switch can scale in terms of ARP and MAC table entries
- **This is a Recommended topology**



Planned Updates

Wireless Controller and AP SW Updates

Controller and AP software upgrades



Controller Updates

Controller update or bug fixes

SMU



PSIRTs, fixes on APs

AP update or bug fixes

AP Service Pack



New AP Model Support

Hot-patchable support for Device Pack

AP Device Pack



Contain impact within release
Fixes for defects and security issues
without need to requalify a new release



Faster resolution to critical issues
Provide fixes to critical issues found in
network devices that are time-sensitive



Controller Patching

using Software Maintenance Updates

Wireless Controller SMU

Wireless Controller SMU installation Options

- Software Maintenance Update (SMU) is the ability to apply patch fixes on a software release in the customer network
- Current mechanism relies on Engineering Specials
 - Entire image is rebuilt and delivered to customer

Hot Patch
(No Wireless Controller reboot)
Auto Install on Standby

Hot-Patching

Inline replace of functions without restarting the process

On SSO Systems, patch will be applied on both active and standby without any reload

Cold Patch
Wireless Controller Reboot

Cold Patching

Install of a SMU will require a system reload

On SSO systems, SMU updates can be installed on the HA Pair with zero downtime

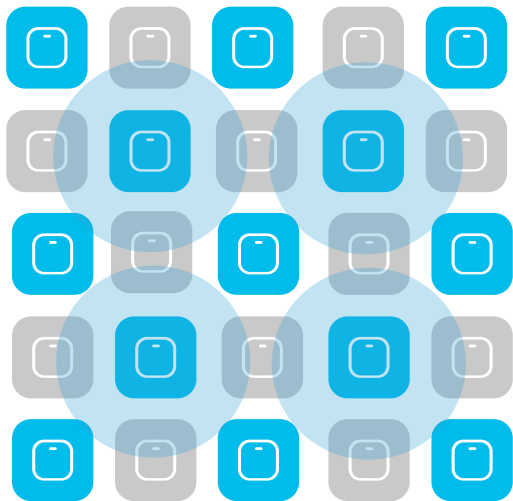
✓ SMUs for C9800 are available starting the first MD Release 16.12



AP Patching

using Rolling AP Infrastructure

Neighbor Marking



User selects % of APs to upgrade in one go [5, 15, 25]

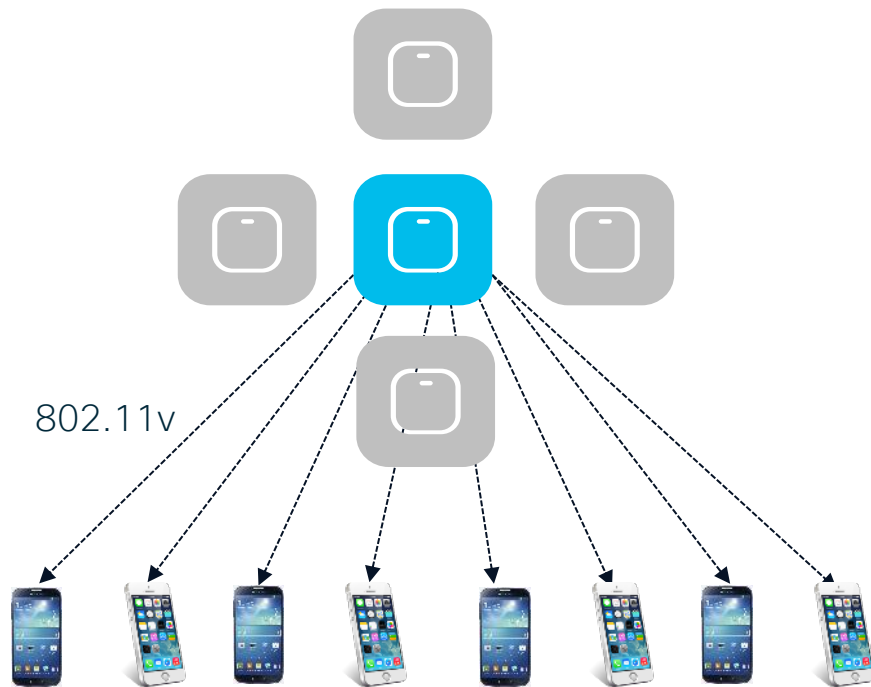
For 25%, Neighbors marked = 6 [Expected number of iterations ~ 5]

For 15%, Neighbors marked = 12 [Expected number of iterations ~ 12]

For 5%, Neighbors marked = 24 [Expected number of iterations ~ 22]

Client Steering

- Clients steered from candidate APs to non-candidate APs
- 802.11v BSS Transition Request
- Dissociation imminent
- If clients do not honor this, they will be de-authenticated before AP reload



Per-site / Per-model AP Service Pack



Supported on all platforms and all deployment scenarios (Flex, Local and Fabric)



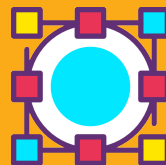
Pre-downloaded to and activated on the affected AP models only



Per-model APSP works in conjunction with site-specific rollout



Per-AP model Service Pack
APSP can have a subset of APs that are affected by the update



Update on Subset APs
Fix applied on a subset of APs in the deployment using a site-filter



Controlled Propagation
Enables user to control the propagation of APSP in the network

APSP Workflow

Applying APSP for 3800/2800 APs on per-site and per model basis

ap image site-filter file APSP1 add SiteA

Install prepare activate

Install activate

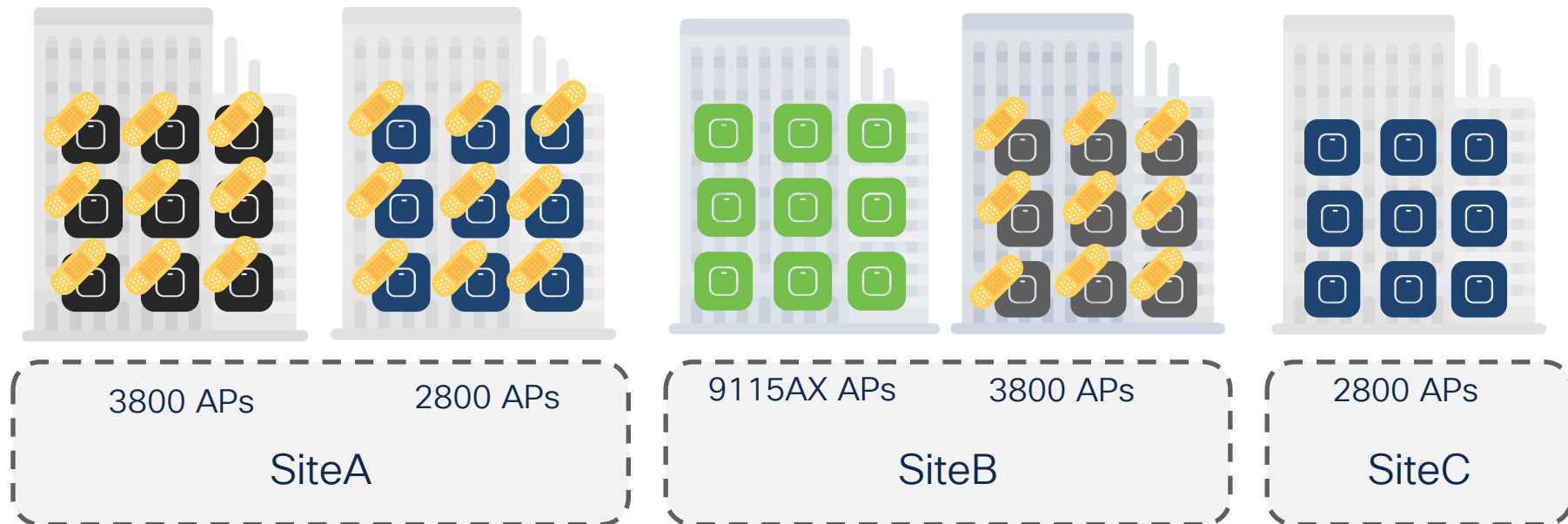
Install commit

ap image site-filter file APSP1 add Site B

ap image file APSP1 site-filter apply

Not applicable for building with 9115AX

Apply on Site A in rolling AP fashion



AP Device Pack

AP Device Pack

Traditionally ..



New AP hardware models need new WLC software



Wait for CCO version and re-qualify new release



Plan for Upgrading entire network



Contain Impact within release

Deploy new hardware without need to requalify a new controller release



Reduce Lifecycle delays

Faster deployment of latest AP hardware and technology



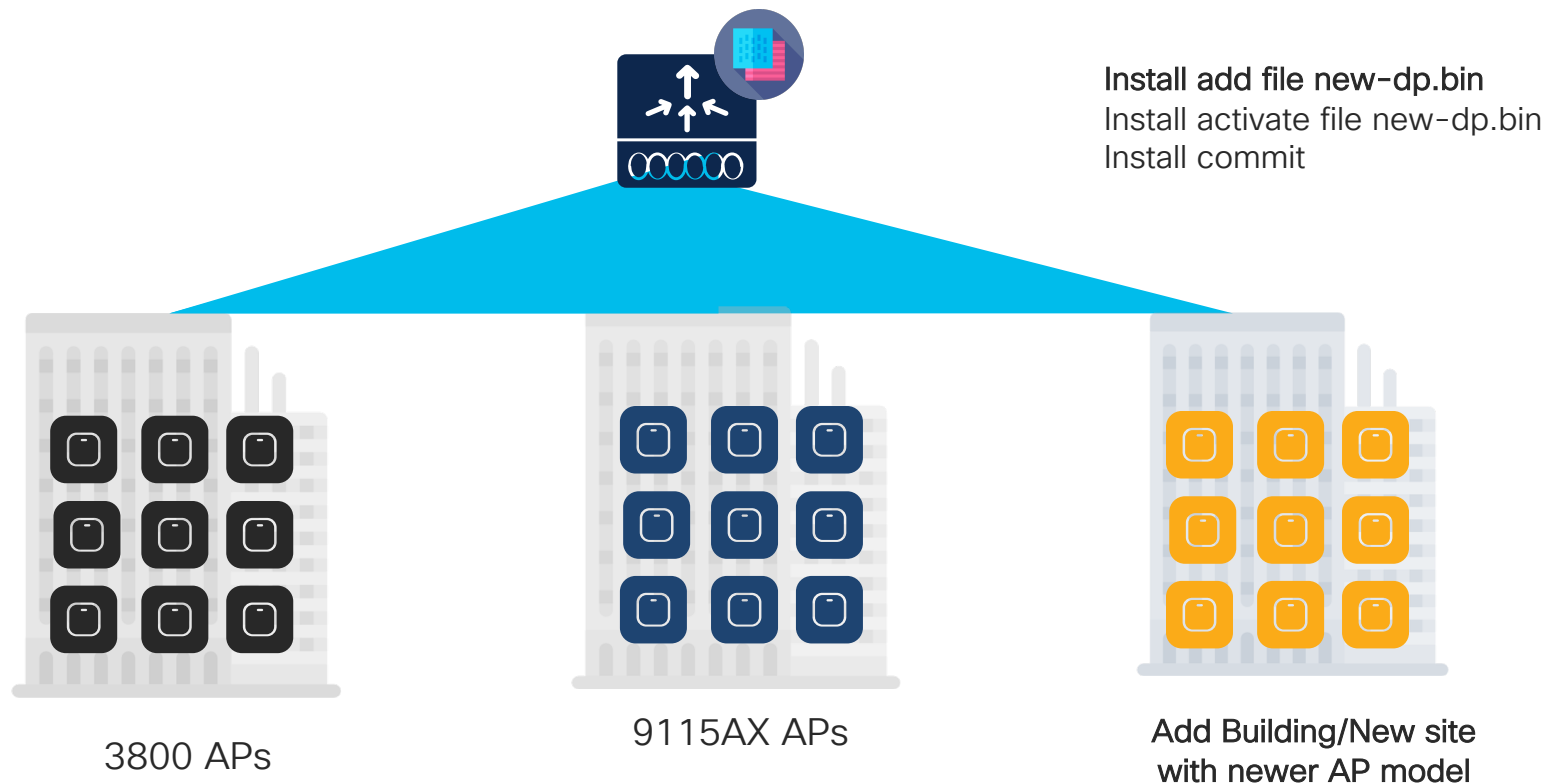
Zero Network Downtime

Applied as HOT patch on the controller with no service impact for APs and Clients

With AP Device Packs

Note : Even if new AP software supports extra wireless functionality, only the functionality supported by WLC will be enabled.

APDP Installation Workflow

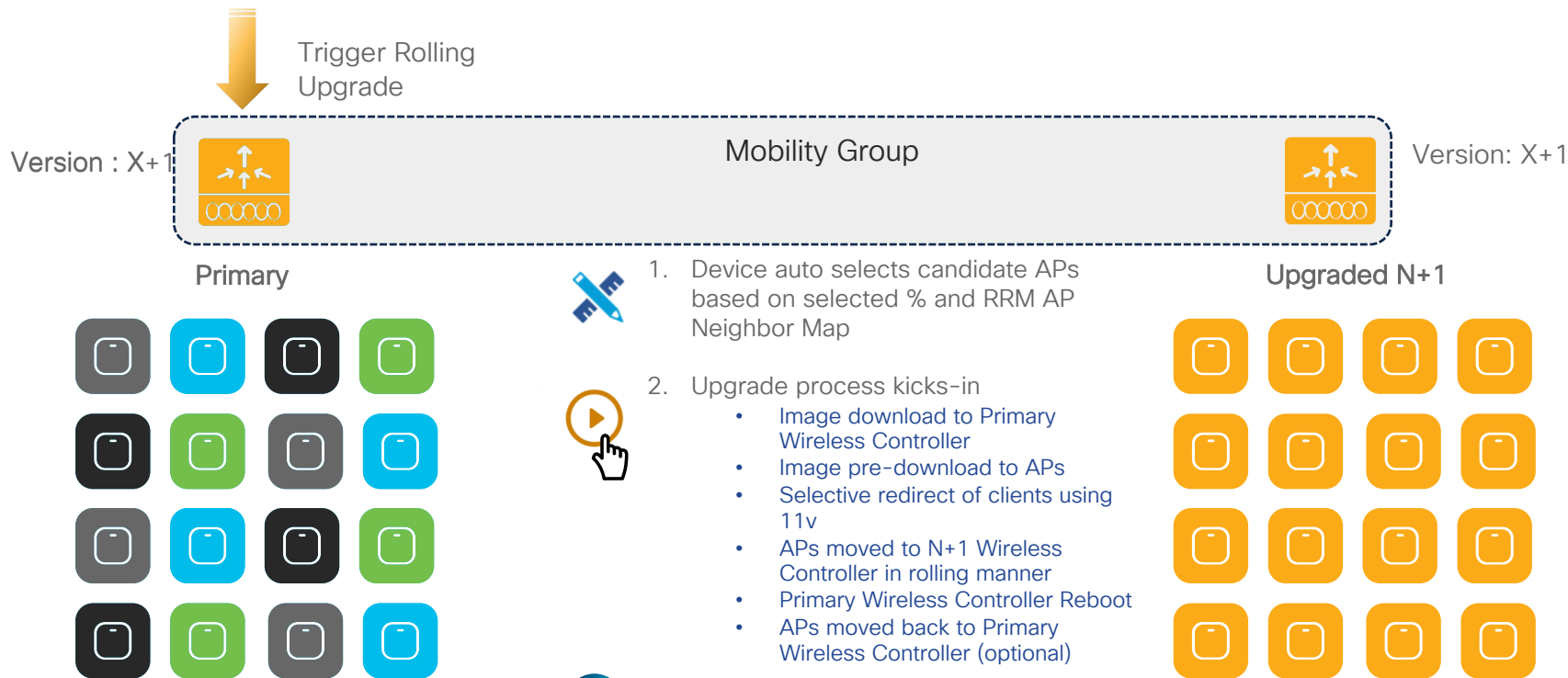



Note: Fixes for the AP installed via APDP will be via AP Service packs like a baseline supported AP

Hitless N+1 Image Upgrade

N+1 Rolling AP Upgrade

Wireless Controller image upgrade using N+1 staging Controller





In-Service Software Upgrade (ISSU)

Why ISSU?

Eliminate network downtime during controller upgrade process



Eliminate the need for a dedicated N+1 controller in the upgrade process



Automate the process of upgrade without manual intervention



What is ISSU ?



Complete image upgrade from one image to another while traffic forwarding continues



All AP/Client sessions are retained during upgrade process

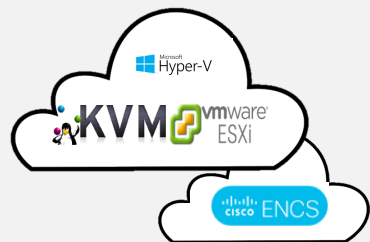


Pre-requisites:

- ✓ Base image is ISSU capable
- ✓ SSO pair in Active-Hot Standby
- ✓ Controllers in INSTALL mode

Supported Platforms for ISSU

Controllers



Catalyst 9800-CL



Catalyst 9800-L



Catalyst 9800-40



Catalyst 9800-80

Access Points



9115, 9117, 9120, 9130 11ax APs



1815W



1815i, 1815M



1832



1842



1852



2802



3802



1700, 2700, 3700,
1570 Wave 1 APs



1540



1560

Wave 2 indoor and outdoor APs



4800

CISCO *Live!*



ISSU WebUI Workflow contd.

Post commit, the ISSU process is completed

The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller WebUI. The top navigation bar includes the Cisco logo, the controller name, a timestamp (17.1.2019 08:26), a welcome message for 'dragon', and various system icons. A search bar for 'APs and Clients' is also present. The left sidebar contains a 'Search Menu Items' bar and a list of navigation options: Dashboard, Monitoring, Configuration, Administration (highlighted), and Troubleshooting. The main content area is titled 'Administration > Software Management' and features a 'Software Upgrade' section. This section includes fields for 'Upgrade Mode' (set to INSTALL), 'Transport Type' (set to TFTP), 'Server IP Address (IPv4/IPv6)*', and 'File Path*'. The 'ISSU Upgrade' checkbox is checked. A 'Download & Install' button is visible. On the right, a 'Status' panel, outlined in red, lists the following steps with green checkmarks: 'Download Image/Package', 'Install Image/Package', 'AP Image Predownload', 'Activate Stand-by', 'Activate Active', 'Switchover', 'AP Image Upgrade' (with 'Percentage complete: 100'), and 'Install Commit'. At the bottom right of the status panel, there are links for 'Show Logs', 'AP Predownload Statistics', and 'AP Upgrade Statistics'.

Cisco Catalyst 9800-CL Wireless Controller
17.1.2019 08:26
Welcome dragon

Administration > Software Management

Software Upgrade

SMU
APSP
APDP

Upgrade Mode: INSTALL
Current Mode (until next reload): INSTALL

Transport Type: TFTP

Server IP Address (IPv4/IPv6)*

File Path*

ISSU Upgrade: ☒

Download & Install

Status

- Download Image/Package
- Install Image/Package
- AP Image Predownload
- Activate Stand-by
- Activate Active
- Switchover
- AP Image Upgrade
Percentage complete: 100
- Install Commit

Show Logs
AP Predownload Statistics
AP Upgrade Statistics

Security

Intent-based wireless networks to secure the Air, Devices and Users with Catalyst 9800



Air



Devices



Users



Rogue detection &
Mitigation



Enhanced threat
detection with ETA



Seamless BYOD
onboarding with ISE

WPA3



Standards compliance
with WPA3*

- Enhanced security on open Wi-Fi
- Robust password protection
- Superior data protection
- Seamless customer migration



Secure device
management with iPSK



Identity based
segmentation with SDA

CISCO *Live!*

**Future*

Security and Threat Mitigation



802.1x
WPA2/AES



WPA3



P2P
Blocking



MAC Auth



802.11w



Rogue Detection



ETA



TrustSec
SGT, SXP



AAA Override
VLAN, ACL, QoS



Local Policy w/
QoS and AVC



BYOD
NAC RADIUS



Client Exclusion

Lower Risk



Cisco Remote Workforce Network

Secure enterprise network for business
resiliency

Secure, Instant Connectivity using Cisco

Remote Workers



Providing **remote teleworkers** with **on-demand internet connection** for high-quality voice, data and video

Pop-up Relief Camps

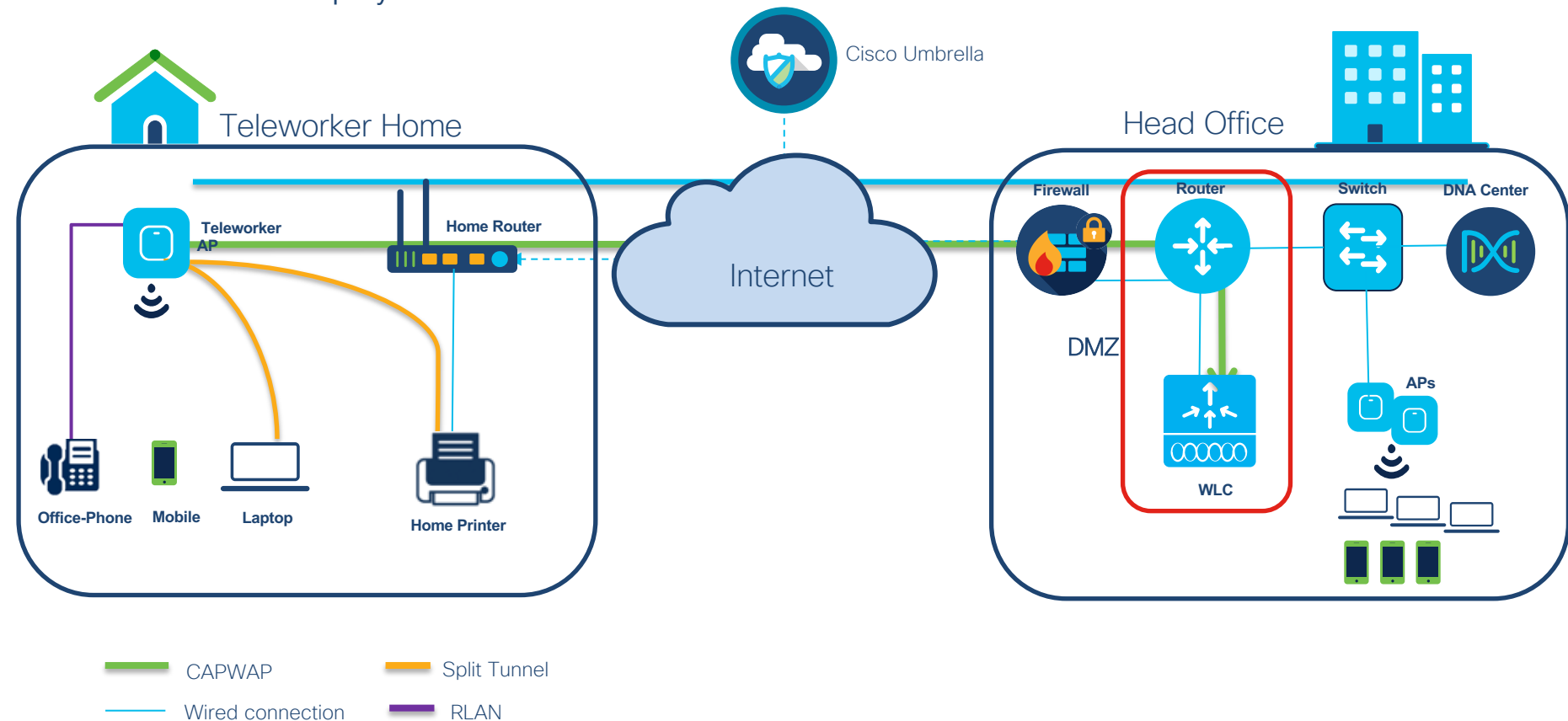


Cloud connectivity for pop-up medical facilities, health & relief camps, urgent care & more

Quarantined Users



Secure access in make-shift facilities connecting quarantined individuals, using cloud apps over Cellular & UDN



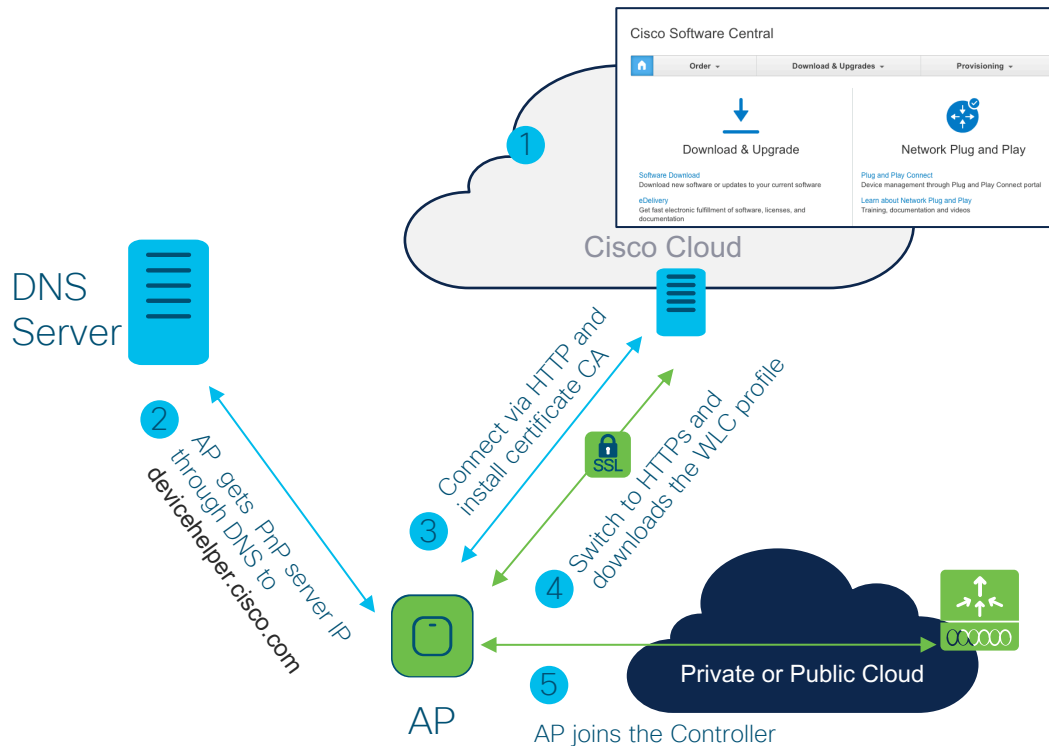
Getting Started with Teleworker/OEAP

- WLC requires a public routable IP address so remote APs can reach WLC from their home network (can be in DMZ)
- That public IP can be added as a NAT IP on WLC management interface
- Some ports like CAPWAP needs to be open on firewall as the Teleworker APs at home need to communicate with WLC in the DMZ using the CAPWAP ports 5246 and 5247
- For non OEAP models AP (for e.g. 1600/2600/3600/2700/3700/1800/3800/4800/C9100 etc. - admin needs to change the AP mode to FlexConnect and then enable OEAP option.
- Pre-configure the OEAPs to join the WLC i.e. configure OEAP with WLC management public IP address.
 - Through Cisco Network Cloud PnP
 - Master WLC

AP Models	Teleworker AP		RLAN/Aux port	9800	AireOs (3504, 5520,8540)
9100 Series	Supported	N/A (AP does not have Aux Ports)		17.3	8.10 MR2
Wave 2 Aps (including 4800)	Supported	28xx/38xx/1850/1810/1815T/1815w supports RLAN		17.3	8.10.MR2

DAY 0 Experience – AP PnP

• AP PnP with Cloud PnP



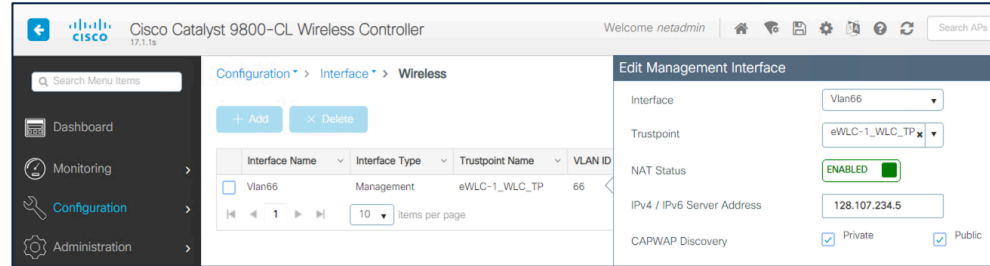
Upon ordering the customer selects a zero \$ SKU for PnP. The AP is automatically added to the device list in the Plug and Play Connect account associated to the customer smart account.

1. User logs in Plug & Play Connect account on `cisco.com` and creates a Wireless Controller profile
2. AP discovers PnP server IP via DNS to a known URL (`devicehelper.cisco.com`)
3. AP connects to PnP Server, synchs the time and download the certificate
4. AP connects to PnP server via HTTPS and download the Wireless Controller information
5. AP joins the Controller

Cisco Teleworker WLC Config -Reference

Step 1: Set up the virtual controller** to be used in DMZ

Step 2: If a publicly reachable IP address is not assigned directly to the controller, enter the NAT IP address by going to **Configuration → Interface → Wireless** under the wireless management interface configuration.



Step 3: Configure the WLAN and Policy for the wireless network that would be extended to the remote user. (Example based 802.1X)

Step 4: Navigate to **Configuration → Tags & Profiles → Flex** and modify the **default-flex-profile** (or create a new one) to enable **Office Extend AP**

Step 5: Go to **Configuration → Tags & Profiles → AP Join** to edit the **default-ap-profile** (or create a new one) and under the CAPWAP Advanced parameters make sure that **Enable Data Encryption** is enable to secure the traffic traversing the internet.

Step 6: Go to **Configuration → Tags & Profiles → Tags** to edit the **default-site-tag** (or create a new one) that is mapped to the Flex Profile from the previous step. Make sure that **Enable Local Site** is unchecked.

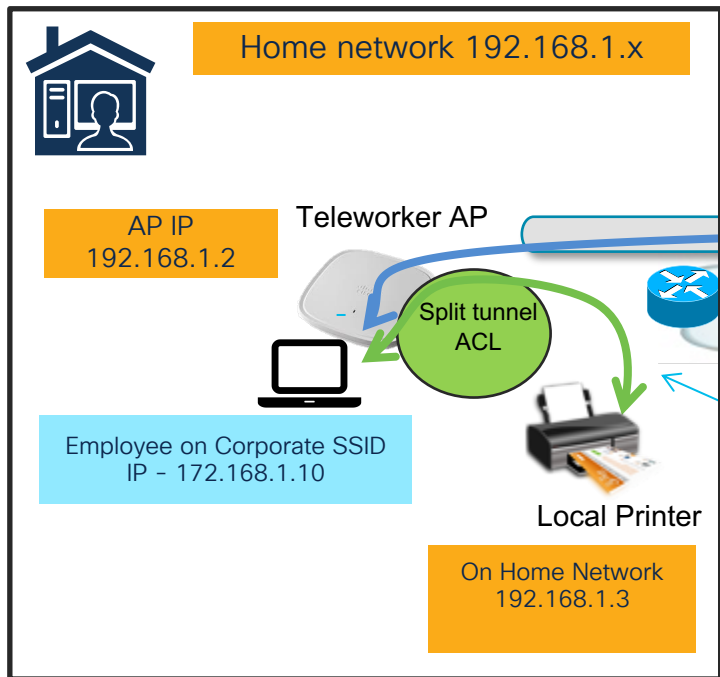


[Watch a 9800 WLC Guided configuration Walk-through](#)

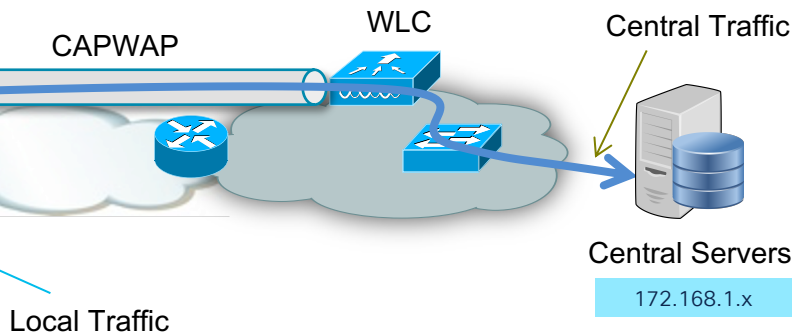
Teleworker Split Tunnel Use case

172.168.1.x Subnet – Central Corporate DHCP

192.168.1.x Subnet – Local DHCP in Home



- ❑ The SSID should be centrally switched SSID with central DHCP
- ❑ All wireless client traffic from will be centrally switched by default
 - ❑ If the Wireless client is trying to reach to local subnet
 - ❑ It will hit the split tunnel rule on AP
 - ❑ AP will NAT this traffic using AP IP (192.168.1.x) IP locally

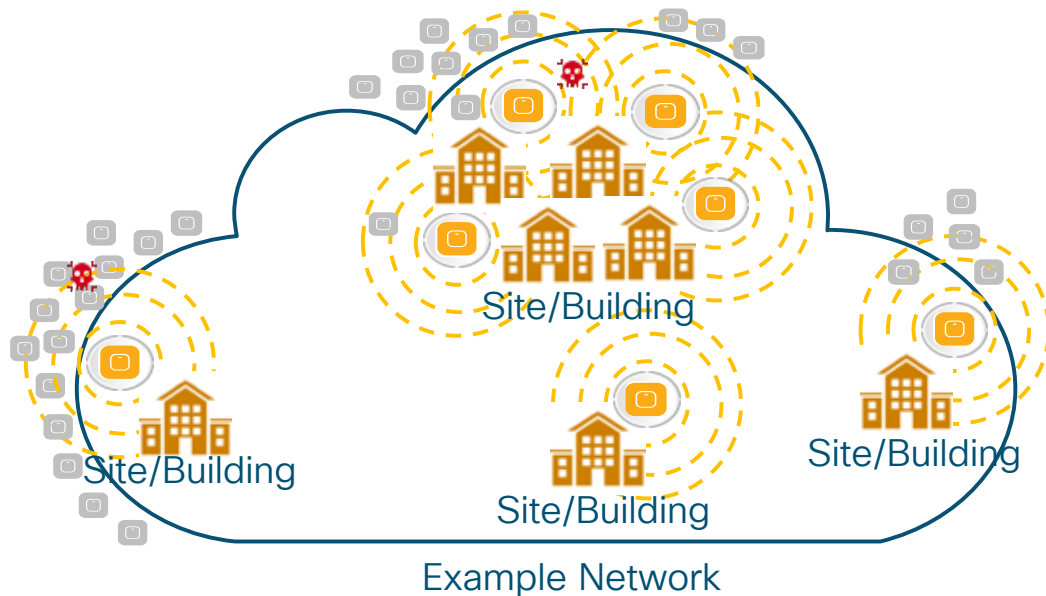


Split Tunnel ACL

- ❑ Allow 192.168.1.x <- Allowed traffic will be switched locally using NAT
- ❑ Deny 172.168.1.x <- Denied traffic on split ACL will be centrally switched
- ❑ Deny all

Rogue and wIPS Management

Customer perspective: Dynamic and high stakes



What devices if any pose a threat to my organization?

How can I possibly stay on top of this across my entire network on an ongoing basis?

How can I report on this internally?
How can I respond if I find a threat?

How can I report on this for compliance purposes as well as for auditors?



Authorized Access Point



Unauthorized Access Point (a.k.a. Rogue)

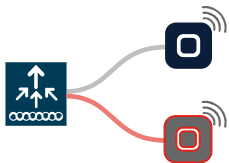


Threat

WLAN has inherent vulnerabilities, exposing it to various threats

On Wire Attacks

Rogue on Wire
Unknown | **Malicious**



✓ Switch-port Tracing

✓ RLDLP

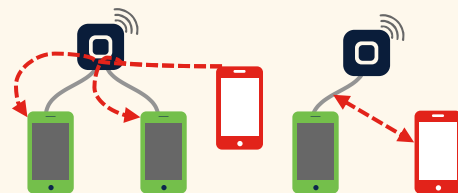
Over-the-Air Attacks

Rogue Access Points | Honeypot or Evil Twin | AP MAC Spoofing



✓ Rogue Management
Basic Wireless Security

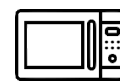
Denial of Service | Reconnaissance | Cracking Tools



✓ WIPS
Advanced Wireless Security

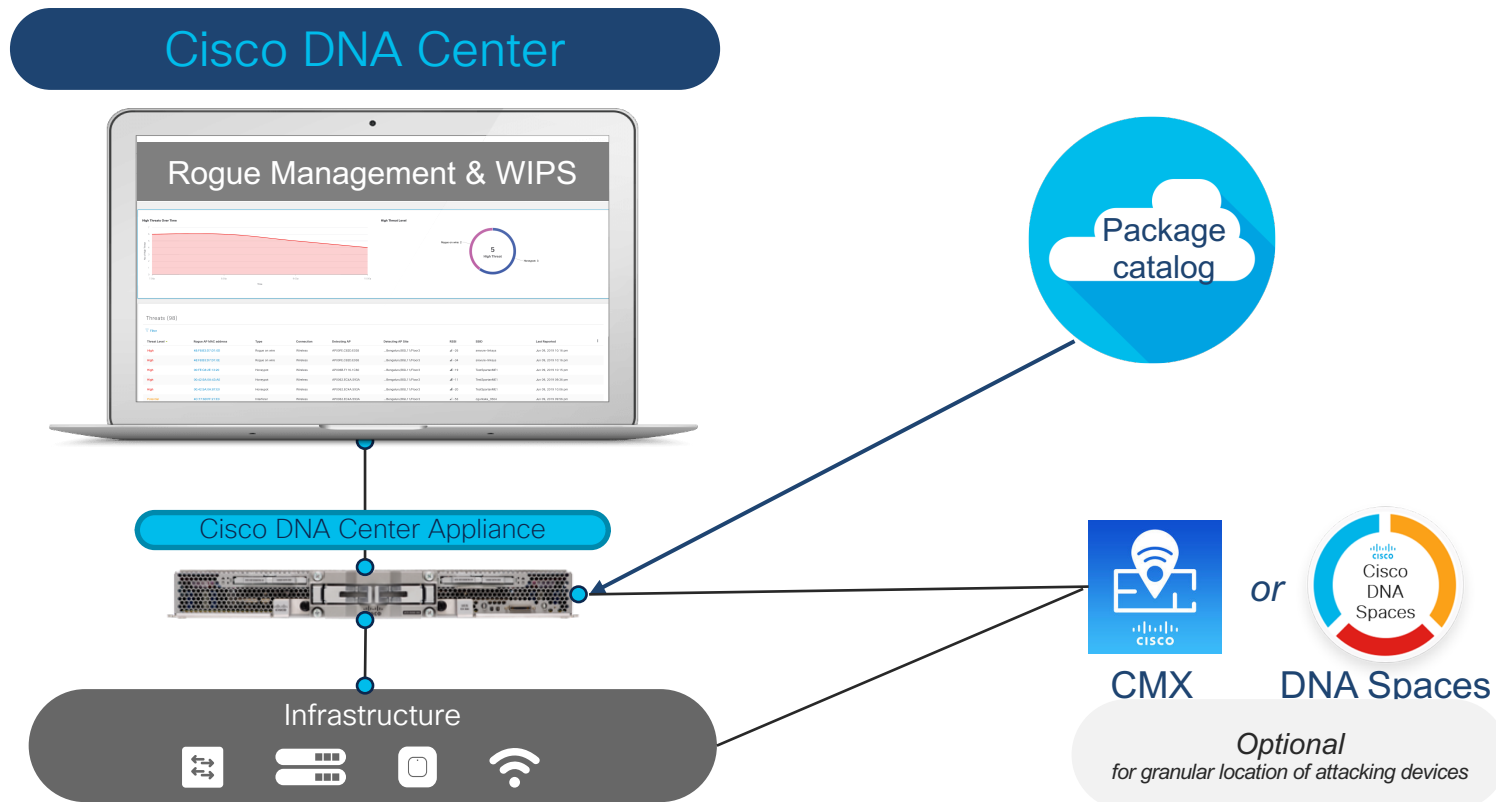
Non-802.11 Interferers

Microwave | Bluetooth
Radar | RF Jammers

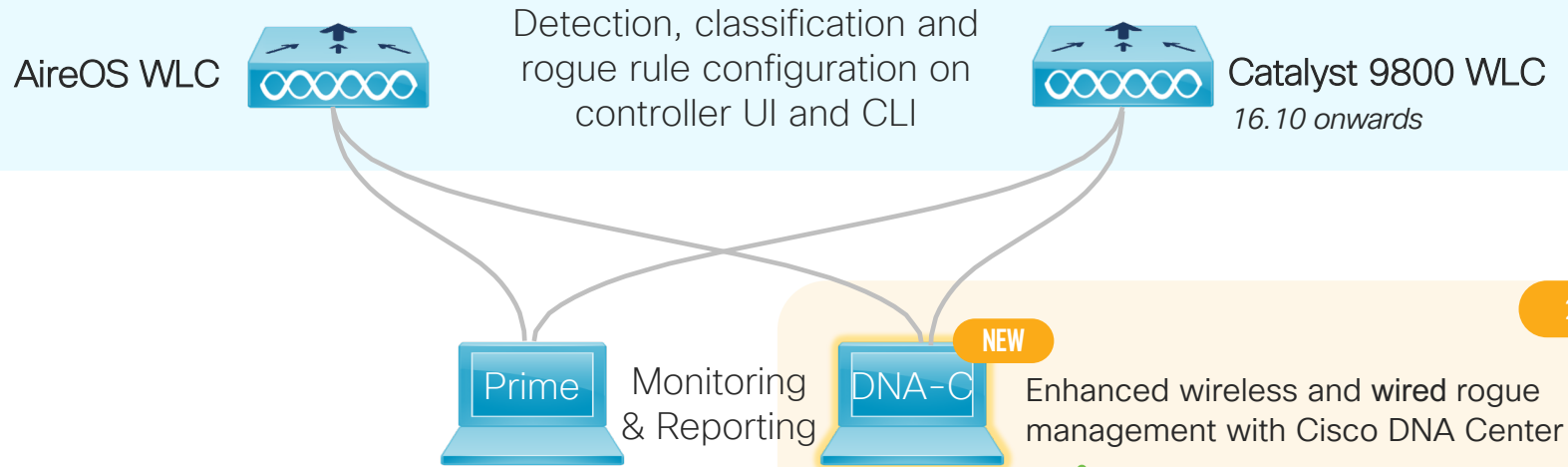


✓ Cisco CleanAir
Visibility of non-Wi-Fi interferers

NextGen Wireless Security on Cisco DNA Center



Rogue Management architecture options



2H 2019


Rogue signatures include: Rogue on Wire, Rogue Access Points, Honeypot or Evil Twin
AP MAC Spoofing (roadmap)

Enhanced accuracy and prioritization of threats on Cisco DNA Center

Improved accuracy and faster time to detection for highest priority rogue alarms

Rogue Devices by Detecting APs

1 Site(s) in the Map



North Atlantic Ocean

United States

México

Gulf of Mexico

Cuba

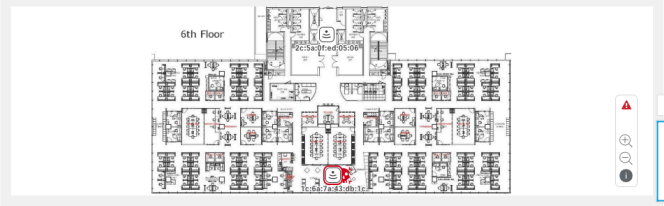
Sargasso Sea

Threat 360: Mac 00:fe:c8:2e:13:20

Export CSV

Threat Level	Threat Type	Status	Rogue Vendor	First Reported	Last Reported
High	Honeypot	Active	Cisco Systems, Inc	Sep 24, 2018 07:56 am	Oct 07, 2018 02:44 pm

Location: ...Bangalore/BGL-11/Floor6



6th Floor

Make a Wish

Filter

Threat Level	Mac Address	Type	Connection	Detecting AP	Det
High	00:fe:c8:2e:13:20	Honeypot	Wireless	3702_84	...
High	00:42:5a:0a:87:e0	Honeypot	Wireless	3702_84	...
High	00:42:5a:0a:43:a0	Honeypot	Wireless	3702_84	...
Potential	c0:7b:bc:76:0f:e0	Interferer	Wireless	3702_84	...
Potential	04:62:73:26:a4:30	Interferer	Wireless	3702_84	...
Potential	00:fc:ba:c8:d7:a0	Interferer	Wireless	3702_84	...
Potential	00:fe:c8:21:1a:00	Interferer	Wireless	3702_84	...

Detecting Access Points (5) Clients (0)

Filter

Detecting AP	AP Domain	Rogue SSID	RSSI	Channels	Radio Type	Security	SNR
3702_84	...Bangalore/BGL-11/Floor6	kukr245	-20	11	802.11abgn	--	44
3702_84	...Bangalore/BGL-11/Floor6	JioFi2_7B5BCD	-21	11	802.11n (2.4)	--	63
3702_84	...Bangalore/BGL-11/Floor6	JioFi2_7B5BCD	-26	136	802.11ac	--	69
2802_84	...Bangalore/BGL-11/Floor6	JioFi2_7B5BCD	-60	136	802.11ac	--	32
2802_84	...Bangalore/BGL-11/Floor6	JioFi2_7B5BCD	-65	11	802.11abgn	--	30

Showing 5 of 5

What's new

- ✓ New classification engine with reduced false positives
- ✓ Global view of threats
- ✓ Threat 360° for detailed view of a threat with additional context

Migration to new rogue management solution

Access Point

No change required. Catalyst 9800 supports Wave1, Wave 2 and 11ax APs

Controller *Optional*

AireOS

Catalyst 9800

Management *Optional*

Prime
Infrastructure

Cisco DNA
Center

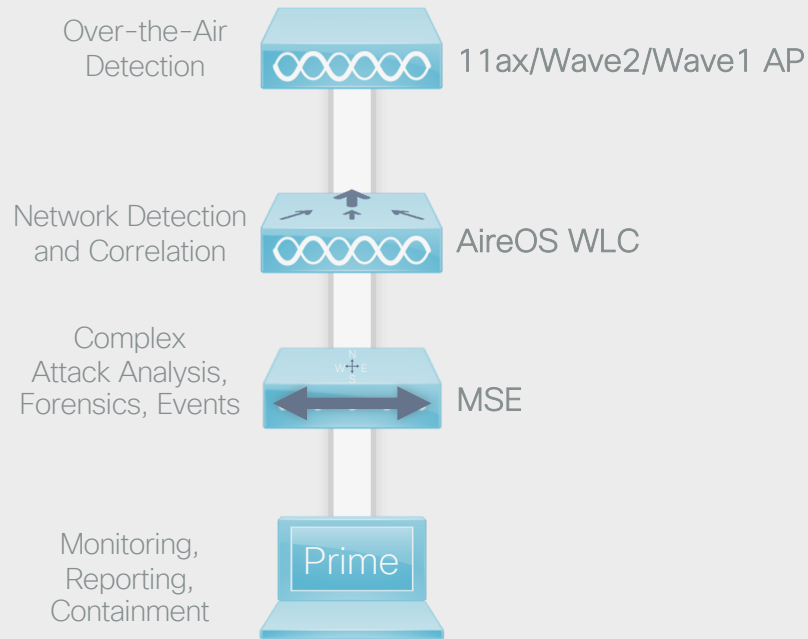
License *If migrating to DNA Center*

Prime License

AIR-DNA-E
DNA Essentials

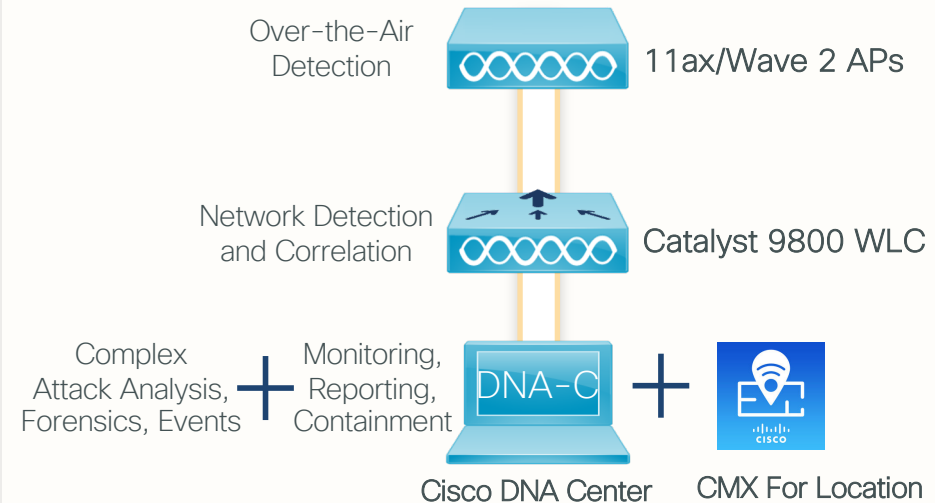
Cisco WIPS Architecture Options

AireOS wIPS Architecture



NextGen wIPS Architecture

CY 2020



- ✓ Low footprint solution
- ✓ Ease of DNA licensing
- ✓ Alarm consolidation

Attacks that matter

AireOS wIPS Architecture

100+ signatures
supported on MSE

Package licensed from third party



>50% are obsolete!

25%

Outdated /
should be
switched off

15%

Covered as
part of rogue
detection

10%

Only applicable
for WEP/WPS
networks

NextGen wIPS Architecture

Starting with key attacks
that impact the network

Developed and built by Cisco Engineering



11 unique signatures

Planned for IOS-XE 17.1-17.3

Outside of Rogue detection and enhancements

"Basic Rogue Detection & Containment & location tracking is **most important** for my customers... Signature based WIPS is additional on top of that. Signatures like mobile hotspot or honeypot or deauth/disassoc flood is **more critical for my customers.**"

- TSA, APJ Enterprise Networking

Supported Platforms for WIPS



Catalyst 9800
Embedded Wireless-AP



Catalyst 9800
Embedded Wireless



Catalyst 9800-L



Catalyst 9800-40



Catalyst 9800-80



Catalyst 9800-CL



Catalyst 9800-CL



Catalyst 9800-CL

Supported on Local, Flex and Fabric deployment modes

Supported Access Points



Catalyst C9100AX Series APs



11AC WAVE-2 APs

Supported on Local, Flex and Monitor mode

Alarms Supported till previous releases

Alarms ID	Alarms
10001	DoS: Authentication Flood Alarm
10002	DoS: Association Request Alarm
10003	DoS: Broadcast Probe flood Alarm
10004	DoS: Disassociation Flood Alarm
10005	DoS: Broadcast Dis-Association Alarm
10006	DoS: De-authentication Flood Alarm
10007	DOS: Broadcast De-authentication Alarm
10008	DOS: EAPOL-Logoff Attack Alarm

New Alarms Supported in 17.3

Alarms ID	Alarms
10009	CTS Flood Alarm
10010	RTS Association Request Alarm

Note:

- Only supported on 11AX and Wave2 APs
- Supported AP modes, local, Flex and Monitor

iPSK – Peer 2 Peer Blocking

Identity PSK

Why do we need IPSK support?

As client joining the WLAN share the same key leading to security issues if keys are shared with unauthorized users

In case of key compromised on one client leads to changing the key for every client associated to that SSID

Most of the IoT devices that use PSK do not have 802.1x supplicant

Leading to the need of supporting keys that are configurable per device or group

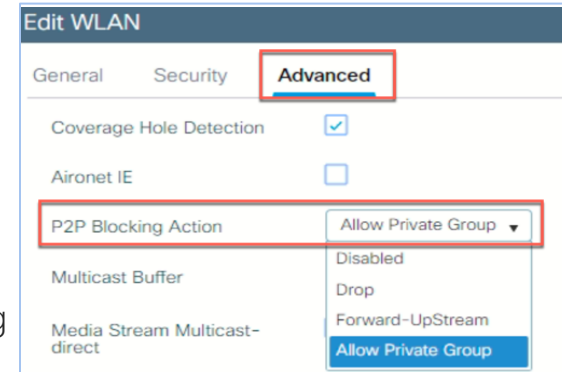
iPSK with P2P Blocking

Begin with release 8.8 the new iPSK feature is available that prevents PSK devices with different Tags communicate to each other

These options will allow the **WLC Data Plane** to block or locally bridge the peer to peer traffic from iPSK clients.

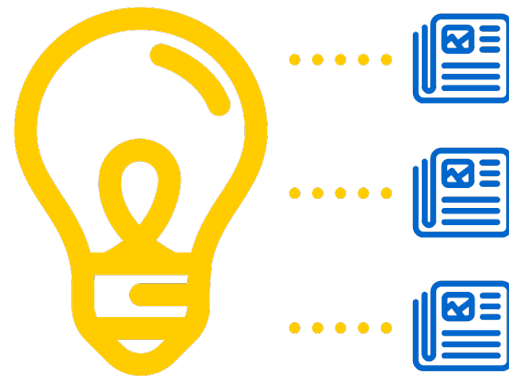
This feature supported on Wave-2 APs with IPv4/IPv6 Clients

- Configuration options for peer to peer blocking:
- Drop - Drop peer to peer traffic (existing option)
- Disable - Bridge peer to peer traffic (existing option)
- Forward-UP Stream - Forward to next hop switch peer to peer traffic (existing option)
- Allow Private Group - Bridge devices with same Tag or Block local bridging traffic if the source and destination client MAC have different Tag values



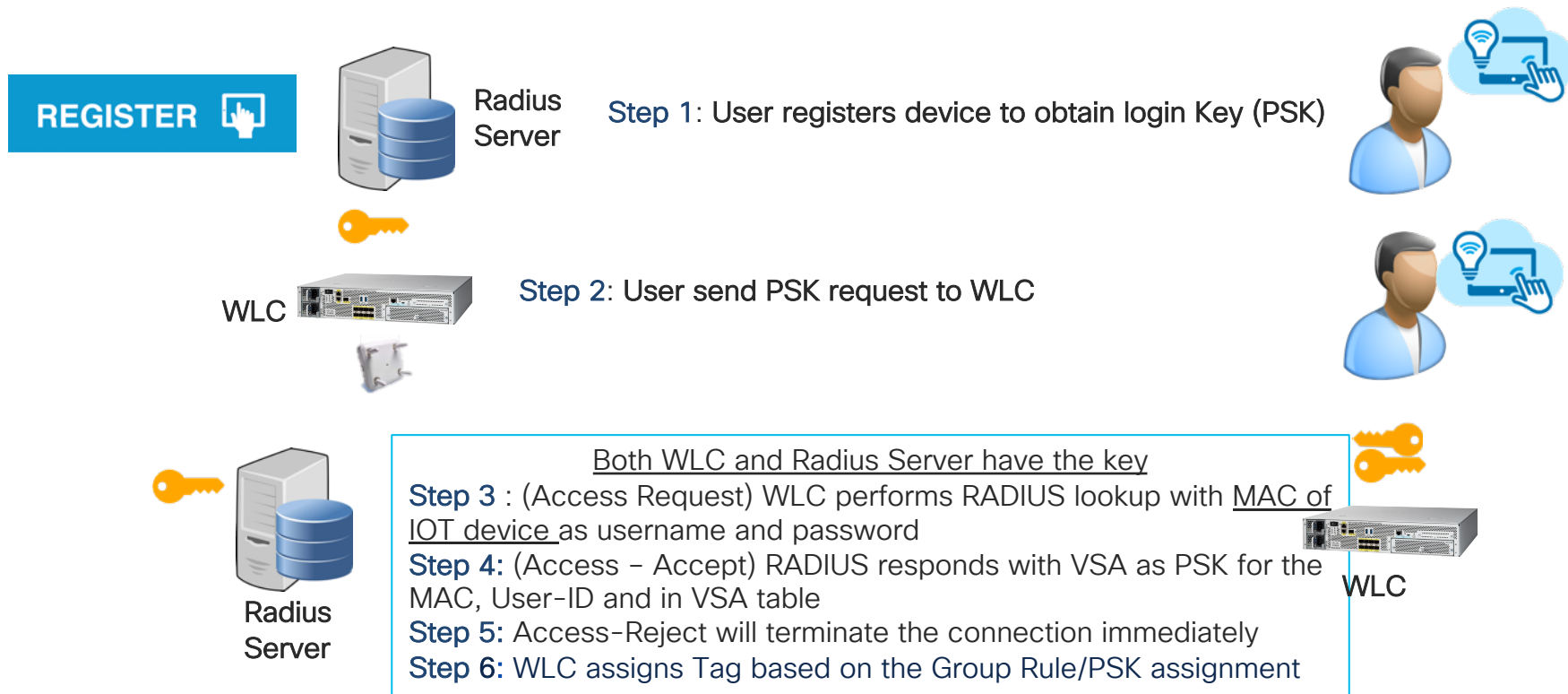
iPSK with P2P blocking Use Case

- A large Service Provider required this feature so that wireless customers in the same group and with the same PSK could communicate to each other
- On the same token wireless customers that belong to different groups as defined in the AAA server, and have different PSK should not be able to communicate

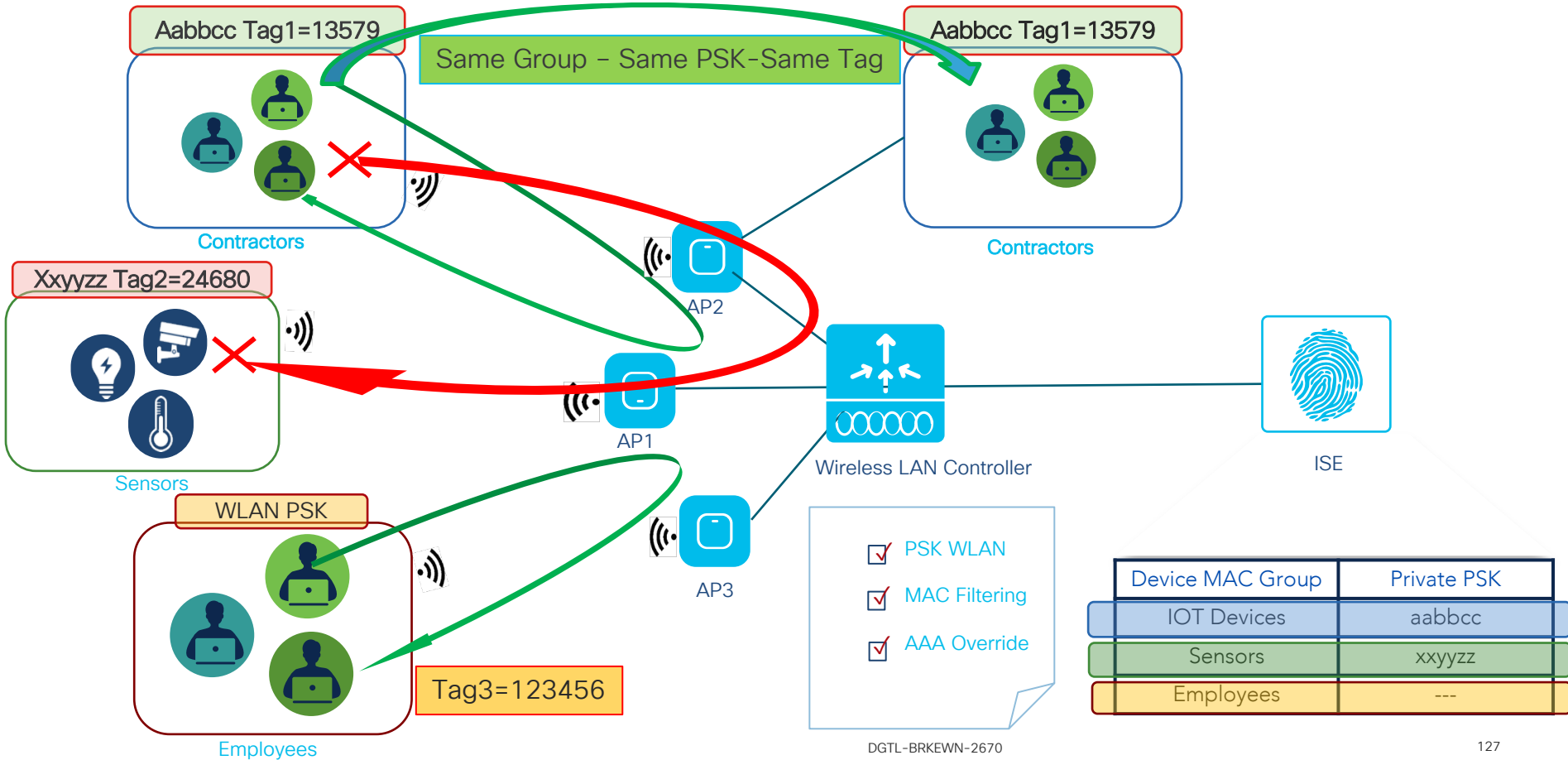


Phase 1-2 deployment scenario

PSK is assigned on external RADIUS Server



Identity PSK with P2P- Central Switching



The background is a dark blue field filled with numerous small, semi-transparent squares and dots in various colors including light blue, green, yellow, orange, and red. These elements are scattered across the frame, with a higher concentration of yellow and orange squares forming a diagonal streak from the top right towards the bottom right.

Application Visibility and Control

AVC-FNF Features Added in IOS XE 17.1

- NBAR on controller: NBAR engine **v38**, protocol pack **v45.0**
- L2 & L3 roaming supported, L2 includes AP NBAR context transfer
- Application-based statistics reporting per WLAN and per client
- External FNF collectors
- AVC Timeline
- Support for Wave-1 and Wave-2 APs. Fabric, Wave-2 only.
- WebUI, CLI, Netconf/Yang and SNMP support
- IPv4 and IPv6 traffic classification, FNF support for IPv6 traffic flows on Wave-2 APs only
- Support for all Cisco C9800 deployment modes

IPv4 and IPv6 Flexible Netflow records exporter is introduced in release 17.1. FNF is sending 17 different data records to the External 3rd Party Netflow collectors such as Stealthwatch

<https://tools.ietf.org/html/rfc3954>

C9800 IOS-XE 17.1 AVC Deployment Modes

C9800 IOS-XE 17.1 Supports 4 deployment modes

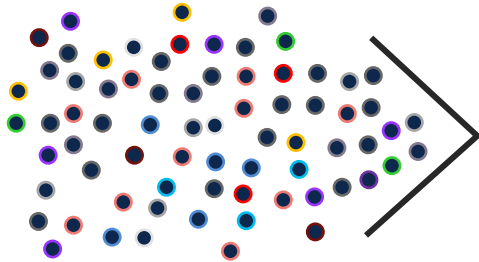
- Flex (a.k.a. “Local switching with APs in FlexConnect mode”)
- Flex Central (a.k.a. “Central switching with APs in FlexConnect mode”)
- Local (a.k.a. “Central switching with APs in local mode”)
- Fabric (a.k.a. eCA DNA)

Umbrella Support on Flex/EWC

Cisco Umbrella- How does it work?

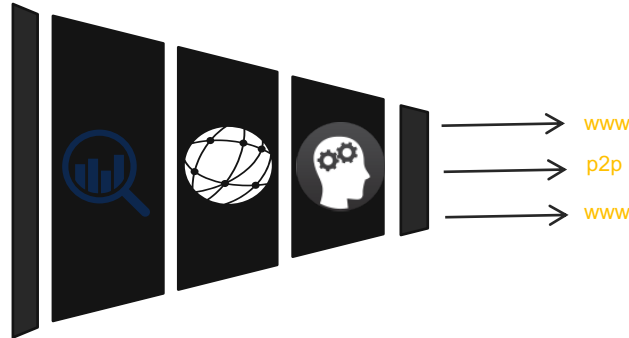
Ingest

Millions of data points per second across markets, geographies, protocols



Apply

Statistical models, Human Intelligence, Anomaly Detection, Temporal Patterns



Identify

Malicious and safe sites



Umbrella Support on Flex/EWC on AP

Use Cases

- Customer wants to provide defense against threats on the internet such as Phishing, malware and ransomware etc..
- Customer wants to gain visibility into internet activity across all locations, devices and also filter/block access to content on the internet

Feature

- Cisco Umbrella can provide comprehensive content filtering capability based on individual sites(www.abc.com) or category(gambling)
- Simple and multi profile registration process via Token
- Both Ignore and Forced mode is supported for WLAN
- DHCP Forced option available on the WLAN to send Umbrella DNS IPs to client instead of what is on DHCP

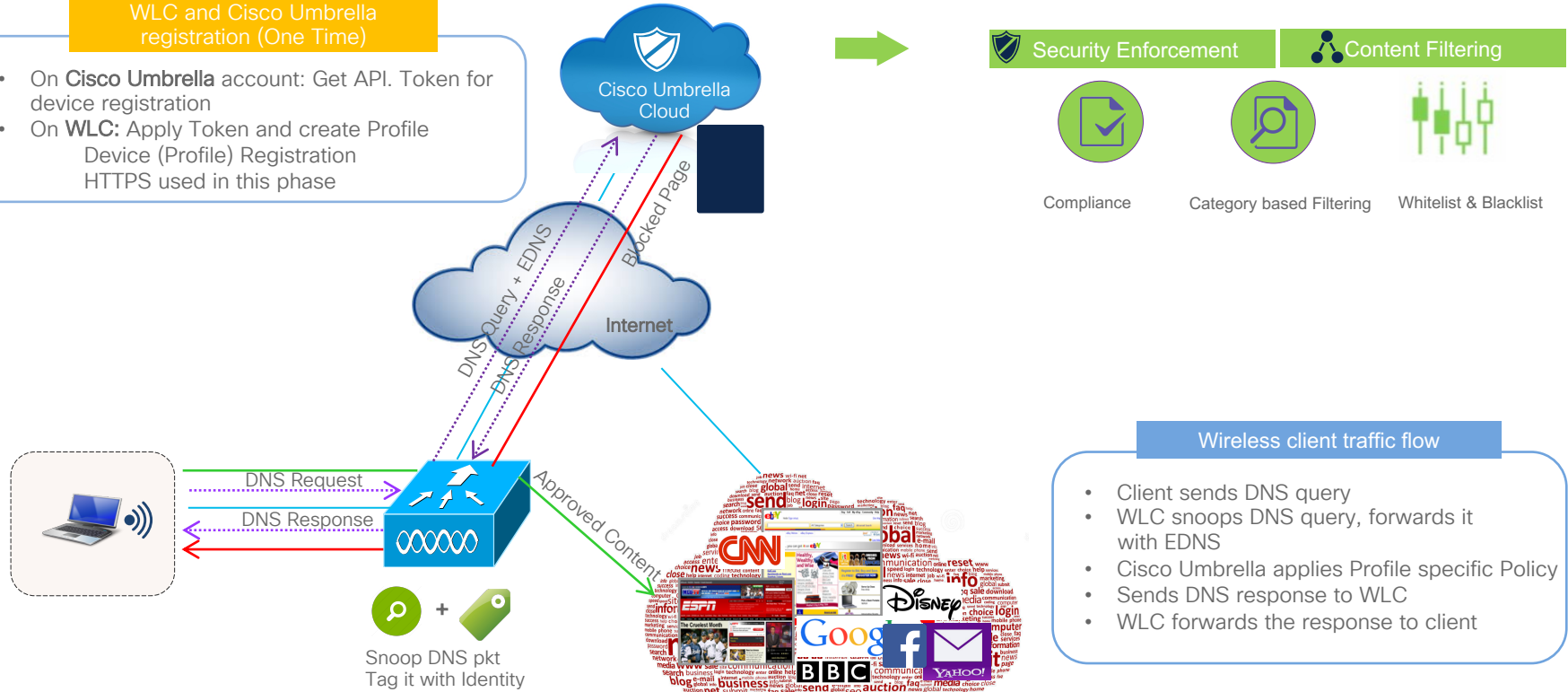
Caveats

- Supported for IPv4 addresses Only
- dnscrypt is not supported
- Split-DNS is not supported
- DHCP DNS override only applies to a maximum of 2 DNS IP addresses in the DHCP packets
- Profile is mapped to WLAN and not individual clients i.e. all clients to the WLAN will see the same policy enforcement.

Existing Cisco Umbrella- WLC Packet Flow

WLC and Cisco Umbrella registration (One Time)

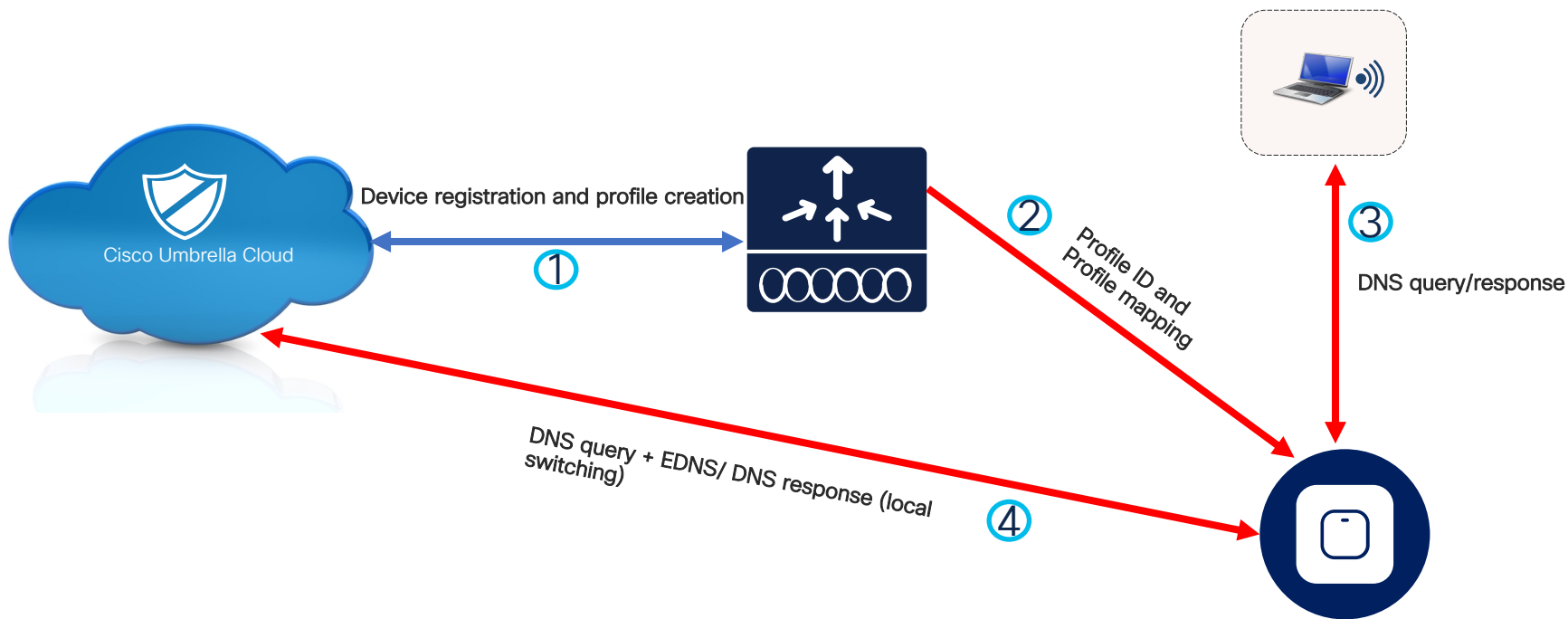
- On **Cisco Umbrella** account: Get API. Token for device registration
- On **WLC**: Apply Token and create Profile Device (Profile) Registration
HTTPS used in this phase



Wireless client traffic flow

- Client sends DNS query
- WLC snoops DNS query, forwards it with EDNS
- Cisco Umbrella applies Profile specific Policy
- Sends DNS response to WLC
- WLC forwards the response to client

Enhanced Work Flow for Flex/EWC



The directed lines in red are the new flows for Umbrella in flex local switch mode

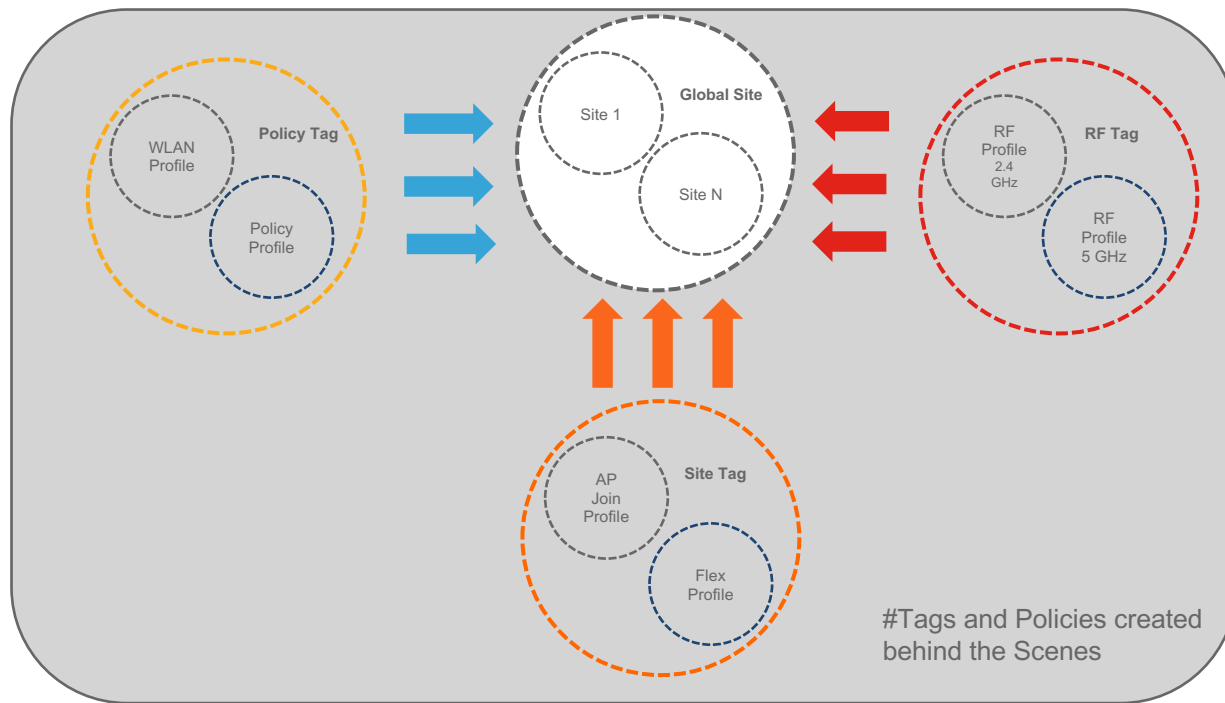
Catalyst 9800 Configuration

Wireless Basic Setup Workflow

Day 1 – Wireless Basic Setup

Intent-based configuration with Sites, WLANs,
Policy and RF attributes

Wireless Basic Configuration Model



- Creation of Local and Remote sites
- Creation of Custom Policy, RF and Site Tags and profiles in the backend

Wireless Basic Configuration – Adding Local Site

[← Back](#)

General

Wireless Networks

AP Provisioning

Location Name*

LocalSite|

Description

Enter Description

Location Type

☒ Local ☐ Flex

Client Density

Low

Typical

High

Local Site Definition and Client Density Selection

× Delete Location

Apply

WLAN Name

WLAN

◀◀ 0 ▶▶

10

items per page

Add existing WLANs to the site OR define a new one

No items to display

Wireless Network Details

WLAN*

Search or Select

vewlc-psk

vewlc-dot1x

or

Define new

Policy Details

VLAN/VLAN Group*

Search or Add New

(E.g. 1,2,5-7)

ACL

Search or Select

or Define new

QoS

Search or Select

×

✓

Wireless Basic Configuration – Adding Remote Site

← Back

General Wireless Networks AP Provisioning

Location Name* RemoteSite

Description Enter Description

Location Type ☐ Local ☒ Flex

Client Density

Native VLAN ID 112

AAA Servers

Available (1)

172.20.226.141

Selected (0)

No AAA servers selected

Add New Server

Remote Site configuration with site specific Native VLAN ID and AAA Servers

← Back

General Wireless Networks AP Provisioning

+ Add Delete

WLANs on this Location

WLAN Name	VLAN/VLAN Group
No items to display	

Wireless Network Details

WLAN* viewlc-psk Network name is required or Define new

Policy Details

VLAN/VLAN Group* Search or Add New (E.g. 1,2,5-7)

ACL Search or Select or Define new

QoS Search or Select

Local Switching Local Authentication

✕ ✓

Local switching and Local authentication options for WLANs defined local to remote site

Adding Remote Site - behind the scenes

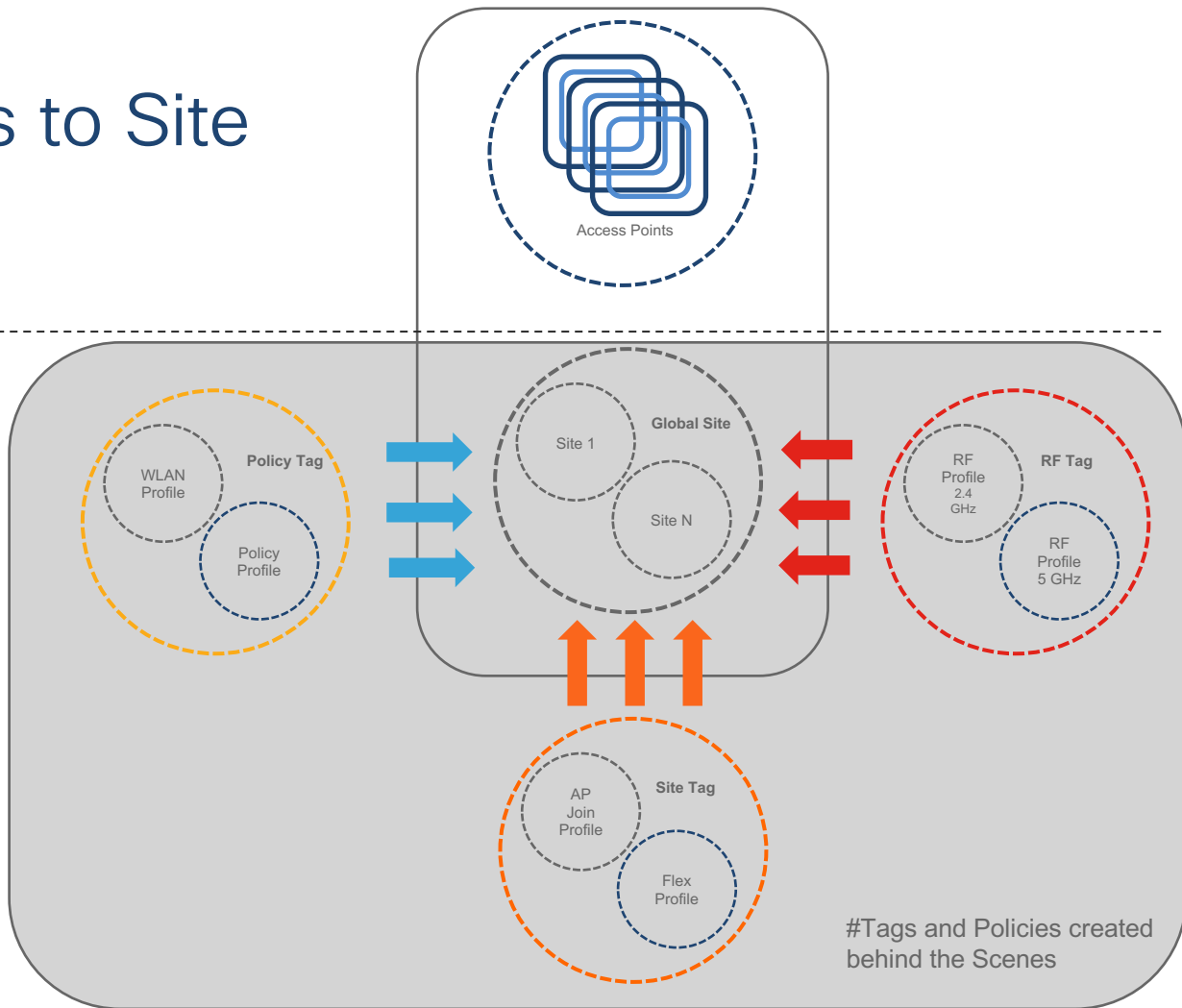


- User simply creates a remote site
- Creation of remote Site involves creation of Flex Profile in the backend.
- Flex Profile is added to Site Tag automatically

Provisioning APs to Site

2. Provision

1. Design + Policy



Wireless Basic Configuration – Provisioning APs to Site

← Back

General Wireless Networks **AP Provisioning**

Static AP MAC Address list to add APs not yet joined to the controller

Delete Location Apply

Add/Select APs

AP MAC Address

Available AP list

Number of selected APs : 1

AP MAC	AP Name
005d.735c.b544	AP005D.735C.B544

1 - 1 of 1 items

APs on this Location

Associated AP list

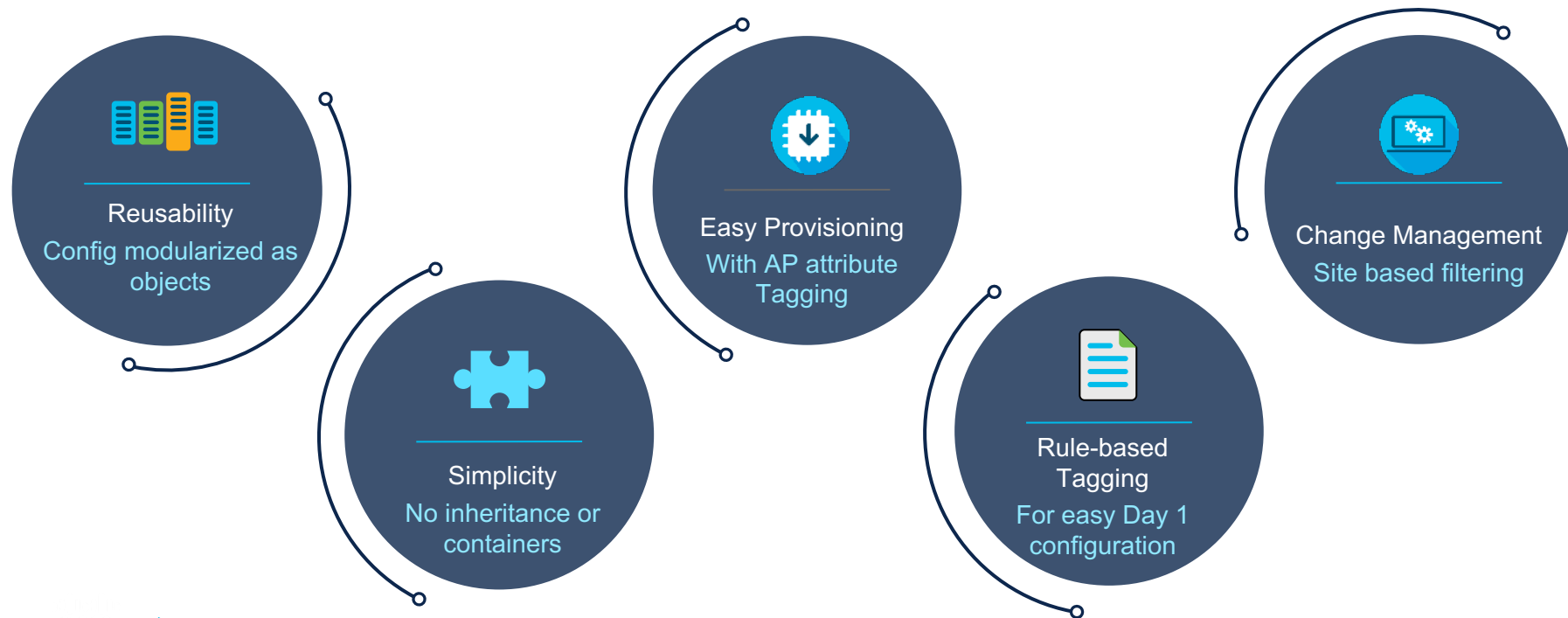
Number of selected APs : 0

AP MAC	AP Name	Status
--------	---------	--------

No items to display

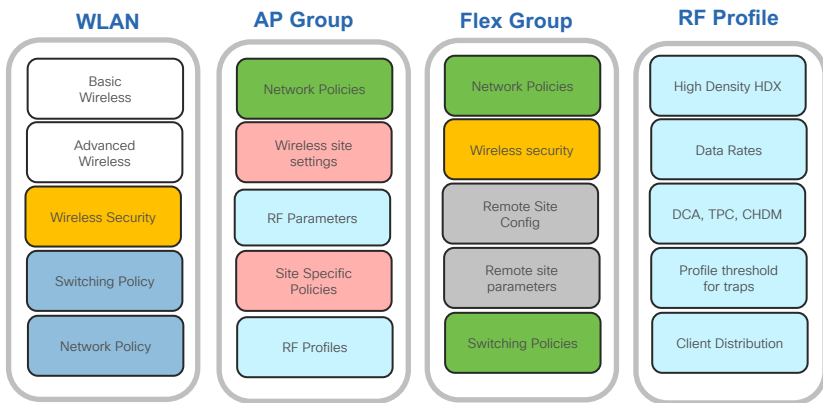
Select from available APs to the Associated AP list for this site

Benefits of New Configuration Model



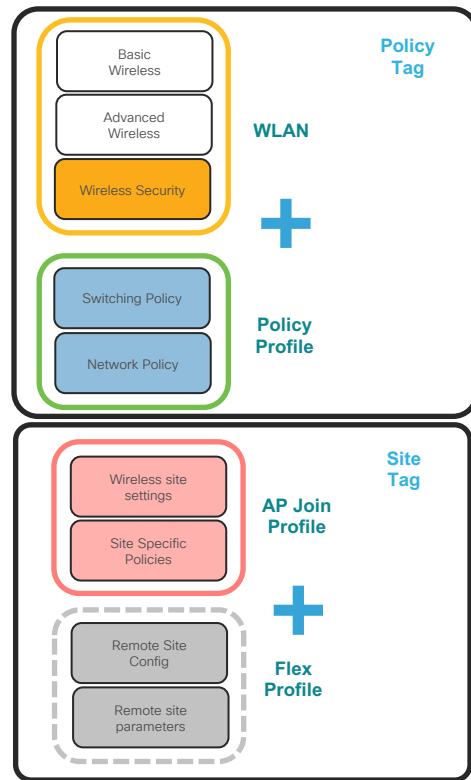
AireOS vs. Catalyst 9800 Config Model

Going towards a more **Modularized and Reusable** model with **Logical decoupling** of configuration entities

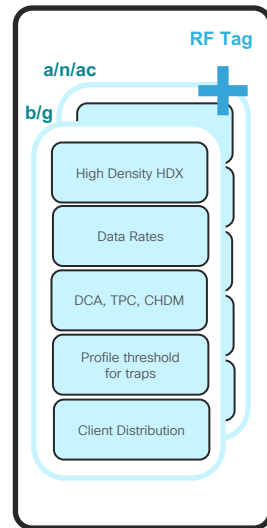
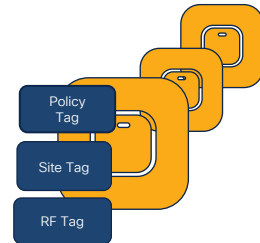


AireOS Config Model

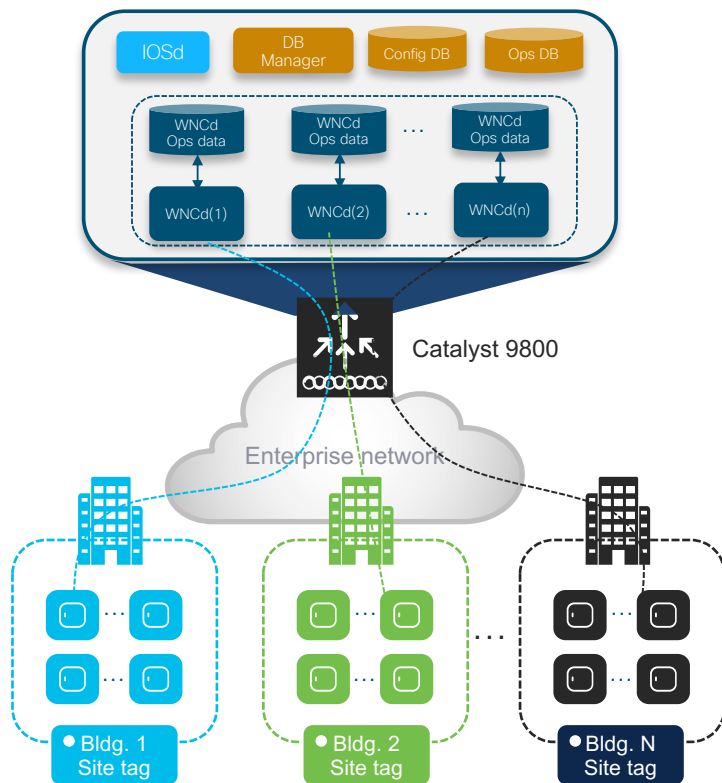
Decouple
Modularize



Granular & simplified
What **Policies** on which **Sites**
with what **RF** characteristics



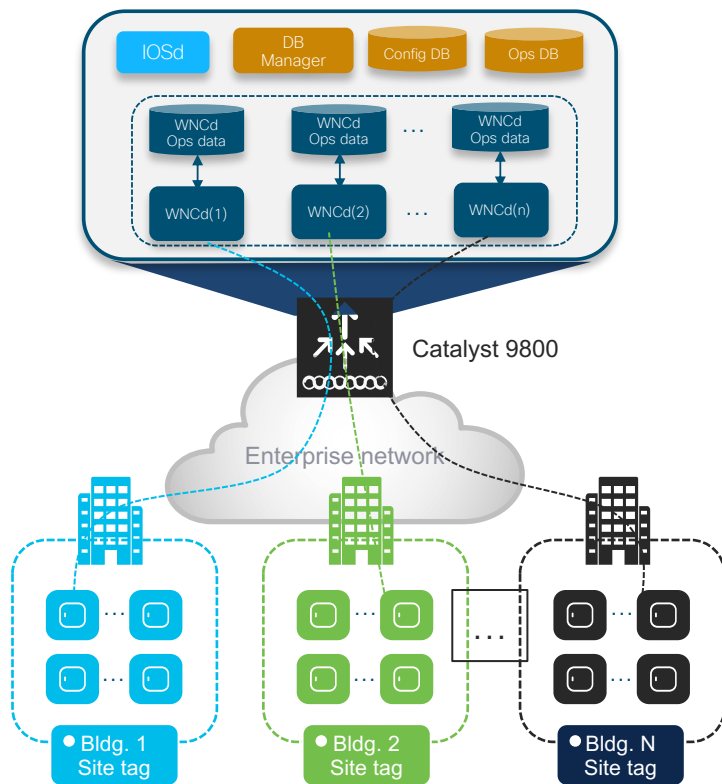
Design: recommended use of AP Site Tags



Important facts:

- C9800 has a multi-process software architecture
- APs are load-balanced across Wireless Network Controller processes (WNCd) within a C9800
- The number of WNCd varies from platform to platform
- Load balancing of APs (and clients) gives better scale and performances
- Today the load balancing is done based on **SITE tags**
- If using default site tag, the APs are load balanced across WNCd instances in round robin fashion

Design: recommended use of AP Site Tags



Design Recommendation:

- The pb: 11k/v, CHD (and in general everything proximity based) are managed within the WNCd. So these features will break if neighbor APs are on different WNCds
- For best performance use site tag to group APs at a roaming domain level > **SITE TAG = Roaming Domain**
- Also make sure that the max number of APs per site tag doesn't exceed 400-500 APs
- A good design choice would be to choose the site tag corresponding to a building.
- Do not use site tag per floor it could break roaming
- **NOTE:** roaming (and fast roaming) works fine across site tags

Recommended use of AP Site Tags



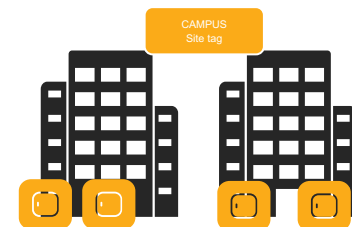
What if my customer has a building with more than 400 APs?

Recommendation: split the building in two from a site tag perspective



What if customer has a roaming domain that spans across multiple buildings with more than 400 APs?

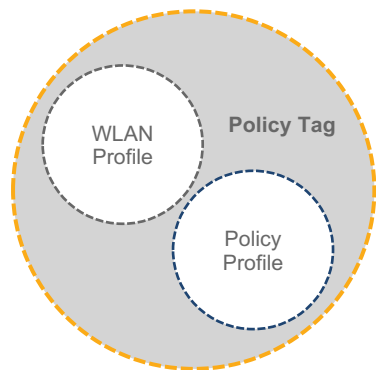
Recommendation: configure a site tag per building. Roaming will work



What if customer has multiple buildings with less than 400 APs?

Recommendation: configure just one name site tag and don't use the default site tag

Components of Policy Tag



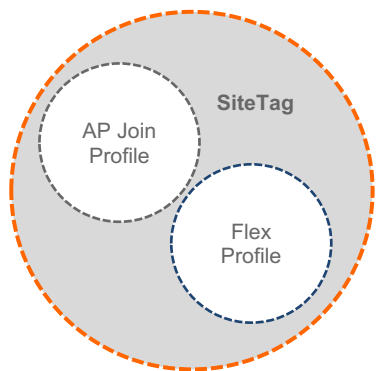
Components of WLAN Profile

- Profile Name
- Status
- WLAN ID
- SSID
- Broadcast SSID
- L2 Security
- L3 Security
- AAA Servers
- Coverage Hole detection
- Aironet IE
- Diagnostic Channel
- P2P blocking
- Max Client connections
- 11v BSS transition Support
- Off channel Scan defer
- Load Balance
- Band Select

Components of Policy Profile

- VLAN - Mgmt. Vlan
- Session timeout - 1800
- Idle time out - 300
- AVC profile - null
- Client Qos(input/and output) - default
- BSSID Qos(input/and output) - default
- ACL - None
- Local switching - disabled (all other related parameters are disabled)
- Central switching - enabled
- Central DHCP - disabled
- Central Assoc - disabled
- Central Authentication - enabled
- Local profiling - disabled
- Policy map - none
- Authentication - Central

Components of Site Tag



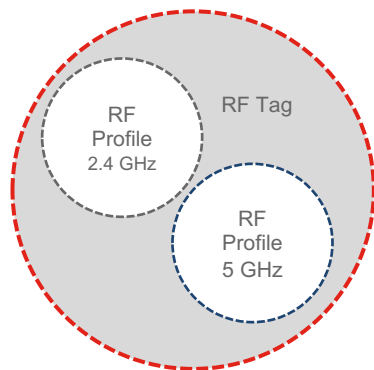
AP Join Profile - defaults

LED state – Enable
Heartbeat timer– 30 secs
Primary discovery timer – 120 sec
Primed join timeout – 0 seconds
Discovery timeout - 10 secs
Fast heart beat timer – 1 sec
Fast heart beat – disabled
TCP/MSS - enabled (set to 1250)
Retransmit count – 5 secs
Retransmit interval – 15 secs
Dot1x authentication – disabled
UDP lite – disabled
11u venue group – unspecified
Username/password – “current default”
Preferred mode – IPV4
11u venue type – unspecified
Client QinQ – disabled
DHCP QinQ – disabled
Reset - Disable
Static nameserver/domain name – current default
Backup primary/secondary – current default
Core dump – “current default”
Syslog - “current default”
Hyperlocation – disable

Components of Flex Profile

Native VLAN ID
HTTP Proxy Port
HTTP Proxy IP Address
Fallback Radio Shut
ARP Caching
Efficient Image Upgrade
Local Authentication
Local Auth Users
Policy ACL
VLAN Name and ID

Components of RF Tag



Components of RF Profile

Data Rates
MCS Settings
Maximum and Minimum Power Level Assignment
Power Threshold v1/v2
DCA Channel Width
DCA Foreign AP Interference Avoid Enable
DCA Channel list
Coverage Hole Detection Parameters (Data/Voice RSSI, Coverage Exception, Coverage Level)
Profile Threshold for Traps (Interference/Clients/Noise/Utilization)
Maximum Clients
Multicast Data Rates
Rx Sop Threshold
Load Balancing (window & denial)
Band Select Parameters (Applicable only for 802.11bg)

Wireless Advanced Setup Workflow

Guided UI Configuration Workflow

Cisco vEWL 16.10.20180828

Welcome admin

Wireless Setup

Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Troubleshooting

Wireless Setup Flow Overview

This screen allows you to design Wireless LAN Configuration. It involves creating Policies and Tags. Once the design is completed, they can be deployed to the Access Points right here.

DESIGN PHASE

Tags & Profiles

- WLAN Policy (Mandatory)
- Site Policy (Optional)
- Radio Policy (Optional)

WLAN Profile | AP Join Profile | RF Profile

Policy Profile | Flex Profile | RF Tag

Policy Tag | Site Tag

DEPLOY PHASE

Apply to APs (Mandatory)

Tag APs

Select APs and push configuration to them

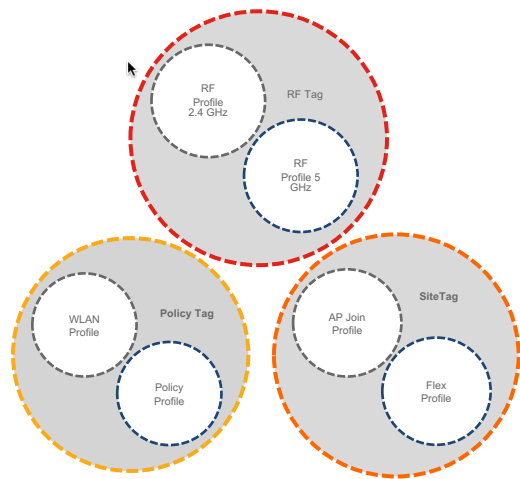
TERMINOLOGY

Tag
WLAN Policy, Policy Profile
Site Policy - AP Profile, Site Profile
Radio Policy - Radio Characteristics

ACTIONS

Go to List View
Create New

Start Now



WLAN Profile

Wireless Setup

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag
- Tag APs

Done

+ Add ✕ Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Name	ID	SSID	Status	Security
<input checked="" type="checkbox"/>	viewlc-psk	2	viewlc-psk	Enable	[WPA2][Auth(PSK)]
<input checked="" type="checkbox"/>	viewlc-dot1x	3	viewlc-dot1x	Enable	[WPA2][Auth(802.1x)]

10 items per page 1 - 2 of 2 items

Back

Create new WLAN or edit existing WLAN for General, Security and Advanced knobs

Add WLAN

General

Profile Name*

SSID

WLAN ID*

Status ☐ Disabled

Radio Policy

Broadcast SSID ☒ Enabled

Cancel Save & Apply to Device

Add WLAN

Security

Layer2

Layer 2 Security Mode

MAC Filtering ☐

Protected Management Frame

PMF

WPA Parameters

Fast Transition

Over the DS ☒

Reassociation Timeout

Cancel Save & Apply to Device

Add WLAN

Advanced

Coverage Hole Detection ☒

Airont IE ☒

Diagnostic Channel ☐

P2P Blocking Action

Multicast Buffer ☒ Disabled

Media Stream Multicast-direct ☐

Max Client Connections

Universal Admin ☐

Load Balance ☐

Band Select ☒

IP Source Guard ☐

WMM Policy

Off Channel Scanning Defer

Defer Priority ☐ 1 ☐ 2

Cancel Save & Apply to Device

Policy Profile

Wireless Setup



Add new Policy profile
or use default-policy-profile

Access Policies, QoS,
AVC, mobility and other advanced
network policy settings

Wireless Setup

Tags & Profiles

- WLAN Profile
- Policy Profile**
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag
- Tag APs

Done

Policy Profile

Policy Profile Name	Description	Status
default-policy-profile	default policy profile	Enable

10 items per page

Add Policy Profile

General Access Policies QoS and AVC Mobility Advanced

WLAN Local Profiling

Name* WLAN Local Profiling

Description HTTP TLV Caching

Status ☐ HTTP TLV Caching

Passive Client ☐ RADIUS Profiling

Encrypted Traff ☐ DHCP TLV Caching

CTS Policy Local Subscriber Policy Name

Inline Tagging ☐ VLAN

SGACL Enforce ☐ VLAN/VLAN Group

Default SGT ☐ Multicast VLAN

Cancel

Add Policy Profile

General Access Policies QoS and AVC Mobility Advanced

QoS and AVC

Auto QoS

QoS SSID Policy

Egress

Ingress

QoS Client Policy

Egress

Ingress

SIP-CAC

Call Snooping ☐

Send Dissociate ☐

Send 486 Busy ☐

Cancel

Add Policy Profile

General Access Policies QoS and AVC Mobility Advanced

Mobility Anchors

Export Anchor ☐

Static IP Mobility ☐ DISABLED

Drag and Drop/double click on the arrow to add/remove Anchors

Available (0) Selected (0)

Anchor IP

No anchors available

Anchor IP

Anchors not

Cancel

Add Policy Profile

General Access Policies QoS and AVC Mobility Advanced

Advanced

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec) ☒ 60

DHCP

DHCP Enable ☐

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override ☐

NAC State ☐

Policy Name

Accounting List

Cancel **Save & Apply to Devices**

Policy Tag

WLAN Profile + Policy Profile

MLC 28

Welcome admin

Wireless Setup

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag**
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag

Apply

- Tag APs

Done

+ Add ✕ Delete

Policy Tag Name	Description
<input type="checkbox"/> default-policy-tag	default policy-tag

1 10 items per page

Default Policy Tag containing default-policy profile

SSID to Policy Profile Mapping to define behavior of client policy

Add Policy Tag

Name* CustomPolicy

Description Enter Description

WLAN ID	WLAN Profile	Map Policy Profile
2	vwlc-psk	Search or Select
3	vwlc-dot1x	Search or Select

1 - 2 of 2 items

10 items per page

Cancel Save & Apply to Device

AP Join profile

Wireless Setup

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile**
- Flex Profile
- Site Tag
- RF Profile
- RF Tag

Apply

Tag APs

Done

+ Add ✕ Delete

AP Join Profile Name	
<input type="checkbox"/>	CustomAP join
<input type="checkbox"/>	default-ap-profile
◀ 1 ▶ 10 items per page	

CAPWAP parameters
such as CAPWAP and
retransmit timers, N+1
configuration

AP Management
features such as AP
Dot1x Credentials

Add AP Join Profile

General Client **CAPWAP** AP Management Rogue AP

High Availability Advanced

CAPWAP Timers

Fast Heartbeat Timeout(sec)* 0

Heartbeat Timeout(sec)* 30

Discovery Timeout(sec)* 10

Primary Discovery Timeout(sec)* 120

Primed Join Timeout(sec)* 0

Retransmit Timers

Count* 5

Interval (sec)* 3

Backup Controller Configuration

Enable Fallback ☒

Primary Controller

Name Enter Name

IPv4/IPv6 Address

Secondary Controller

Name Enter Name

IPv4/IPv6 Address

Cancel Save & Apply to Device

Add AP Join Profile

General Client CAPWAP AP **Management** Rogue AP

Device User **Credentials** CDP Interface

Dot1x Credentials

Local Username Enter Local Username Local Credentials Flag ☐

Local Password Enter Local Password Local Credentials Flag ☐

Local Password Type clear

Dot1x Username Enter dot1x Username

Dot1x Password Enter Dot1x Password

Dot1x Password Type clear

Max Session Limit(sec)* 0

Cancel Save & Apply to Device

Flex Profile

Wireless Setup

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile
- Flex Profile**
- Site Tag
- RF Profile
- RF Tag

Apply

- Tag APs

Done

+ Add **x Delete**

Flex Profile Name	Description
<input type="checkbox"/> default-flex-profile	Default Flex profile

1 10 items per page

CAPWAP parameters such as CAPWAP and retransmit timers, N+1 configuration

Local authentication EAP Profile and local auth user entries

Add Flex Profile

General **Local Authentication** **Policy ACL** **VLAN**

Name* Multicast Overridden Interface ☐

Description Fallback Radio Shut ☐

Native VLAN ID Flex Resistant ☐

HTTP Proxy Port ARP Caching ☐

HTTP Proxy IP Address Efficient Image Upgrade ☒

CTS Policy Office Extend AP ☐

Inline Tagging ☐ Join Minimum Latency ☐

SGACL Enforcement ☐

Cancel **Save & Apply to Device**

Add Flex Profile

General **Local Authentication** **Policy ACL** **VLAN**

Radius Server Group LEAP ☐

EAP Fast Profile PEAP ☐

TLS ☐

RADIUS ☒

Users

+ Add **x Delete**

Username

10 items per page

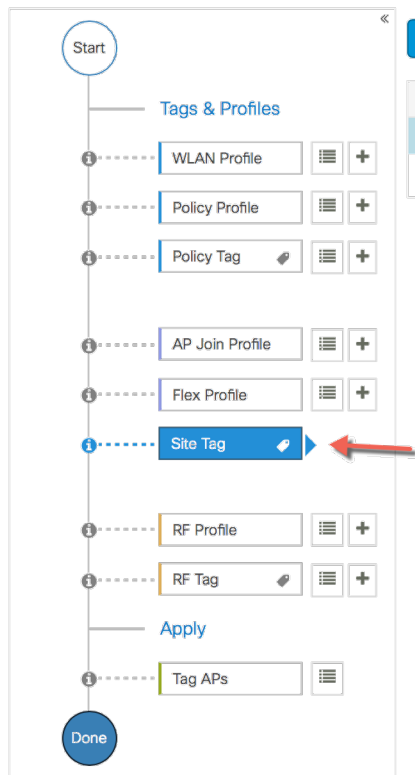
No items to display

Cancel **Save & Apply to Device**

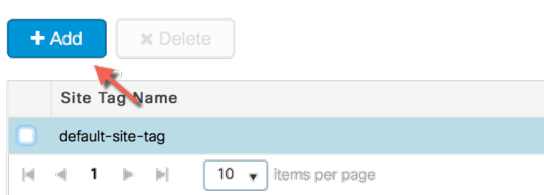
Site Tag

- AP Join Profile + Flex Profile (only for Remote Site)


Wireless Setup



The Wireless Setup navigation pane shows a sequence of steps: Start, Tags & Profiles, WLAN Profile, Policy Profile, Policy Tag, AP Join Profile, Flex Profile, Site Tag (highlighted with a red arrow), RF Profile, RF Tag, Apply, and Tag APs. The Site Tag step is the current active step.

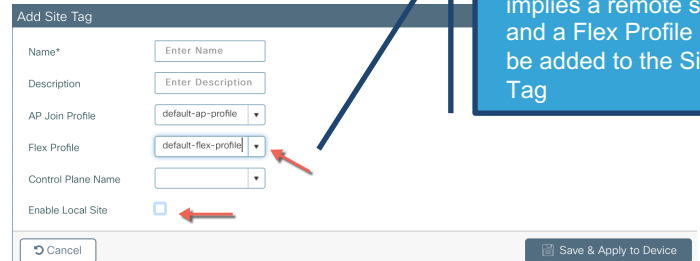


The Site Tag list shows a table with the following columns: Site Tag Name. The table contains one entry: default-site-tag. The table has a pagination bar showing 10 items per page.



The Add Site Tag form shows the following fields: Name* (Enter Name), Description (Enter Description), AP Join Profile (default-ap-profile), Control Plane Name, and Enable Local Site (checked). The AP Join Profile field is highlighted with a red box. The form has a Cancel button and a Save & Apply to Device button.

Enable Local Site for sites in the Campus. Associate AP Join profile



The Add Site Tag form shows the following fields: Name* (Enter Name), Description (Enter Description), AP Join Profile (default-ap-profile), Flex Profile (default-flex-profile), Control Plane Name, and Enable Local Site (unchecked). The Flex Profile field is highlighted with a red box. The form has a Cancel button and a Save & Apply to Device button.

Disabling Local Site implies a remote site and a Flex Profile can be added to the Site Tag

RF Profile

Wireless Setup

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile**
- RF Tag

[Back](#)

[+ Add](#) [x Delete](#)

Pre-canned RF profiles for Low, Typical and High Density on 2.4 and 5GHz

RF Profile Name	Band	State	Description
<input type="checkbox"/> Low_Client_Density_rf_5gh	802.11a	Enable	pre configured Low Client Density rfprofile for 5gh radio
<input type="checkbox"/> High_Client_Density_rf_5gh	802.11a	Enable	pre configured High Client Density rfprofile for 5gh radio
<input type="checkbox"/> Low_Client_Density_rf_24gh	802.11b/g	Enable	pre configured Low Client Density rfprofile for 2.4gh radio
<input type="checkbox"/> High_Client_Density_rf_24gh	802.11b/g	Enable	pre configured High Client Density rfprofile for 2.4gh radio
<input type="checkbox"/> Typical_Client_Density_rf_5gh	802.11a		
<input type="checkbox"/> Typical_Client_Density_rf_24gh	802.11b/g		

1 10 items per page

Add RF Profile

General 802.11 **RRM** Advanced

General Coverage TPC DCA

Profile Thresholds for Traps

Interference (%)* 10

Clients* 12

Noise(dBm)* -70

Utilization(%)* 80

[Cancel](#) [Save & Apply to Device](#)

802.11, RRM and Advanced RF features

RF Tag

2.4 RF Profile + 5 GHz RF Profile

Wireless Setup

The screenshot displays the 'Wireless Setup' interface. On the left, a sidebar contains a 'Start' button at the top and a 'Done' button at the bottom. Between them is a vertical list of configuration steps: 'Tags & Profiles', 'WLAN Profile', 'Policy Profile', 'Policy Tag', 'AP Join Profile', 'Flex Profile', 'Site Tag', 'RF Profile', 'RF Tag' (highlighted in blue with a right-pointing arrow), and 'Tag APs'. The main area shows a table of RF Tags. At the top are '+ Add' and 'x Delete' buttons. The table has two columns: 'RF Tag Name' and 'Description'. It lists one entry: 'default-rf-tag' with the description 'default RF tag'. Below the table is a pagination control showing '1' and a dropdown for '10 items per page'. A blue callout box points to the 'default-rf-tag' entry with the text: 'Default RF Tag is a combination of Global Configurations on 2.4 and 5GHz'. Below the table is a modal window titled 'Add RF Tag' with a close button 'x'. It contains four input fields: 'Name*' (with value 'CustomRFTag'), 'Description' (with placeholder 'Enter Description'), 'Dot 11a RF Profile' (with dropdown value 'High_Client_Density'), and 'Dot 11b RF Profile' (with dropdown value 'Low_Client_Density'). At the bottom of the modal are 'Cancel' and 'Save & Apply to Device' buttons. A blue callout box points to the 'Save & Apply to Device' button with the text: 'Custom RF Tags can have Custom RF Profiles for 2.4 and 5GHz Band'.

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag**
- Tag APs

Done

+ Add x Delete

RF Tag Name	Description
default-rf-tag	default RF tag

1 10 items per page

Default RF Tag is a combination of Global Configurations on 2.4 and 5GHz

Add RF Tag

Name* CustomRFTag

Description Enter Description

Dot 11a RF Profile High_Client_Density

Dot 11b RF Profile Low_Client_Density

Cancel Save & Apply to Device

Custom RF Tags can have Custom RF Profiles for 2.4 and 5GHz Band

Tagging Access Points

Wireless Setup

Back

Start

Tags & Profiles

- WLAN Profile
- Policy Profile
- Policy Tag
- AP Join Profile
- Flex Profile
- Site Tag
- RF Profile
- RF Tag

Apply

Tag APs

Done

+ Tag APs

Number of APs: 1
Selected Number of APs: 1

<input type="checkbox"/>	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag	Location	Country
<input checked="" type="checkbox"/>	AP005D.735C.B544	AIR-AP3802I-B-K9	b4de.31d0.5800	Local	Enabled	Registered	default-policy-tag	default-site-tag	default-rf-tag	default location	US

10 items per page

1 - 1 of 1 items

Tag APs

Tags

Policy

Site

RF

Changing AP Tag(s) will cause associated AP(s) to reconnect

AP Tagging with
Policy, Site and RF
Tags

Manage Tags

Policy

Site

RF

AP

Tag Source

Static

Filter

+ Add

✕ Delete

AP MAC Address

Policy Tag Name

Site

RF Tag Name

No items to display

Associate Tags to AP

AP MAC Address*

Policy Tag Name

Site Tag Name

RF Tag Name

Cancel

Save & Apply to Device

Static assignment of AP
MAC address to Policy,
Site and RF Tags



Q Search Menu Items



Dashboard



Monitoring



Configuration



Administration



Troubleshooting

Manage Tags

Policy

Site

RF

AP

Tag Source

Static

Filter

+ Add

✕ Delete

Associate Tags to AP

Rule Name*

Enter Rule Name

AP name regex

Enter Rule

Active

YES



Priority*

0-127

Policy Tag Name

Search or Select



Site Tag Name

Search or Select



RF Tag Name

Search or Select



↶ Cancel

📄 Save & Apply to Device

Rule Based filter to map AP MAC address to Policy, Site and RF Tags

RF Tag Name

No items to display

Release
16.12

Best Practices

Best Practices

- Infrastructure
 - Security
 - RF Management
 - Apple Devices
-
- In Cisco IOS-XE Release 16.12 and higher

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

Administration > Best Practices

Best Practice Score

3/28

INFRASTRUCTURE

+ Disable Aironet IE

+ Disable Management Over Wireless

+ HTTPS for Management

✓

+ More Optimizations...

SECURITY

+ WLAN with WPA2 or 802.1X

✓

+ Client Exclusion

✓

+ User Login Policies

RF MANAGEMENT

+ Auto Coverage Hole Detection

✓

+ Auto Dynamic Channel Assignment

✓

+ Auto Transmit Power Control

✓

+ More Optimizations...

APPLE DEVICES

+ WLAN Configuration

+ Optimized Roaming Disabled

✓

+ 5GHz EDCA fastlane

+ More Optimizations...

DGTL-BRKEWN-2670

170

Catalyst 9800 Controller Migration



AireOS

Wireless LAN
Controller




C9800

Wireless Controller Positioning and Transition

Refresh old 2504, 5508, 8510 to 9800 and position 9800 in new opportunities

Up to
100 APs



SMB, Small Campus
and branch



Mobility
Express



2504

Wireless Controller



Embedded Wireless in Catalyst APs

100-
150 APs



Distributed Branch,
Small Campus



3504

Wireless Controller



C9800-L



C9800-CL

C9800 for cloud

150 to
1500 APs



Medium Campus



5508, 5520

Wireless Controller



C9800-40



C9800-CL

C9800 for cloud

1500 to
6000 APs

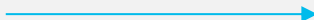


Large Campus



7510, 8510, 8540

Wireless Controller



C9800-80

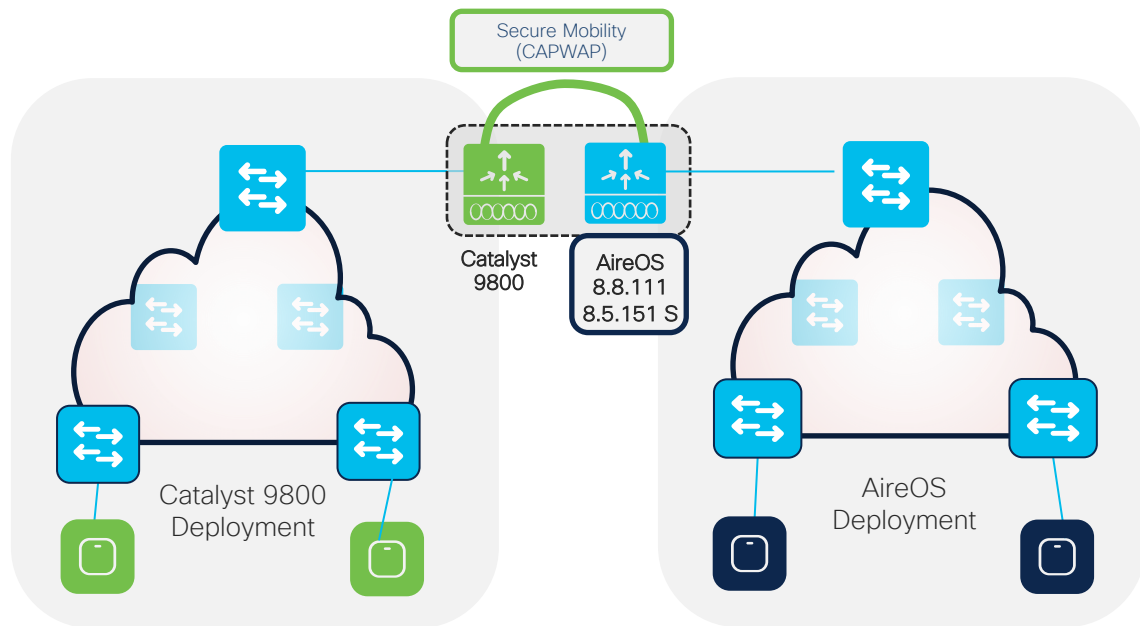


C9800-CL

C9800 for cloud

AireOS and C9800 coexistence

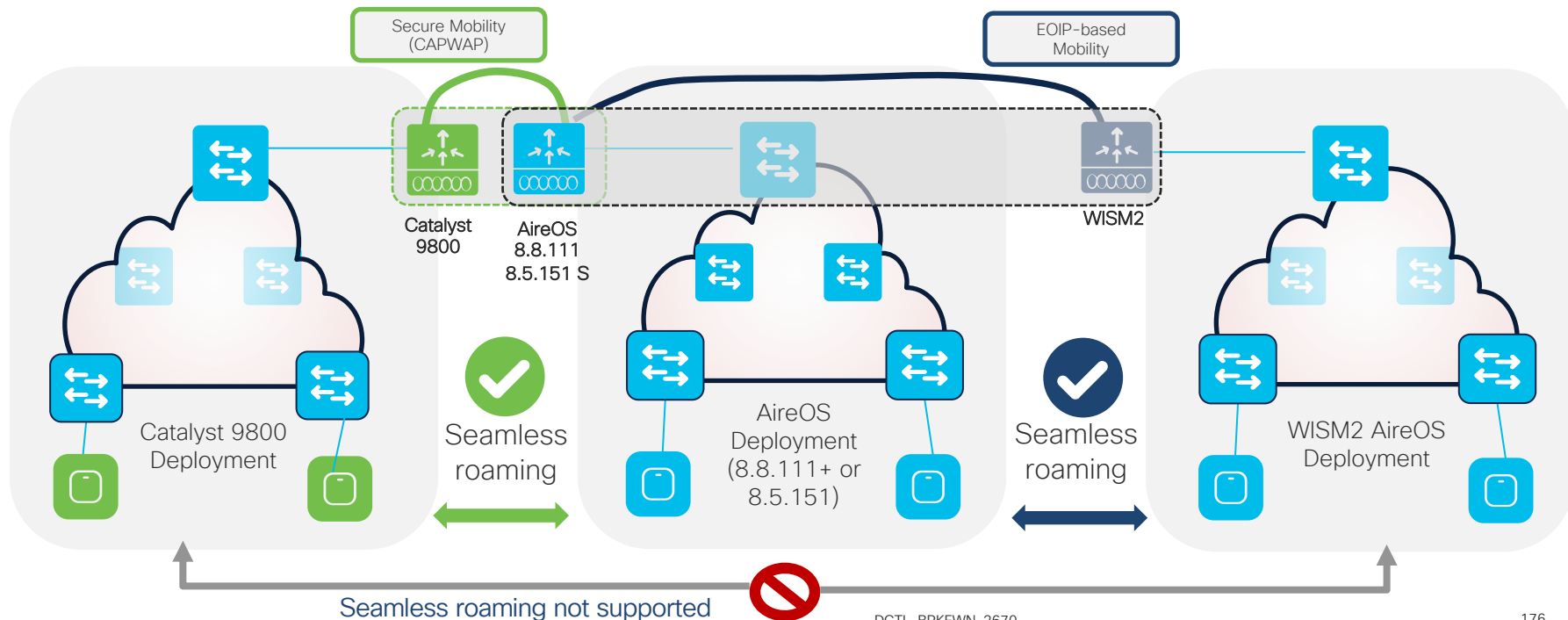
AireOS to C9800 migration - Roaming



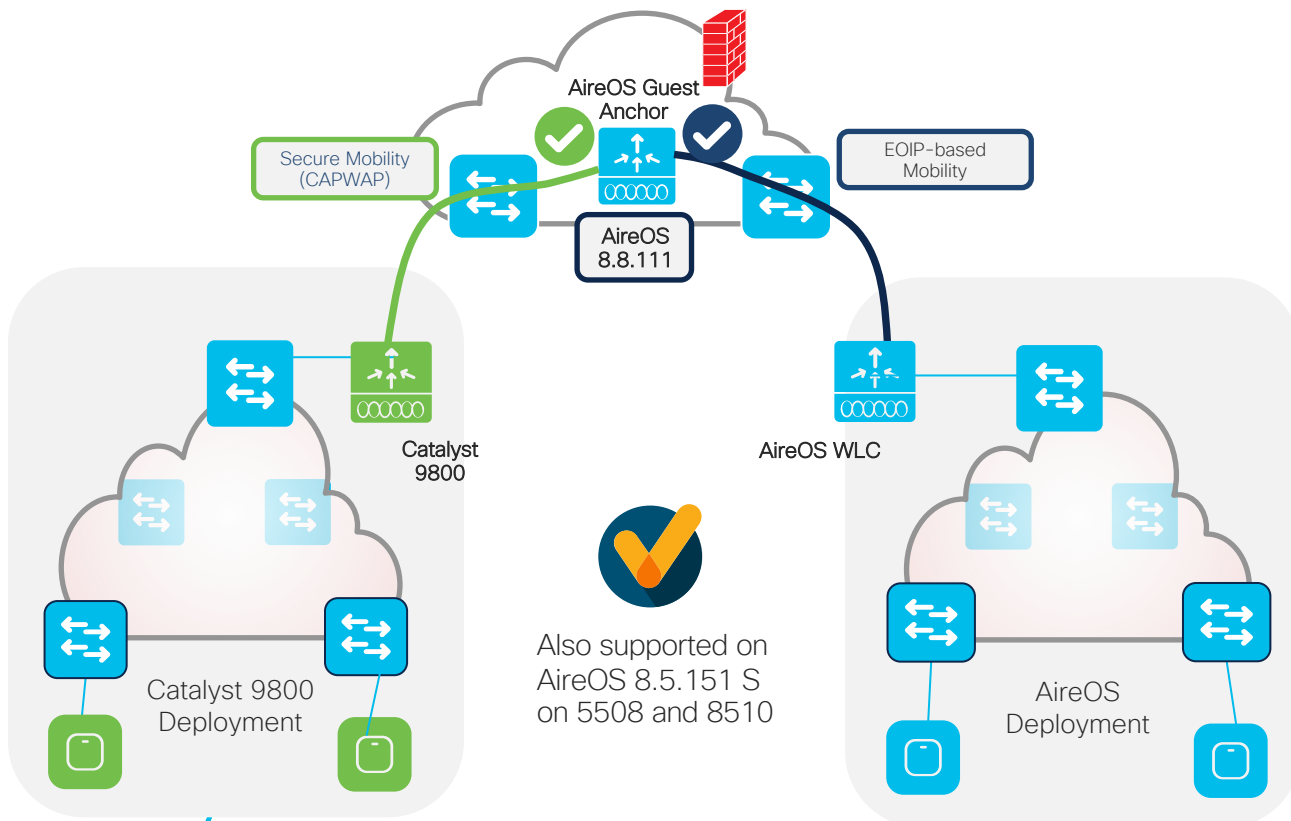
- Mobility Group provides seamless roaming between wireless controllers
- Mobility Group between AireOS and IOS-XE WLCs is only supported on:
 - 3504, 5520, 8540 with 8.8.111 and higher
 - 5508 and 8510 with 8.5.151 special
- This is because C9800 only support CAPWAP based mobility tunnels (Secure Mobility)
- **Note: Secure Mobility is NOT supported on WISM2, 7510, 2500**

AireOS to C9800 migration - Roaming

- For migration with older AireOS WLC it is necessary to use a 5520/8540/3504 to “bridge” the mobility gap and form a mobility group with the C9800



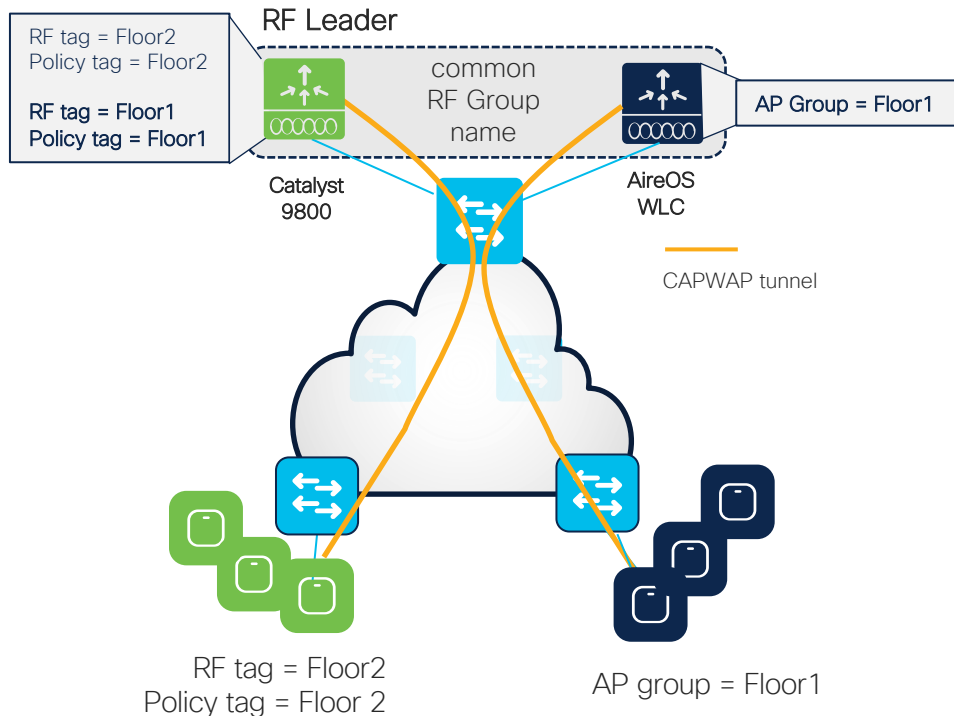
AireOS to C9800 migration - Guest



- For Guest, AireOS WLC running 8.8.111 and higher can talk both tunneling protocols
- It can provide Guest Anchor functionalities for both the new C9800 based deployments and the legacy AireOS based network

AireOS to C9800 migration – common RF Group

RRM works in a mixed controller environment and we can have one RF master:



- C9800 and AireOS controllers can create one RF domain and share a **common RF plan**
- The **RF group name** on both AireOS and C9800 controllers needs to match
- 8.8 is required on AireOS (8.8.111 recommended)
 - A RF leader is elected (based on controller capacity) and common channel and power plan will be used for all APs
 - APs will be not show up as rogue on the other controller
- **NOTE:** in a scenario where you want to have custom RF profiles or enable FRA, then the leader (e.g. C9800 controller) needs to have Policy and RF tags matching the names of the AP Group names on AireOS WLC. Of course the settings of RF profiles on both controllers need to match as well.

AireOS to C9800 migration

Moving APs between Controllers

AP migration should happen in chunks (floor or roaming domain/building)

Things to keep in mind:

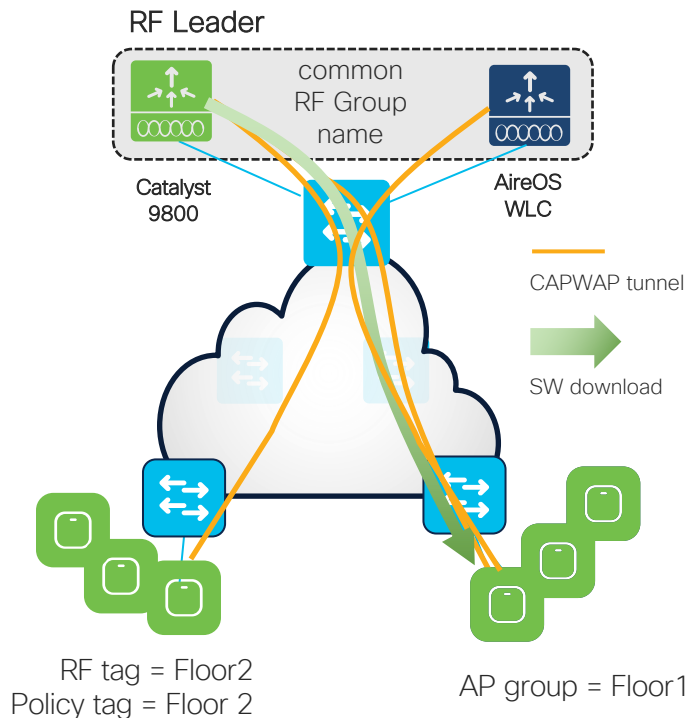
- Make sure the AP can join the C9800 (W1/W2/AX APs)
- To move the AP from AireOS to C9800:

from GUI:



from CLI: *“capwap ap primary-base <name> <IPaddress>”*

- The first time you move an AP from AireOS to C9800 (or vice versa), the AP will download the new image, reboot and join the new controller
- If the AP has the image as a backup because had already joined that controller, then there is no download



Migration Tools

Migration tool

- Migration tool is now alive and managed by TAC
- Tool is available here <https://cway.cisco.com/tools/WirelessConfigConverter/>

The screenshot displays the Cisco TAC Tool interface for the migration tool. On the left, a sidebar shows the 'Converted Config Lines' section with a 'Run' button and a list of categories: Translated Config, Unsupported Config, Not Applicable Config, and Unmapped Config. The main panel shows the 'Converted Config Lines' section with a 'Run' button and a list of categories. The 'Translated Config' category is expanded, showing a list of translated configuration lines. Two blue arrows point from the list to the right, highlighting the translated configuration lines.

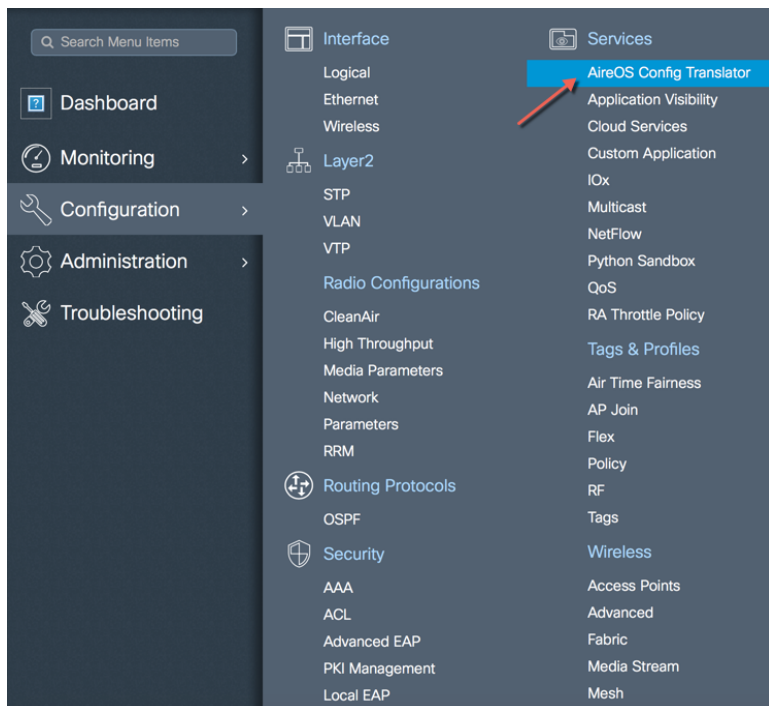
```
=====  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!  
! Interface Configuration  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!  
! config interface vlan management 113  
!  
! config interface address management 207.129.102.249 255.255.255.0 207.129.102.254  
!  
vlan 113  
!  
name "management"  
!  
no shutdown  
!  
interface vlan 113  
!  
description "management"  
!  
ip address 207.129.102.249 255.255.255.0  
!  
no shutdown  
!  
!
```

Tool provides following config:

- Translated
- Unmapped
- Unsupported
- Not Applicable
- AireOS CLIs and the correspondent translated IOS-XE commands
- Always recommended to analyze the translated config before paste it

AireOS Config Translator

To access the tool, go under Configuration > Services > AireOS Config Translator



Migration from AireOS WLC to C9800 with DNAC



- It covers AireOS to C9800 migration using DNAC
- Step by step configuration
- **Note:** DNAC only learns a subset of configurations from AireOS, the ones that are mapped to the Design flow
- [Direct link](#)



Catalyst 9800
Wireless Controller is
ready for prime time!

Don't miss the Cisco Wireless book!



It's an e-book and you can download it from here

<https://www.cisco.com/c/dam/en/us/products/collateral/wireless/nb-06-wireless-wifi-starts-here-ebook-cte-en.pdf>

- [Deployment guides](#)
- [Configuration Examples and Tech notes](#)
- [Cisco Wireless YouTube channel](#)

Additional Resources

Thank you



Possibilities

#CiscoLive