ALERT
ADAPT
ACHIEVE

ALERT
ADAPT
ACHIEVE

SAMART TELCOMS 2022

SAMART
TELCOMS

โครงการค่าจัดหาระบบโทรศัพท์ (IP Telephony) เพื่อการสื่อสารแบบครบวงจร ของกระทรวงมหาดไทย สำนักงานปลัดกระทรวงมหาดไทย

สัญญาเลขที่ 45/2563 ลงวันที่ 13 กรกฎาคม 2563

ระยะเวลาโครงการ 14 กรกฎาคม 2563 – 5 มีนาคม 2565

(600 วัน)

กระทรวงมหาดไทย

ALERT
ADAPT
ACHIEVE

MOI IPPHONE Network Training

SAMART
TELCOMS

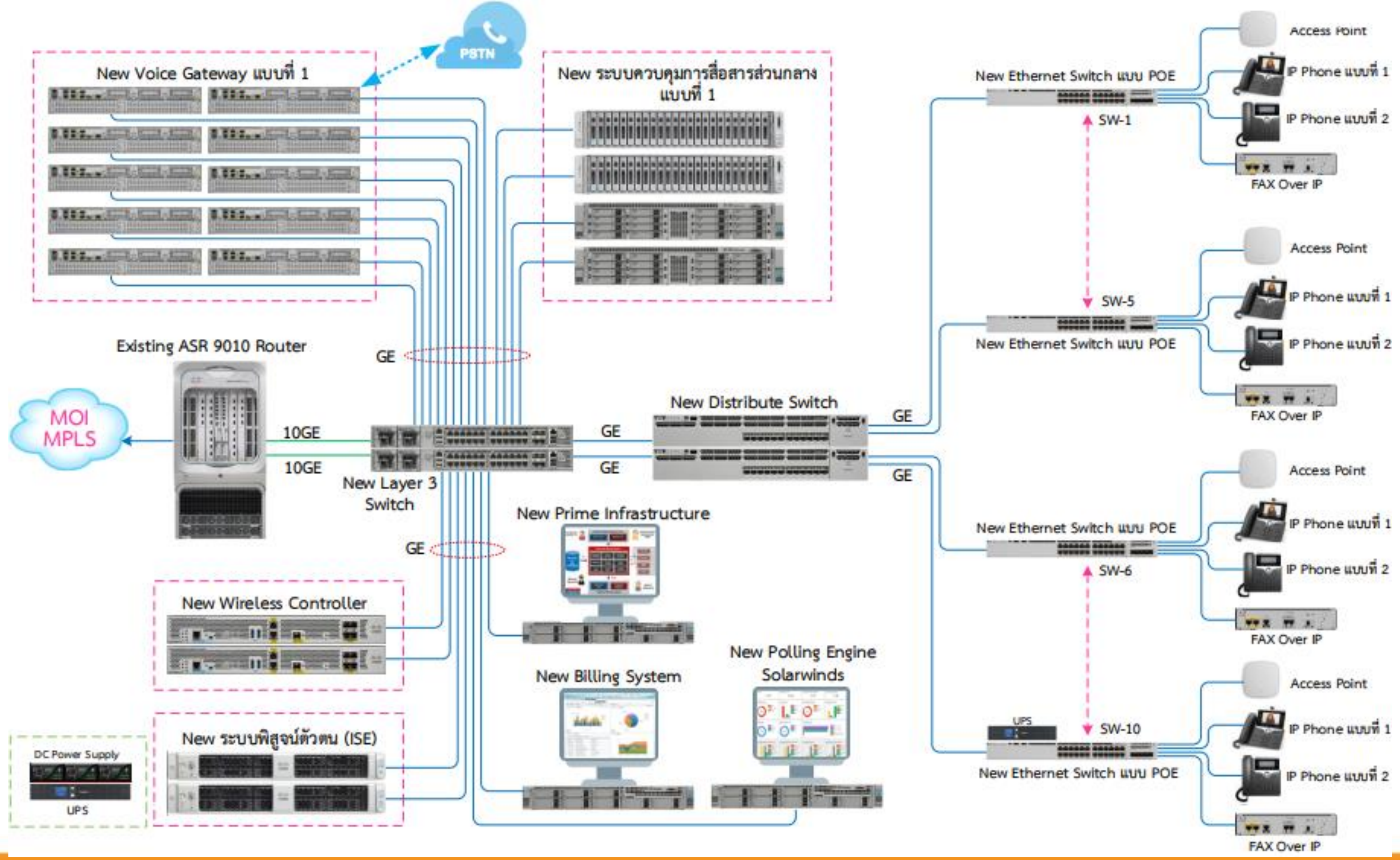
ALERT
ADAPT
ACHIEVE

Cisco Hardware & Network Diagram

SAMART
TELCOMS

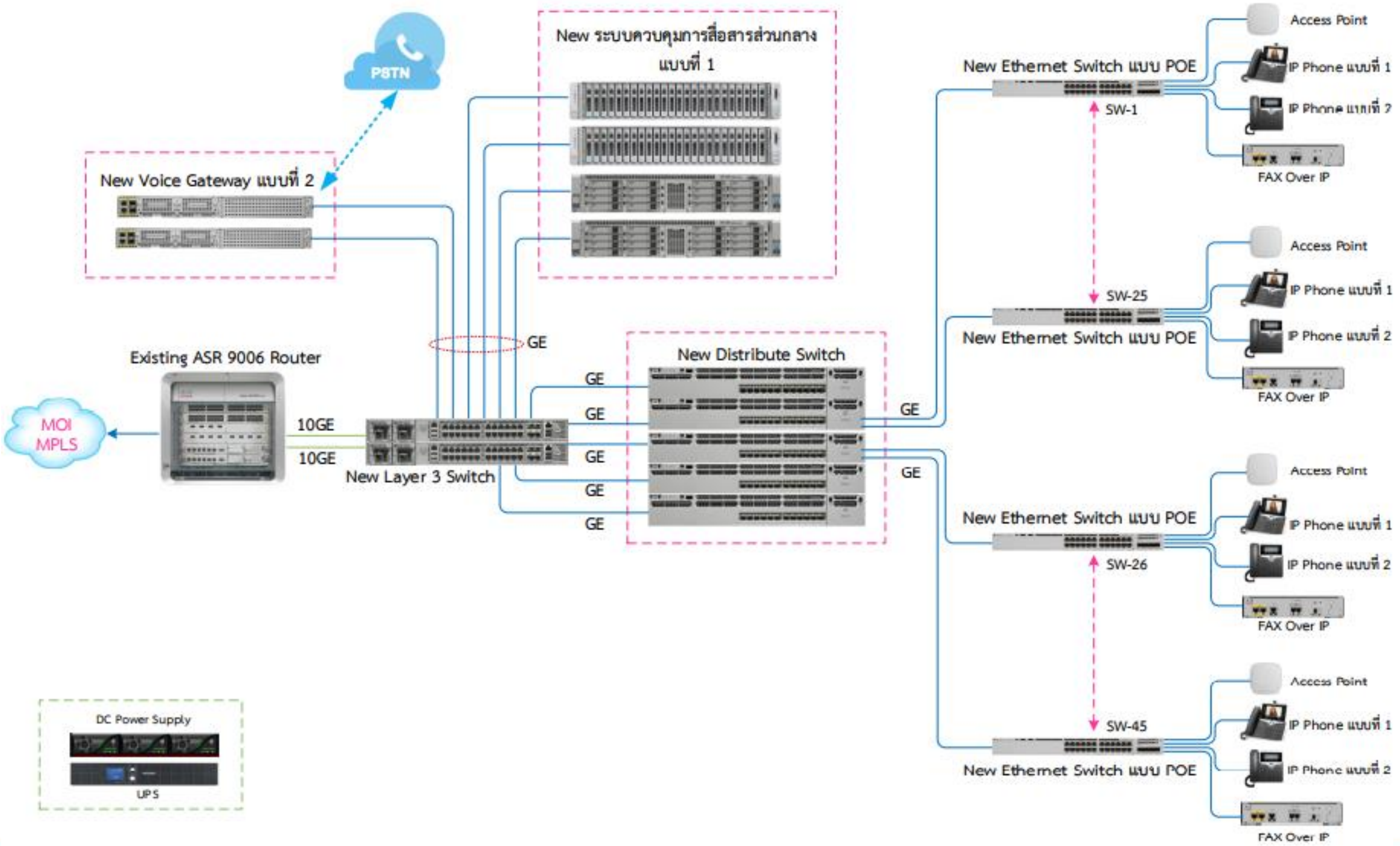
ALERT
ADAPT
ACHIEVE

Network Diagram ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สป.มท.



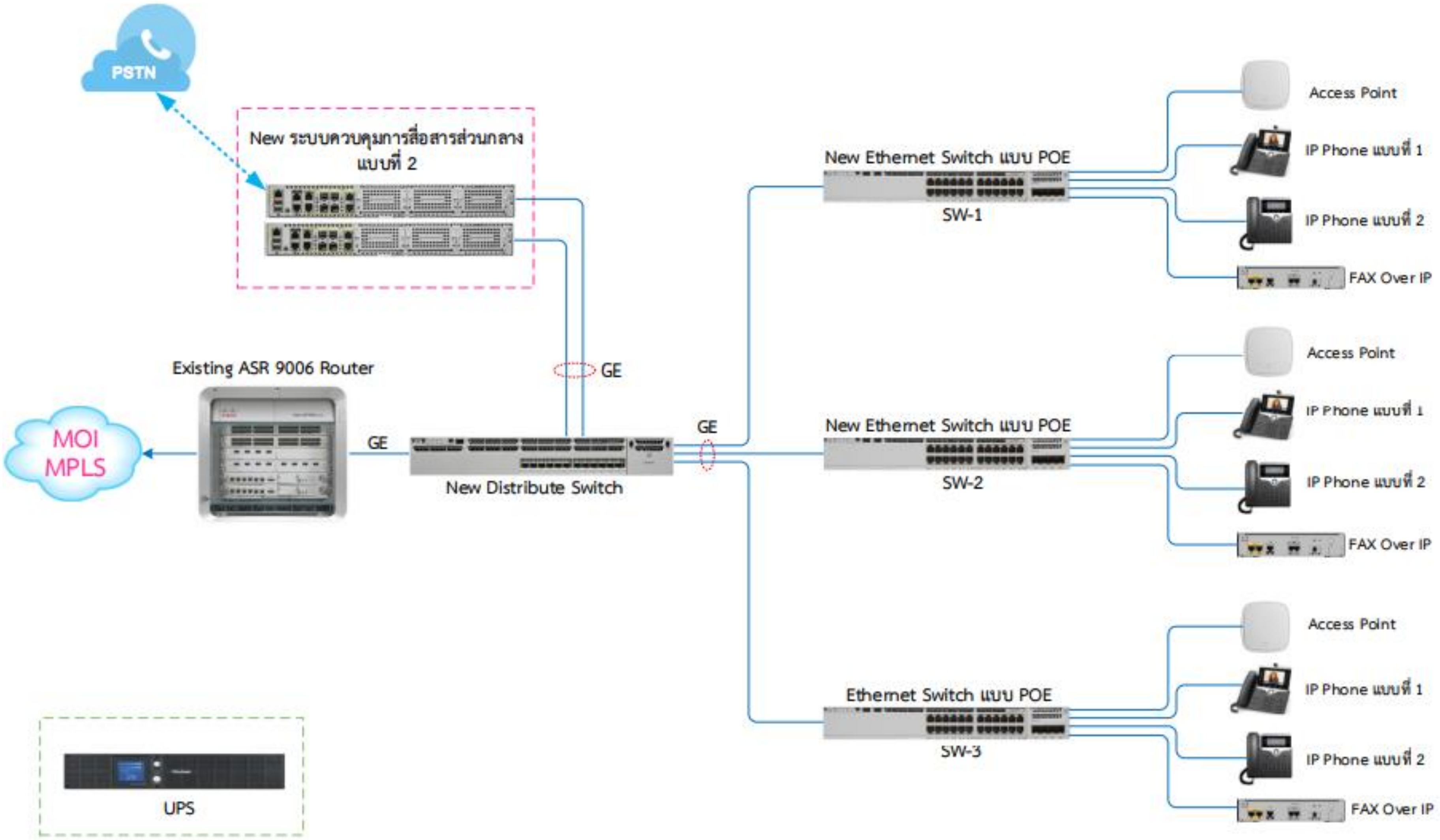
SAMART
TELCOMS

Network Diagram กระทรวงมหาดไทย



ALERT
ADAPT
ACHIEVE

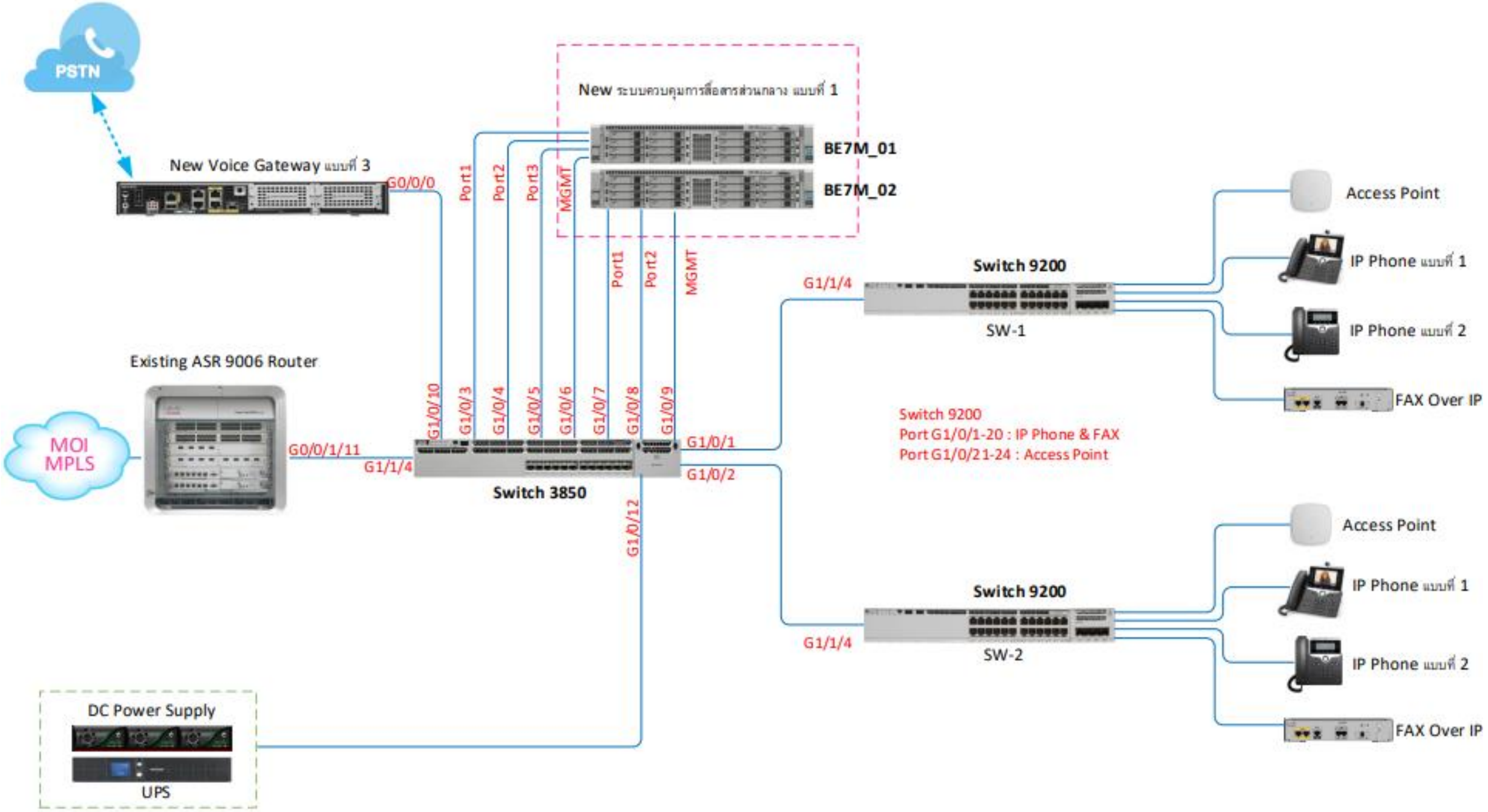
Network Diagram ศูนย์พัฒนาบุคลากรเทคโนโลยีสารสนเทศและการสื่อสาร (ลาดโตนด)



SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

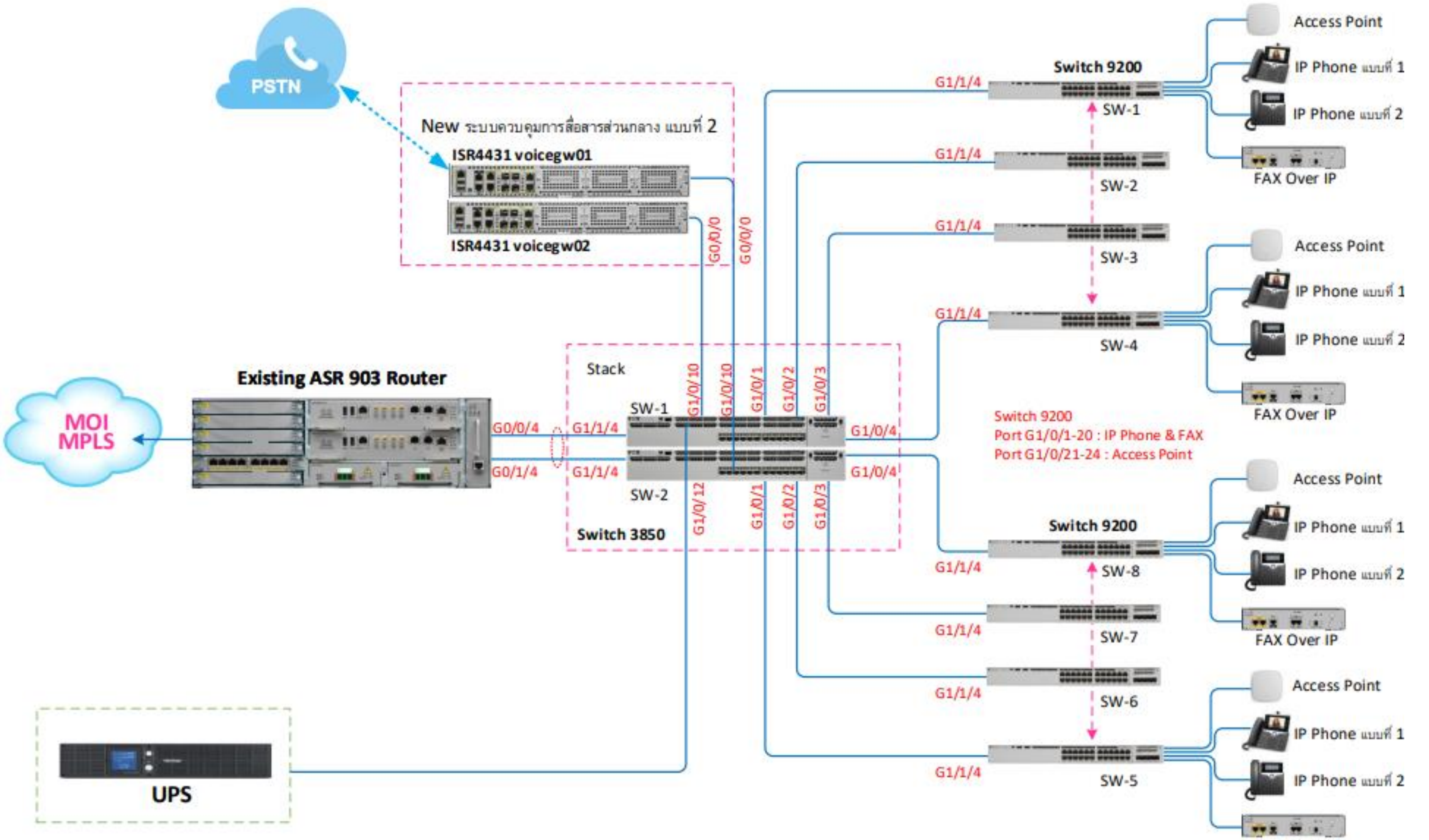
Network Diagram ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเขต



Switch 9200
Port G1/0/1-20 : IP Phone & FAX
Port G1/0/21-24 : Access Point

SAMART
TELCOMS

Network Diagram ศาลากลางจังหวัด



Switch 9200
Port G1/0/1-20 : IP Phone & FAX
Port G1/0/21-24 : Access Point

ASR 920

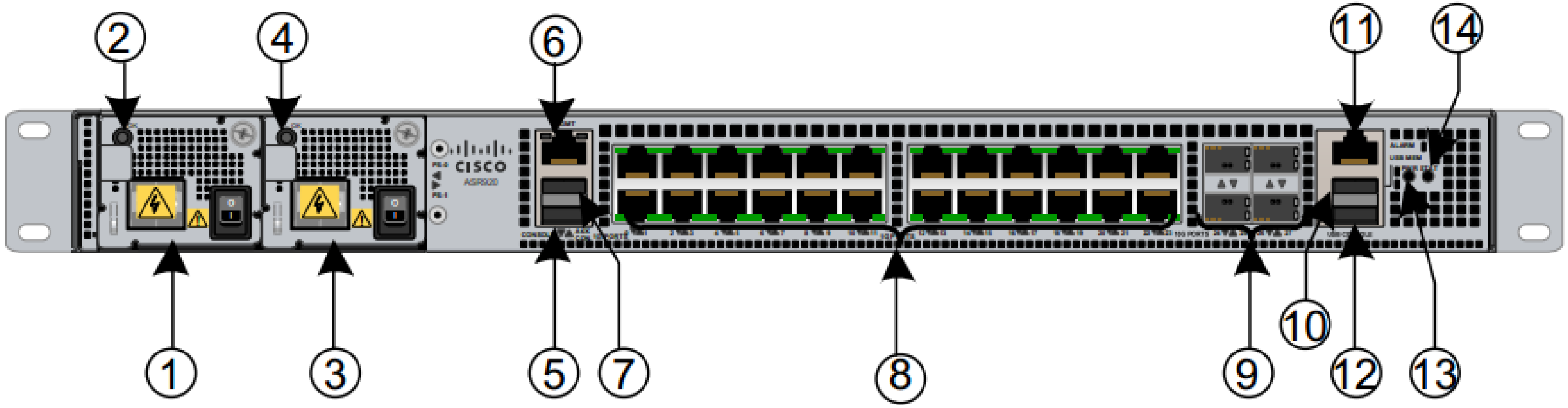


Figure 32 ASR-920-24TZ-M Front Panel Component Indicator

1	Power Supply 0	8	24x1GE SFP Copper
2	Power Supply 0 LED	9	4x10GE SFP+
3	Power Supply 1	10	USB Memory port
4	Power Supply 1 LED	11	Alarm port
5	Console port (TIA/EIA-232F)	12	USB Console port
6	Management port	13	Board power LED
7	Auxiliary Console port	14	System Status LED

The Catalyst 3K Family

Catalyst 3850
Stackwise-480,
Stackpower
Data/PoE/PoE+/UPoE
FRU Uplinks

Catalyst 3650
Stackwise-160,
-
Data/PoE/PoE+/
Fixed Uplinks

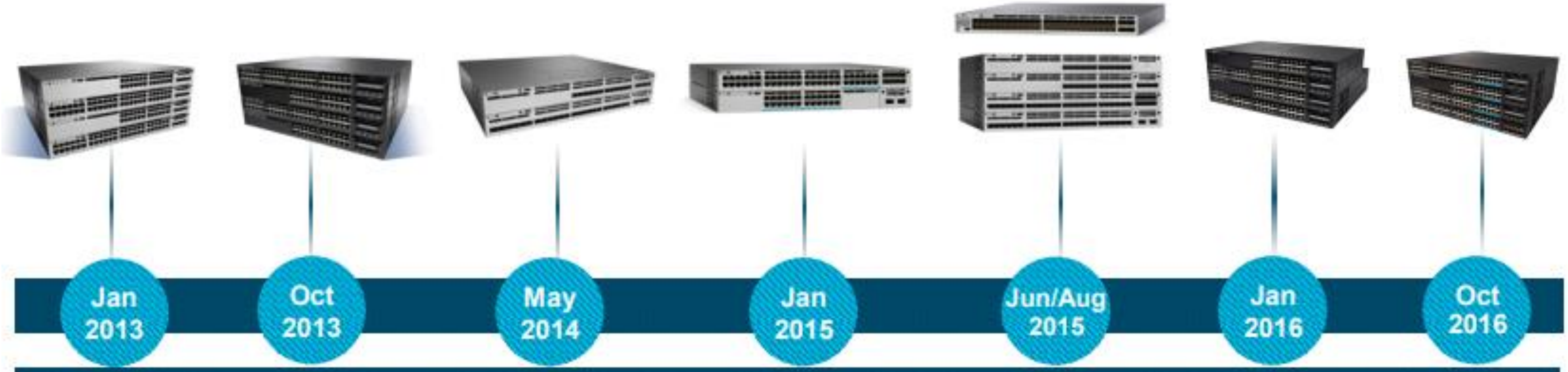
Catalyst 3850 SFP
Stackwise-480,
Stackpower
12 and 24 Port Versions
FRU Uplinks

Catalyst 3850 mGig
Stackwise-480,
Stackpower
24 and 48 Port Versions
Stacks with any Catalyst 3850

Catalyst 3850 SFP+
Stackwise-480,
Stackpower
12, 24 and 48 Port Versions
Enabling 10G Aggregation

Catalyst 3650 Mini
Stackwise-160,
Data/PoE/PoE+/
Fixed Uplinks
Stacks with any 3650

Catalyst 3650 Mgig
Stackwise-160,
Data/PoE/PoE+/UPOE
Fixed Uplinks
Stacks with any 3650



Built on Cisco's Innovative "UADP" ASIC

One Switch – Multiple Deployment scenarios

MultiGigabit

1 Gigiagbit

Catalyst 3850 Copper

Copper SKUs Data and
PoE/UPoE Switches

480G Stacking Capacity

MultiGigabit

Mini – Shallow Depth

1 Gigabit

Catalyst 3650 Copper

Copper SKUs Data and
PoE/UPoE Switches

160G Stacking Capacity

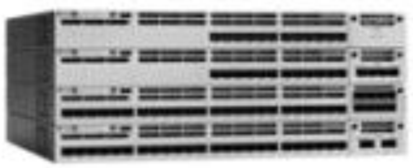
SFP

Catalyst 3850 Fiber SFP

Fiber SKUs SFP Versions

48 Port SFP+ Version
No Stackwise 480

SFP+



Catalyst 3850 Fiber SFP+

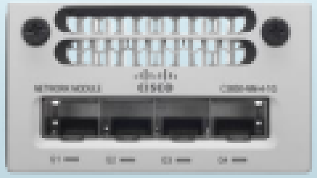
Fiber SKUs SFP+ Versions

Enterprise Class Access Layer

Smaller Core & Aggregation Option

Based on a Common ASIC and Software

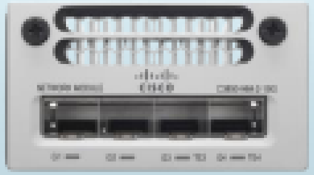
Uplink Network Module Options on Catalyst 3850



C3850-NM-4-1G

4x1Gig

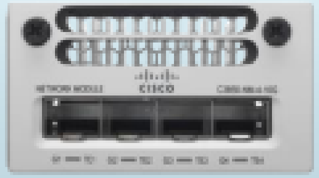
SFP



C3850-NM-2-10G

2x1Gig+2x10Gig

SFP/SFP+



C3850-NM-4-10G

4x10Gig

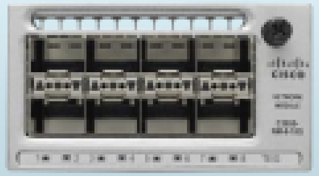
SFP/SFP+

48 Ports or 12+ SFP+

C3850-NM-2-40G

2x40Gig

QSFP



C3850-NM-8-10G

8x10Gig

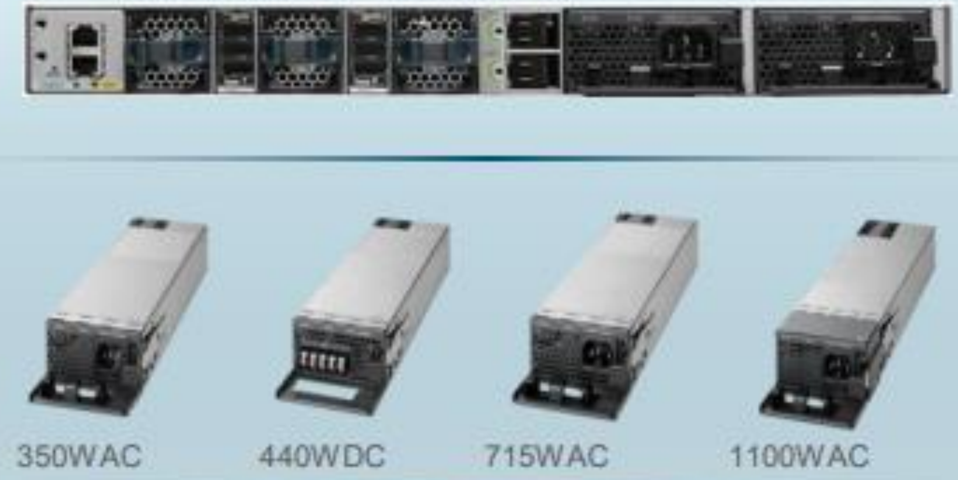
SFP/SFP+

For MultiGigabit and SFP+ Versions only

Flexibility & Investment Protection

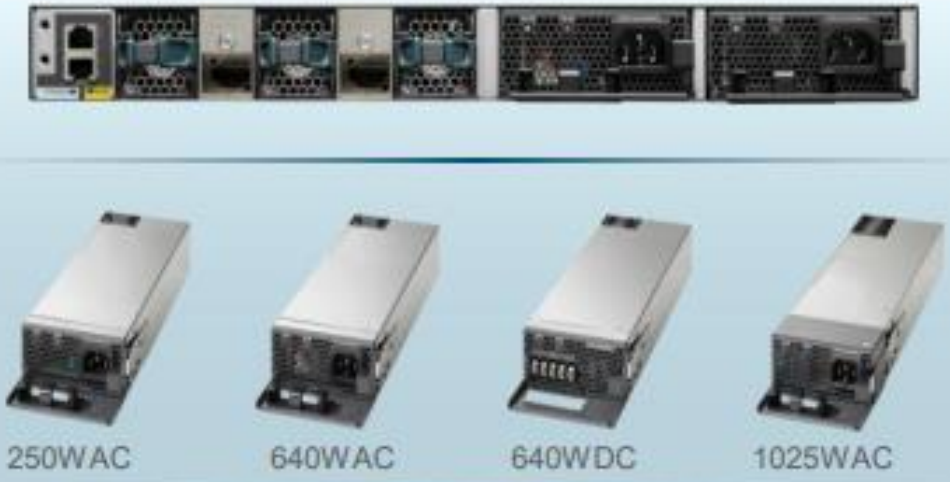
Power Supplies

Catalyst 3850



Same as 3750-X—
Interchangeable New PIDs

Catalyst 3650

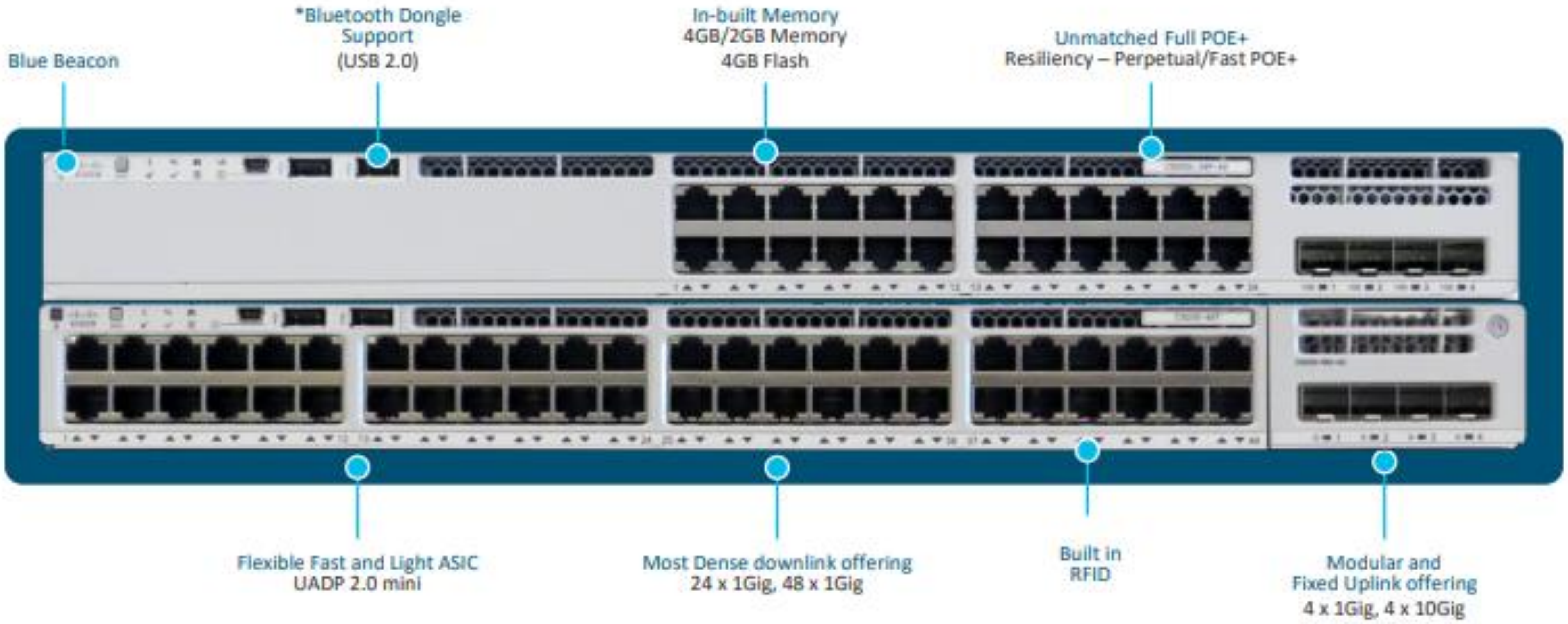


Wider Than 3850/3750-X PSs
Different Watts Capacity

Catalyst 9K Family

June 2017

Fastest Growing Product in Cisco's History



Blue Beacon

*Bluetooth Dongle Support
(USB 2.0)

In-built Memory
4GB/2GB Memory
4GB Flash

Unmatched Full POE+
Resiliency – Perpetual/Fast POE+

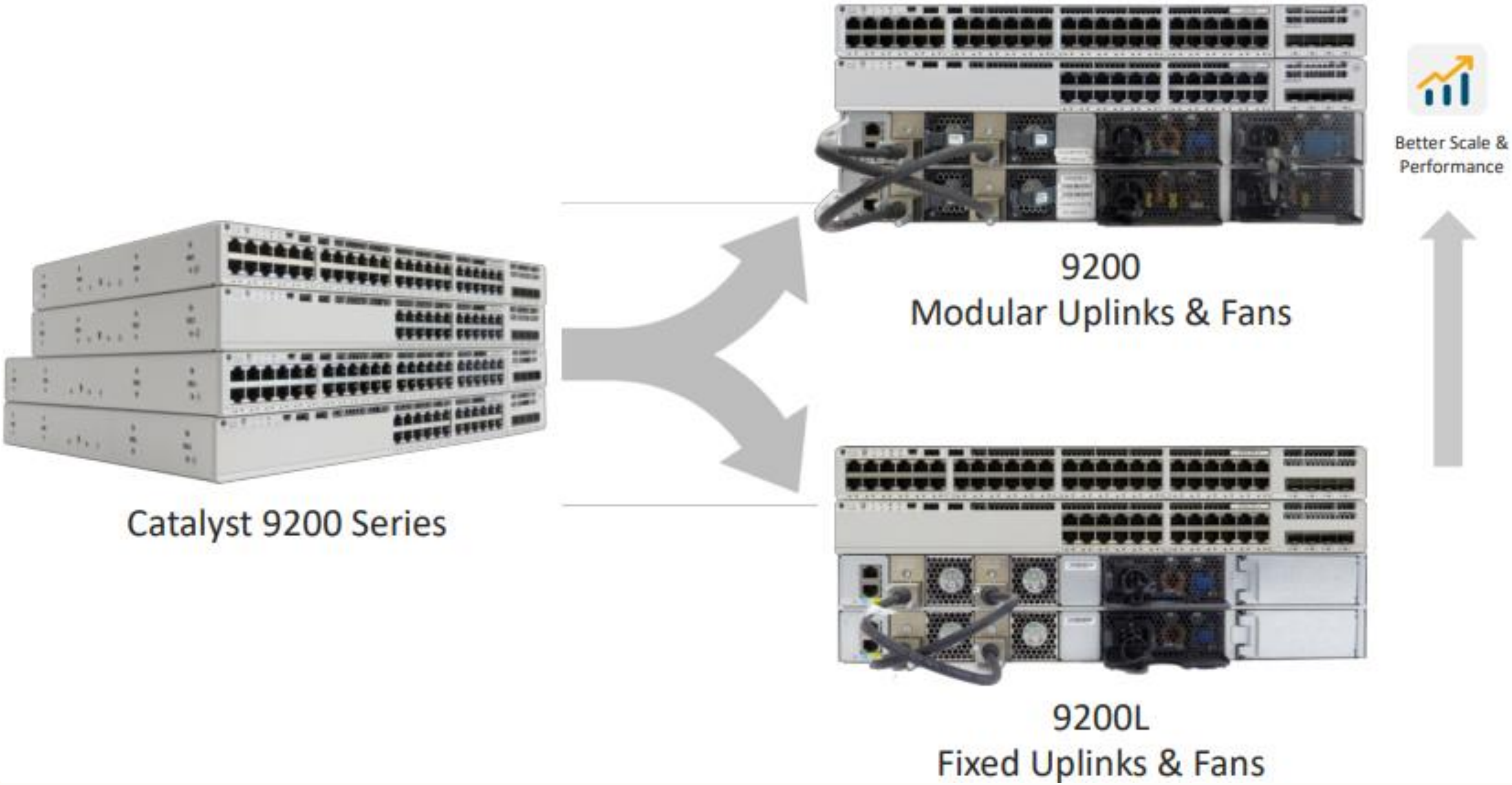
Flexible Fast and Light ASIC
UADP 2.0 mini

Most Dense downlink offering
24 x 1Gig, 48 x 1Gig

Built in
RFID

Modular and
Fixed Uplink offering
4 x 1Gig, 4 x 10Gig

Catalyst 9200 Extends **Intent Based Networking** Everywhere



Catalyst 9200 Series

9200
Modular Uplinks & Fans

9200L
Fixed Uplinks & Fans

Better Scale & Performance

Full PoE+ (30W on All Ports)

Separate Data SKUs Available

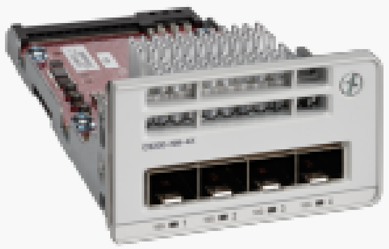
Catalyst 9200 Offers **Best in Class PoE+**

Redundant Modular Power Supplies

- 1+1 Redundancy OR Combined Mode
- Field Replaceable Unit – FRUable Power Supplies
- Universal Power Supplies 110-240 Volts
- PoE+ with Platinum Rated Power Supplies

Catalyst 9200 Offers **Full Power Resiliency**

Catalyst 9200



4 x 10 Gig
SFP/SFP + Transceivers

4 x 1 Gig
SFP Transceivers

Catalyst 9200L

4 x 10 Gig
SFP/SFP + Transceivers

4 x 1 Gig
SFP Transceivers

- Modular Uplinks Supported on All 9200s
- Modular Uplinks FRUable
- 10G /1G Speed
- SFP/SFP+ Auto Sensing

ALERT
ADAPT
ACHIEVE

Catalyst 9200

Modular Redundant Fans

Catalyst 9200L

Fixed Redundant Fans

- Modular Fans FRUable
- Variable Speed based on Temperature
- 1+1 Redundancy

ALERT
ADAPT
ACHIEVE

Catalyst 9200

Stackwise-160

Catalyst 9200L

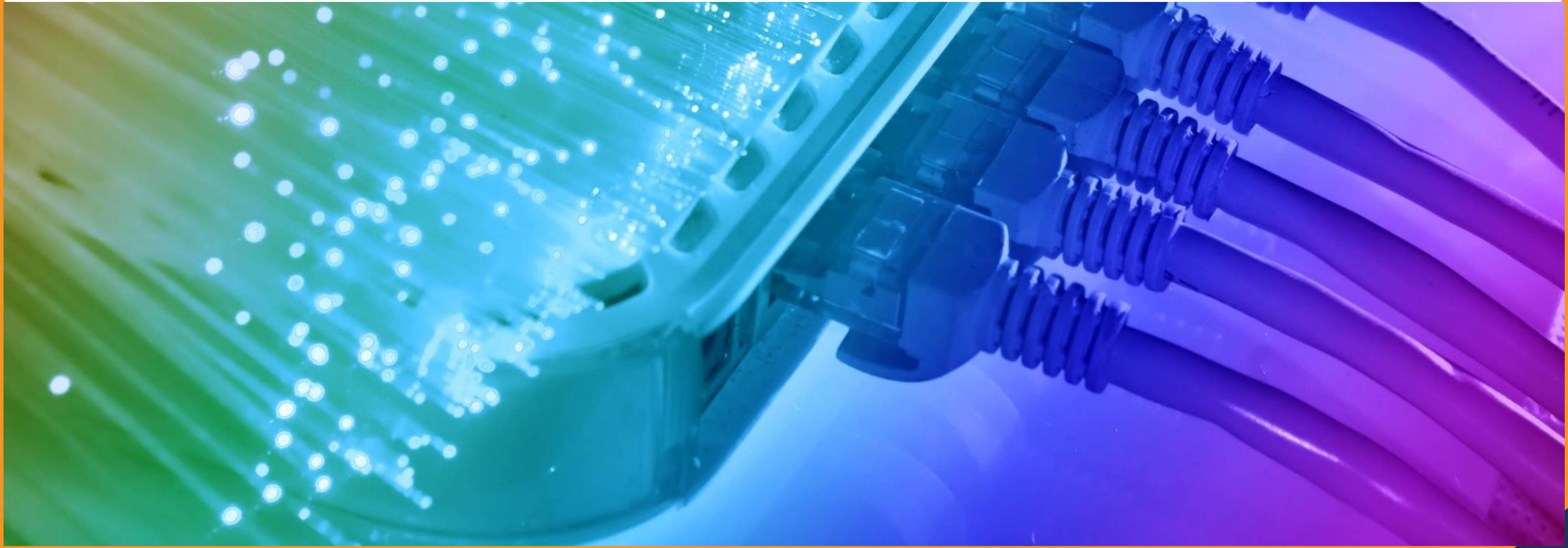
Stackwise-80

- Stackwise-160/80 Technology
- Stack Ring Architecture
- Optional Stacking Kit

SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

Ethernet LAN



SAMART TELCOMS

Ethernet LAN

- LAN ย่อมาจาก Local Area Network คือระบบเครือข่าย แบบเชื่อมต่อคอมพิวเตอร์และอุปกรณ์เข้าด้วยกันในระยะจำกัด เช่น ในอาคารเดียวกัน หรือบริเวณเดียวกันที่สามารถลากสายถึงกันได้โดยตรง ส่วนมากจะใช้สายเคเบิ้ล หรือ ที่เรียกกันว่า สาย LAN เป็นตัวกลางในการเชื่อมต่อ

- อีเทอร์เน็ต (Ethernet) เป็นชื่อเรียกวิธีการสื่อสารในระดับล่างหรือที่เราเรียกว่าโพรโทคอล (Protocol) ของ LAN ที่พัฒนาขึ้นโดย 3 บริษัทใหญ่ คือบริษัท Xerox Corporation, Digital Equipment Corporation (DEC) และ Intel ปัจจุบัน Ethernet เป็นเทคโนโลยีเครือข่ายที่ได้รับความนิยมมาก

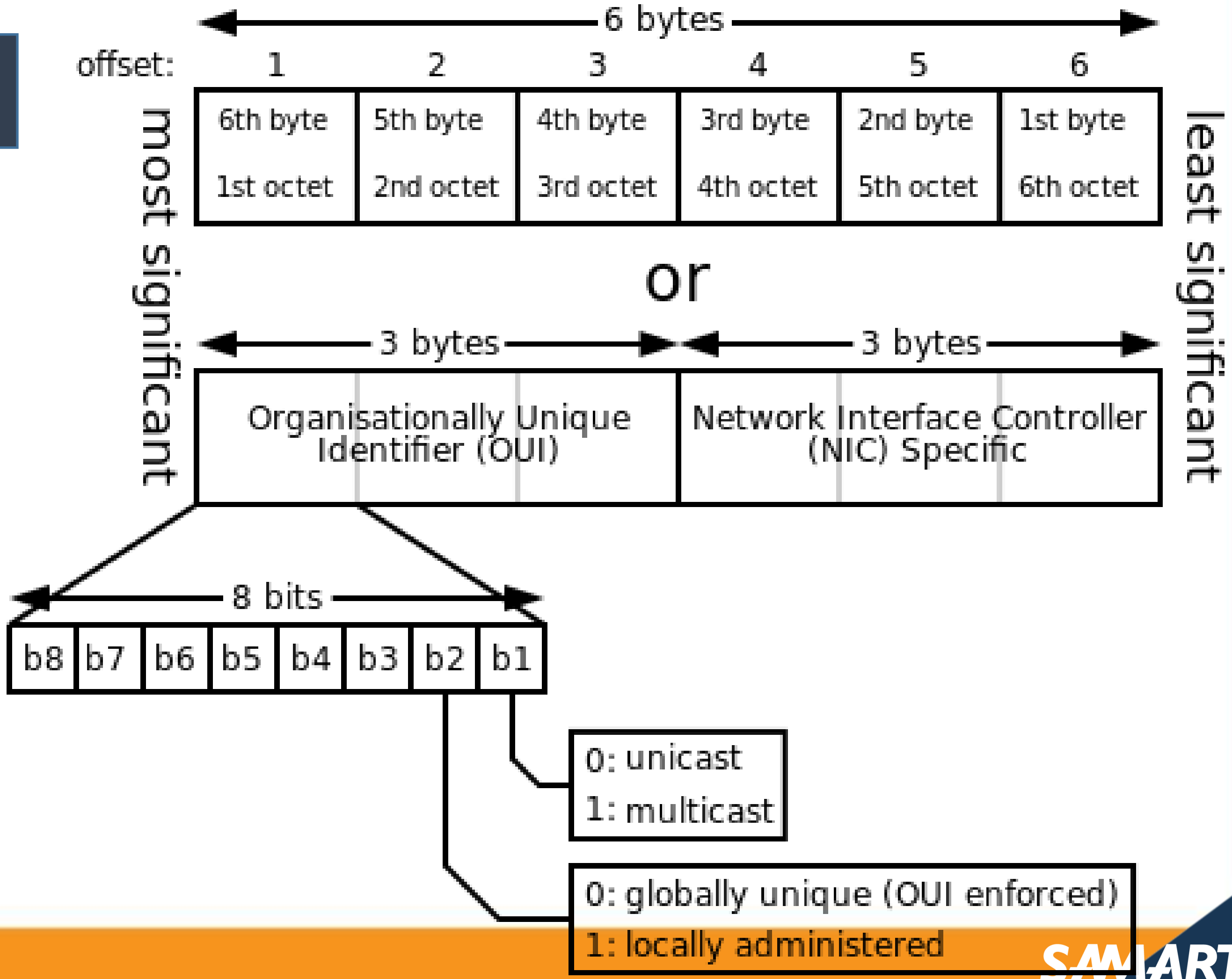
MAC Address

MM : MM : MM : SS : SS : SS

- Physical address → ถูกกำหนดค่ามาจากโรงงานที่ผลิต ซึ่งเป็นค่าตายตัวบน interface และไม่ซ้ำ
- 24 bits แรก = ID ผู้ผลิต (ตาม IEEE)

  24 bits หลัง = serial number ของอุปกรณ์ที่ผู้ผลิตกำหนดให้

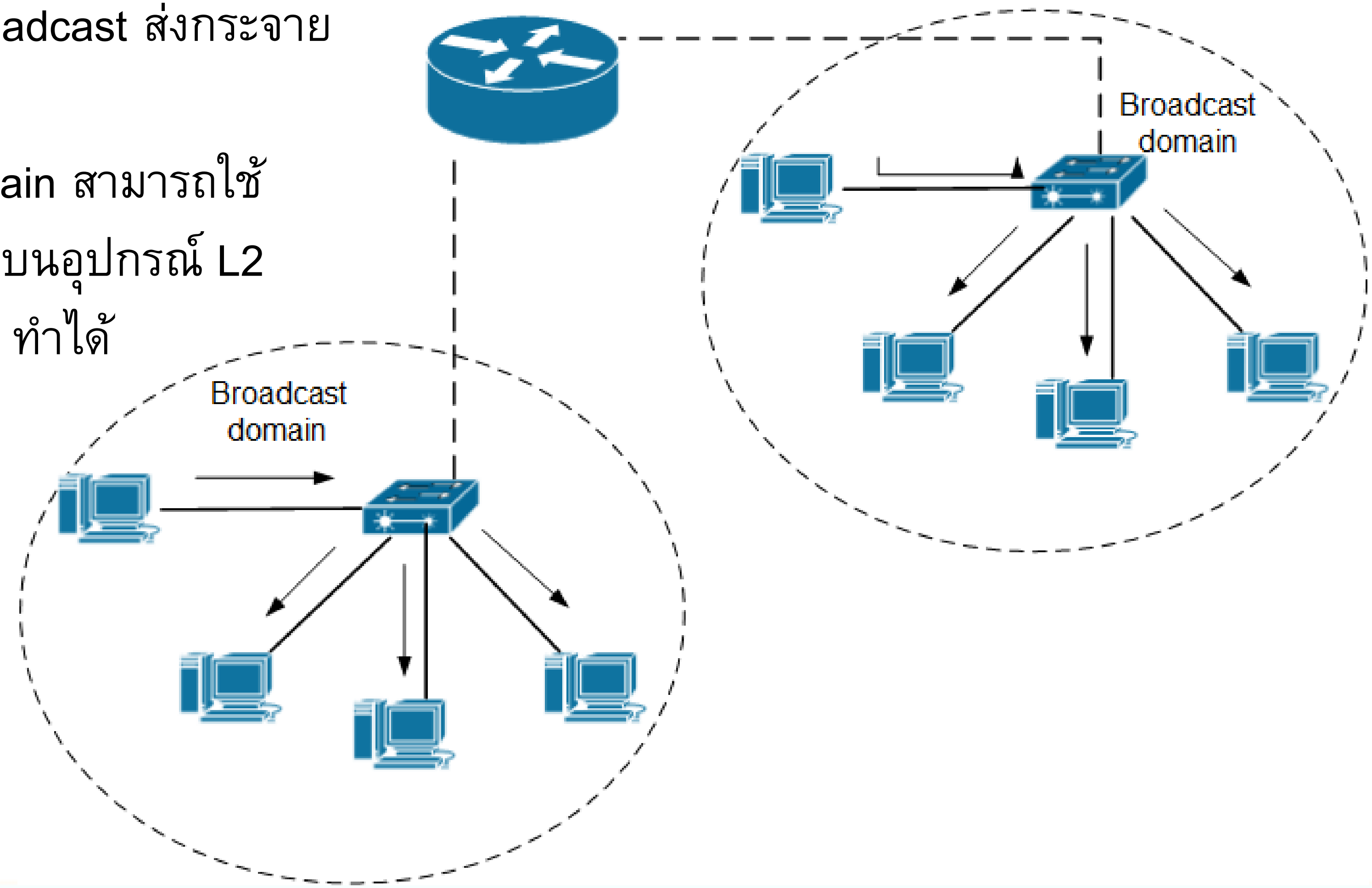
6 octets หรือ 6 bytes = 6x8 = 48 bits



ALERT
ADAPT
ACHIEVE

Broadcast Domain

- Broadcast Domain คือขอบเขต หรือเครือข่ายที่ข้อมูลแบบ broadcast ส่งกระจายไปถึงผู้รับภายในนั้น
- การแบ่ง Broadcast Domain สามารถใช้อุปกรณ์ L3 หรือ feature บนอุปกรณ์ L2 (แบ่ง VLAN ด้วย switch) ทำได้

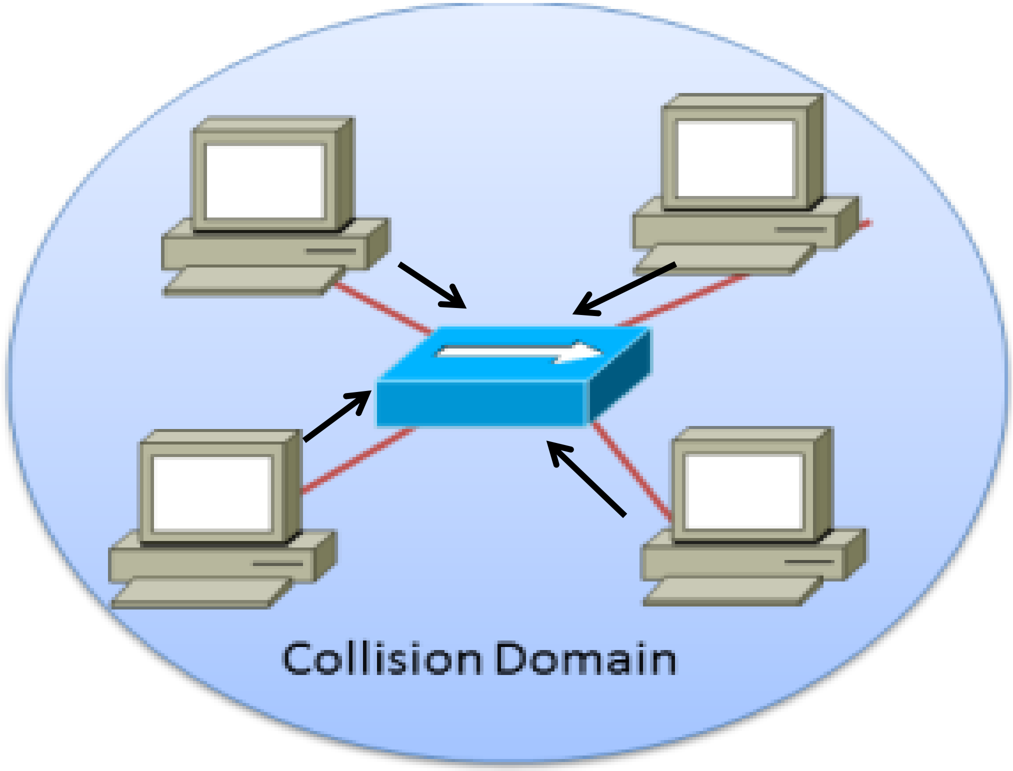


SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

Collision Domain

- Collision Domain คือขอบเขต หรือ ส่วนของเครือข่ายซึ่งอุปกรณ์ตั้งแต่ 2 ตัวขึ้นไปทำการแบ่งใช้ bandwidth เดียวกัน ทำให้ข้อมูลสามารถวิ่งชนกันได้
- การแบ่ง Collision Domain สามารถใช้อุปกรณ์ L2 ขึ้นไป (ดังนั้นจะเกิดในเครือข่ายที่ใช้ Hub)

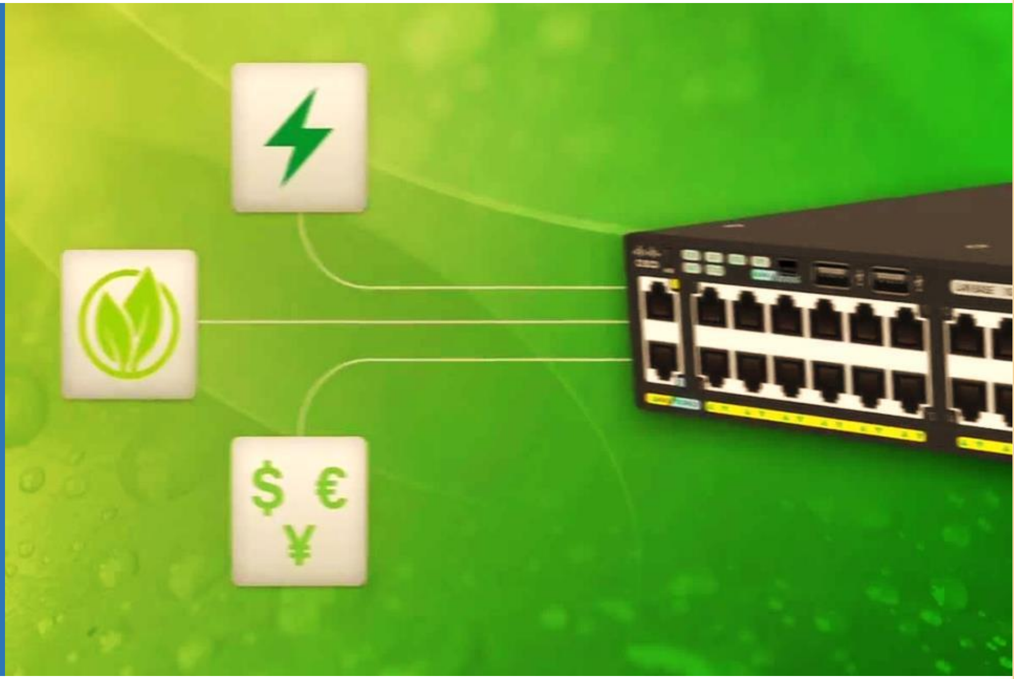


SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

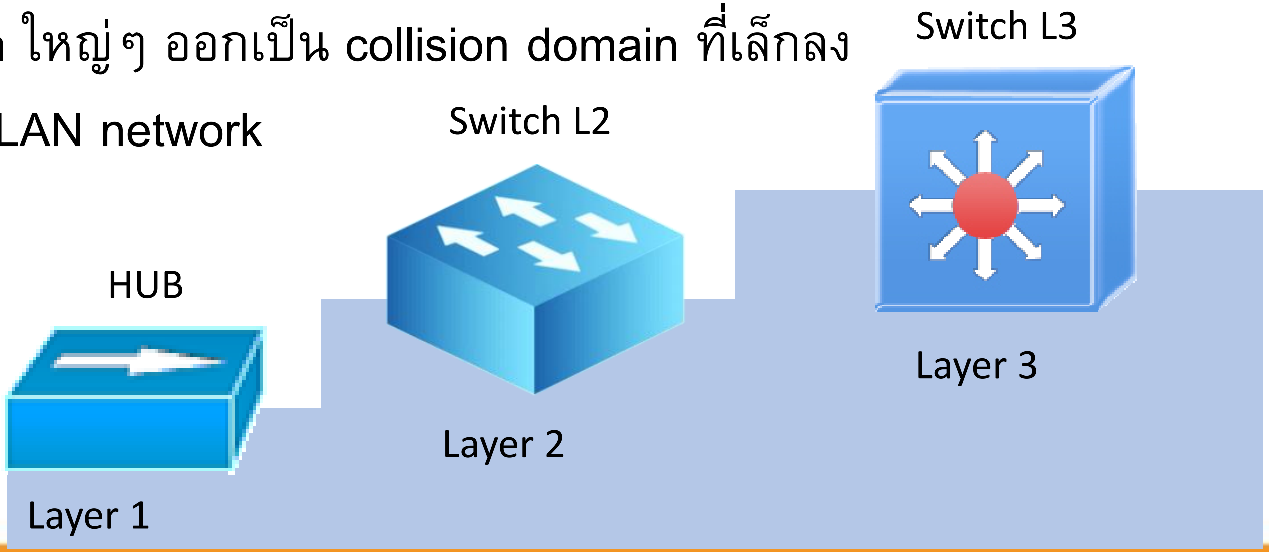
Catalyst Switch

Medium-Sized Switched
Network Construction



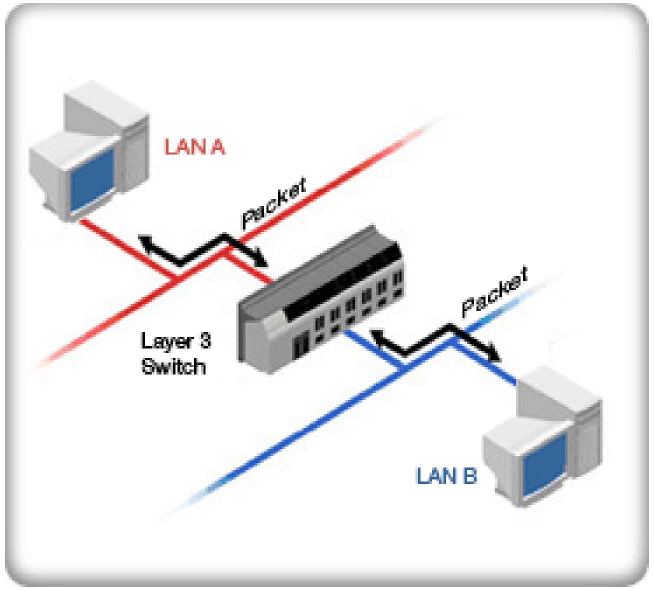
SAMART
TELCOMS

- Hub & Switch หน้าที่หลักจะเหมือนกันคือ เชื่อมต่อให้เครื่องคอมพิวเตอร์ที่ตั้งอยู่คนละที่สามารถติดต่อสื่อสารกันได้
- HUB นั้นเวลาส่งข้อมูลนั้นจะเป็นแบบ broadcast กระจายไปทุกเครื่องแต่ถ้าเป็น switch นั้น จะดูว่าข้อมูลนี่เป็น ของเครื่องไหนแล้วค่อยส่งไปยังเครื่องนั้น
- Hub จะทำงานที่ Layer 1 ทำหน้าที่ทวนซ้ำสัญญาณ ถ้าในเวลาเดียวกัน เครื่องหนึ่งในเครือข่ายต้องการส่งข้อมูล เครื่องอื่นๆ จะไม่สามารถส่งข้อมูลได้
- Switch จะทำงานเหมือนกับ Hub แต่ ขณะที่เครื่องหนึ่ง ส่งข้อมูลไปยังอีกเครื่อง เครื่องอื่นๆ จะยังสามารถส่งข้อมูลได้พร้อมๆ กัน
- Switch ทำหน้าที่แตก collision domain ใหญ่ๆ ออกเป็น collision domain ที่เล็กลง
- ควรใช้ switch แทน Hub ใน Ethernet LAN network

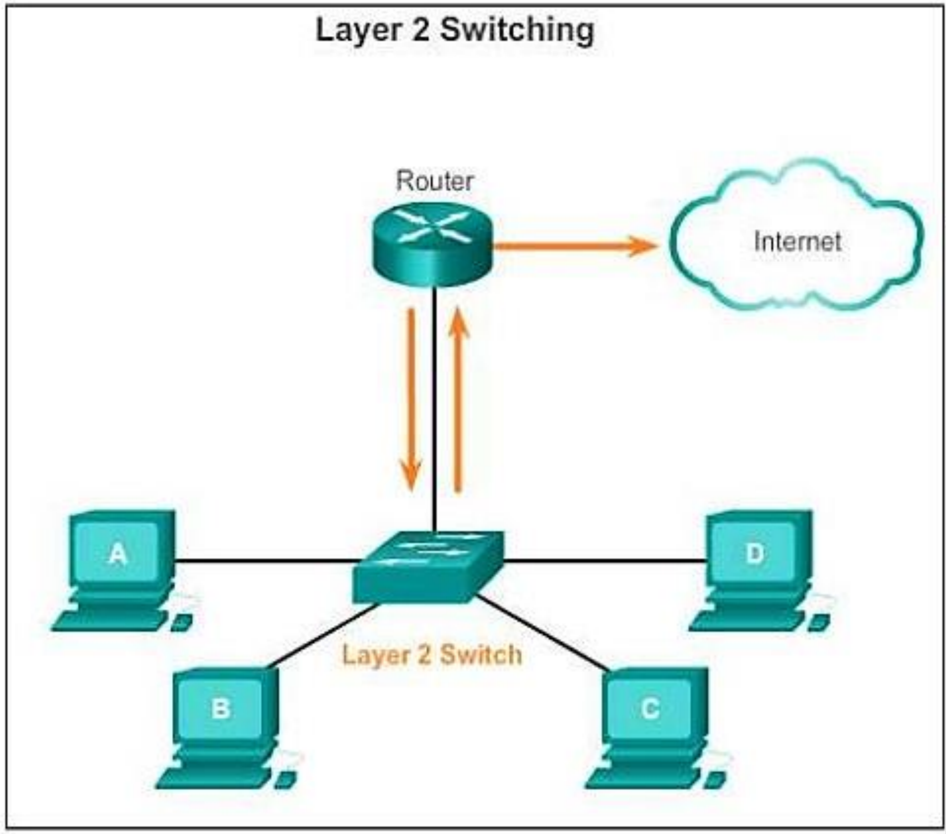


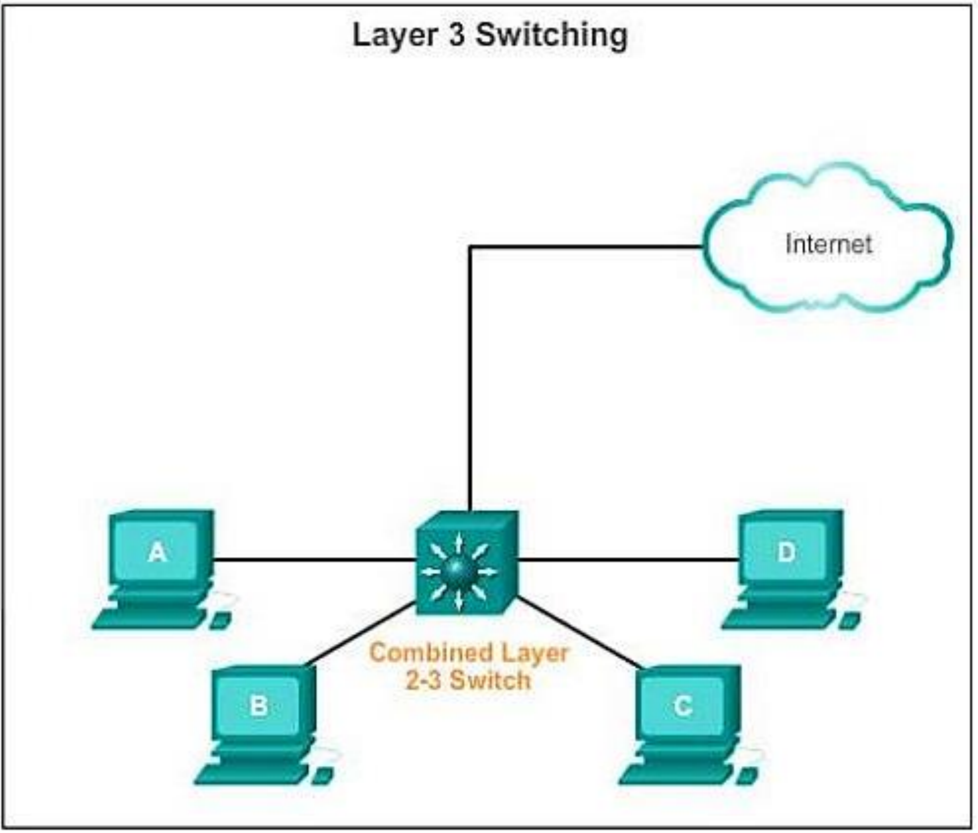
Layer 3 Switch

- สามารถทำงานได้ในทั้งระดับของ layer 2 และ layer 3
- ถ้าเป็นการส่งข้อมูลกันในระดับ layer 2 จะคงพิจารณา MAC address เหมือนเดิม แต่ถ้าเป็นการติดต่อกันในระดับ layer 3 switch จะพิจารณา ip address เป็นหลัก
- ข้อมูล ที่ layer 3 switch จะส่งต่อออกมานั้น ถ้ามันทำงานในระดับของ layer 2 ก็จะส่งข้อมูลออกมาเป็น frame แต่ถ้าทำงานในระดับ layer 3 นั้นจะส่งผ่านข้อมูลเป็นลักษณะของpacket
- layer 3 switch มีความสามารถด้านการจัดการเส้นทางส่งข้อมูลไปปลายทาง (route) และใช้ routing protocol ได้ เหมือนกับพวก router ด้วย (แต่จะต่างกับ router คือ ไม่กันการส่ง broad cast ข้ามเครือข่าย)



Layer 2 vs. Layer 3 Switching





ALERT
ADAPT
ACHIEVE

Address Learning

- ขั้นตอนการส่ง frame เมื่อเปิด switch ใหม่

Learning

เรียนรู้และจับคู่ MAC ต้นทางกับ interface จาก frame ที่เข้ามา

Flooding

ส่ง frame ออกไปยังทุก port ยกเว้น port ต้นทาง โดยใช้วิธี

- Unknown Unicast

- Multicast

- Broadcast

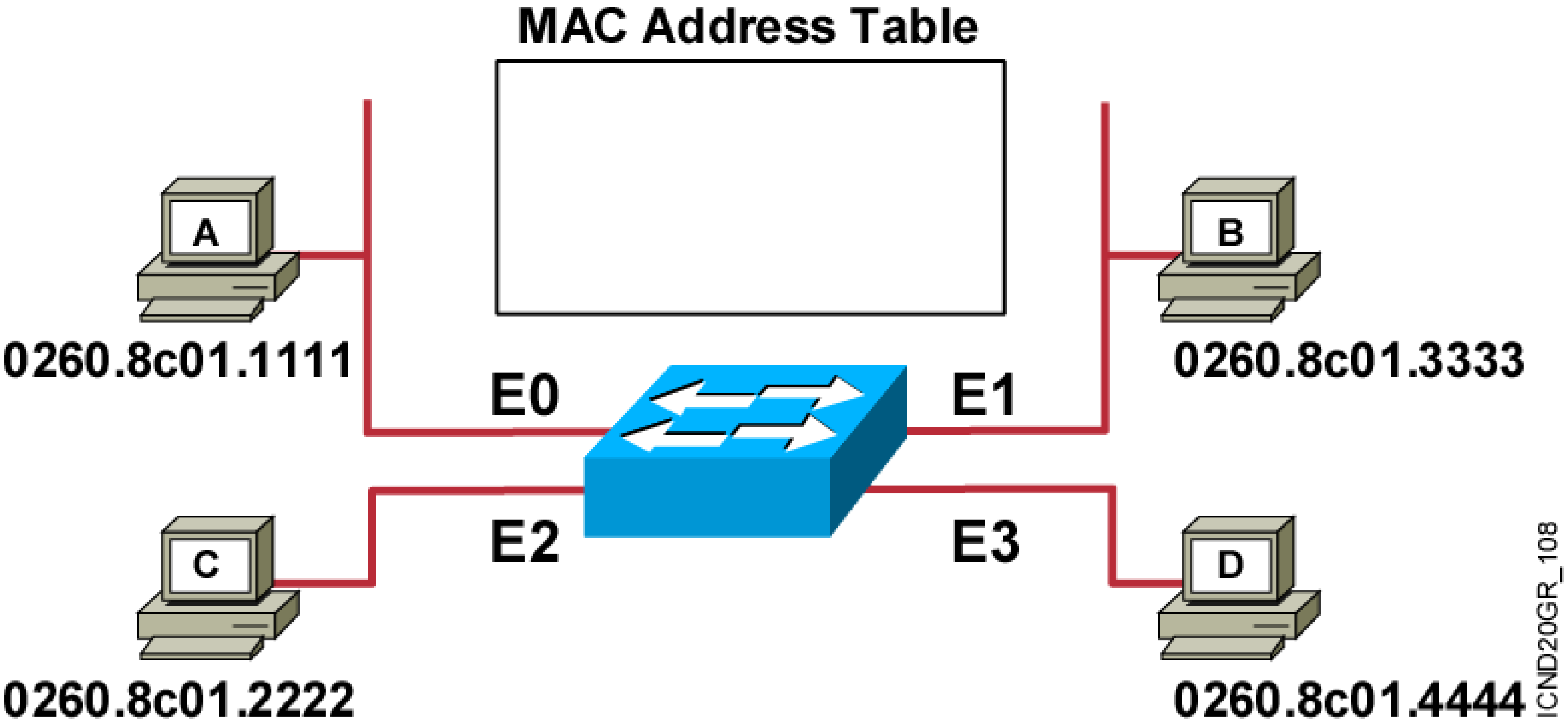
Forwarding/Filtering

- Forwarding : ส่ง frame ที่พบ Des MAC ในฐานข้อมูลออกไปเฉพาะ port ที่จับคู่ไว้

- Filtering : กั้นการส่ง frame ออกใน port อื่นที่ไม่ได้ถูกจับคู่กับ Des MAC นั้น

ALERT
ADAPT
ACHIEVE

MAC Address Table



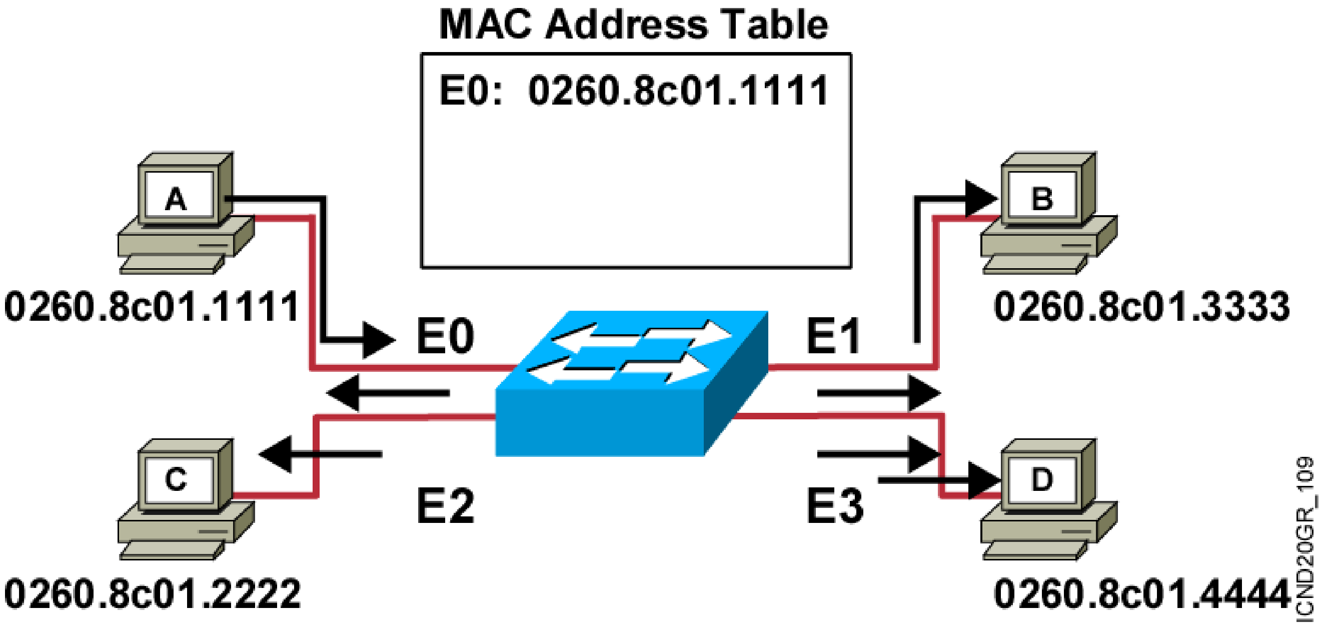
- **Initial MAC address table is empty.**

เริ่มแรก ตาราง MAC Address จะยังคงไม่มีข้อมูล

SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

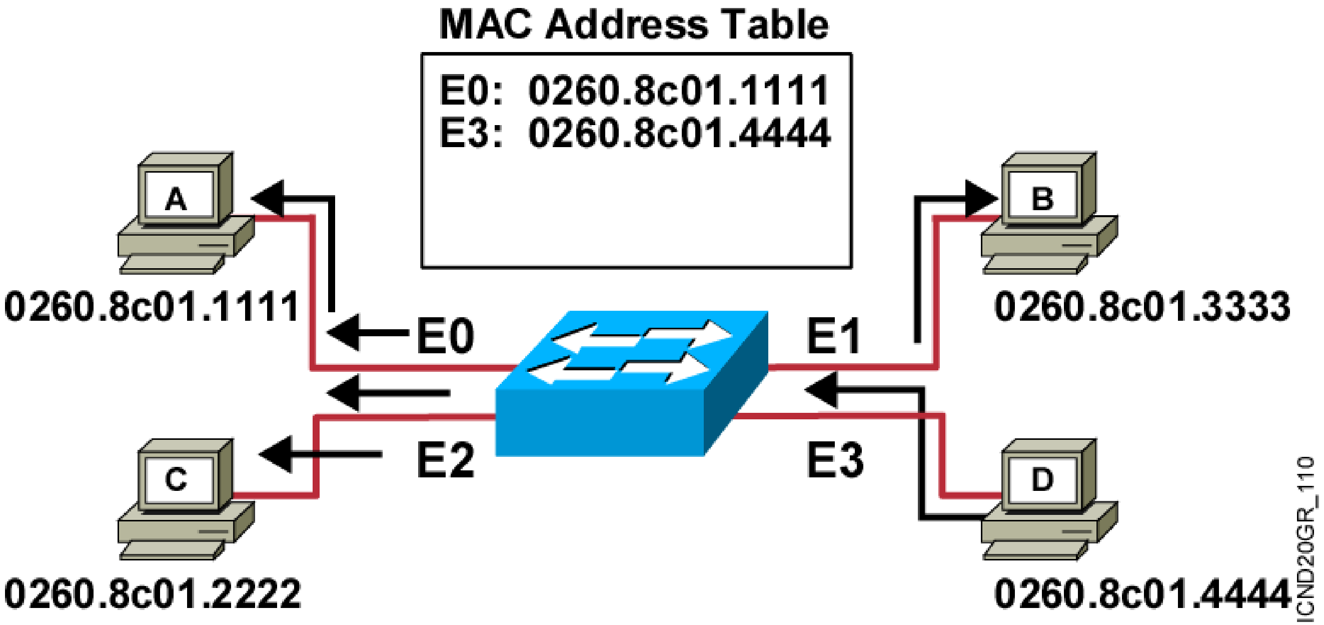
Learning Addresses



- Station A sends a frame to station C. สถานี A ส่ง frame ข้อมูล ให้ C
- Switch caches the MAC address of station A to port E0 by learning the source address of data frames. Switch เรียนรู้ที่อยู่ต้นทางจาก frame และบันทึก MAC ของ A ยัง port E0
- The frame from station A to station C is flooded out to all ports except port E0 (unknown unicasts are flooded). Frame จาก A ถูกกระจายไปยังทุก port ยกเว้น E0 เพื่อให้ไป C

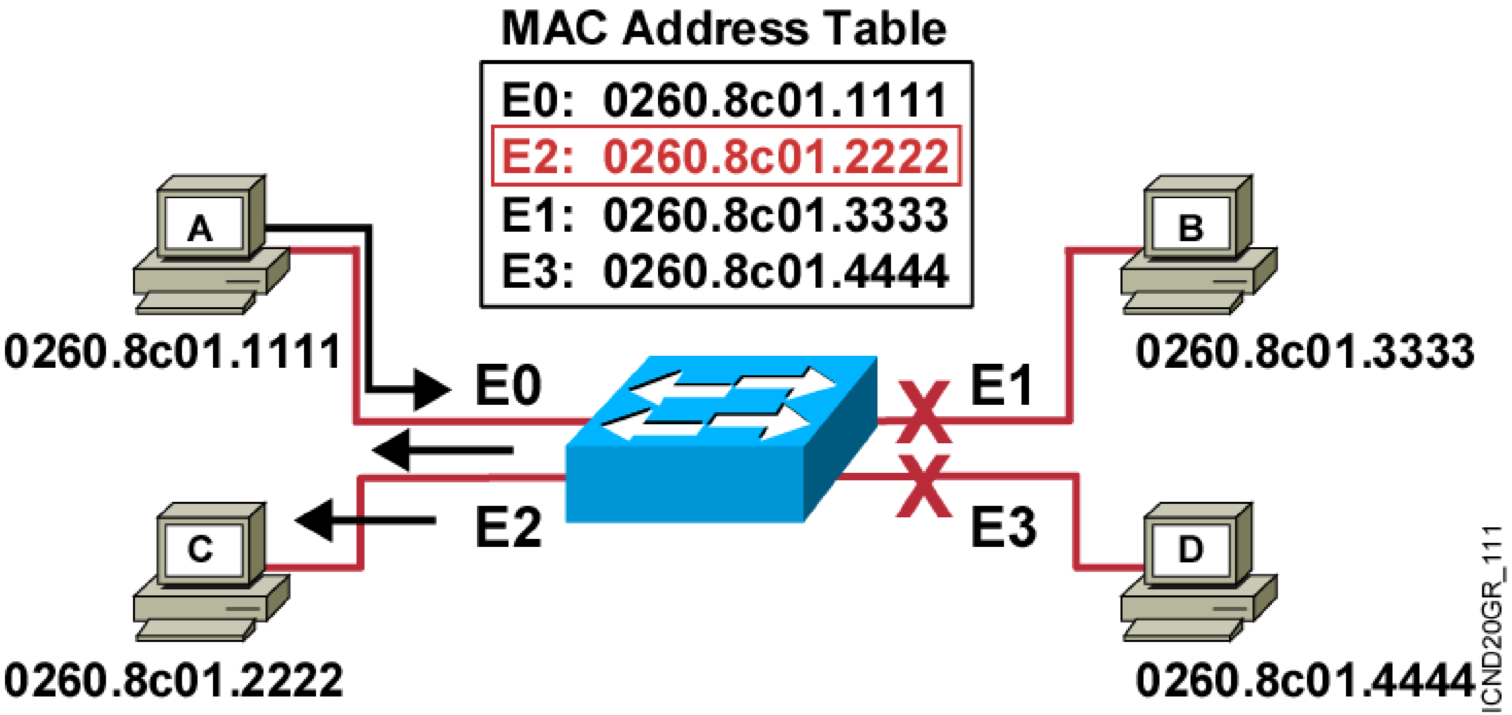
SAMART
TELCOMS

Learning Addresses (Cont.)



- Station D sends a frame to station C. สถานี D ส่ง frame ข้อมูลไปยัง C
- Switch caches the MAC address of station D to port E3 by learning the source address of data frames. Switch เรียนรู้ที่อยู่ต้นทางจาก frame และบันทึก MAC ของ D ยัง port E3
- The frame from station D to station C is flooded out to all ports except port E3 (unknown unicasts are flooded). Frame จาก D ถูกกระจายไปยังทุก port ยกเว้น E3 เพื่อให้ไป C

Filtering Frames

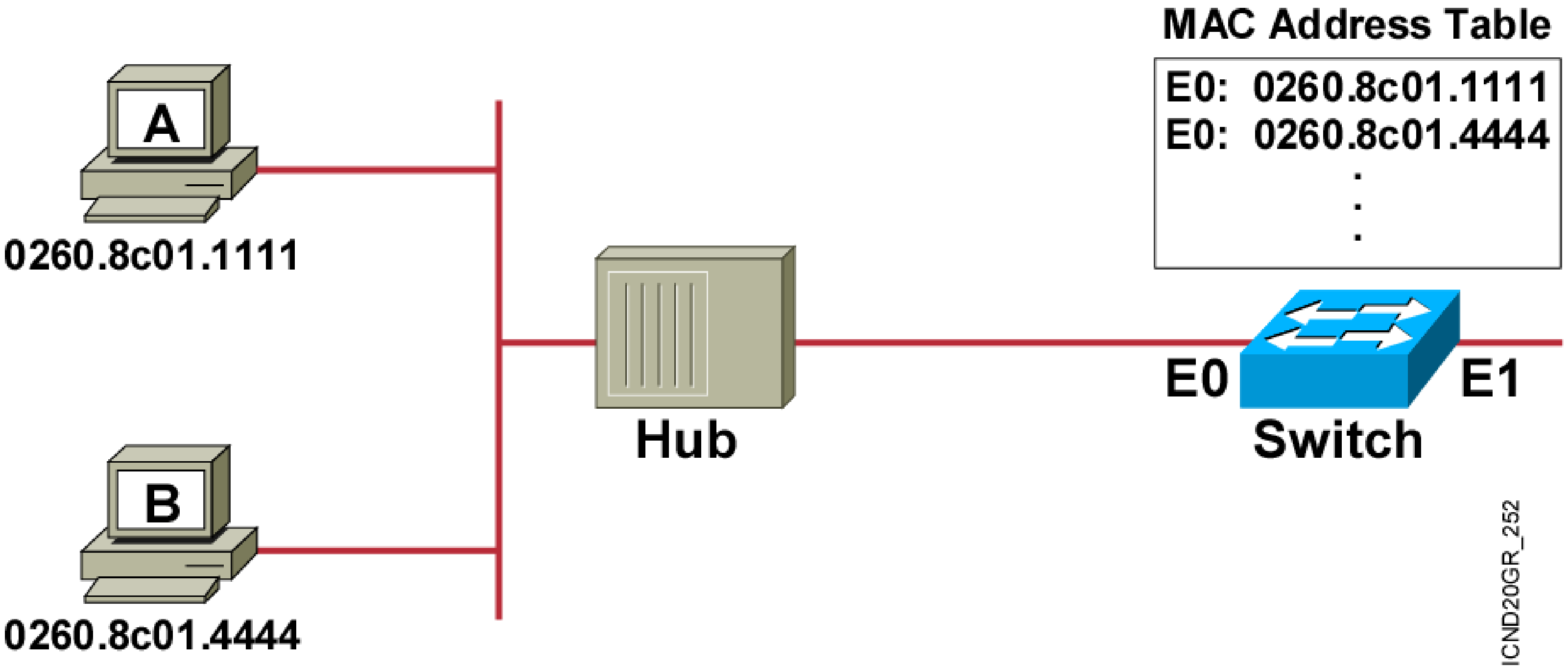


MAC Address Table

E0:	0260.8c01.1111
E2:	0260.8c01.2222
E1:	0260.8c01.3333
E3:	0260.8c01.4444

- Station A sends a frame to station C. สถานี A ส่ง frame ข้อมูล ไปยังสถานี C
- Destination is known; frame is not flooded. รู้ปลายทางแล้ว frame จะไม่ถูกกระจายอีกต่อไป

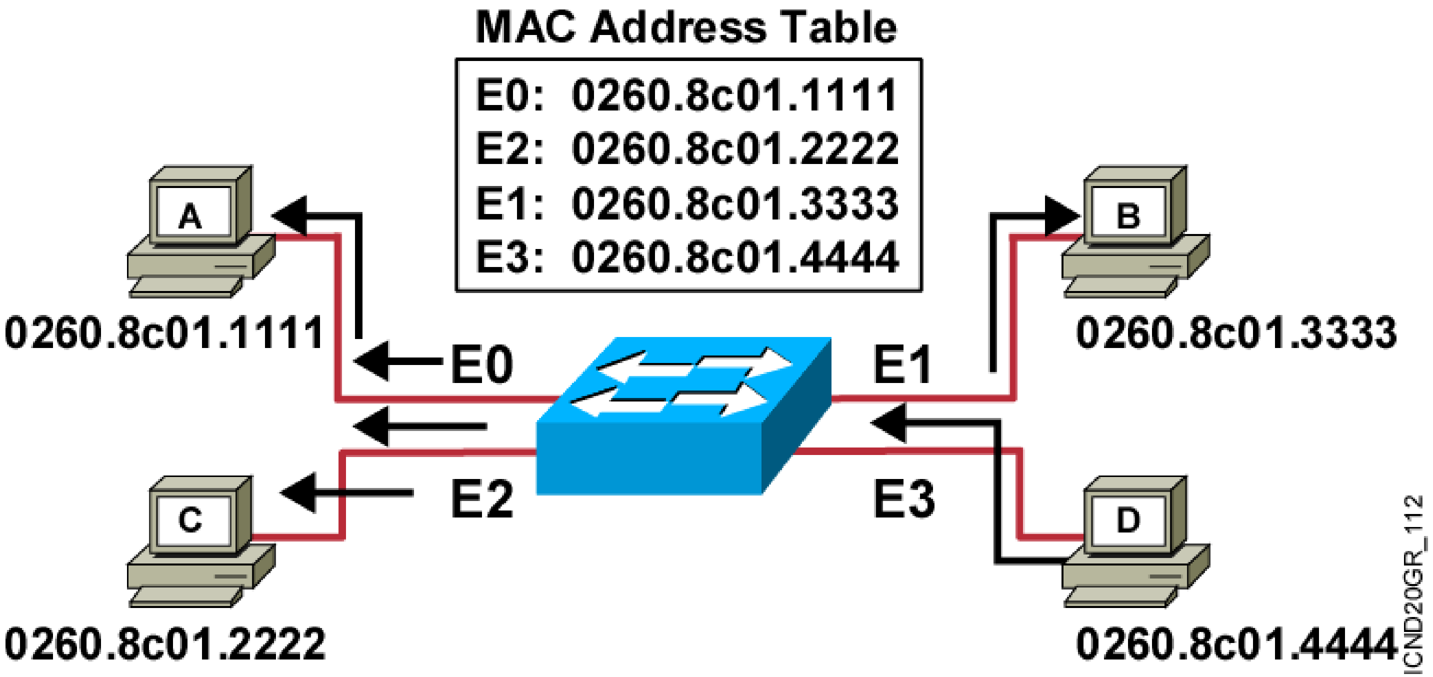
Filtering Frames (cont.)



- Station A sends a frame to station B. สถานี A ส่ง frame ข้อมูลไปสถานี B
- The switch has the address for station B in the MAC address table.

  switch มีที่อยู่ของสถานี B แล้ว ในตาราง MAC Address

Broadcast and Multicast Frames



MAC Address Table

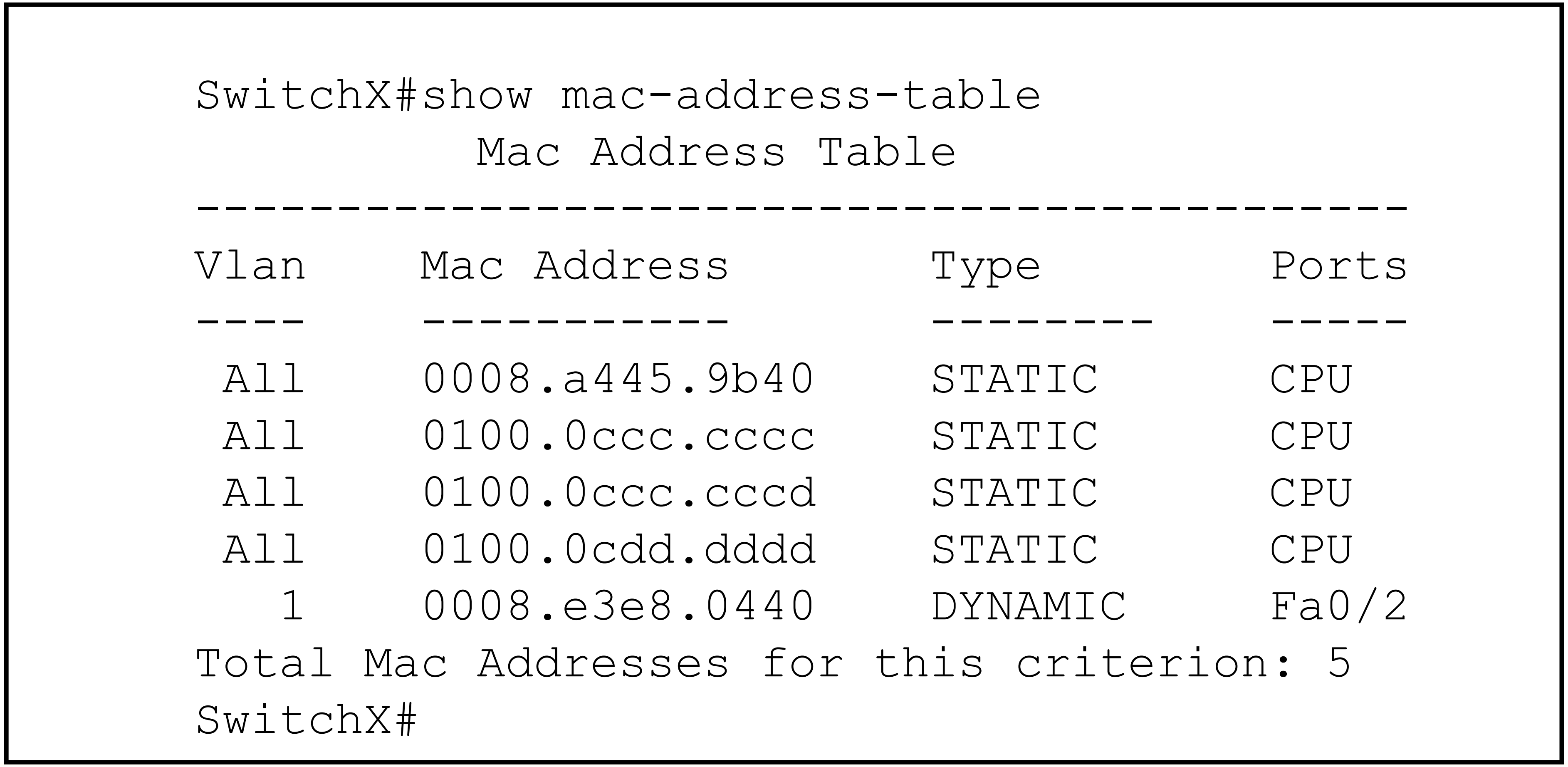
E0: 0260.8c01.1111
E2: 0260.8c01.2222
E1: 0260.8c01.3333
E3: 0260.8c01.4444

- Station D sends a broadcast or multicast frame.
- Broadcast and multicast frames are flooded to all ports other than the originating port.

Broadcast frame และ multicast frame จะถูกกระจายไปยังทุก ports อื่นๆ นอกจาก port ที่เป็นต้นทาง

Managing the MAC Address Table

Catalyst 2960 Series

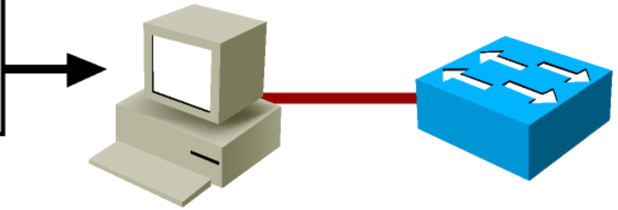


```
SwitchX#show mac-address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0008.a445.9b40    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0008.e3e8.0440    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 5
SwitchX#
```

Configuring a Switch Password

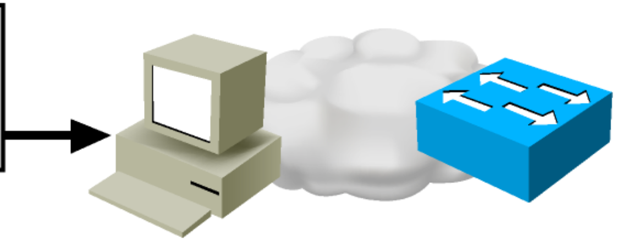
Console Password

```
SwitchX(config)#line console 0
SwitchX(config-line)#login
SwitchX(config-line)#password cisco
```



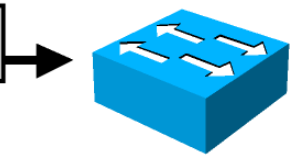
Virtual Terminal Password

```
SwitchX(config)#line vty 0 4
SwitchX(config-line)#login
SwitchX(config-line)#password sanjose
```



Enable Password

```
SwitchX(config)#enable password cisco
```



Secret Password

```
SwitchX(config)#enable secret sanfran
```

Service Password-Encryption Commands

```
SwitchX(config)#service password-encryption
SwitchX(config)#no service password-encryption
```

301P_256

Configuring SSH

- การ access เข้าไปที่ Router หรือ Switch ด้วยการ Telnet ถือว่าไม่มีความปลอดภัย ดังนั้นควรจะ access โดยการใช้ SSH ซึ่งจะมีความปลอดภัยมากกว่า เพราะจะมีการเข้ารหัส หรือ encryption

```
Switch(config)#username admin privilege 15 password cisco
Switch(config)#ip domain-name ninehua.com
Switch(config)#crypto key generate rsa
#768
Switch(config)#ip ssh version 2
Switch(config)#line vty 0 4
Switch(config-line)#login local
```

Implementing VLANs and Trunks

Medium-Sized Switched Network Construction

ALERT
ADAPT
ACHIEVE

Issues in a Poorly Designed Network

- Unbounded failure domains

ขาดการจำกัดขอบเขตของการเสียหาย

- Large broadcast domains

Broadcast domain ใหญ่

- Large amount of unknown MAC unicast traffic

MAC Unicast traffic จำนวนมากที่ไม่รู้ที่มา

- Unbounded multicast traffic

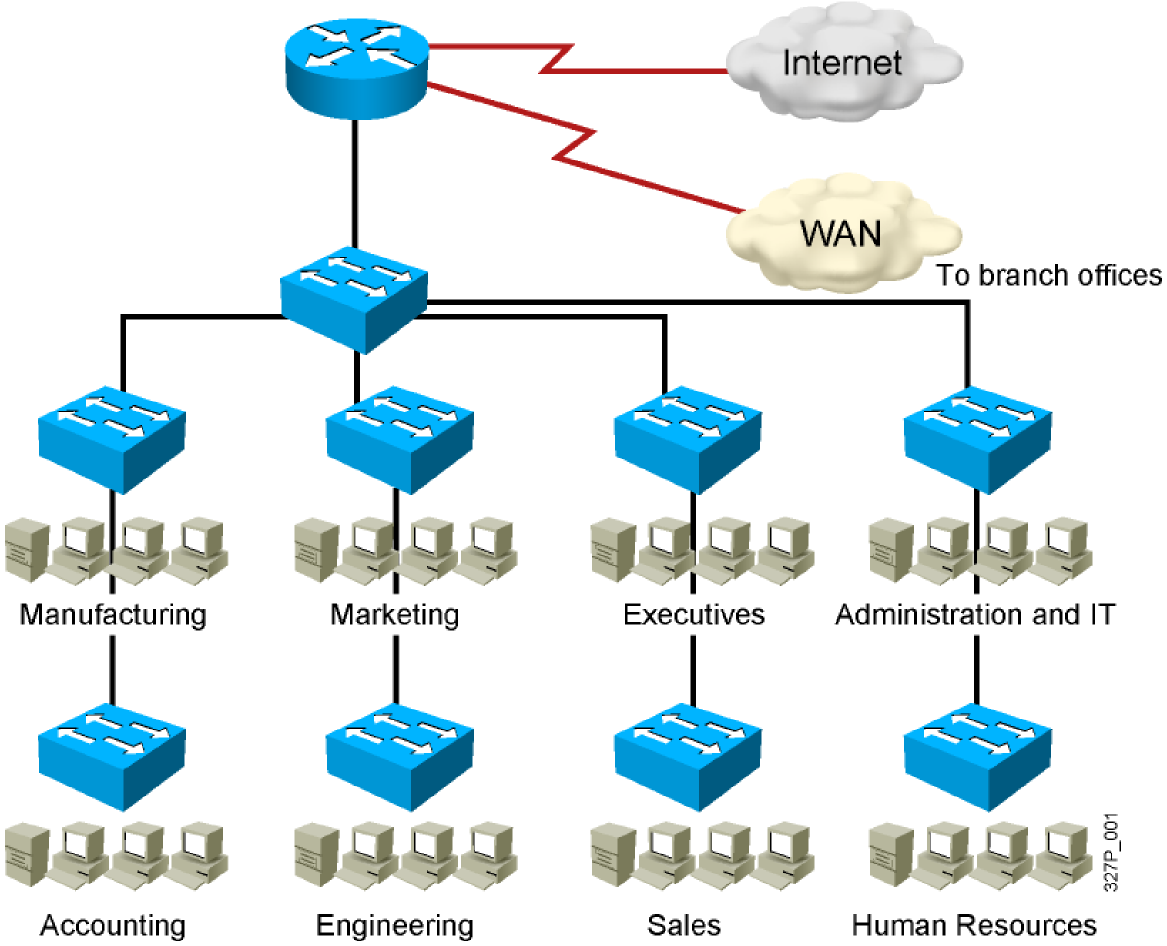
ขาดการจำกัดขอบเขตของ multicast traffic

- Management and support challenges

การบริหารจัดการและสนับสนุนการใช้งานทำได้ยาก

- Possible security vulnerabilities

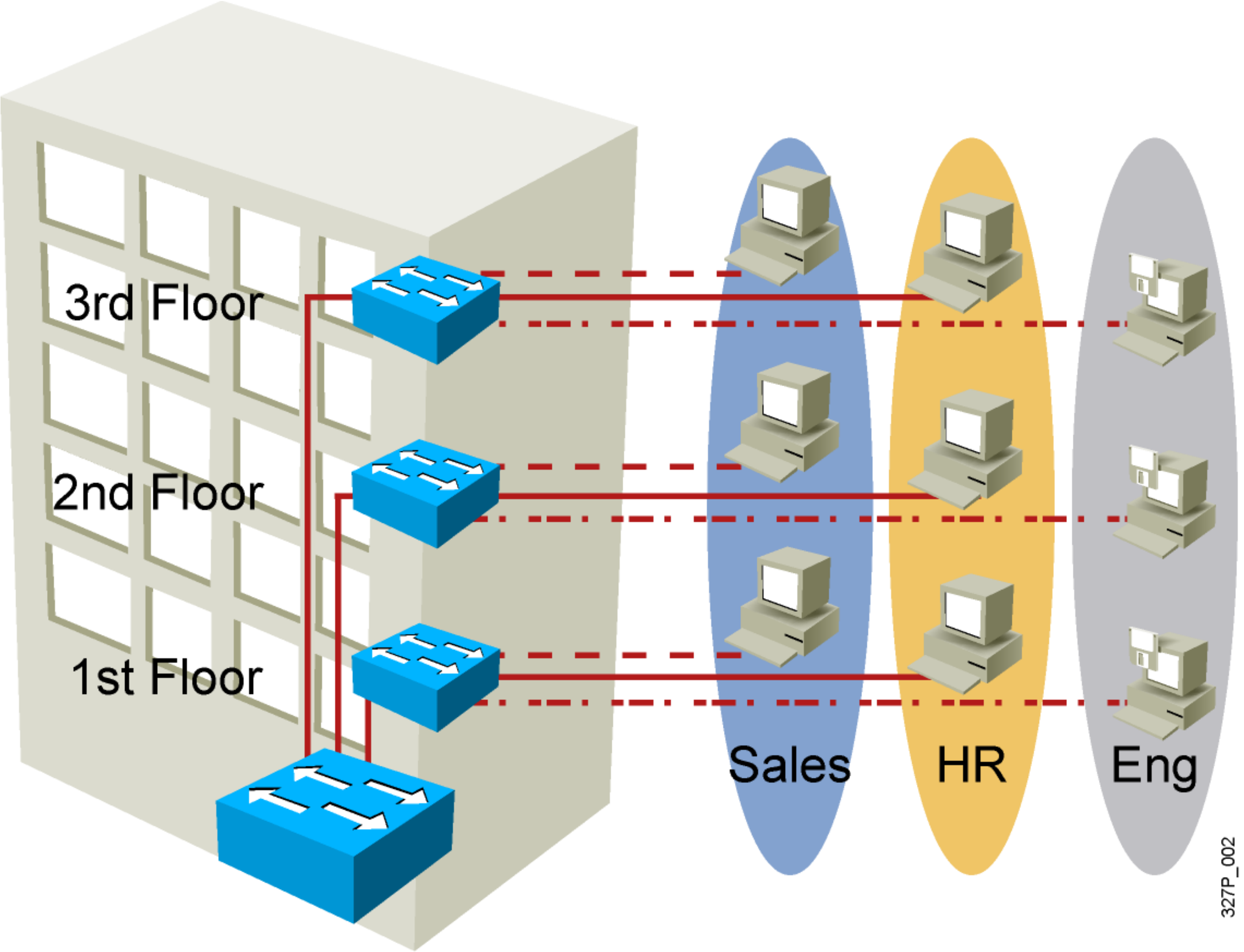
อาจเกิดช่องโหว่ในการรักษาความมั่นคงปลอดภัยเครือข่าย



SAMART TELCOMS

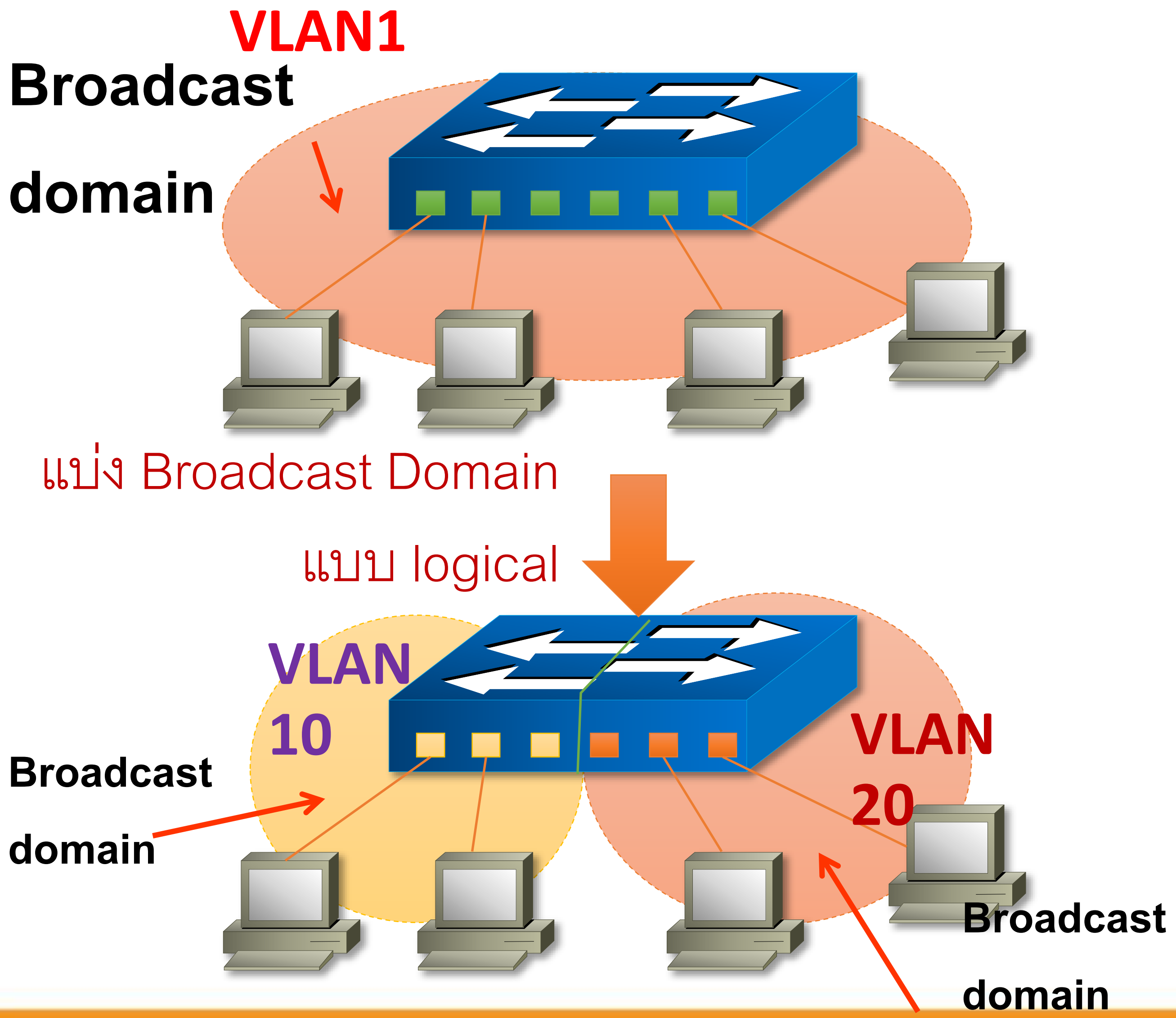
VLAN Overview – Virtual LAN

- Segmentation
- Flexibility
- Security



VLAN = Broadcast Domain = Logical Network (Subnet)

VLAN



- VLAN คือ การแบ่งกลุ่มการใช้งานของ switch เชิง logical โดยการสร้าง VLAN ล้วนำ interface แบ่งเข้าไปเป็นสมาชิกในแต่ละ VLAN
- เครื่องภายใต้ VLAN เดียวกัน ติดต่อสื่อสารกันได้
- ติดต่อข้าม VLAN ต้องใช้อุปกรณ์ Layer 3 เข้ามา route ระหว่าง VLAN
- ถ้า switch ไม่แบ่ง VLAN = ทุก port อยู่ใน VLAN 1 เดียวกัน โดย default

VLAN Benefits

- **ใช้ Bandwidth คุ้มค่าขึ้น**

  ลดจำนวน broadcast traffics ที่เป็นสาเหตุของปัญหาความคับคั่งภายในเครือข่าย รวมทั้งยังมีผลทำให้อุปกรณ์ต้องใช้ทรัพยากรในการประมวลผลสูงขึ้นโดยไม่จำเป็น

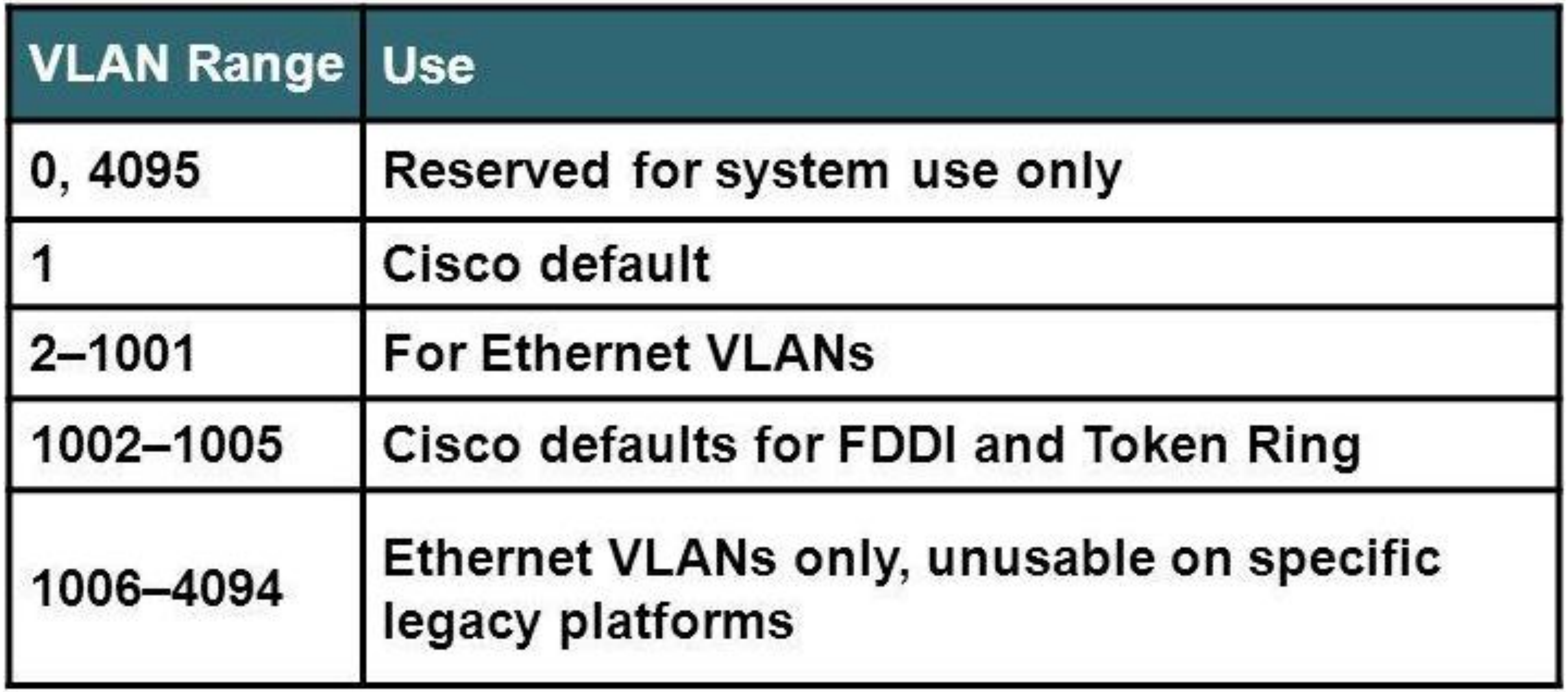
- **เพิ่มความปลอดภัย**

  จำกัดการเข้าถึงข้าม VLAN ด้วย feature layer 3 เช่น ACL (Access Control List) จะช่วยจำกัดข้อมูลให้อยู่ในวงที่เหมาะสม เช่น จำกัดการเข้าถึง server การจำกัดวงข้อมูลของแผนกหนึ่งจากแผนกอื่นที่ไม่เกี่ยวข้อง ลดความเสี่ยงการโดนโจมตีแบบ spoofing (หลอกเหยื่อให้ไปปลายทางผิดเพื่อขโมยข้อมูล/ข้อมูลไม่ถึงปลายทาง)

- **มีความยืดหยุ่นในการใช้งาน**

  สามารถขยายเครือข่าย หรือ ย้าย VLAN ได้ง่าย โดยใช้การตั้งค่า แทนการย้ายสาย รองรับการปรับเปลี่ยนโครงสร้างองค์กร

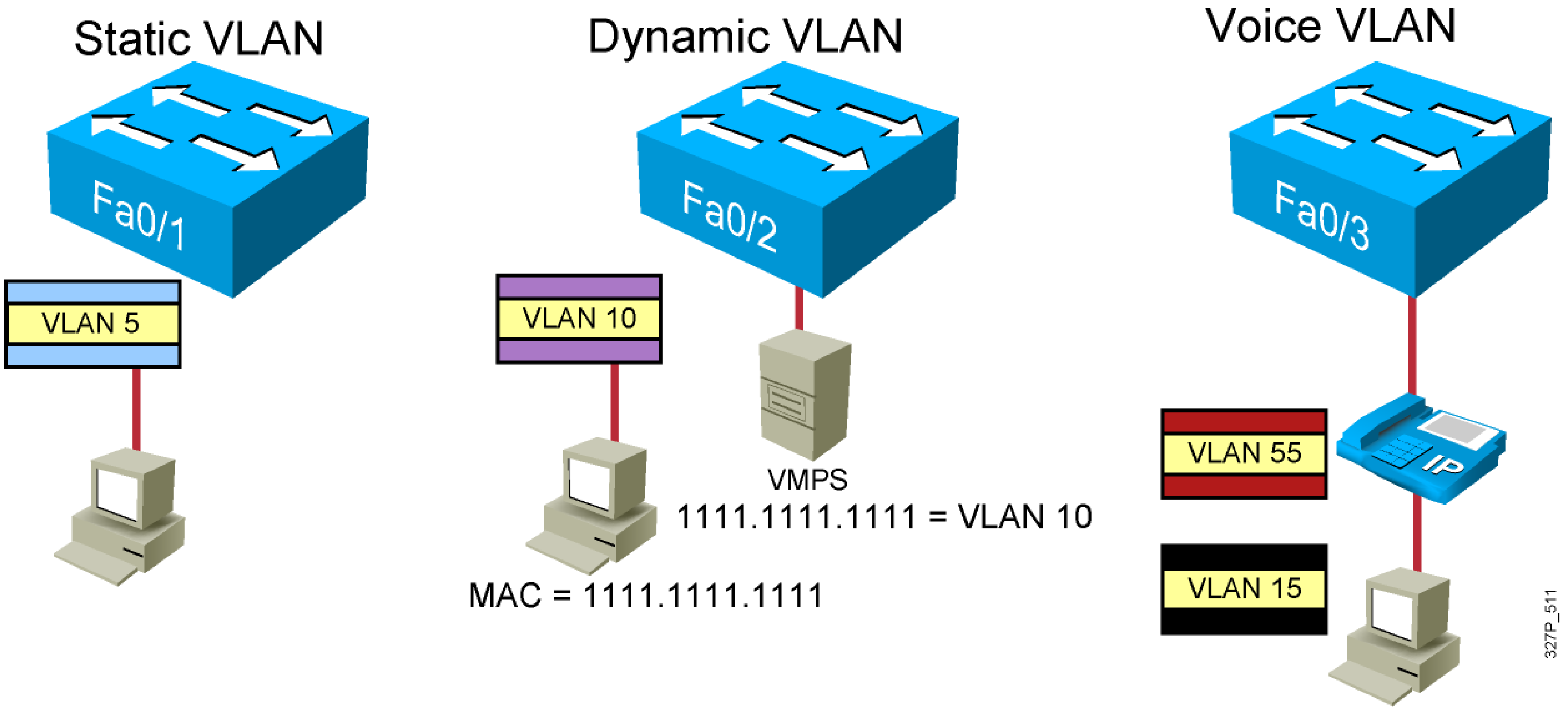
VLAN Range



VLAN Range	Use
0, 4095	Reserved for system use only
1	Cisco default
2–1001	For Ethernet VLANs
1002–1005	Cisco defaults for FDDI and Token Ring
1006–4094	Ethernet VLANs only, unusable on specific legacy platforms

ALERT
ADAPT
ACHIEVE

VLAN Membership Modes



SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

VLAN Configuration

- สร้าง VLAN

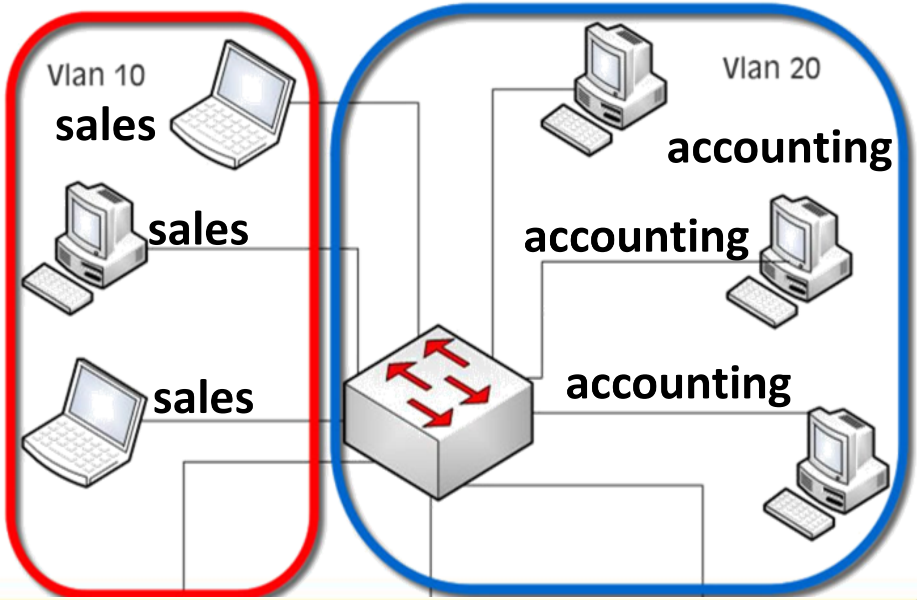
```
Switch(config)#vlan [vlan-id]
```

- กำหนดชื่อ VLAN

```
Switch(config-vlan)#name [vlan's name]
```

ตัวอย่าง

```
Switch# configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name sales
Switch(config-vlan)# end
```

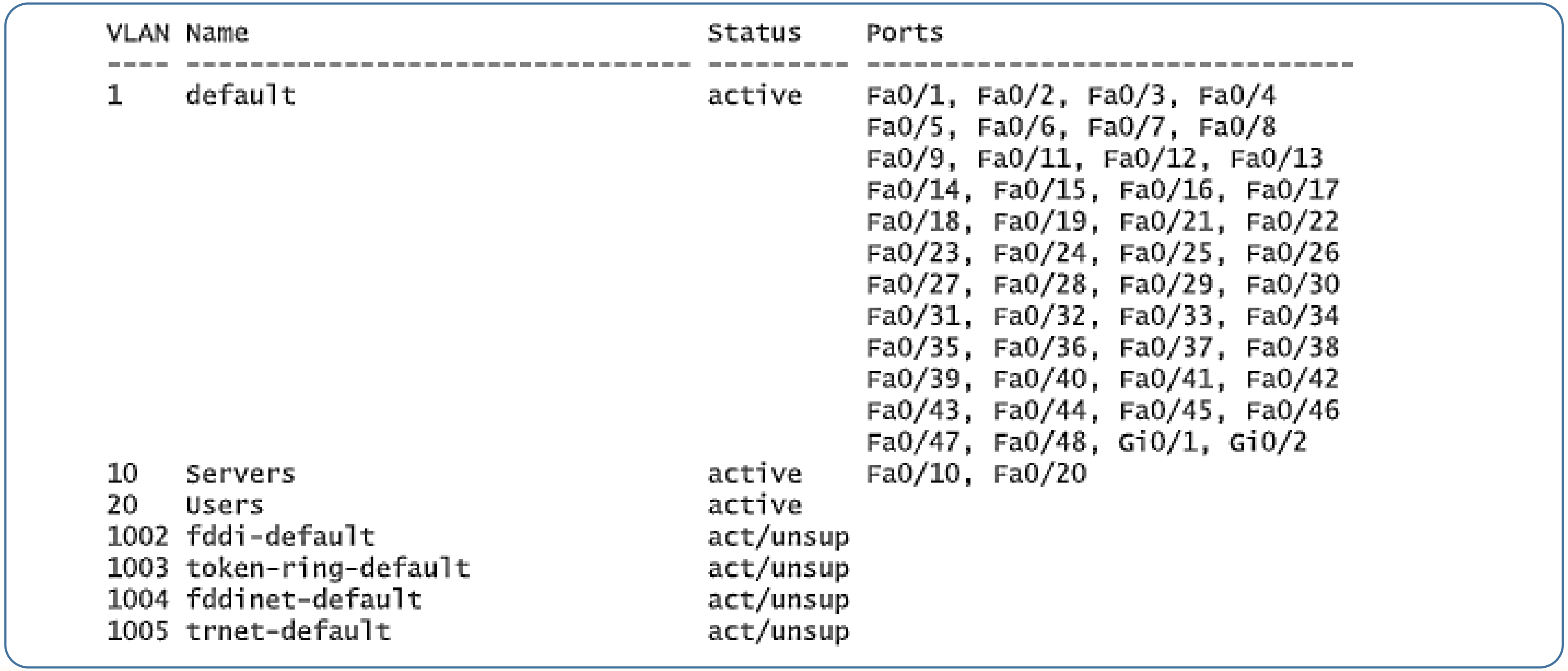


SAMART TELCOMS

VLAN Configuration

- **Verify VLAN**

```
Switch #show vlan brief
```



```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Fa0/25, Fa0/26
                                                Fa0/27, Fa0/28, Fa0/29, Fa0/30
                                                Fa0/31, Fa0/32, Fa0/33, Fa0/34
                                                Fa0/35, Fa0/36, Fa0/37, Fa0/38
                                                Fa0/39, Fa0/40, Fa0/41, Fa0/42
                                                Fa0/43, Fa0/44, Fa0/45, Fa0/46
                                                Fa0/47, Fa0/48, Gi0/1, Gi0/2
10   Servers                          active    Fa0/10, Fa0/20
20   Users                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

VLAN Database

- ในการสร้าง VLAN ขึ้นมา ข้อมูลของ VLAN จะไม่ได้เก็บใน RAM เหมือนการตั้งค่าทั่วไป แต่จะเก็บอยู่บนหน่วยความจำ flash ชื่อว่า VLAN.DAT

```
Switch# dir flash:
Directory of flash:/
1 -rw-     3058048        Mar 01 2015 04:12:16     c3550-i5k2l2q3-mz.121-13.EA1a.bin
2 -rw-     736            Mar 01 2015 04:12:16     vlan.dat
```

- ถ้าต้องการลบ VLAN ทั้งหมดทิ้ง จะต้องลบไฟล์ VLAN.DAT บน flash

```
Switch# delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#erase startup-config
<output omitted>
Switch#reload
```

VLAN operation

ในการสร้าง VLAN นั้น port ของ switch นั้นจะทำหน้าที่อยู่ 2 ประเภท คือ Access port และ Trunk port

Access Port

- เป็น Port ที่ทำหน้าที่เชื่อมต่อระหว่าง Client ไปยัง switch ซึ่งเราจะใช้สาย LAN แบบสายตรง (Straight Through) ในการเชื่อมต่อ
- port ที่ถูก set เป็น Access Port นี้จะมี traffic ของ VLAN เพียง VLAN เดียวที่วิ่งผ่านหรือ port นี้จะต่ออยู่กับอุปกรณ์ที่มีค่า MAC address เพียงค่าเดียวนั่นเอง เช่น

- port ที่ set ระหว่าง switch และ Client

- port ที่ set ระหว่าง switch และ Server

- port ที่ set ระหว่าง switch และ Router (มีข้อแม้ว่า Router ที่เชื่อมต่อนั้น จะต้องไม่ใช่ Router ที่ทำหน้าที่ในการ Route Traffic ระหว่าง VLAN)

Access Port Configuration

- ตั้งค่า Access Port

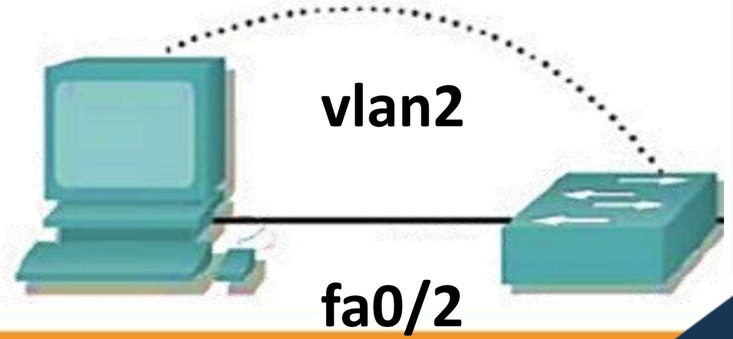
```
Switch (config)# interface [interface module/port]
Switch (config-if)# switchport mode access
```

- นำ port เข้ามาเป็นสมาชิกของ VLAN

```
Switch (config-if)# switchport access vlan [vlan id]
```

- ตัวอย่าง

```
Switch> enable
Switch# configure terminal
Switch (config)# interface fa0/2
Switch (config-if)# switchport mode access
Switch (config-if)# switchport access vlan 2
Switch (config-if)# no shutdown
```



Access Port Configuration

- เราสามารถ manage port หลาย port พร้อมกันได้

port เรียงต่อกัน → range

```
Switch (config)# interface range fa0/2-3
Switch (config-if-range)# switchport mode access
Switch (config-if-range)# switchport access vlan 2
Switch (config-if-range)# no shutdown
```

port ไม่เรียงต่อกัน → range แล้วใช้ลูกน้ำคั่น (,)

```
Switch (config)# interface range fa0/2 , fa0/5 , fa0/10 ,
fa0/20
```

VLAN operation

Trunk Port

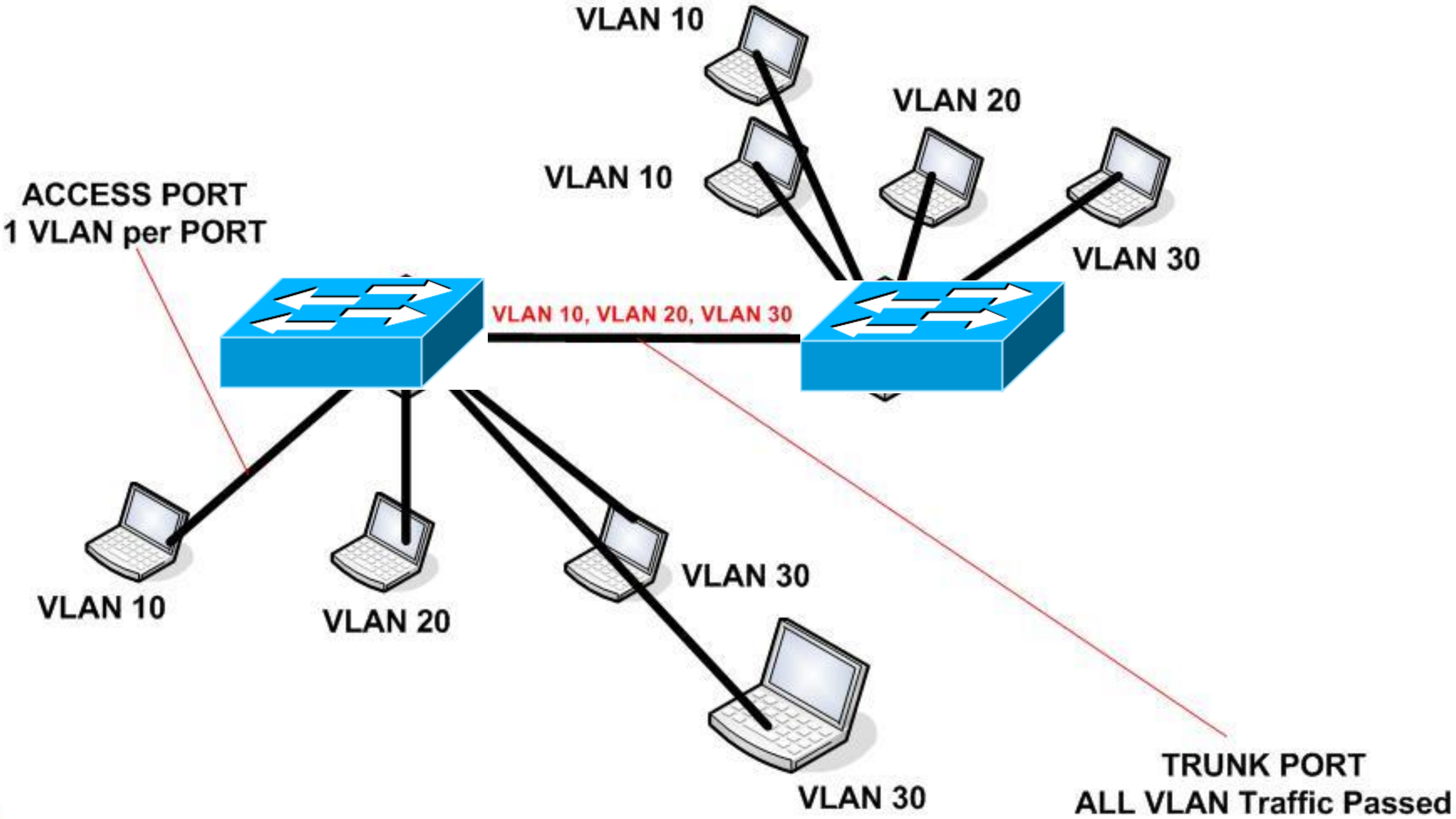
- เป็น port ที่ทำหน้าที่เชื่อมต่อ switch ตัวอื่น ๆ ที่เป็นสมาชิกของ VLAN ต่างๆ ให้มาอยู่ด้วยกัน และทำหน้าที่ส่งผ่าน traffic ซึ่งวิ่งผ่านได้มากกว่า 1 VLAN ให้กระจายไปยัง switch ตัวอื่นๆ ที่มี port ที่ถูกกำหนดให้เป็น VLAN เดียวกันกับ switch ตัวต้นทางได้ หรือ ที่เรียกกันโดยทั่วไปว่า Uplink Port
- Trunk port เป็น port ที่มีค่าหลายๆ ค่าวิ่งผ่าน เช่น VLAN หลายๆ VLAN หรือมีค่า Mac address หลายๆ ค่าวิ่งผ่าน
- ตัวอย่างในการ set port ให้เป็น Trunk port เช่น

  - port ที่ทำหน้าที่ connect ไปยัง switch ตัวอื่น ๆ เช่น Uplink Port

  - port ที่ทำหน้าที่เชื่อม ไปยัง Router ตัวที่ทำหน้าที่ Route Traffic ระหว่าง VLAN

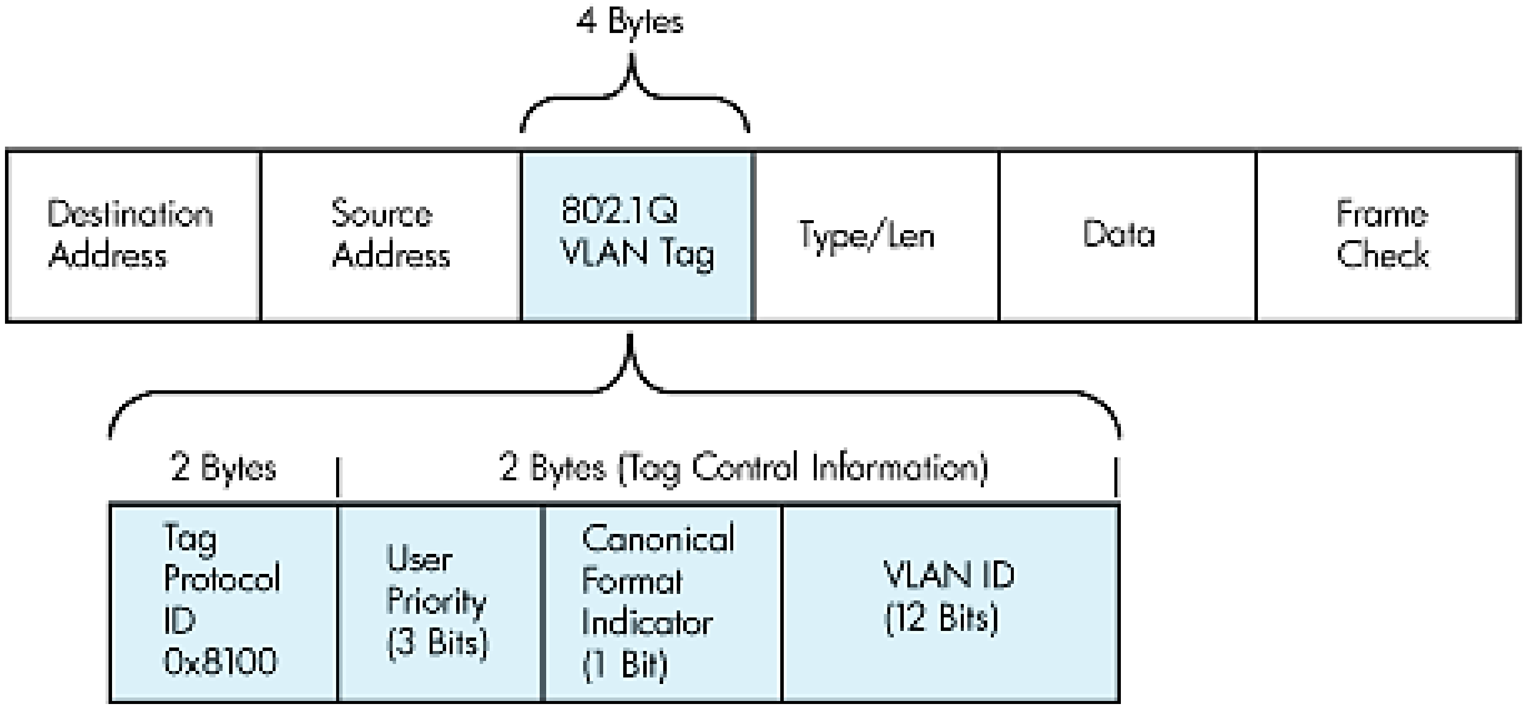
ALERT
ADAPT
ACHIEVE

VLAN operation



SAMART TELCOMS

Encapsulation on Trunk

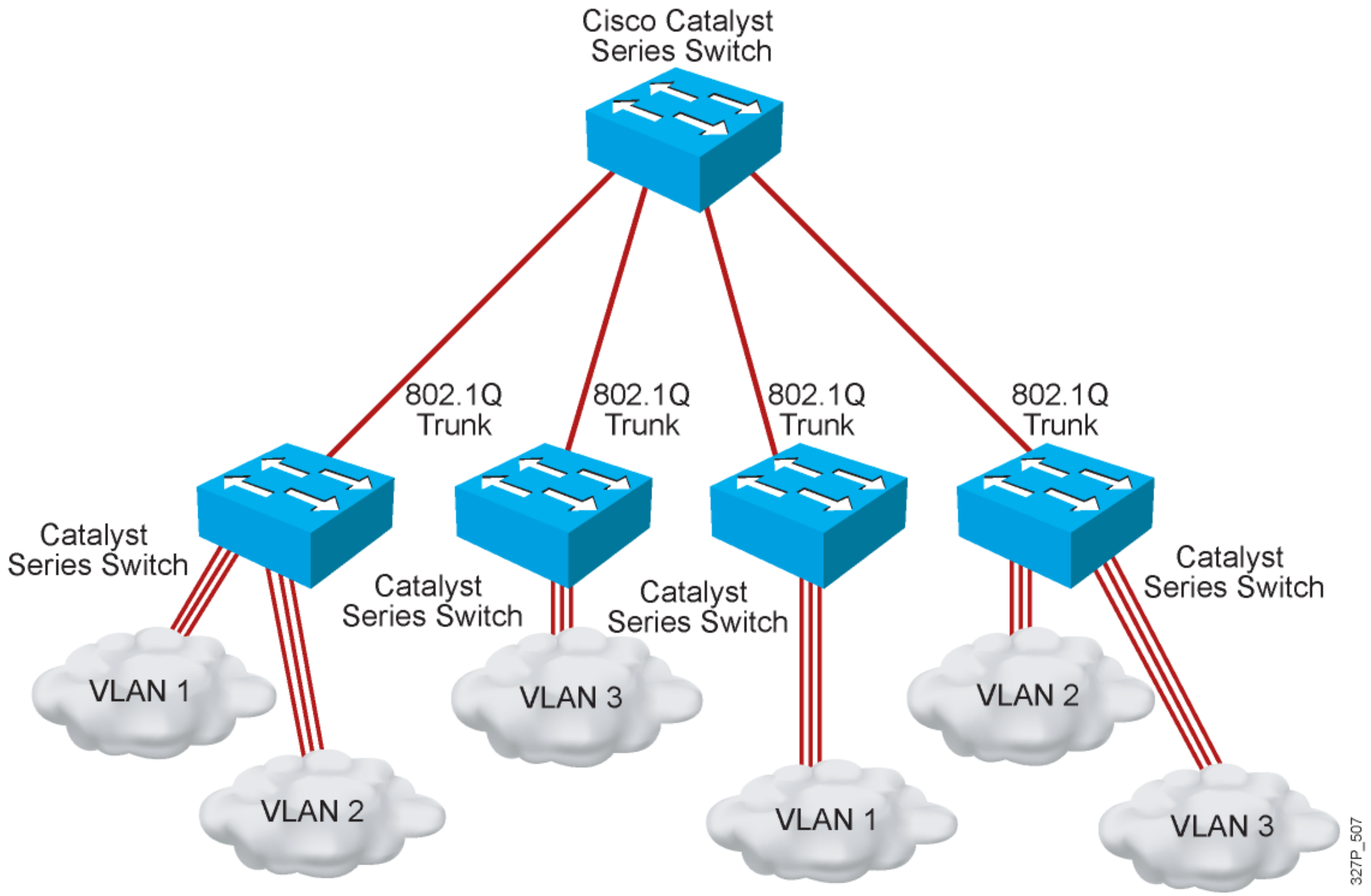


IEEE 802.1Q

- ใช้วิธีเพิ่ม field ขนาด 4 bytes ประกอบด้วย หมายเลข VLAN ขนาด 12 bits เข้าไปประหว่าง Ethernet frame (แบบนี้ไม่มีการ encapsulate Ethernet frame แต่เป็นการแทรก field ลงไป)
- รองรับการทำ native LAN

ALERT
ADAPT
ACHIEVE

802.1Q Trunking



SAMART TELCOMS

Trunk Configuration

- ตั้งค่า Trunk Port

```
Switch (config)# interface [interface module/port]
Switch (config-if)# switchport trunk encapsulation [isl/dot1q]
Switch(config-if)#switchport mode trunk
```

✓ ระบุประเภท encapsulation ก่อนที่จะเปลี่ยนให้อยู่ mode trunk

✓ Switch บางรุ่น ใช้ได้แต่ dot1q เท่านั้น ก็จะไม่ต้องเลือก สามารถใส่คำสั่ง **switchport mode trunk** ได้เลย

- ตัวอย่าง

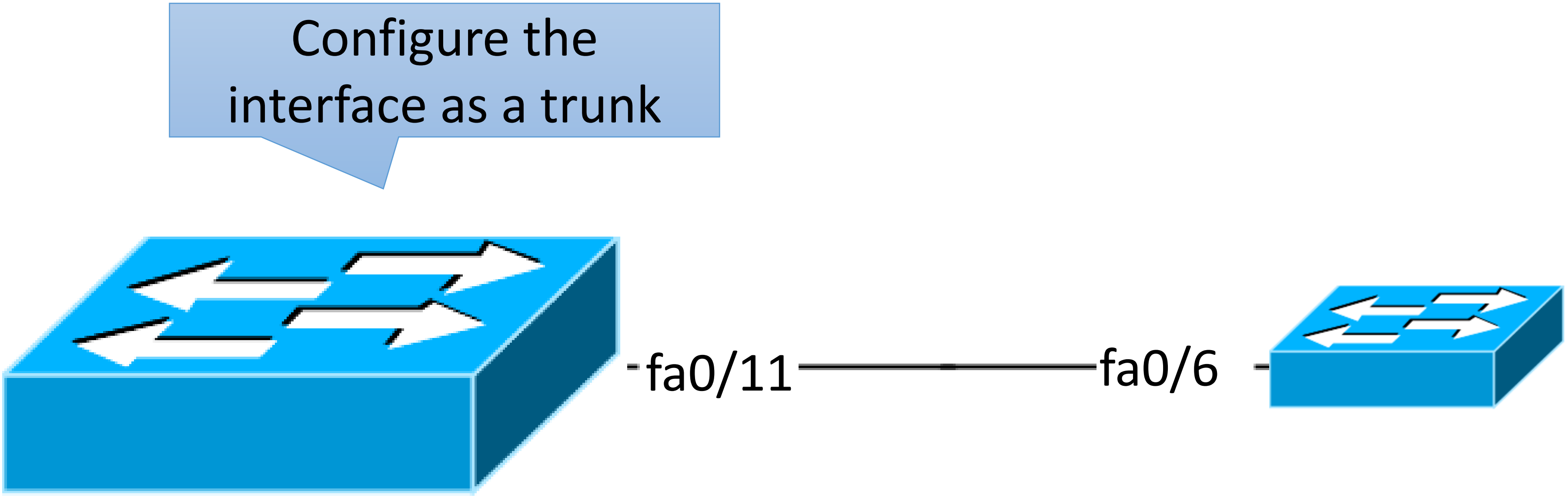
1. ISL

```
Switch(config)#interface Fa 0/1
Switch(config-if)#switchport trunk encapsulation isl
Switch(config-if)#switchport mode trunk
```

2. 802.1q

```
Switch(config)#interface Fa 0/1
Switch(config-if)#switchport trunk encapsulation 802.1q
Switch(config-if)#switchport mode trunk
```

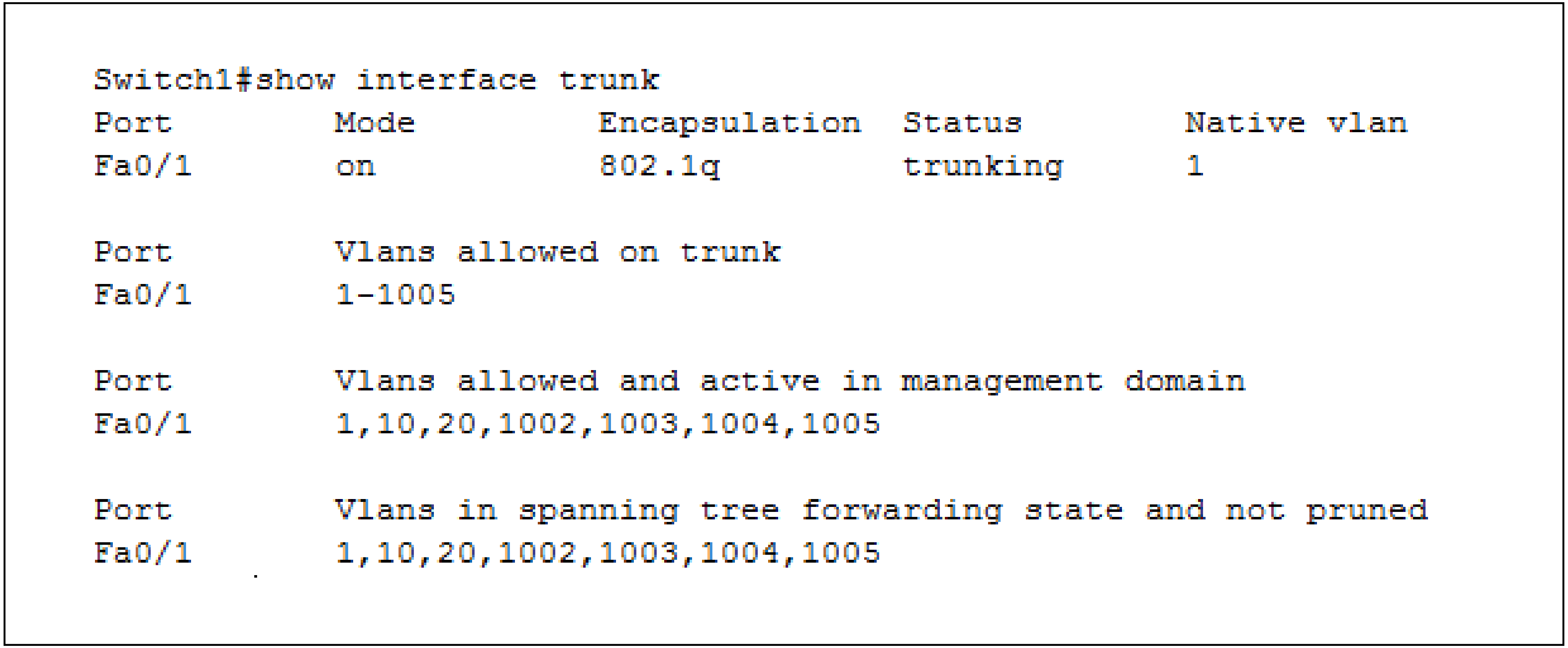
Trunk Configuration


Configure the interface as a trunk

```
SW1(config)# interface fa0/11
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allow vlan 10,20
SW1(config-if)#switchport trunk native vlan 99
```

- **VLAN 1 = default native VLAN**

Trunk Verification



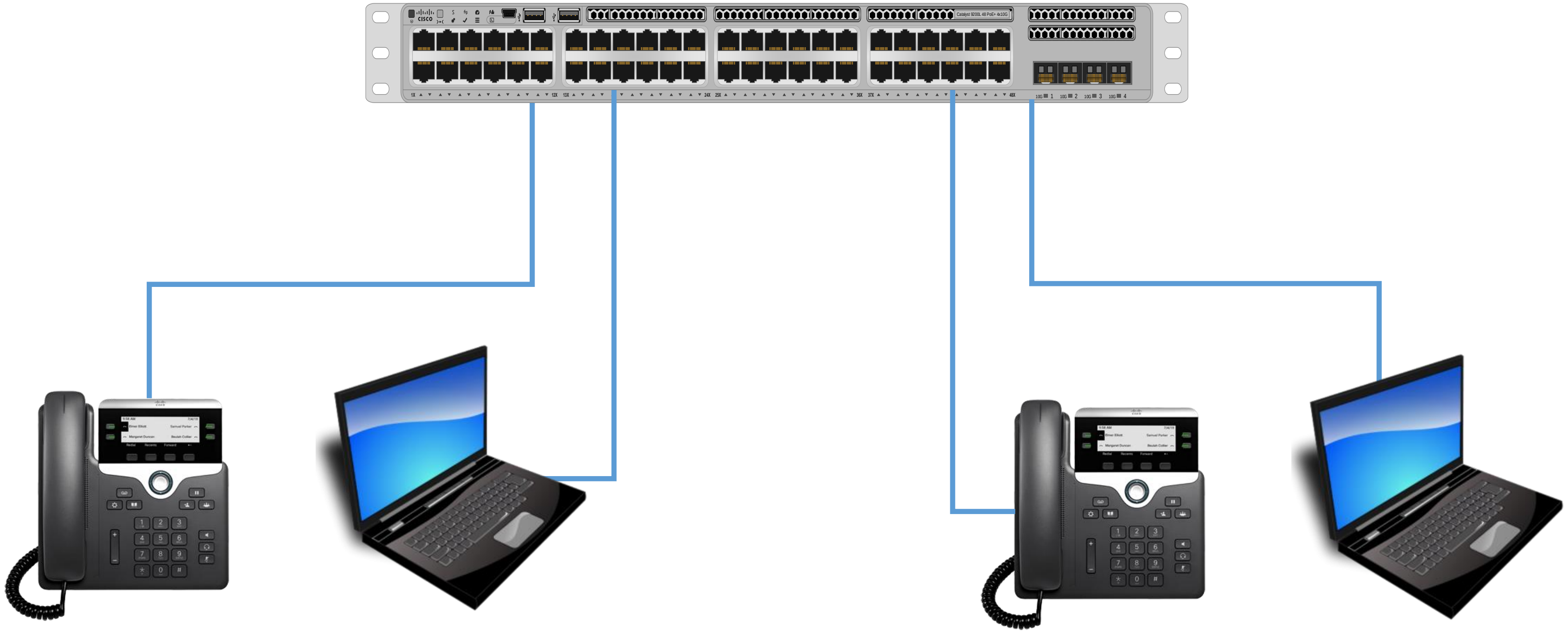
```
Switch1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,1002,1003,1004,1005

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,1002,1003,1004,1005
```

ALERT
ADAPT
ACHIEVE

Voice VLAN

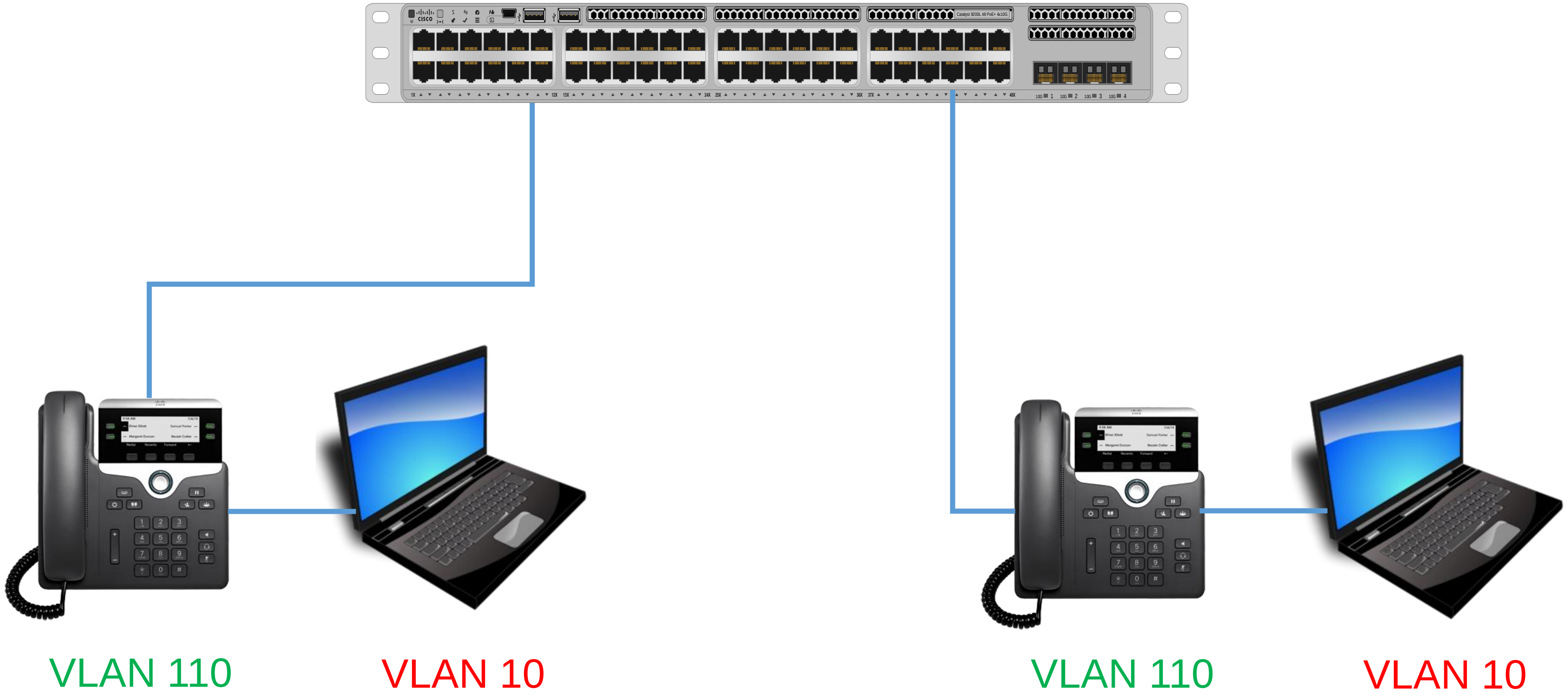
SAMART TELCOMS

Physical Diagram Non-Voice VLAN



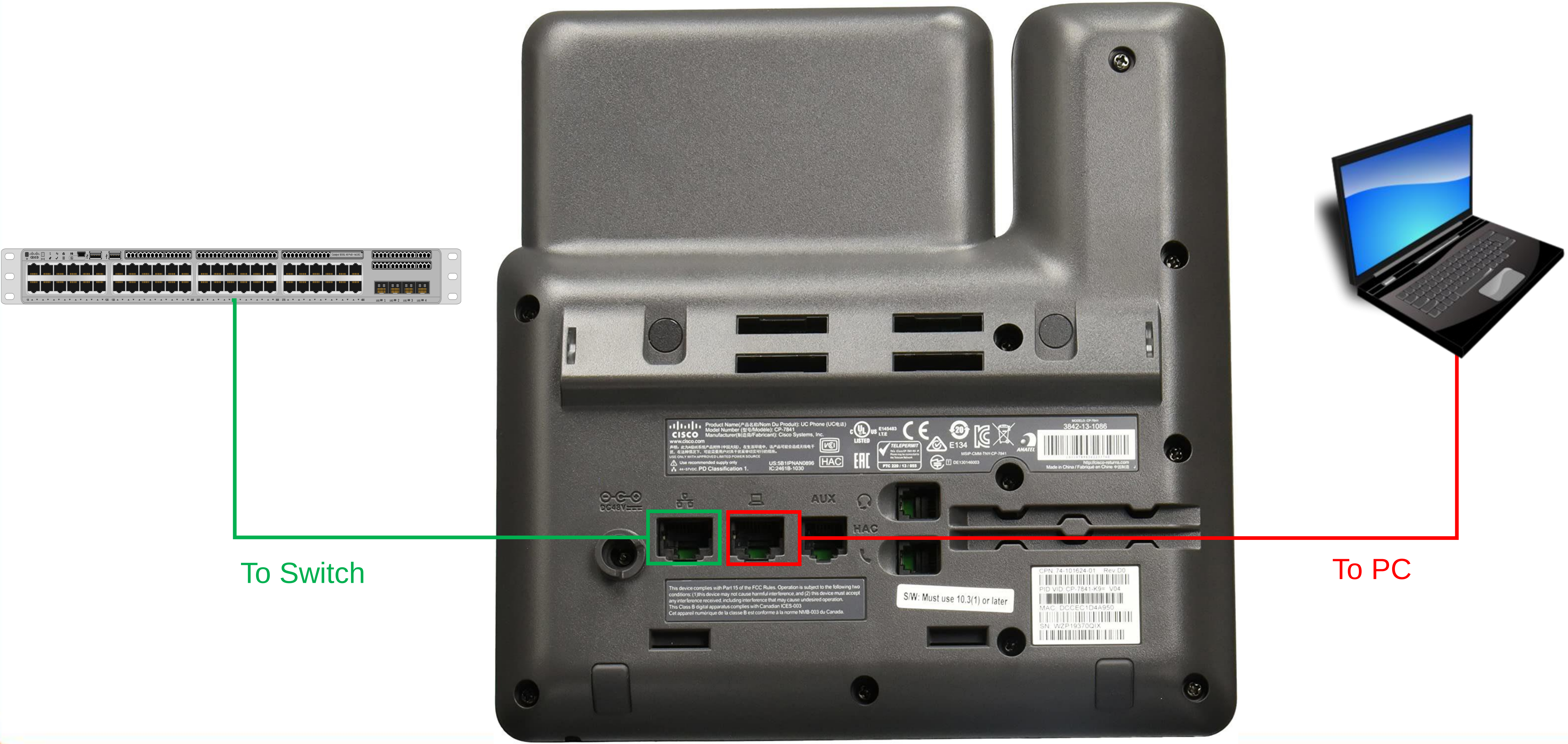
ALERT
ADAPT
ACHIEVE

Physical Diagram Voice VLAN



SAMART TELCOMS

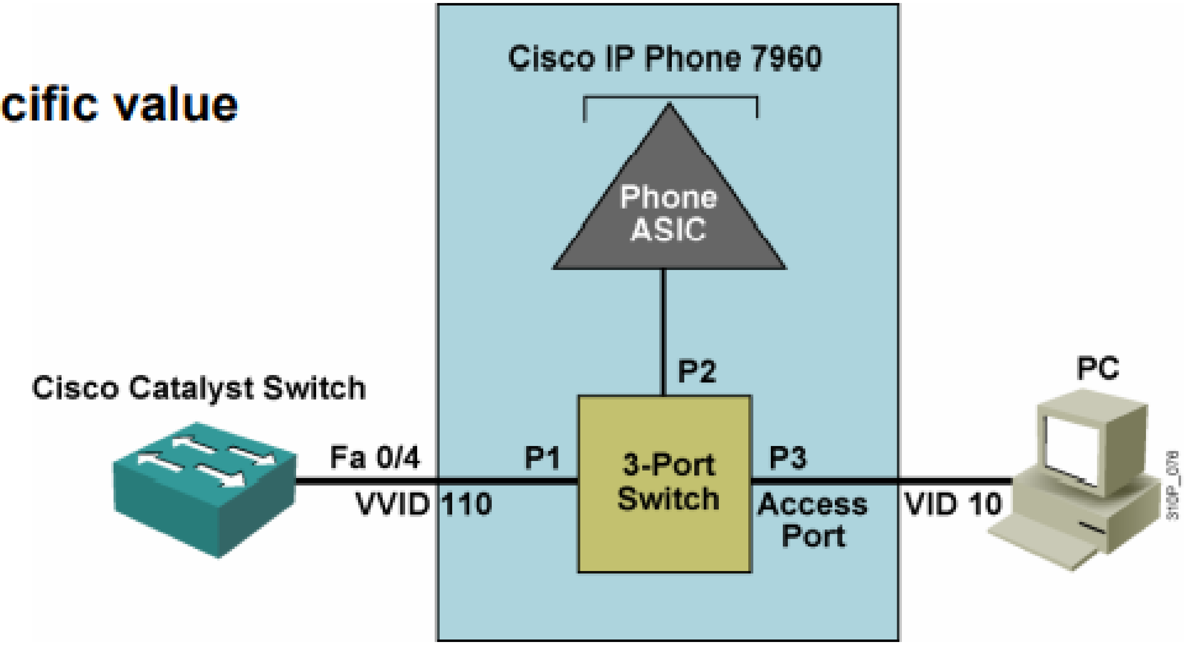
Physical Diagram Voice VLAN



ALERT
ADAPT
ACHIEVE

Configuring a Switch for Attachment of a Cisco IP Phone

- Voice traffic tagged for voice VLAN
- Data VLAN traffic from PC can be
  - Untrusted
  - Trusted
  - Set to a specific value



SAMART TELCOMS

Basic Switch Commands to Support Attachment of a Cisco IP Phone

Configure voice VLAN

- switchport voice vlan 110

Configure trust and CoS options

- mls qos trust cos
- mls qos trust device cisco-phone
- mls qos extend trust
- switchport priority extend cos cos_value

Verify configuration

- show interfaces fa 0/4 switchport
- show mls qos interface fa 0/4

Configuration Example

```
Switch(config)# interface fastethernet 0/4
Switch(config-if)# switchport voice vlan 110

Switch(config-if)# switchport access vlan 10
```

Display Voice VLAN

```
COPI_SWC92_F2_01#sh interfaces Gig 1/0/13 switchport
Name: Gi1/0/13
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1800 (Data_Wired)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: disabled
Voice VLAN: 120 (Services_Voice)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

Display Voice VLAN

```
COPI_SWC92_F2_01#sh interfaces Gig 1/0/13 trunk

Port        Mode        Encapsulation       Status              Native vlan
Gi1/0/13    off         802.1q              not-trunking        1

Port        Vlans allowed on trunk
Gi1/0/13    120,1800

Port        Vlans allowed and active in management domain
Gi1/0/13    120,1800

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/13    120,1800
```

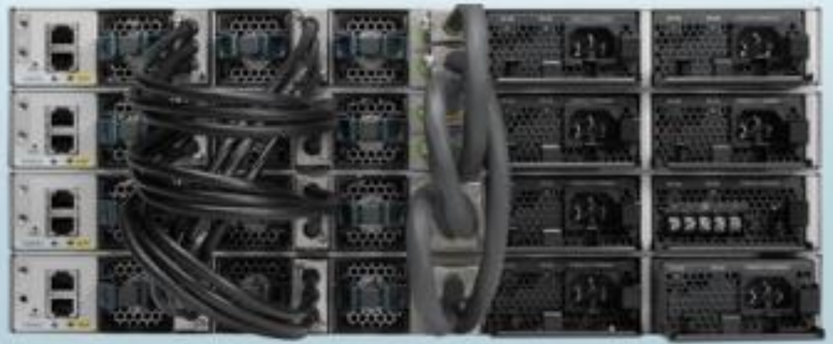
Switch Stack

Why stack?

- Benefits of a 9300 / 3850 stack
  - Add as you grow
  - Port density
  - Redundancy
  - Single control plane
  - Central management
  - 8 switch ring, up to 480G stack bandwidth
  - Support for PoE, PoE+, UPOE, QoS, ACLs, Flex NetFlow, many more

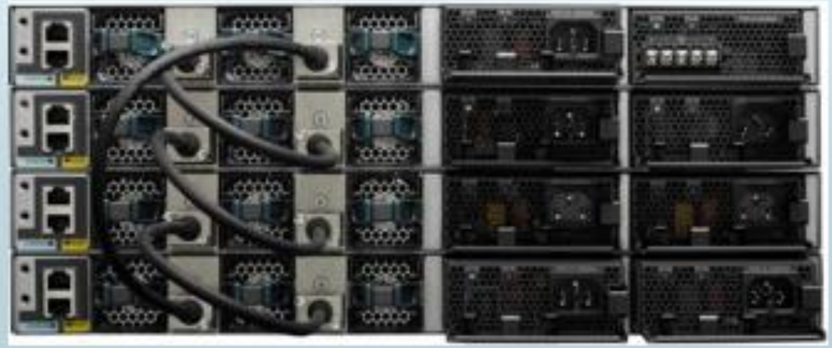
Stack–Cables and Components

Catalyst 3850



3 lengths of cable, 0.5 1 and 3 Meters

Catalyst 3650



1 ring in 3650 vs 3 rings in 3850

Discovery and Election

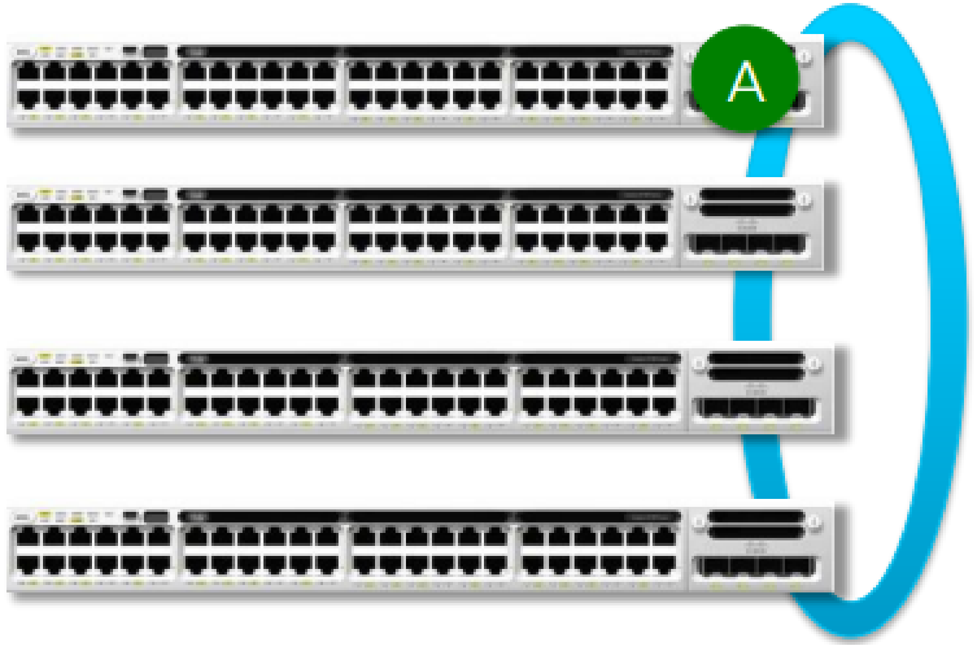
SDP discovers the stack topology using broadcasts at bootup. Member switches elect Active switch during 120 second window after discovery.

- Active election is determined by highest priority and then lowest MAC
- Default priority is 1 / highest priority is 15
- Once Active switch discovers all member switches, a Standby is elected

Stack Active Election

1) The stack (or switch) whose member has the higher user configurable **priority 1–15**

2) The switch or stack whose member has the **lowest MAC address**



```
%IOSXE-1-PLATFORM: process stack-mgr: %STACKMGR-1-ACTIVE_ELECTED: Switch 3 has been elected ACTIVE.
```

Important Points to Remember

- 9300 / 3850 stack tips
  - Switch priority is manually configured but takes effect after a reload
  - A switch boots fully into IOS will become Active regardless of priority
  - Switch numbers remain persistent even after reload and even after switch is removed from the stack
  - Active switch will renumber a member to resolve number conflicts
  - Switch number and port number are not changed upon removal of a member from a stack
  - Switch numbering does NOT reflect the physical switch location in a stack

Config Switch Stack

1

```
COPI_SWC38_01(config)#switch 2 provision ws-c3850-12s

COPI_SWC38_01#switch 1 priority 15

COPI_SWC38_01#copy run start

COPI_SWC38_01#reload
```

2

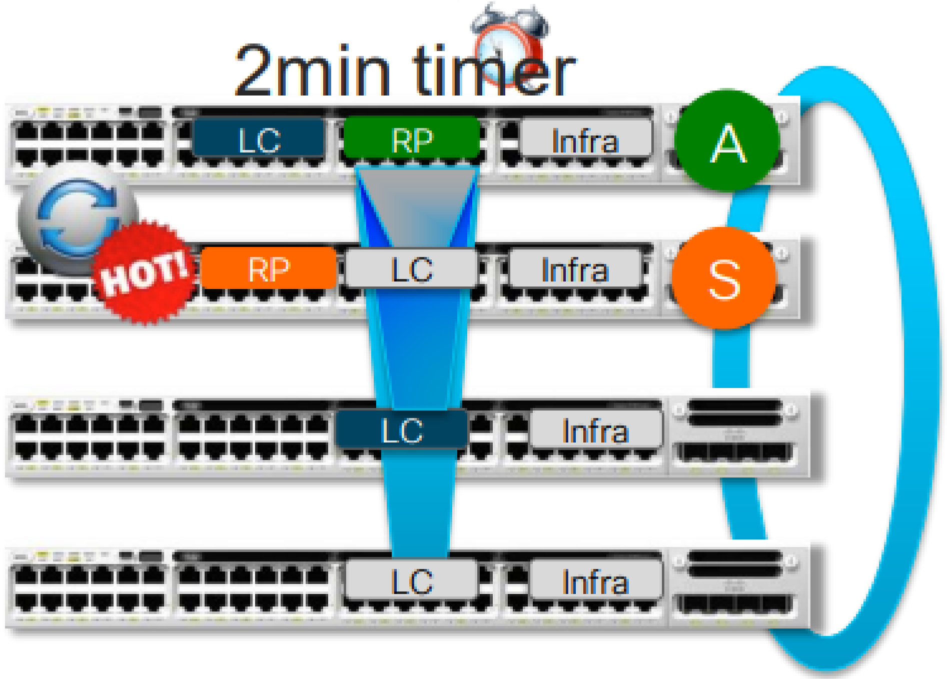
Connect Stack Cable

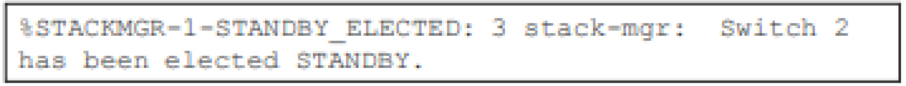
3

```
COPI_SWC38_01#switch 2 priority 10

COPI_SWC38_01#copy run start

COPI_SWC38_01#reload slot 2
```

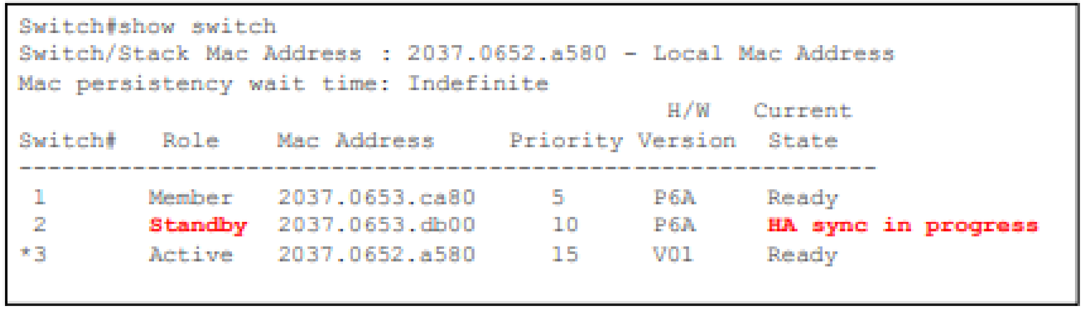
Stack Initialization

- Active starts RP Domain (IOSd, WCM, etc) locally
- Programs hardware on all LC Domains
- Traffic resumes once hardware is programmed
- Starts 2min Timer to elect Standby in parallel
- Active elects Standby
- Standby starts RP Domain locally
- Starts Bulk Sync with Active RP
- Standby reaches “Standby Hot”



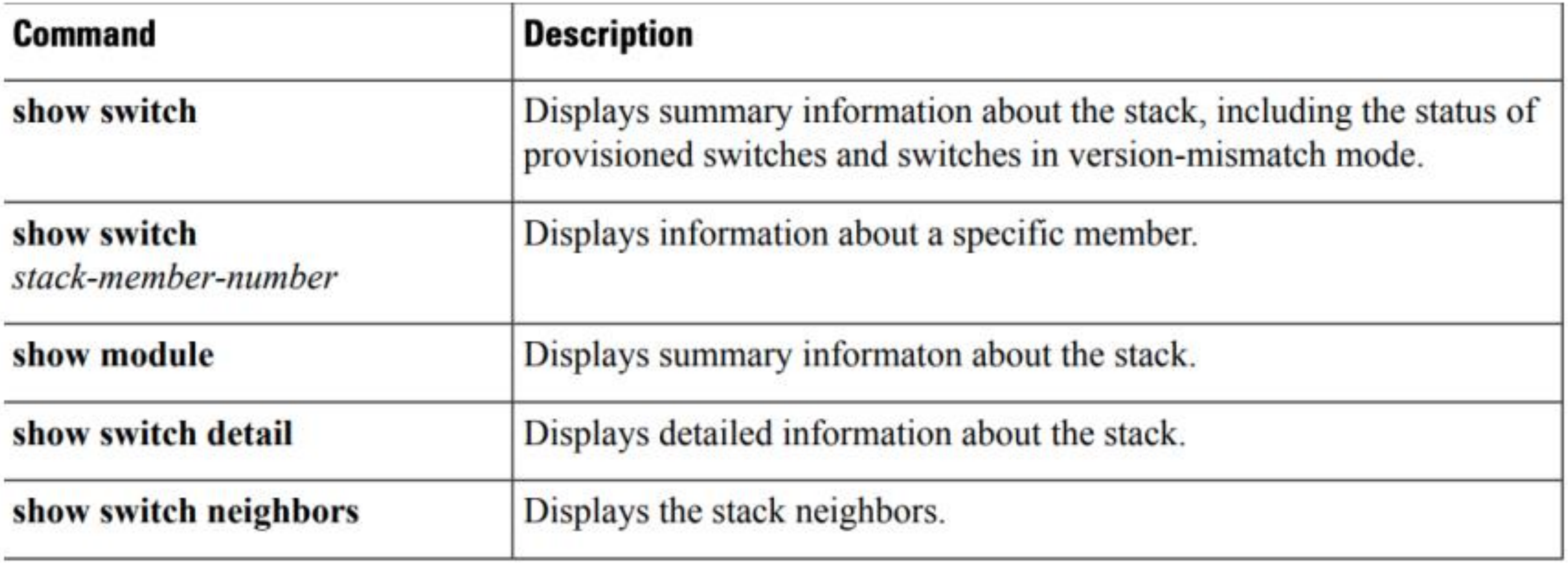


```
%STACKMGR-1-STANDBY_ELECTED: 3 stack-mgr:  Switch 2
has been elected STANDBY.
```



```
Switch#show switch
Switch/Stack Mac Address : 2037.0652.a580 - Local Mac Address
Mac persistency wait time: Indefinite
                                            H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------
 1        Member  2037.0653.ca80     5      P6A     Ready
 2        Standby 2037.0653.db00     10     P6A     HA sync in progress
*3        Active  2037.0652.a580     15     V01     Ready
```

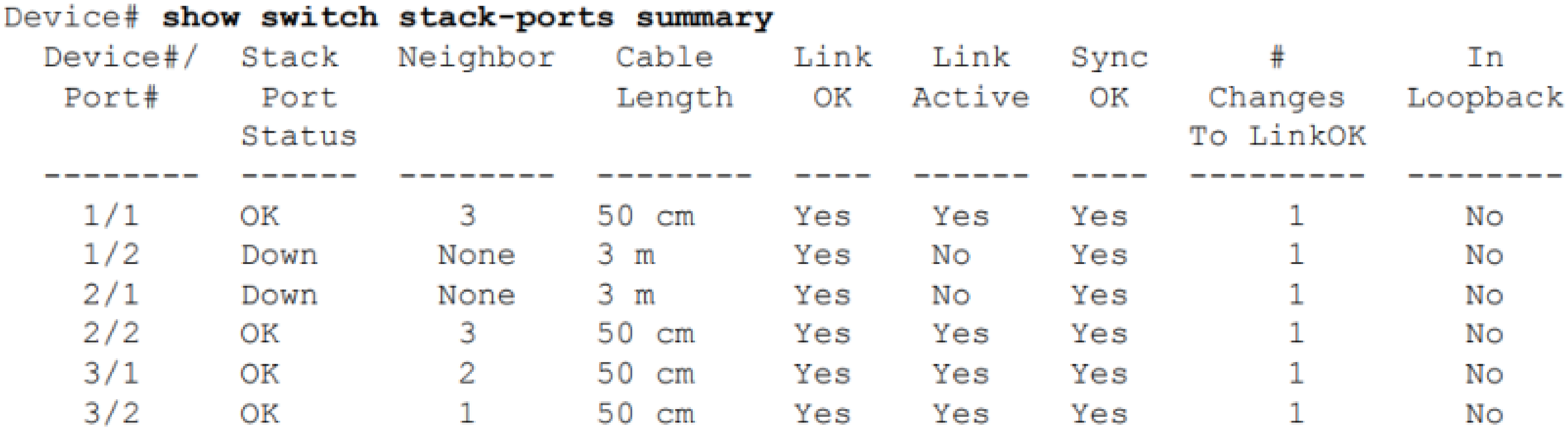
Commands for displaying stack information



Command	Description
show switch	Displays summary information about the stack, including the status of provisioned switches and switches in version-mismatch mode.
show switch *stack-member-number*	Displays information about a specific member.
show module	Displays summary informaton about the stack.
show switch detail	Displays detailed information about the stack.
show switch neighbors	Displays the stack neighbors.

Tips for validation and troubleshooting

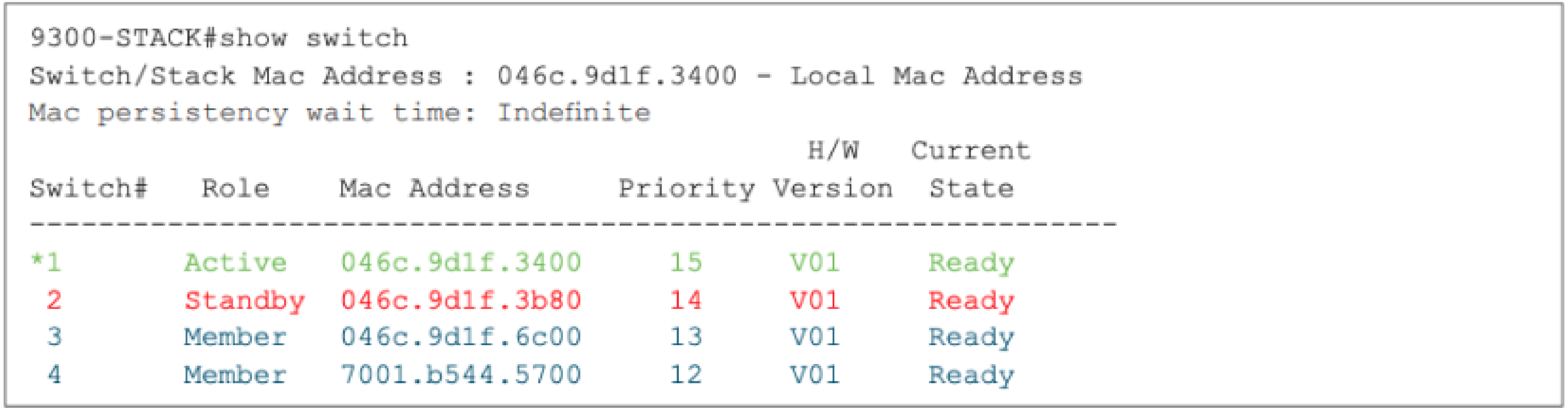
- Check stack port status with the ‘show switch stack-ports summary’ command



```
Device# show switch stack-ports summary
  Device#/   Stack   Neighbor   Cable     Link   Link    Sync      #          In
   Port#      Port              Length     OK   Active    OK    Changes    Loopback
             Status                                            To LinkOK
  --------   ------  --------  --------   ----  ------   ----  ---------  --------
    1/1      OK         3       50 cm     Yes    Yes     Yes       1         No
    1/2      Down      None     3 m       Yes    No      Yes       1         No
    2/1      Down      None     3 m       Yes    No      Yes       1         No
    2/2      OK         3       50 cm     Yes    Yes     Yes       1         No
    3/1      OK         2       50 cm     Yes    Yes     Yes       1         No
    3/2      OK         1       50 cm     Yes    Yes     Yes       1         No
```

Tips for validation and troubleshooting

- Check stack switch roles with the ‘show switch’ command



```
9300-STACK#show switch
Switch/Stack Mac Address : 046c.9d1f.3400 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role     Mac Address     Priority Version  State
---------------------------------------------------------------
*1        Active   046c.9d1f.3400     15       V01      Ready
 2        Standby  046c.9d1f.3b80     14       V01      Ready
 3        Member   046c.9d1f.6c00     13       V01      Ready
 4        Member   7001.b544.5700     12       V01      Ready
```

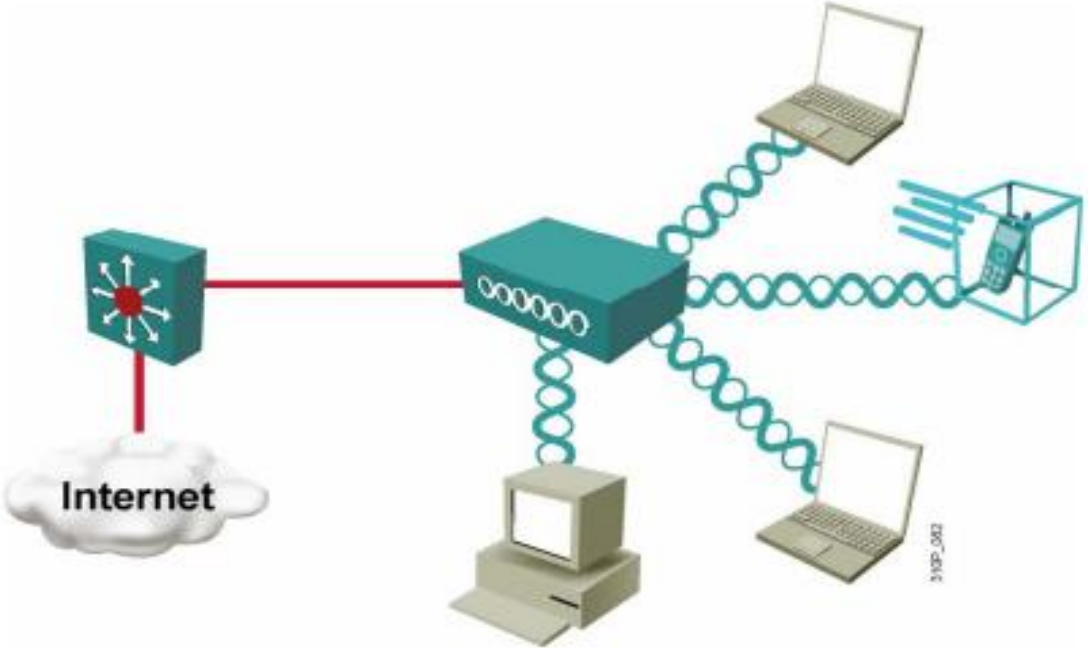
ALERT
ADAPT
ACHIEVE

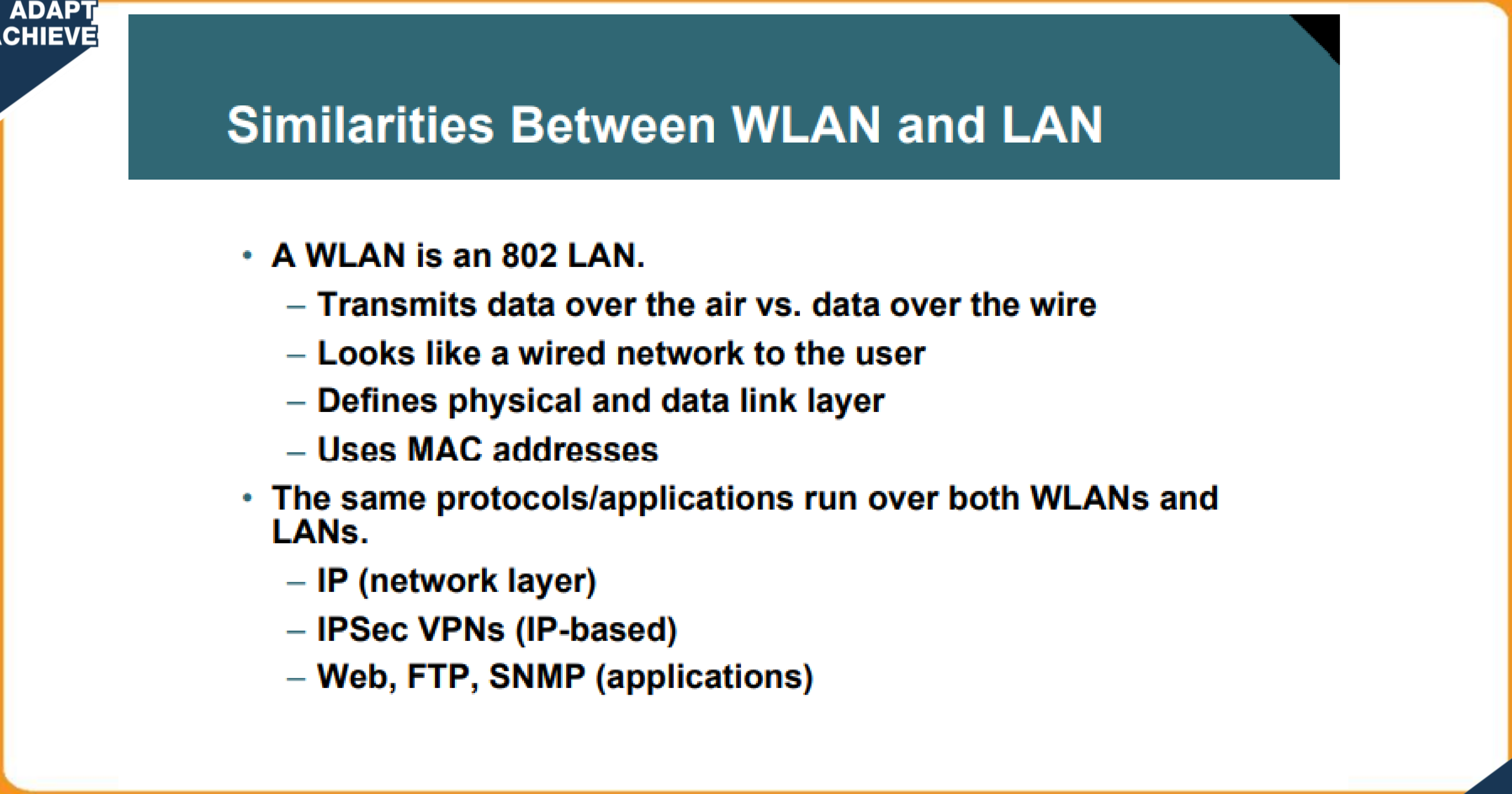
Wireless Lan Overview

SAMART TELCOMS

Wireless LAN (WLAN)

- A WLAN is a shared network.
- An access point is a shared device and functions like a shared Ethernet hub.
- Data is transmitted over radio waves.
- Two-way radio communications (half-duplex) are used.
- The same radio frequency is used for sending and receiving (transceiver).



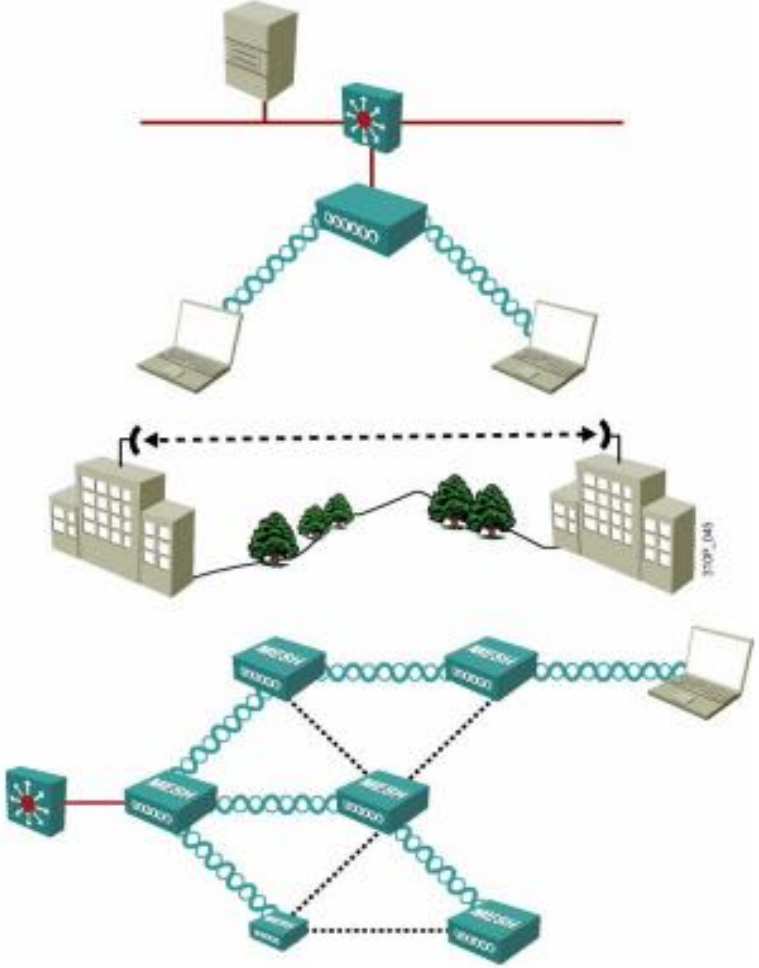


Similarities Between WLAN and LAN

- A WLAN is an 802 LAN.
  - Transmits data over the air vs. data over the wire
  - Looks like a wired network to the user
  - Defines physical and data link layer
  - Uses MAC addresses
- The same protocols/applications run over both WLANs and LANs.
  - IP (network layer)
  - IPSec VPNs (IP-based)
  - Web, FTP, SNMP (applications)

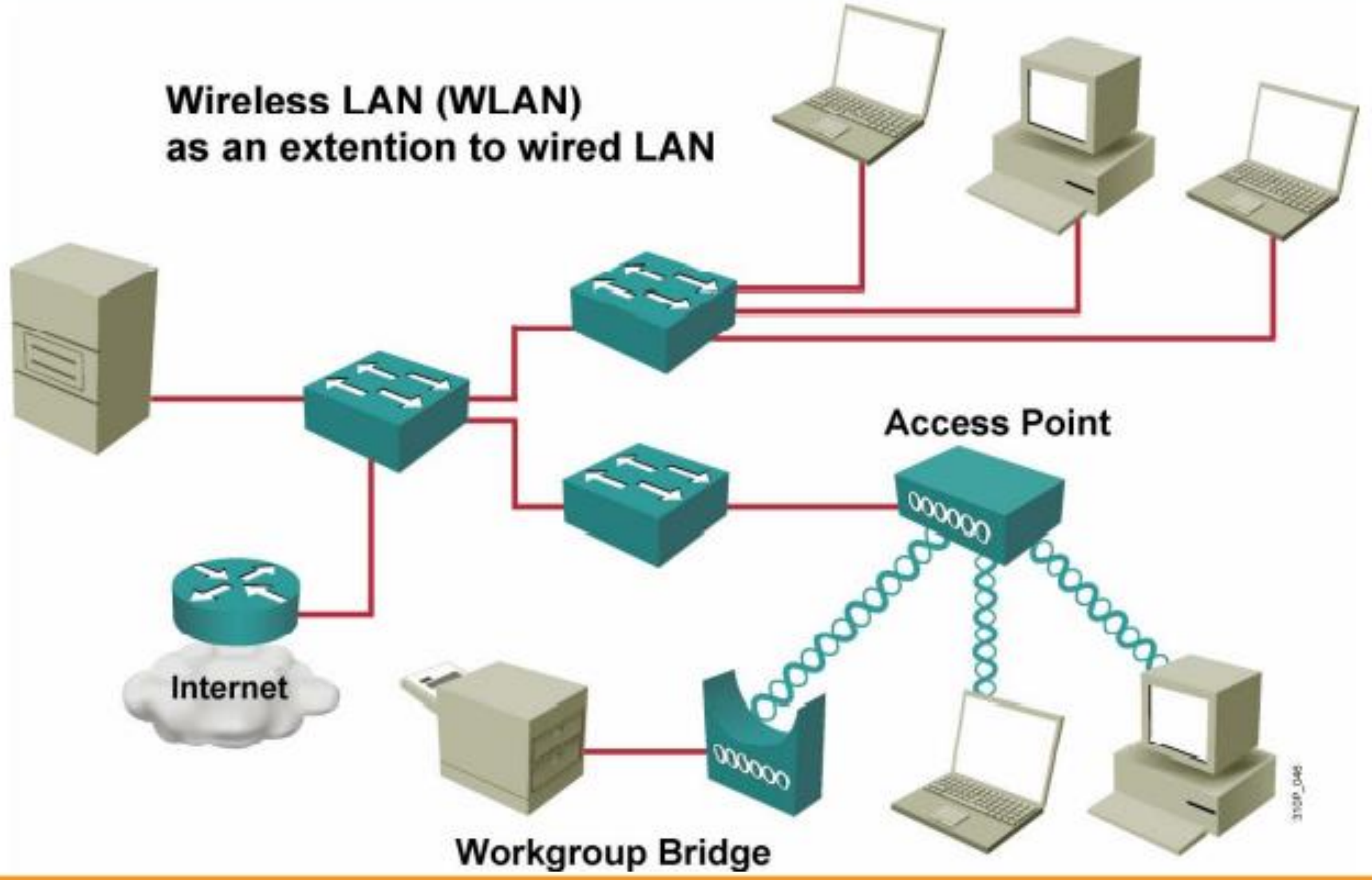
WLAN Topologies

- Wireless client access
  - Mobile user connectivity
- Wireless bridging
  - LAN-to-LAN connectivity
- Wireless mesh networking
  - Combination of bridging and user connectivity



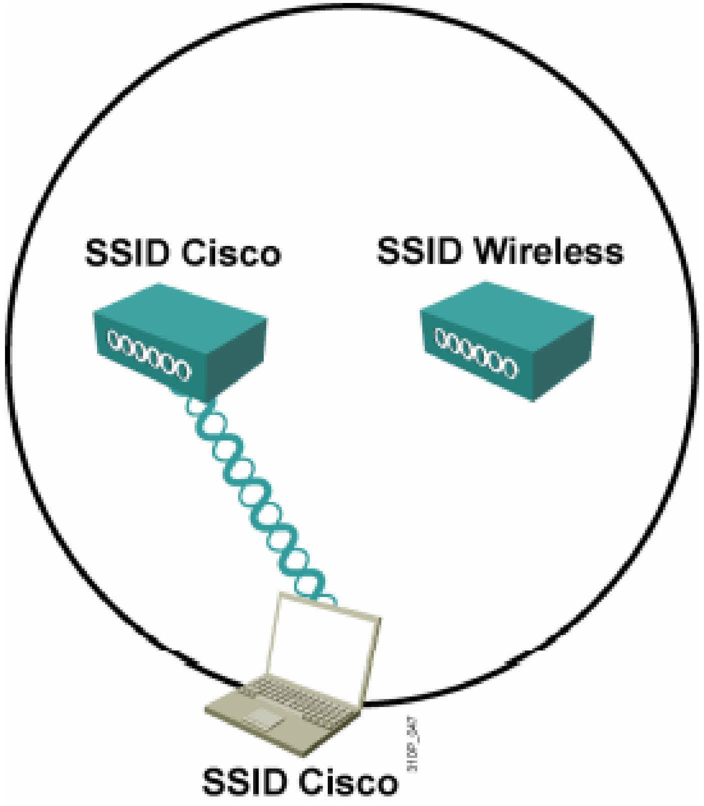
WLAN and LAN

Wireless LAN (WLAN)
as an extention to wired LAN



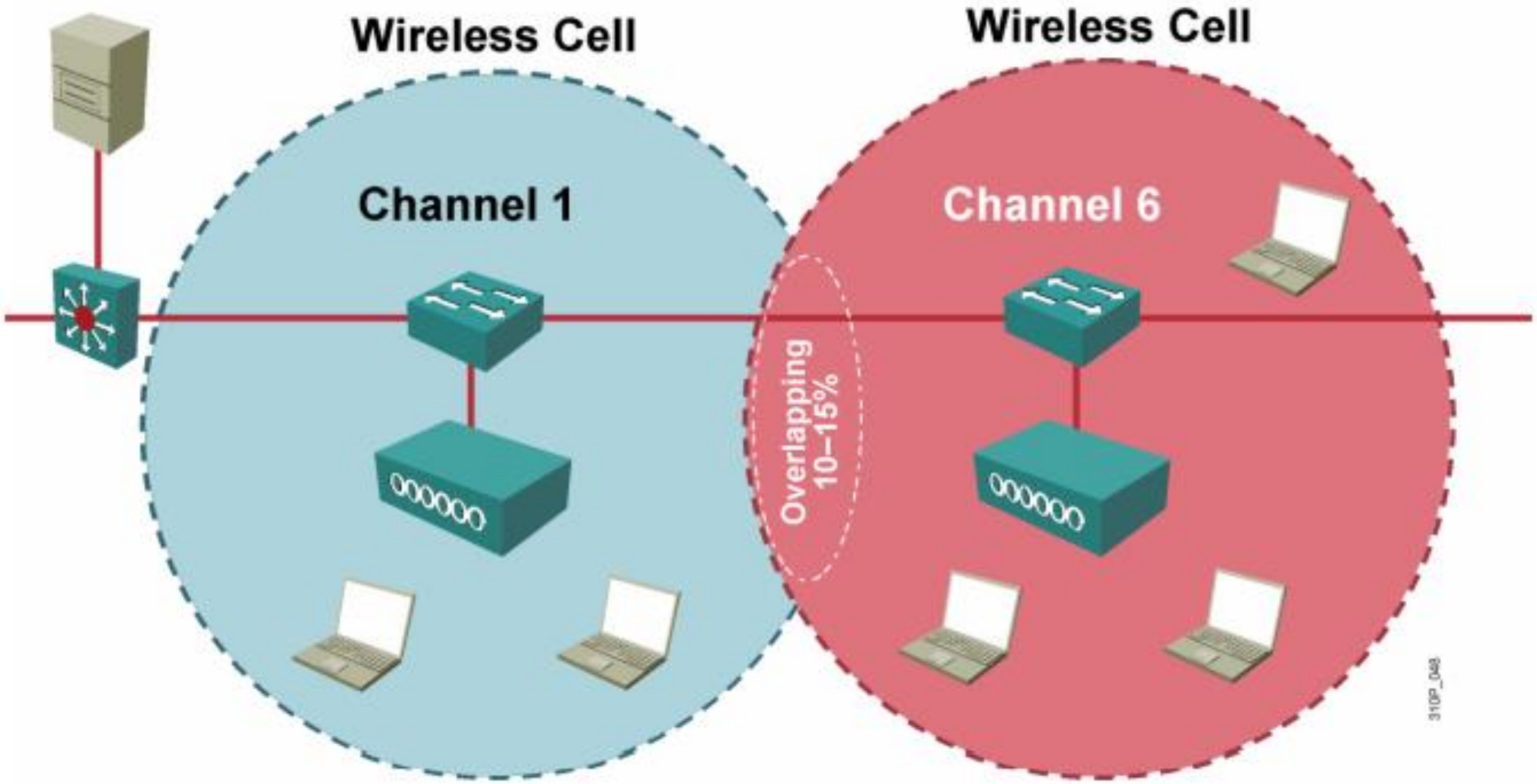
Service Set Identifier (SSID)

- SSID is used to logically separate WLANs.
- The SSID must match on client and access point.
- Access point broadcasts one SSID in beacon.
- Client can be configured without SSID.
- Client association steps:
  1. Client sends probe request.
  2. A point sends probe response.
  3. Client initiates association.
  4. A point accepts association.
  5. A point adds client MAC address to association table.



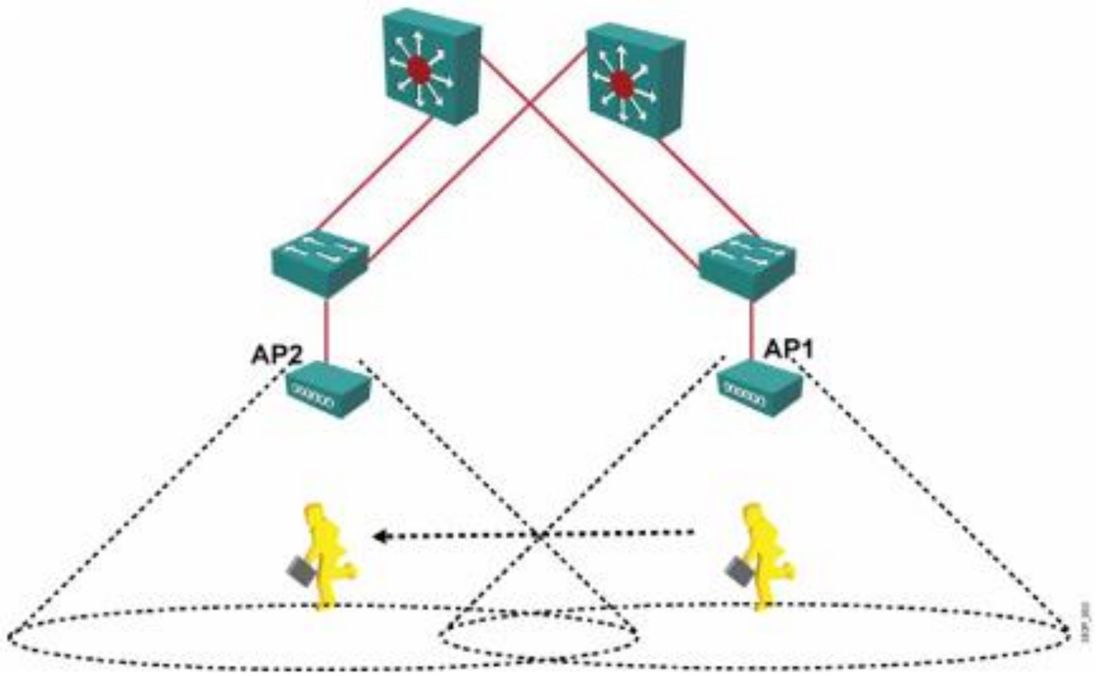
ALERT
ADAPT
ACHIEVE

WLAN Access Topology



SAMART
TELCOMS

Client Roaming

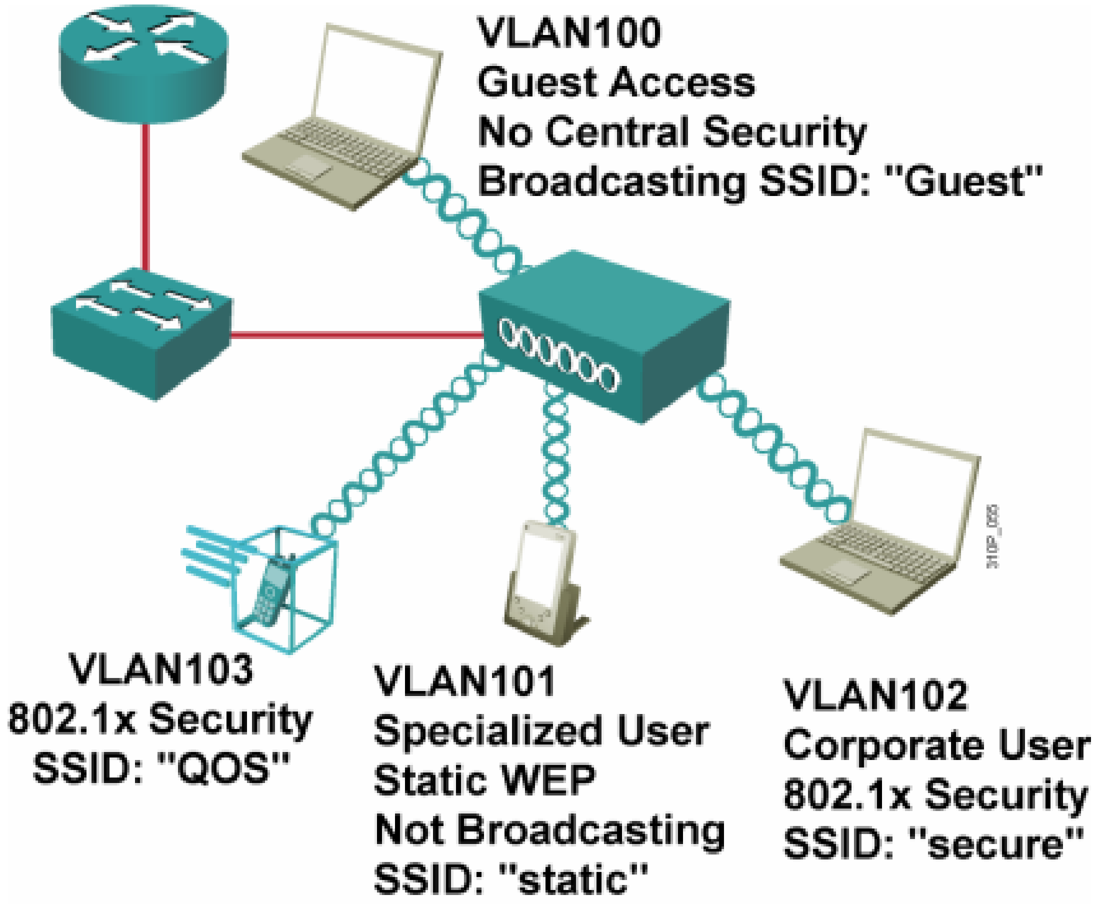


- Maximum data retry count exceeded
- Too many beacons missed
- Data rate shifted
- Periodic intervals

- Roaming without interruption requires the same SSID on all access points.

Wireless VLAN Support

- Multiple SSIDs
- Multiple security types
- Support for multiple VLANs from switches
- 802.1Q trunking protocol



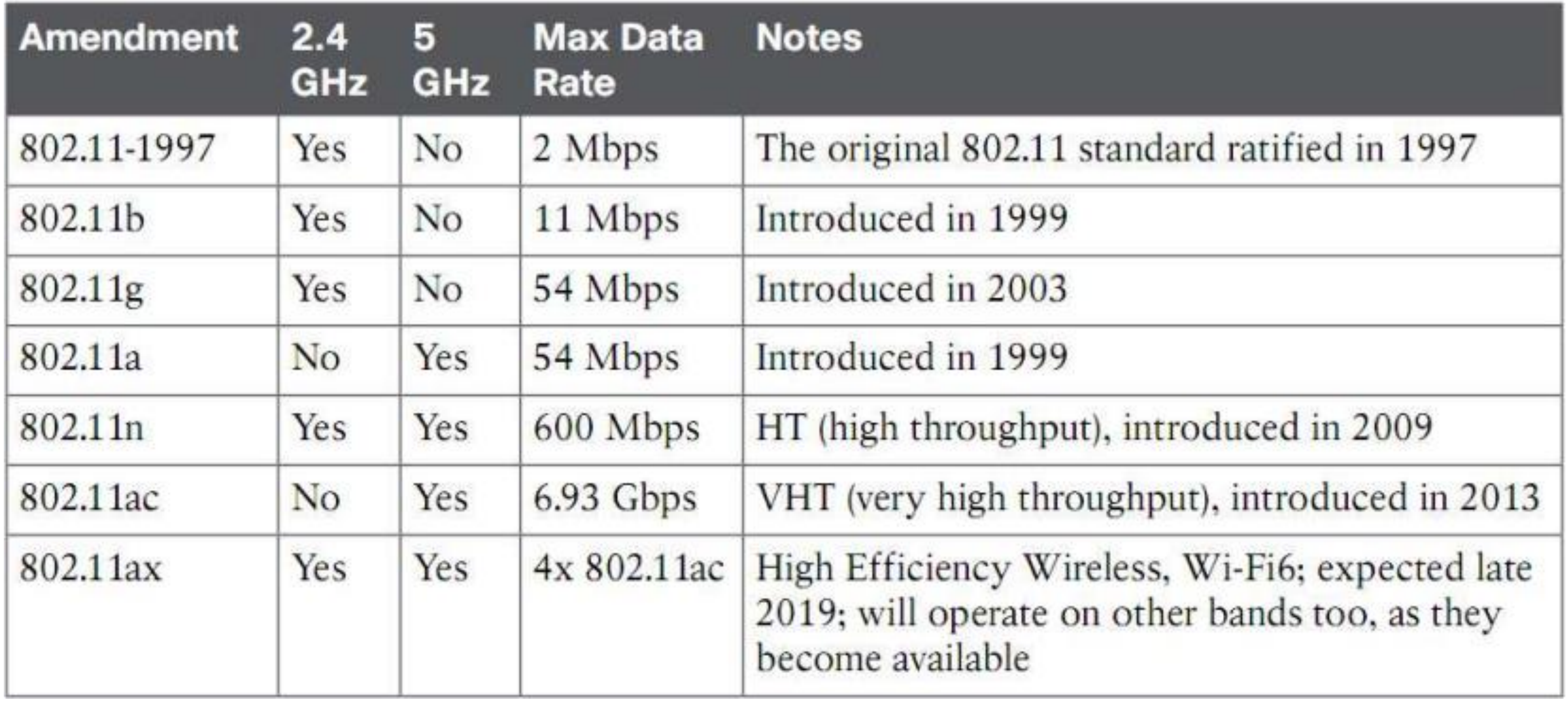
VLAN100
Guest Access
No Central Security
Broadcasting SSID: "Guest"

VLAN103
802.1x Security
SSID: "QOS"

VLAN101
Specialized User
Static WEP
Not Broadcasting
SSID: "static"

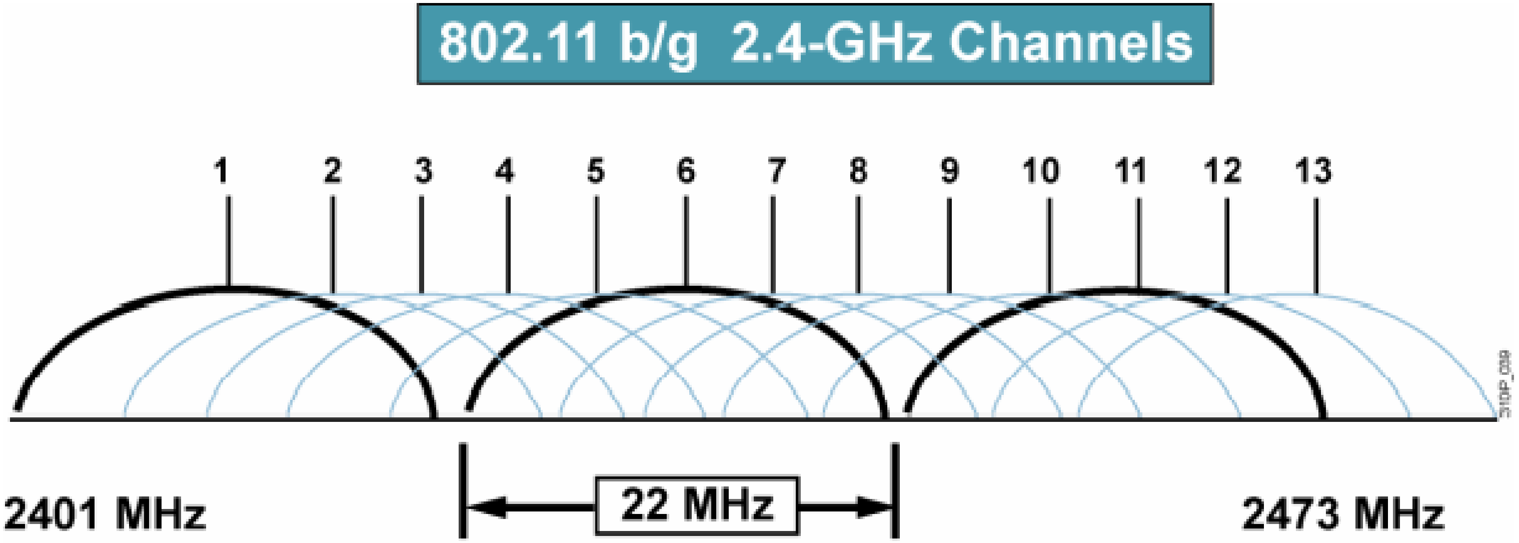
VLAN102
Corporate User
802.1x Security
SSID: "secure"

Standard Wireless Lan



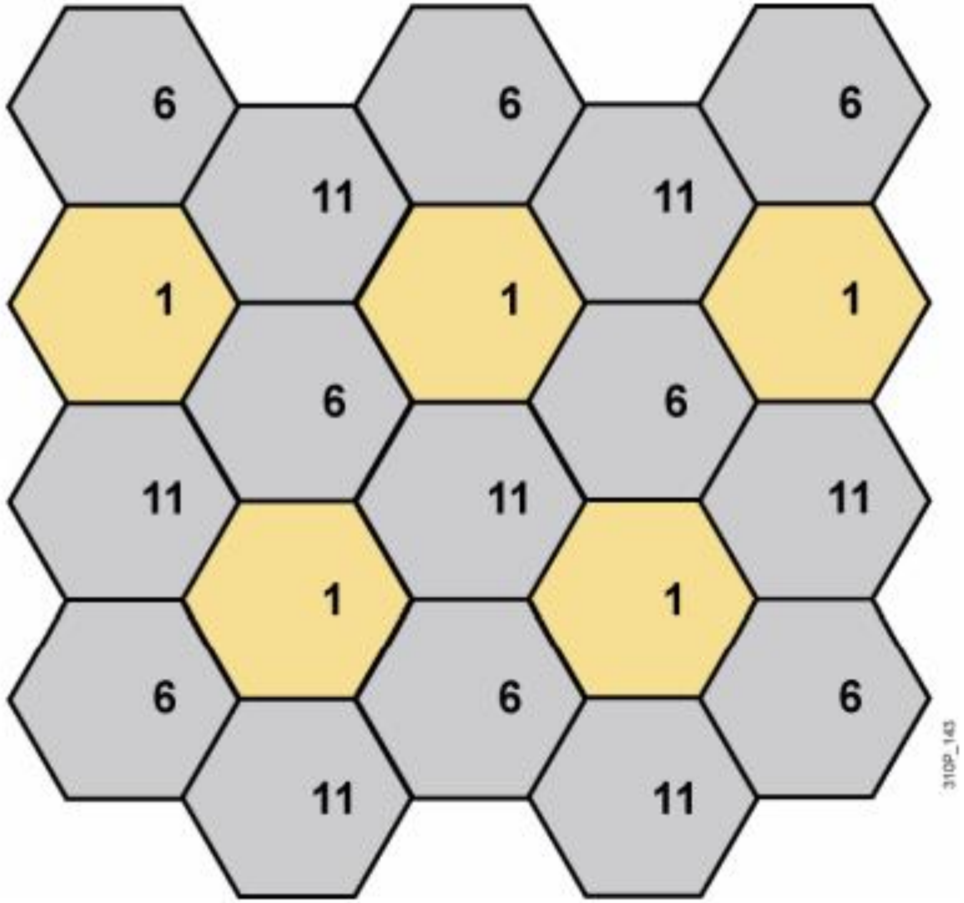
Amendment	2.4 GHz	5 GHz	Max Data Rate	Notes
802.11-1997	Yes	No	2 Mbps	The original 802.11 standard ratified in 1997
802.11b	Yes	No	11 Mbps	Introduced in 1999
802.11g	Yes	No	54 Mbps	Introduced in 2003
802.11a	No	Yes	54 Mbps	Introduced in 1999
802.11n	Yes	Yes	600 Mbps	HT (high throughput), introduced in 2009
802.11ac	No	Yes	6.93 Gbps	VHT (very high throughput), introduced in 2013
802.11ax	Yes	Yes	4x 802.11ac	High Efficiency Wireless, Wi-Fi6; expected late 2019; will operate on other bands too, as they become available

2.4-GHz Channel Use



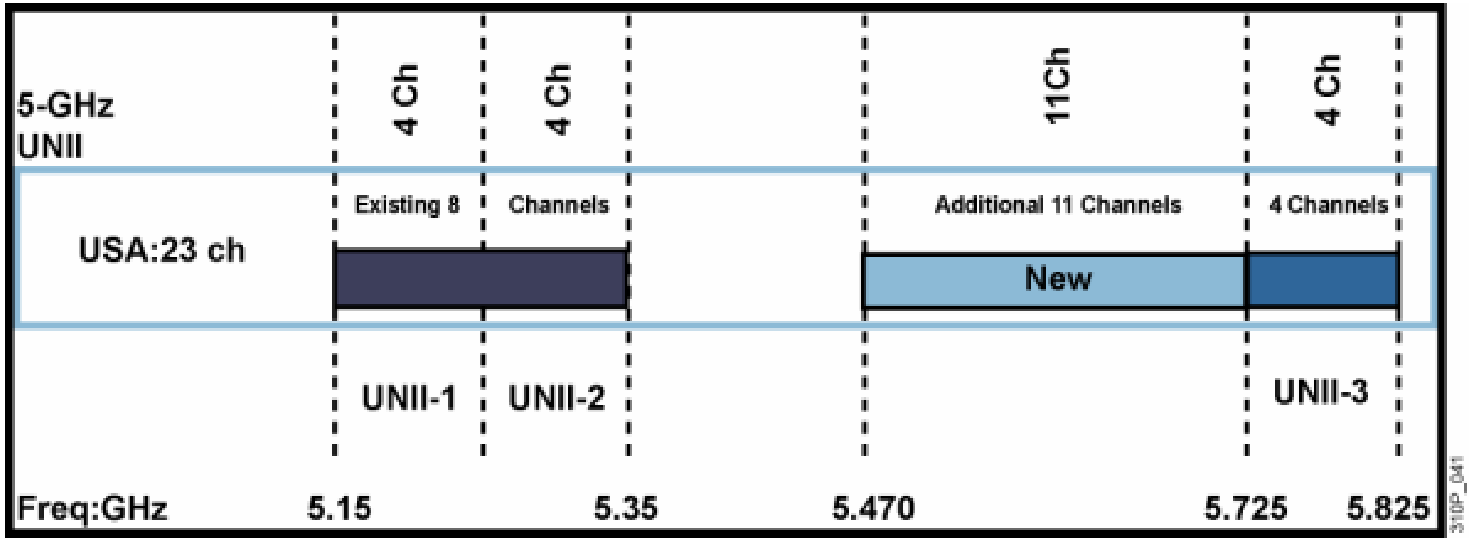
- Each channel is 22 MHz wide.
- North America: 11 channels.
- Europe: 13 channels.
- There are three nonoverlapping channels: 1, 6, 11.
- Using any other channels will cause interference.
- Three access points can occupy the same area.

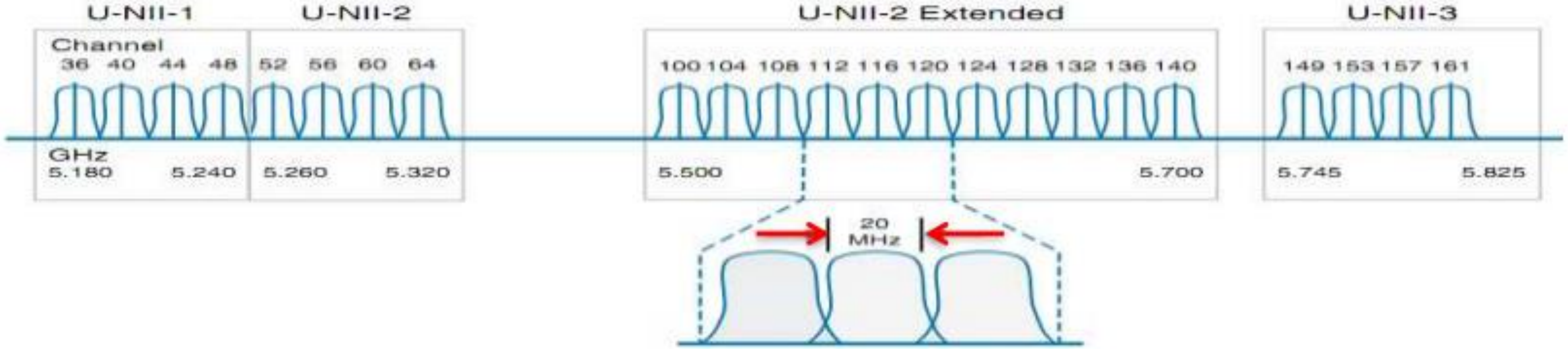
802.11b/g (2.4 GHz) Channel Reuse



ALERT
ADAPT
ACHIEVE

5-GHz Channels with 802.11h

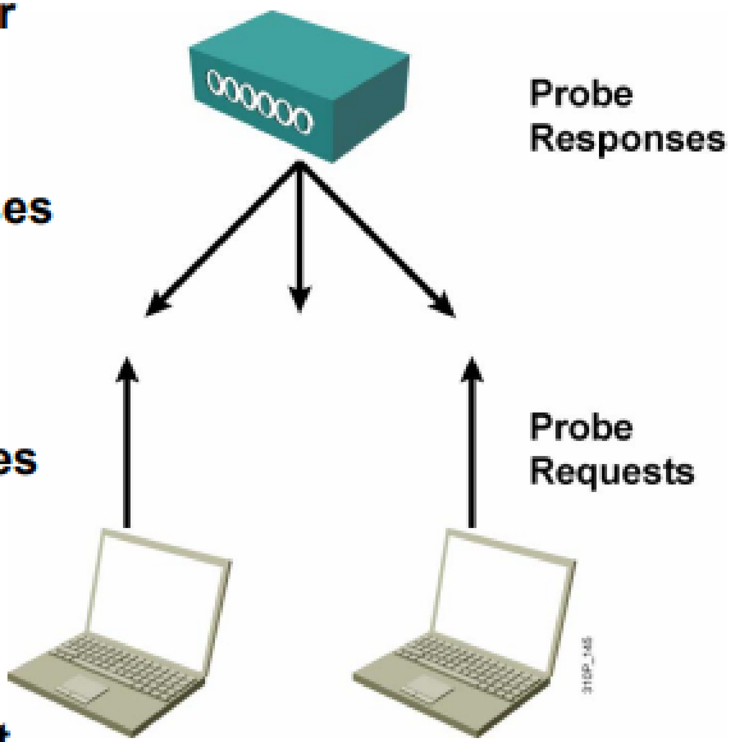




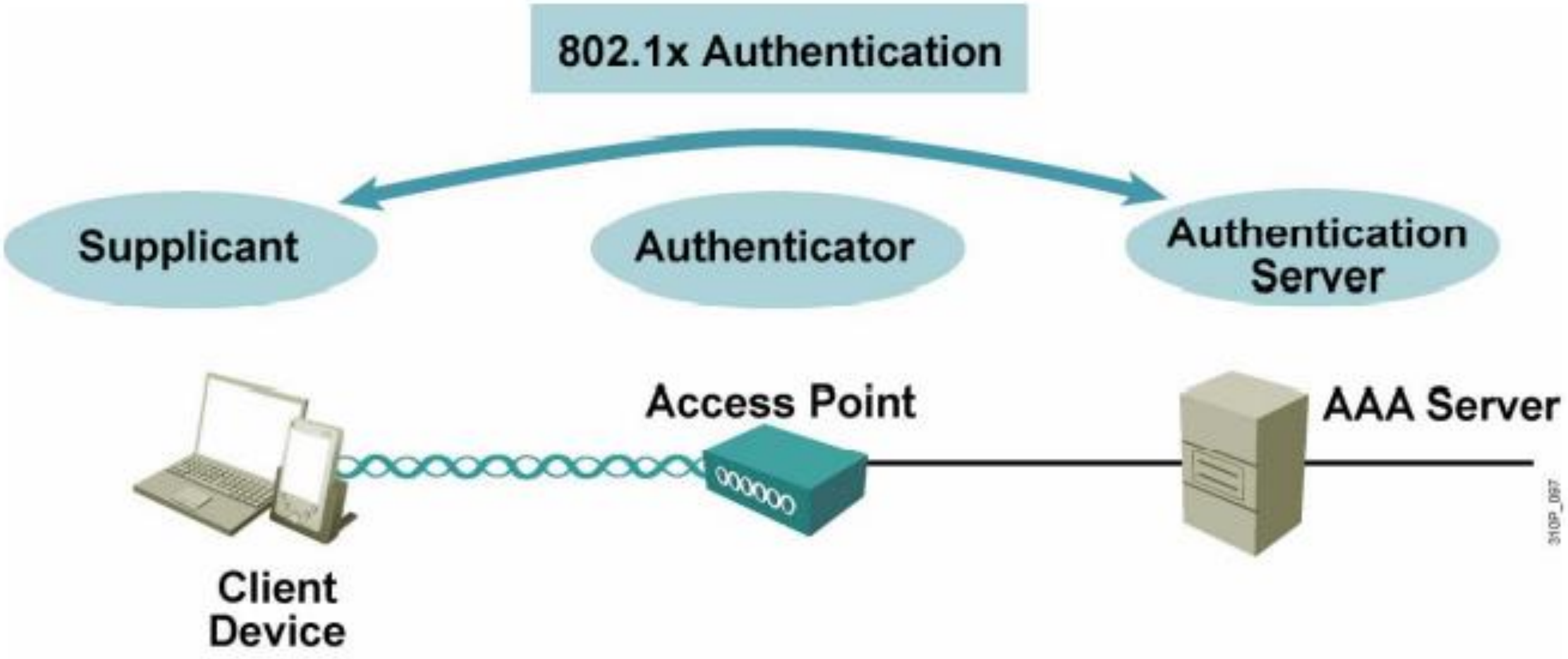
SAMART
TELCOMS

Wireless Client Association

- Access points send out beacons announcing SSID, data rates, and other information.
- Client scans all channels.
- Client listens for beacons and responses from access points.
- Client associates to access point with strongest signal.
- Client will repeat scan if signal becomes low to reassociate to another access point (roaming).
- During association SSID, MAC address and security settings are sent from the client to the access point and checked by the access point.



WPA and WPA2 Authentication



802.1x Authentication

Supplicant

Authenticator

Authentication Server

Access Point

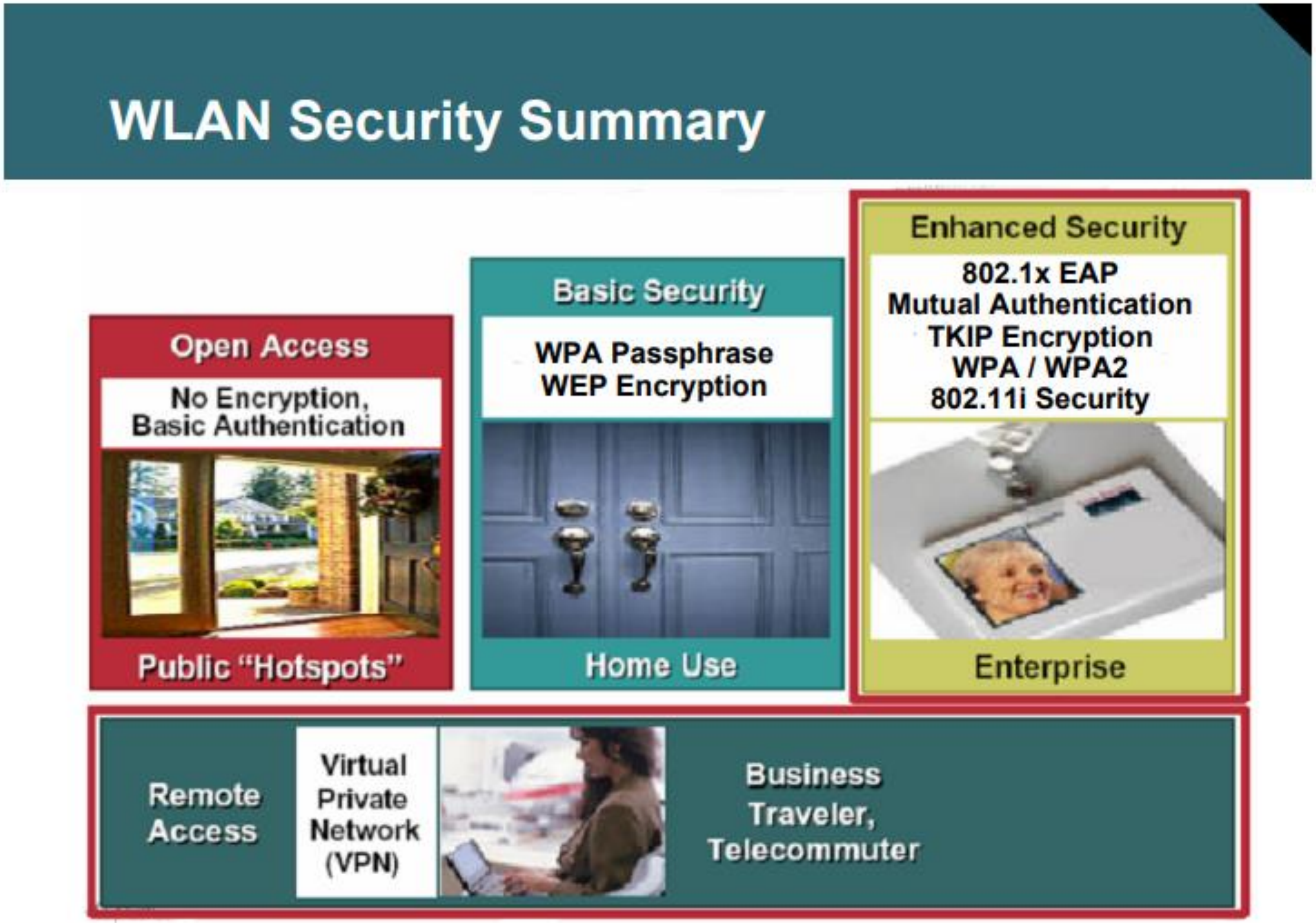
AAA Server

Client Device

Supplicant for 802.1x Type: LEAP, PEAP, EAP-FAST, etc.

802.1x Support

Server Support for 802.1x Type: LEAP, PEAP, EAP-FAST, etc.



WLAN Security Summary

Open Access

No Encryption, Basic Authentication

Public "Hotspots"

Basic Security

WPA Passphrase
WEP Encryption

Home Use

Enhanced Security

802.1x EAP
Mutual Authentication
TKIP Encryption
WPA / WPA2
802.11i Security

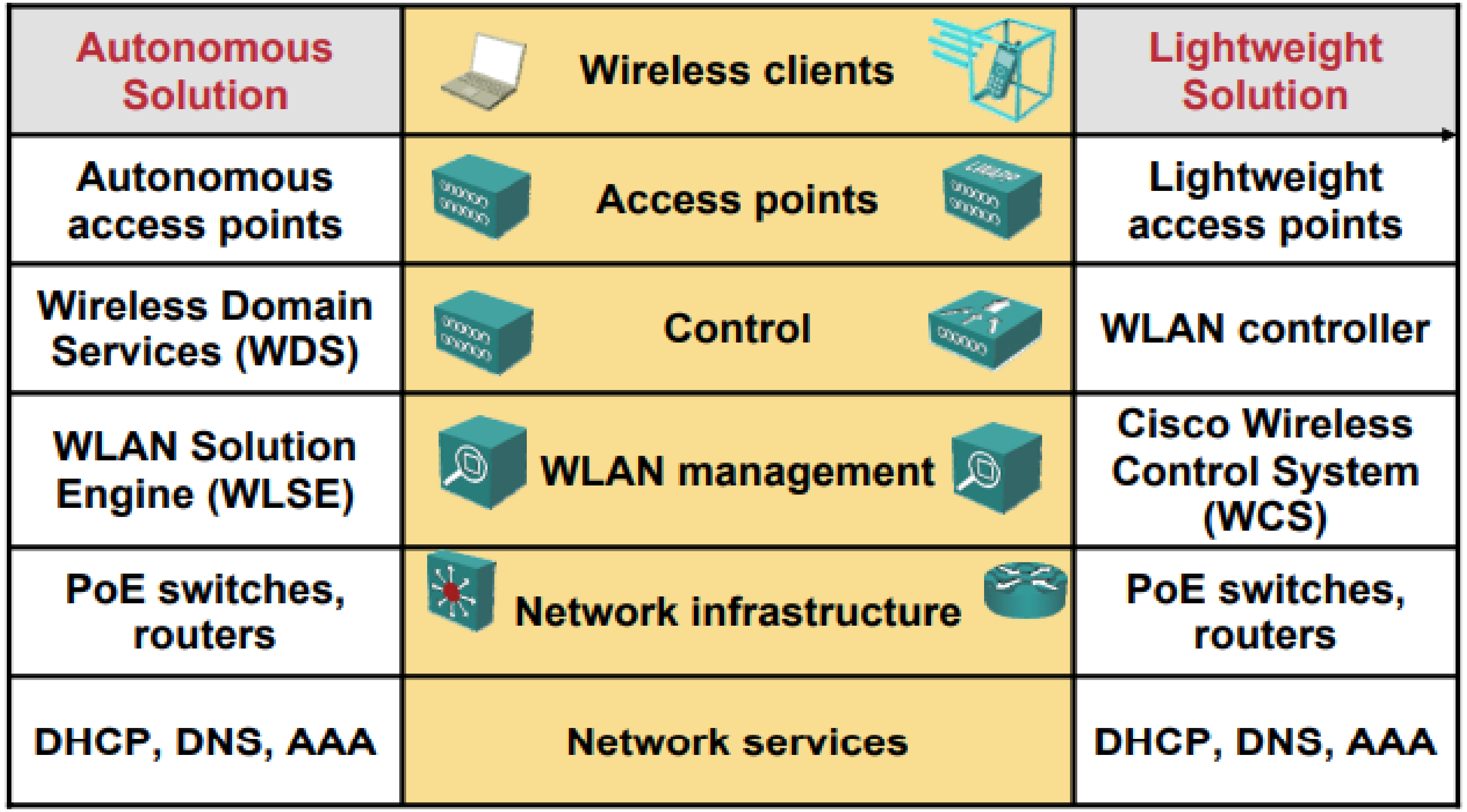
Enterprise

Remote Access

Virtual Private Network (VPN)

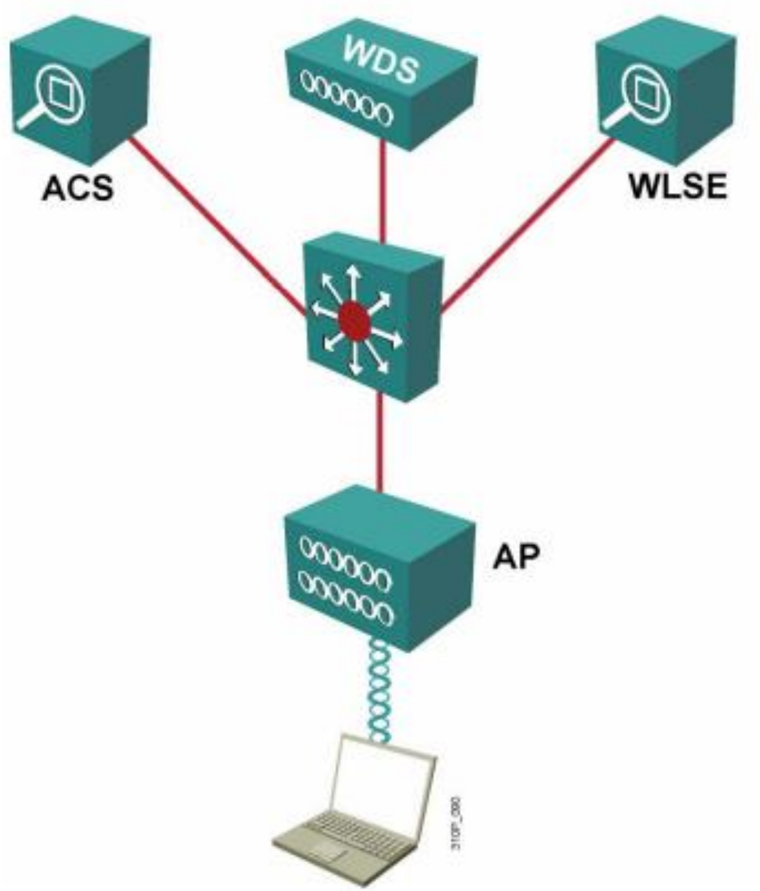
Business Traveler, Telecommuter

WLAN Components

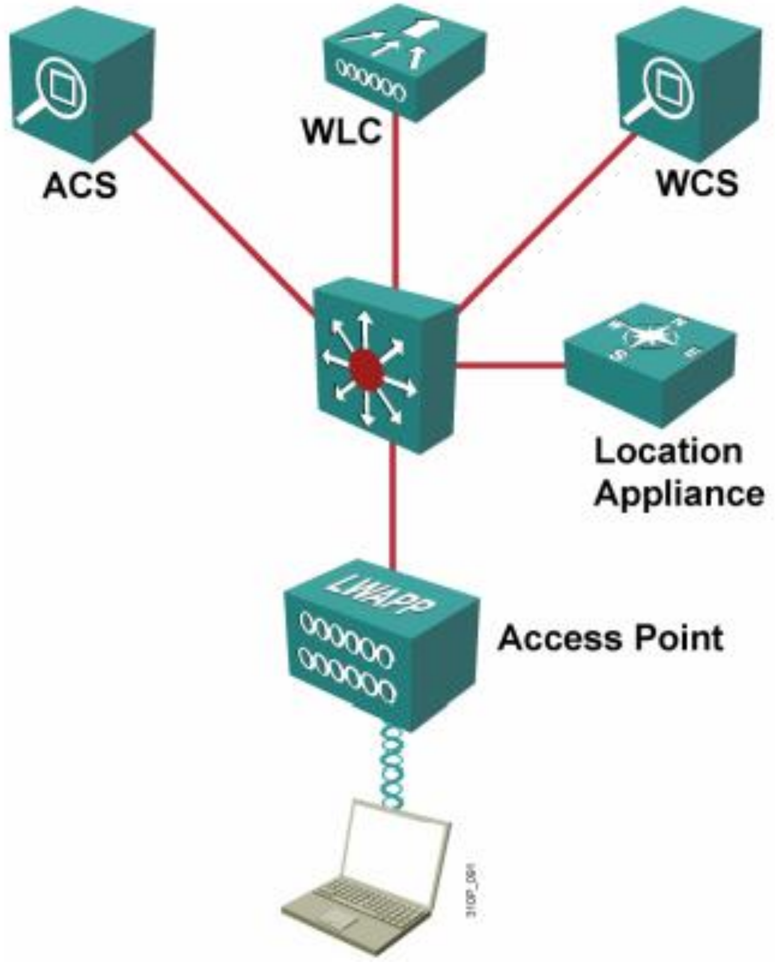


Autonomous Solution	Wireless clients	Lightweight Solution
Autonomous access points	Access points	Lightweight access points
Wireless Domain Services (WDS)	Control	WLAN controller
WLAN Solution Engine (WLSE)	WLAN management	Cisco Wireless Control System (WCS)
PoE switches, routers	Network infrastructure	PoE switches, routers
DHCP, DNS, AAA	Network services	DHCP, DNS, AAA

Autonomous WLAN Solution

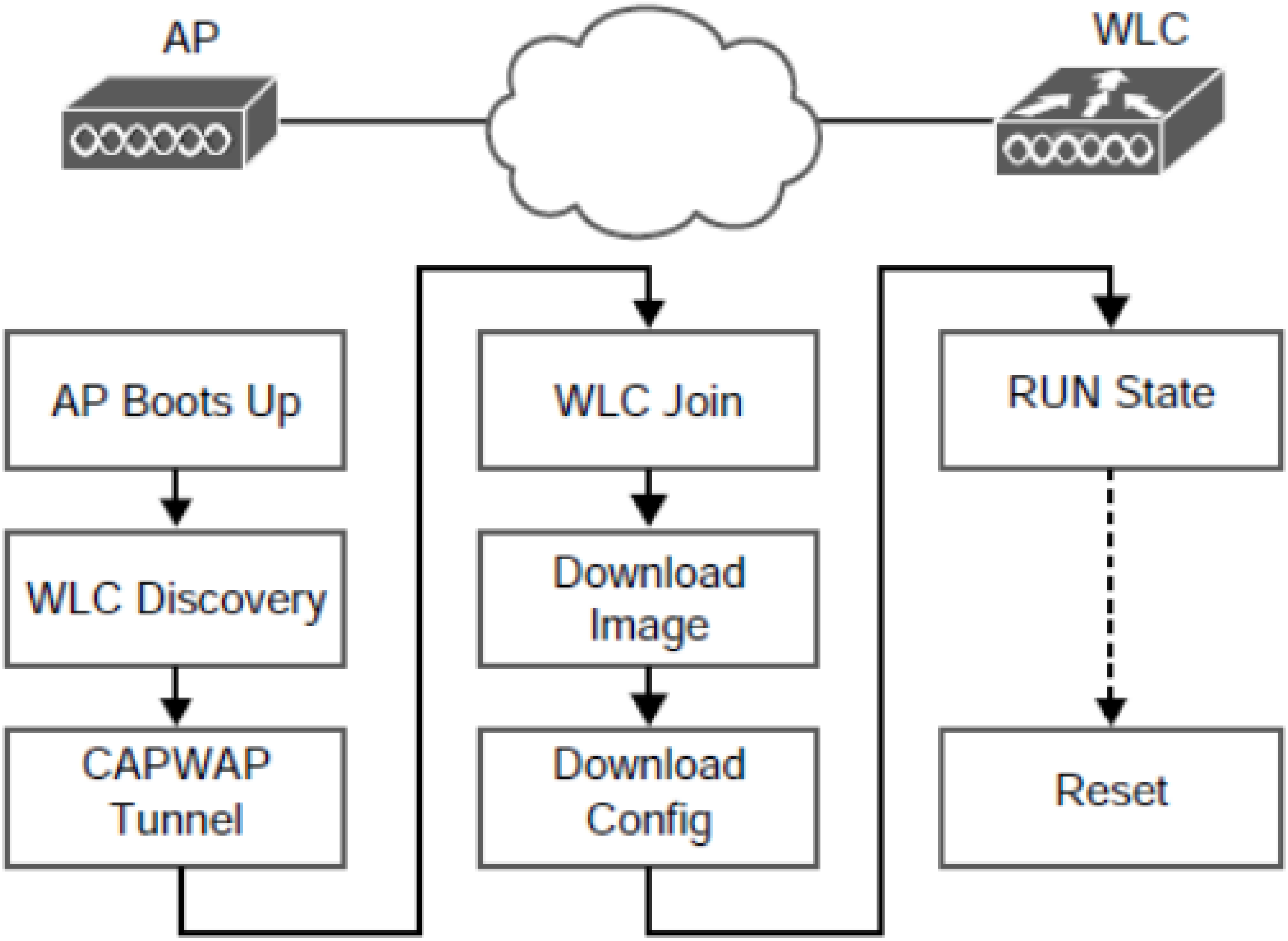


Wireless Lan Controller Solution



ALERT
ADAPT
ACHIEVE

Wireless Lan Controller Solution

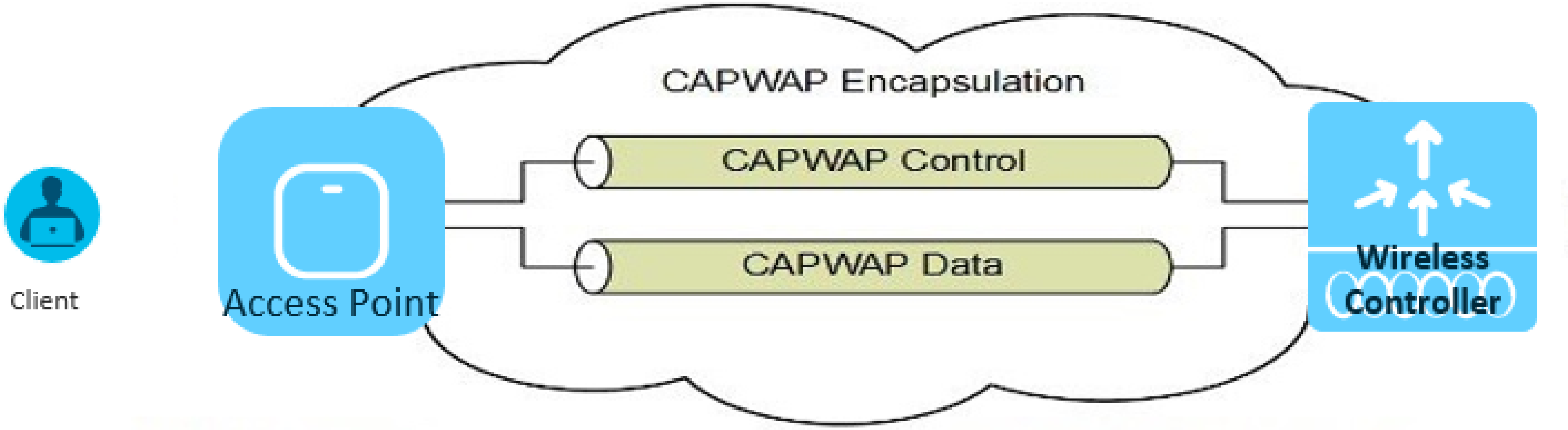


SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

CAPWAP (RFC 5415)

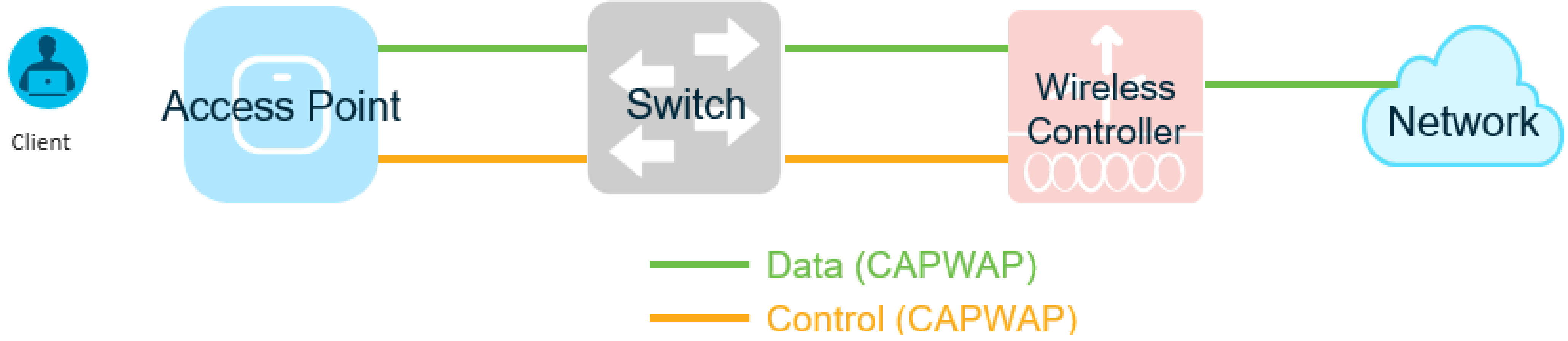
- CAPWAP: **C**ontrol **A**nd **P**rovisioning of **W**ireless **A**ccess **P**oints is used between APs and Wireless controller and based on Cisco's LWAPP over IPv4 or IPv6
- CAPWAP carries both control and data traffic between AP and Wireless Controller
  - Control plane is DTLS encrypted
  - Data plane is DTLS encrypted (encryption optional)



SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

- Control Traffic run through the controller (Centralized Control Plane)
- Data Traffic run through the controller (Centralized Data Plane)



SAMART TELCOMS

Cisco WLAN Product Portfolio Overview

Access Points

You make the power of data **possible**

Leading the industry with Wi-Fi innovations

For every major change in WLAN over the last 20+ years

Cisco
Wi-Fi
leadership

Autonomous access

Cisco CleanAir®: Interference detection and mitigation

Application Visibility and Control

Flexible Radio Assignment (FRA) (dual 5 GHz)

Intelligent Capture and real-time telemetry

1999 | 2011 | 2014 | 2016 | 2018 | 2019

Controller and coordinated access points

Connected Mobile Experiences

Hyperlocation

Software-Defined Access

What's next?

Cisco Next-Generation Wireless Stack

802.11b/g | **802.11n** | **802.11ac Wave 1** | **802.11ac Wave 2**

Aironet® 3500 Series

Aironet 3600 Series

Aironet 3700 Series

Aironet 3800 Series

Aironet 4800

ALERT
ADAPT
ACHIEVE

New Cisco Catalyst 9100 Series Access Points

Ideal for small to medium-sized deployments

Mission critical

Catalyst 9115
(Wi-Fi 6 certifiable)

- 4x4 + 4x4
- MU-MIMO, OFDMA
- Spectrum Intelligence
- 1 x 2.5 mGig
- TWT

Catalyst 9117
(Wi-Fi 6 compatible)

- 8x8 + 4x4
- MU-MIMO, OFDMA (only DL)
- Spectrum intelligence
- 1 x 5 mGig
- Non Triggered TWT
- Integrated Antenna only

Powered by Cisco RF ASIC

Catalyst 9120
(Wi-Fi 6 certifiable)

- 4x4 + 4x4
- Cisco RF ASIC for Next gen CleanAir
- Dual 5GHz, HDX
- RF signature capture
- IoT ready (Zigbee, Thread)
- Container support for IOT apps
- 1 x 2.5 mGig
- TWT

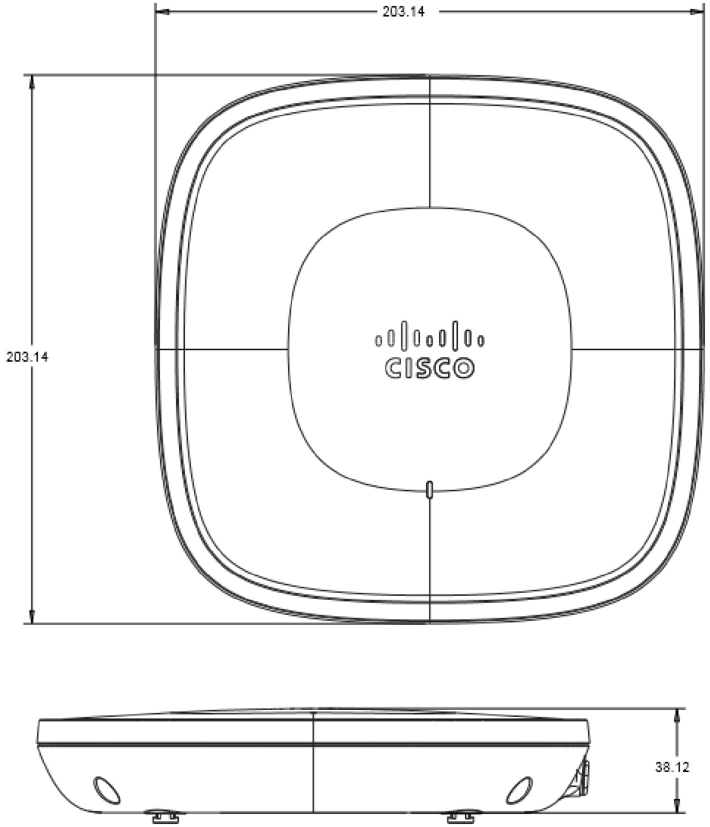
DNA Assurance with iCAP	Bluetooth 5	USB	Integrated or external antenna SKUs

SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

Dimensions and Weight comparison

SKU	Physical Dimensions	Weight
Catalyst 9115AXI	**8.0” x 8.0” x 1.5”**	1.98 lb (0.9 kg)
Catalyst 9115AXE	**8.0” x 8.0” x 1.7”**	2.43 lb (1.1 kg)
Catalyst 9117AX	**8.70” x 8.70” x 1.94”**	3.02 lb (1.4 kg)
Catalyst 9120AX	**8.5”x8.5”x1.7”**	2.87lb (1.3 kg)
AIR-AP2800	**8.66” x 8.68” x 2.17”**	3.12 lb (1.41 kg)
AIR-AP1830I	**8.3” x 8.3” x 2”**	**2.05 lb (930 grams)**
AIR-AP1850I	**8.3” x 8.3” x 2”**	**3.12 lb (1.41 kg)**



Cisco Catalyst 9117AX

You make the power of data **possible**

ALERT
ADAPT
ACHIEVE

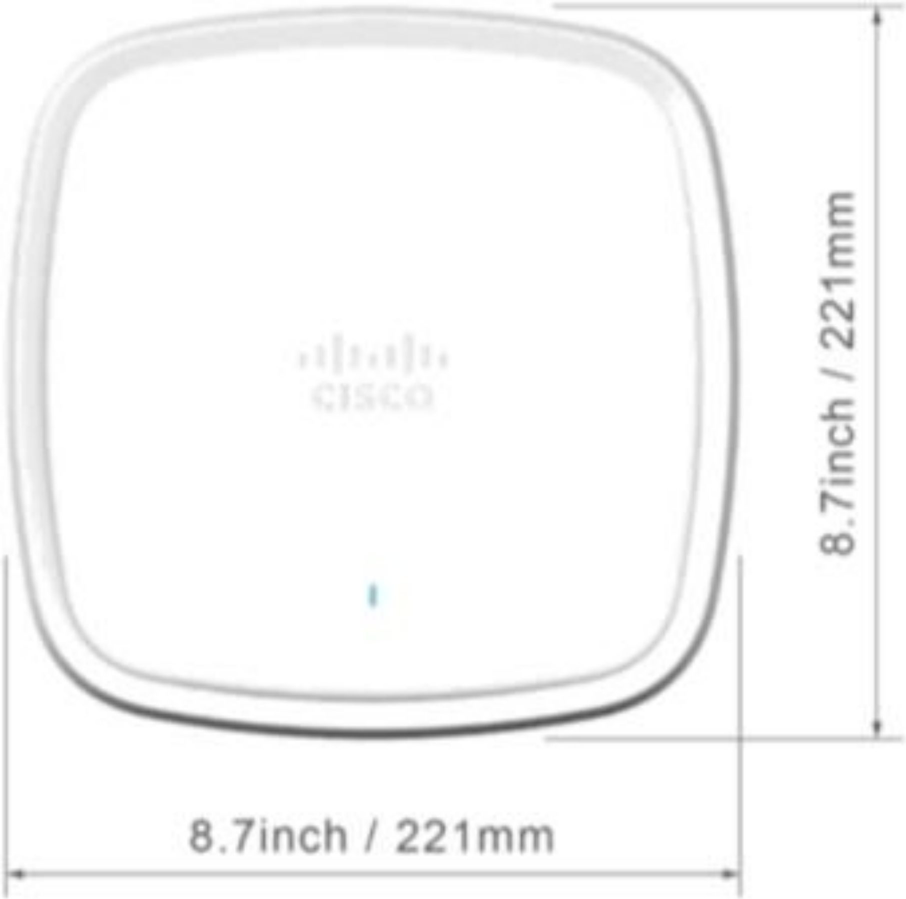
Cisco Catalyst 9117AX Series Access Points: Next-generation 8x8 802.11ax

- Next-generation 802.11ax access points with 8x8 MIMO with eight spatial streams:
  - 8x8:8 on 5 GHz with MU-MIMO and downlink OFDMA
  - 4x4:4 on 2.4 GHz with MU-MIMO and downlink OFDMA
  - Combined data rate of 10.1 Gbps

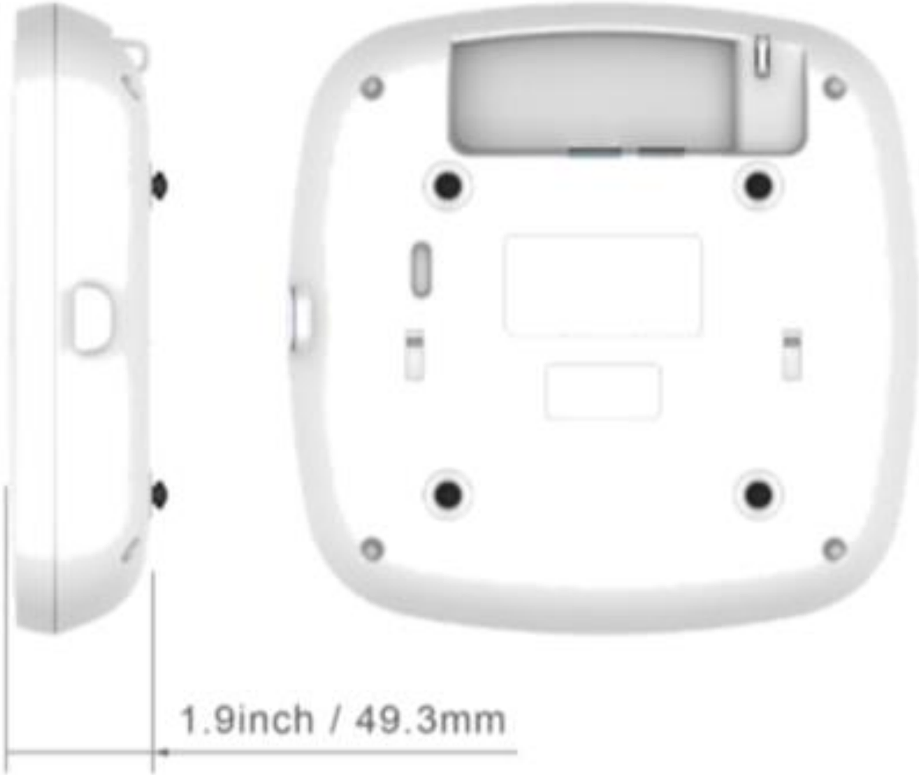
- **Cisco DNA ready**
- **Analytics enabled with Intelligent Capture**
- Built-in BLE radio (Bluetooth 5.0)
- Multigigabit Ethernet (1 Gbps, 2.5 Gbps, 5 Gbps)
- USB
- Supports up to 500 Wi-Fi devices
- Internal antenna only
- 8x8 .11ax compatible – Note: Uplink OFDMA not supported

ALERT
ADAPT
ACHIEVE

Cisco Catalyst 9117AX Series mechanicals



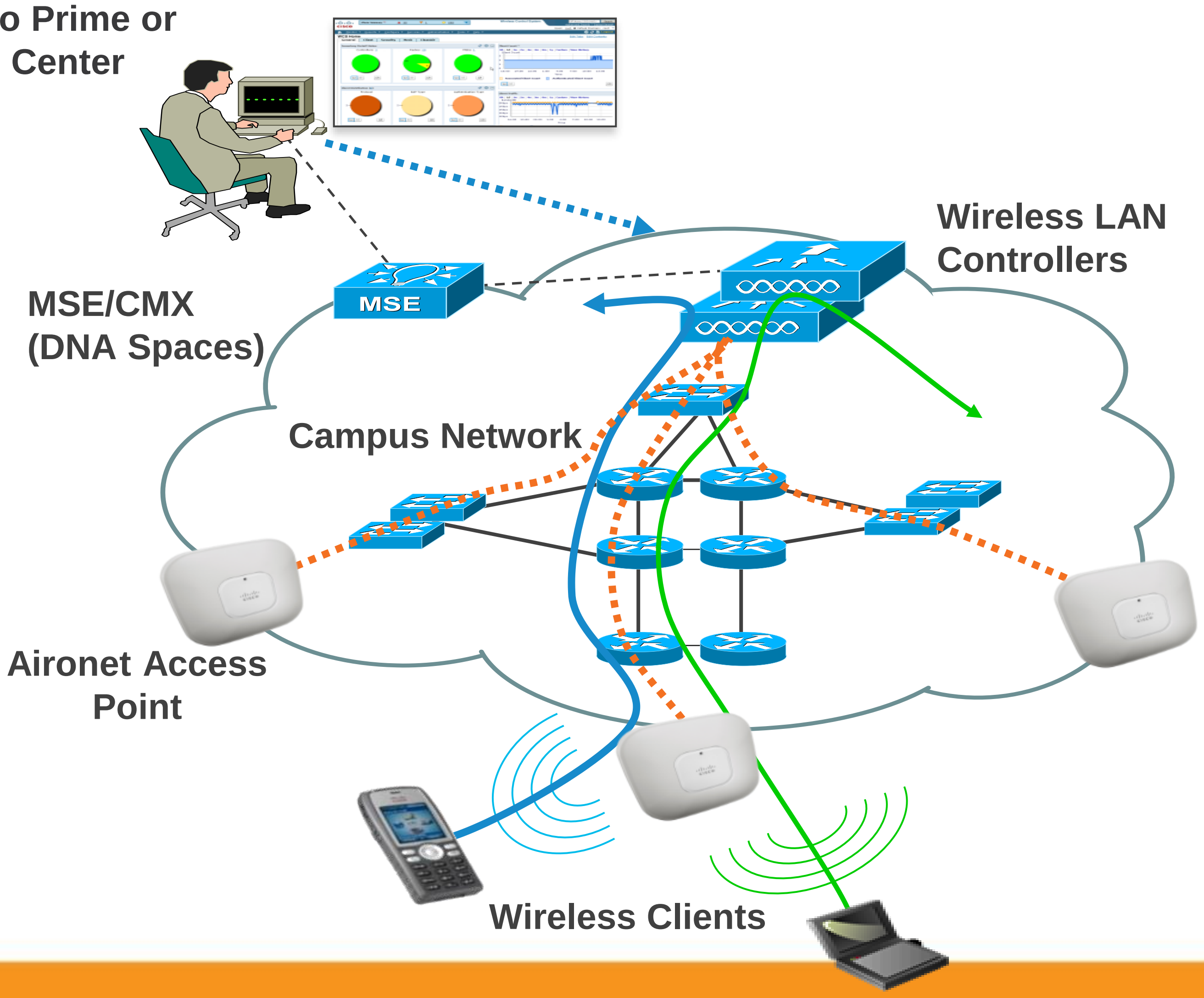
Cisco Catalyst 9117AX Series mechanicals



Wireless LAN Controllers

You make the power of data **possible**

Cisco Unified Wireless Principles



Cisco Prime or DNA Center

Wireless LAN Controllers

MSE/CMX (DNA Spaces)

Campus Network

Aironet Access Point

Wireless Clients

ALERT
ADAPT
ACHIEVE

Cisco WLAN Controller Key Functions

Centralized control of Access Points

- Provides a central management point for Access Points in an Enterprise Network, using CAPWAP protocol
  - Central point for configuration of wireless network
    - Examples: WLANs, Security, Policy, RF & Radio Parameters.
  - Performs central software upgrade for Aps
- Manages association and authentication of wireless clients
- Traffic forwarding between Wireless clients & Network
- Manages seamless roaming of clients
- Manages Radio Frequency (RF) dynamically
  - Radio Resource Management (RRM) – DCA, TPC, CHD etc.
- Helps in monitoring & troubleshooting of wireless network.

Wireless LAN Controllers

	Physical	Virtual
AireOS	Mobility Express WLC 3504 WLC 5520 WLC 8540	vWLC * _(Flex Only)_
IOS-XE	Catalyst 9800-80 Catalyst 9800-40	Catalyst 9800-CL - Private & Public

ALERT
ADAPT
ACHIEVE

New Cisco Catalyst 9800 Series Wireless Controllers

Powered by IOS XE

Open and Programmable
Trustworthy Solutions
Modular operating system

Always-on

- Software updates with no disruption
- Rolling AP upgrades
- Seamlessly add new AP models

Secure

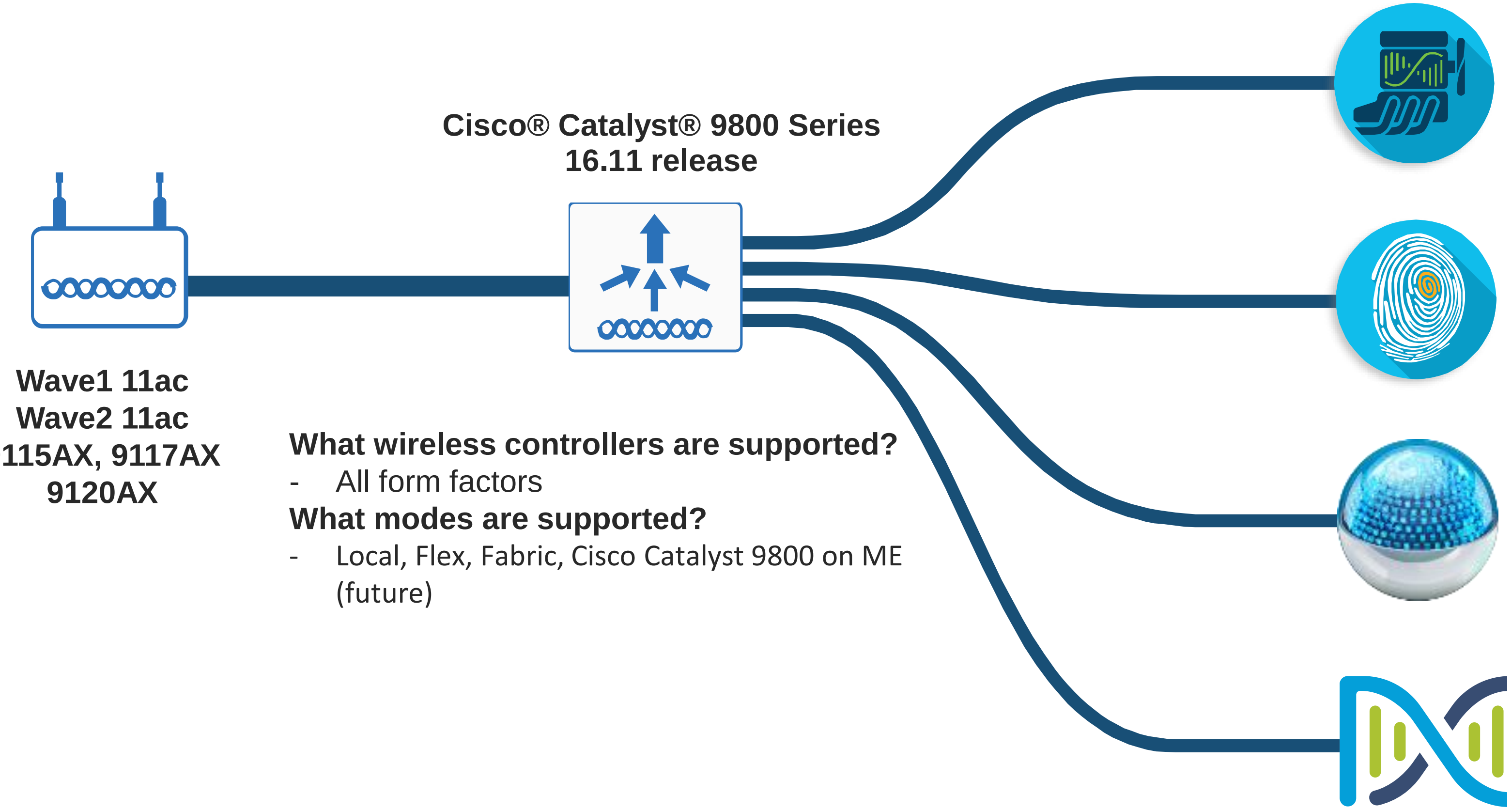
- Detect encrypted threats with ETA
- Automated macro/micro segmentation with SDA
- WPA3 Support*

Deploy Anywhere

- On-Prem, Private/Public cloud, Embed wireless on a Switch
- GovCloud ready
- Scale as you grow

SAMART TELCOMS

Cisco Catalyst 9800 interoperability



Cisco® Catalyst® 9800 Series
16.11 release

Wave1 11ac
Wave2 11ac
9115AX, 9117AX
9120AX

What wireless controllers are supported?

- All form factors

What modes are supported?

- Local, Flex, Fabric, Cisco Catalyst 9800 on ME (future)

Cisco DNA Center 1.3

- Automation
- Assurance
- Maps and topology

Cisco Identity Services Engine (ISE) 2.4 and higher

- BYOD
- Guest access

Cisco Prime® Infrastructure 3.6

-Configuration
-Monitoring

CMX 10.6.1, Cisco DNA Spaces

- See - Act - Extend
- Bluetooth Low Energy (BLE)

Catalyst 9800 Wireless Controller Portfolio (IOS-XE)

Deploy It the Way You Want It

Catalyst 9800-SW*

200 APs, 4K Clients

ENCS

KVM vmware ESXi

Catalyst 9800-CL^{+}

1000 APs, 10K Clients

aws

KVM vmware ESXi

Catalyst 9800-CL

3000 APs, 32K Clients

KVM vmware ESXi

Catalyst 9800-CL

6000 APs, 64K Clients

250 APs — 1000 APs — 2000 APs — 3000 APs — 6000 APs

Catalyst 9800-L

250 APs, 5K Clients, 5 Gbps

Catalyst 9800-40

2000 APs, 32K Clients, 40 Gbps

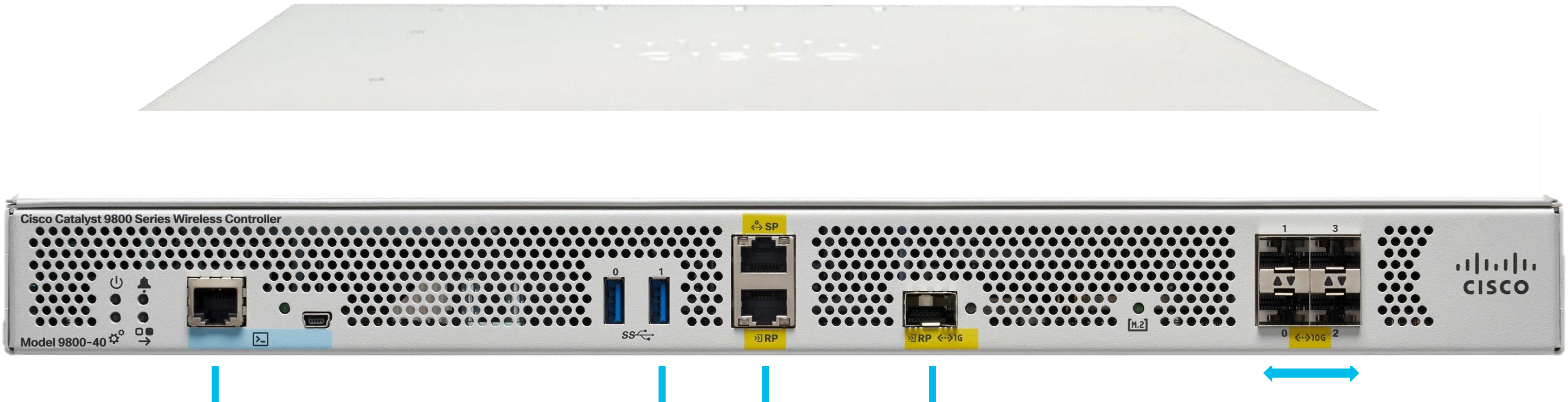
Catalyst 9800-80

6000 APs, 64K Clients, 80 Gbps

On-premise Appliance | Public or Private Cloud | On a Switch

C9800-40: industry’s first fixed wireless controller with seamless software updates

Up to 2,000 APs	Up to 32,000 Clients	40 Gbps



Console

USB 3.0

SP/RP Port

Fiber RP Port

4 x 1GE/10GE Ports

Fully programmable multi-core network processor	Support for Netflow, AVC and ETA

C9800-40-K9 Front Panel

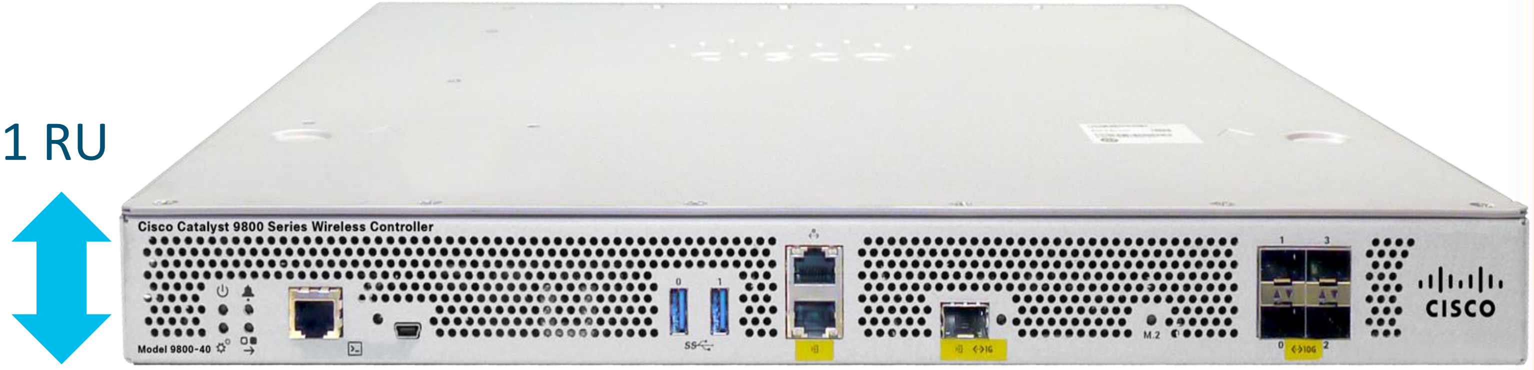
DUAL AC POWER SUPPLY

EXTERNAL INTERFACES

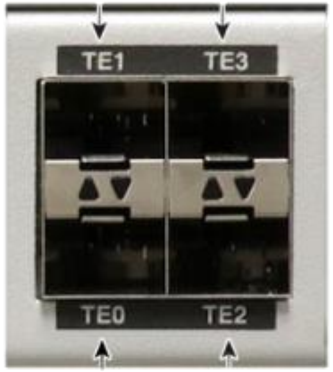
- RJ-45 Console Port
- Mini USB Console Port
- 2 External USB Ports
- RJ-45 Ethernet Management Port (SP)
- RJ-45 Ethernet Redundancy port (RP)
- SFP Gigabit RP Port
- 4 x 10GE/1GE SFP and SFP+ ports

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

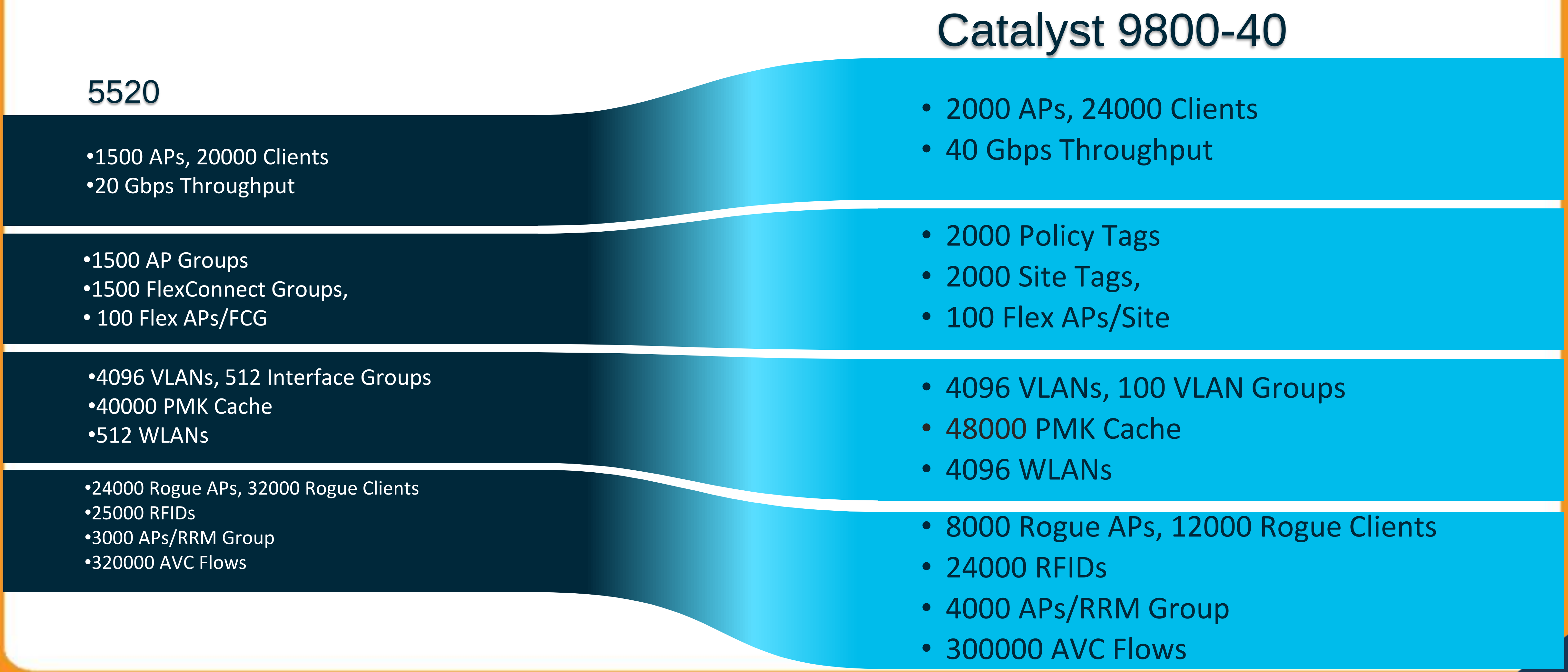
AIR-CT-5508-K9

AIR-CT-5520-K9

*compared to 30.98” (786 mm) in 5520

Evolution of Wireless Controllers

Enterprise Campus and Full-Service Branch



5520

- 1500 APs, 20000 Clients
- 20 Gbps Throughput

- 1500 AP Groups
- 1500 FlexConnect Groups,
- 100 Flex APs/FCG

- 4096 VLANs, 512 Interface Groups
- 40000 PMK Cache
- 512 WLANs

- 24000 Rogue APs, 32000 Rogue Clients
- 25000 RFIDs
- 3000 APs/RRM Group
- 320000 AVC Flows

Catalyst 9800-40

- 2000 APs, 24000 Clients
- 40 Gbps Throughput

- 2000 Policy Tags
- 2000 Site Tags,
- 100 Flex APs/Site

- 4096 VLANs, 100 VLAN Groups
- 48000 PMK Cache
- 4096 WLANs

- 8000 Rogue APs, 12000 Rogue Clients
- 24000 RFIDs
- 4000 APs/RRM Group
- 300000 AVC Flows

ALERT
ADAPT
ACHIEVE

SFP/SFP+ Support for C9800-40-K9

SFP MODULES

- GLC-BX-D
- GLC-BX-U
- GLC-LH-SMD
- GLC-SX-MMD
- GLC-ZX-SMD
- GLC-TE

Note:
SFP-GE-S, SFP-GE-L and SFP-GE-Z are End-of-Sale, and will not be officially supported

10G ports will operate in 1GE mode but will not support operation at 10/100M. Hence the 10G ports will not support the following SFPs for 10/100M:

- *GLC-GE-100FX=*
- *SFP-GE-T*
- *GLC-TE*

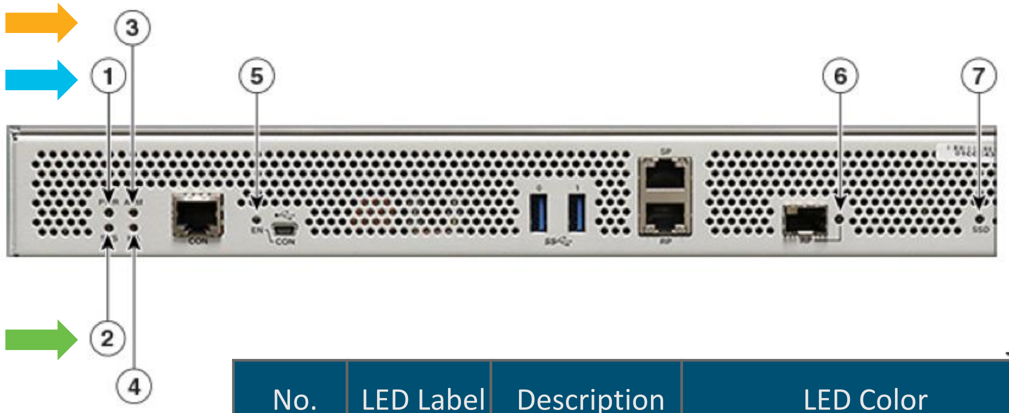
SFP+ MODULES

- SFP-10G-SR
- SFP-10G-SR-X
- SFP-10G-LR
- SFP-10G-LRM
- SFP-10G-LR-X
- SFP-10G-ER
- SFP-10G-ZR
- SFP-H10GB-ACU7M
- SFP-H10GB-ACU10M
- DWDM-SFP10G-30.33 –DWDM-SFP10G-61.41

SAMART
TELCOMS

ALERT
ADAPT
ACHIEVE

C9800-40-K9 LEDs: PWR, SYS, ALM

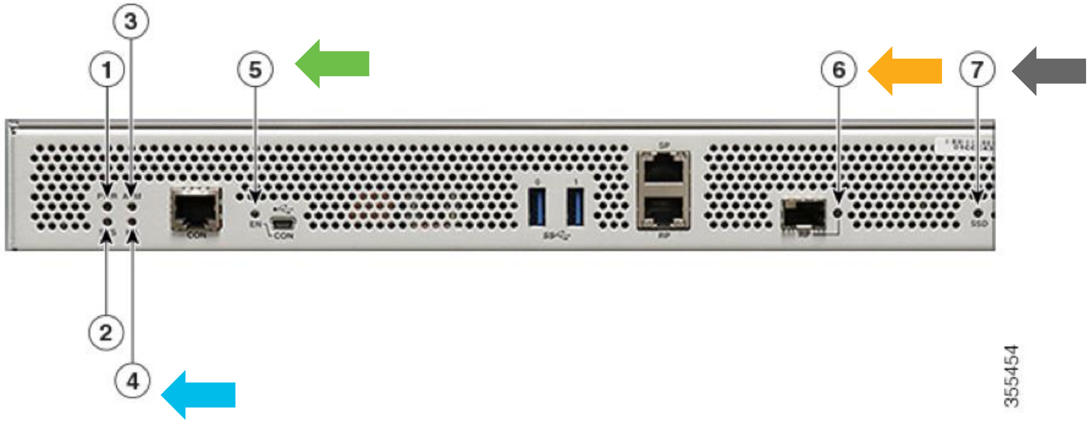


No.	LED Label	Description	LED Color	Behavior
1	PWR	Power	Green	If all the power rails are based on the specification.
2	SYS	System	On	Remains ON during IOS boot complete.
			Blinking Green	Remains blinking when IOS booting is in progress.
			Amber	Remains ON during system crash.
			Blinking Amber	Remains blinking during secure boot failure
			Off	Remains OFF during ROMMON boot.
3	ALM	Alarm	Green	Remains ON during ROMMON boot complete.
			Blinking Green	Remains blinking when system upgrade is in progress.
			Amber	Remains ON during ROMMON and SYSTEM boot ups.
			Blinking Amber	Remains blinking during temperature error and secure boot failure.
			Red	Critical Warnings

SAMART
TELCOMS

ALERT
ADAPT
ACHIEVE

C9800-40-K9 LEDs: HA, EN, LINK, SSD

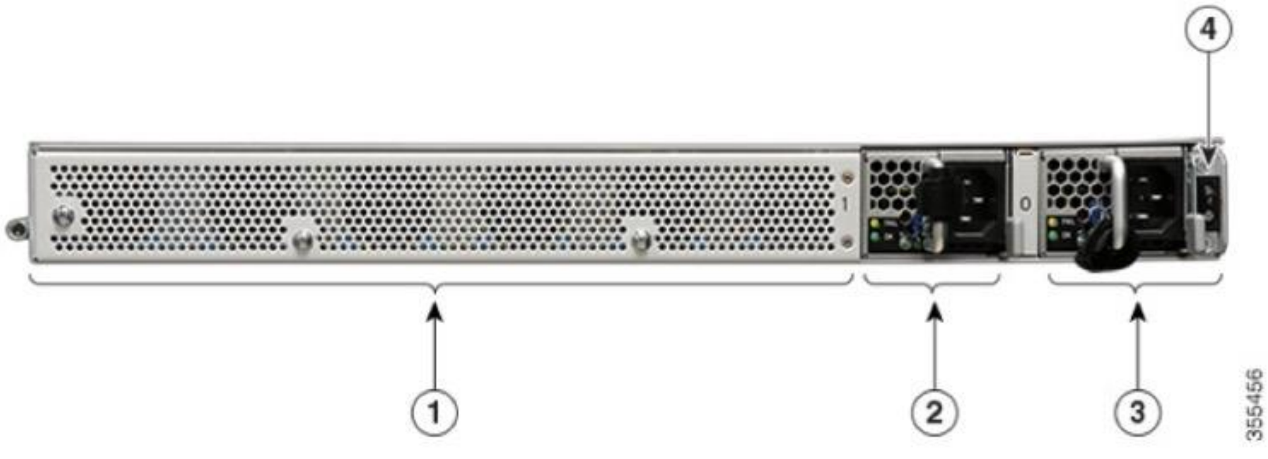


No.	LED Label	Description	LED Color	Behavior
4	HA	High Availability	Green	Remains ON when HA is active.
			Blinking Green	Remains blinking when HA Standby Hot.(Future)
			Amber	Blinks slowly when booted or HA Standby Cold. (Future)
			Blinks Fast	Blinks fast during HA maintenance. (Future)
5	EN	USB console enabled	Green	Indicates that the mini USB connector is used as the console.
6	LINK	Management	Solid Green	Indicates that the RJ-45 connector is not used as the console.
			Flash Green	Indicates that the RJ-45 connector is being used as the console.
		Built-in Module (1 SFP + Port Status of 4 LEDs with 1 per SFP)	Off	Indicates that the port is not enabled.
			Amber	Port enabled with a problem in the Ethernet link.
			Green	Port enabled with a valid Ethernet link.
7	SSD	SSD Activity	Green	Remains ON during the SSD activity.

ALERT
ADAPT
ACHIEVE

C9800-40-K9 **Rear Panel**

- Power Supply (PEM 0 and PEM 1)
  - Hot-swappable
  - FRU
  - Power Supply Fans
- Integrated Module Fans
- Power/Standby switch



1	Fans	3	Power supply (PEM 0)
2	Power supply (PEM 1)	4	Power/standby switch

Power Supply Condition	Green (OK) LED Status	Amber (FAIL) LED Status
No AC power to all power supplies	OFF	OFF
Power Supply Failure (includes over voltage, over current, over temperature and fan failure)	OFF	Red for Power Supply Failure Amber for Fan Failure
Power Supply Warning events where the power supply continues to operate (high temperature, high power and slow fan)	OFF	1Hz Blinking
AC Present/3.3VSB on (PSU OFF)	1Hz Blinking	OFF
Power Supply ON and OK	ON	OFF

SAMART
TELCOMS

Cisco Wireless Architecture

You make networking **possible**

Cisco Wireless Principles

4

Services

Cisco DNA Spaces

- Client Location
- Location Analytics
- Operation Insights

3

Network Management

DNA-Center

Prime Infrastructure

- Automation
- Assurance
- Management
- Reporting

2

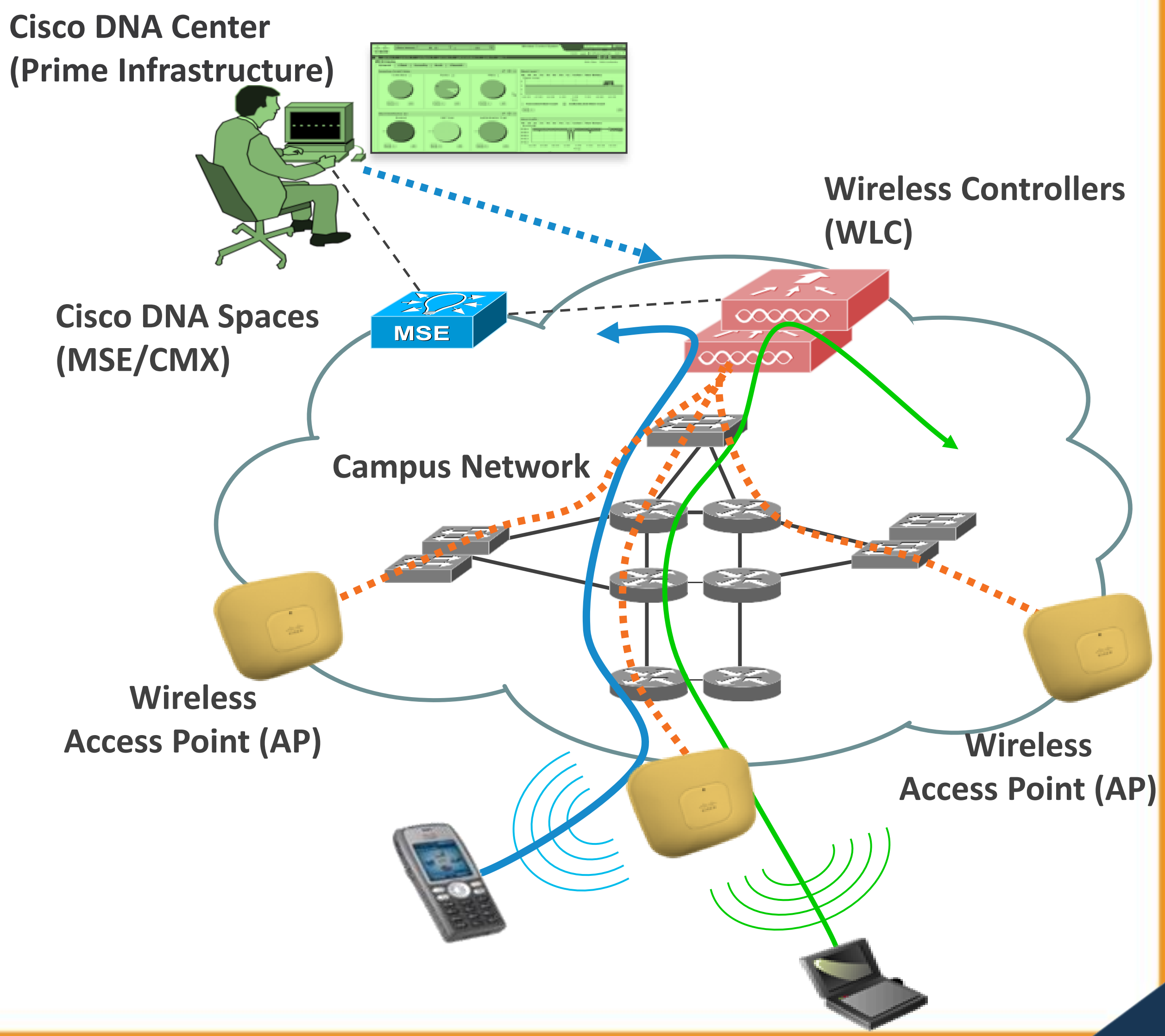
Wireless LAN Controller

- AP Management
- Radio Resource Management
- High Availability
- Client Mobility
- Security

1

Access Points

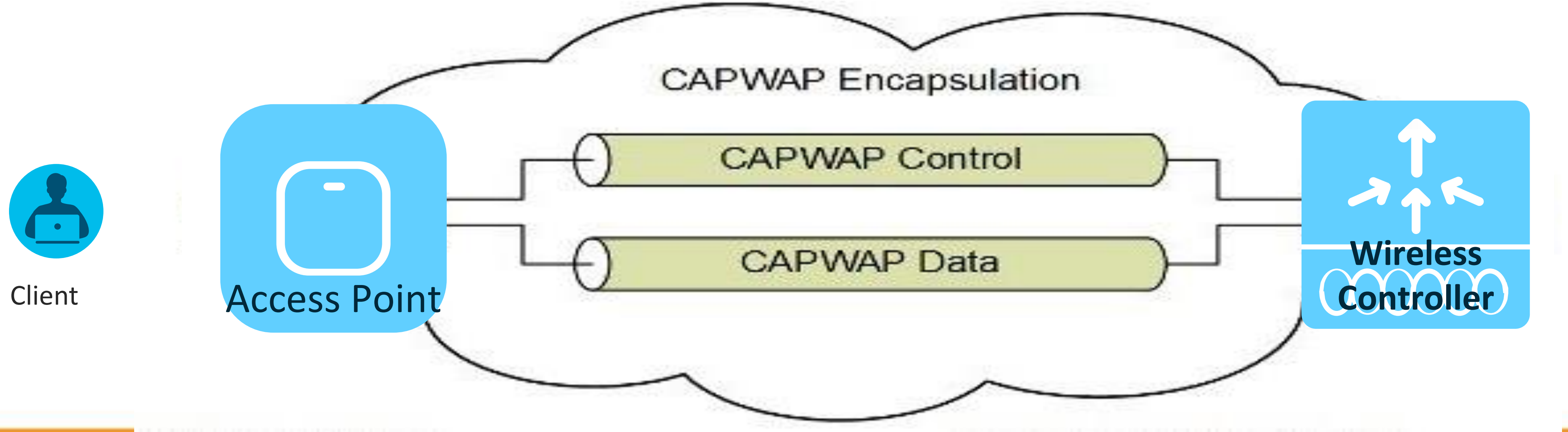
- CleanAir
- Hyperlocation
- Client Coverage
- Flexible Radio Assignment
- Over the Air Encryption



ALERT
ADAPT
ACHIEVE

CAPWAP (RFC 5415)

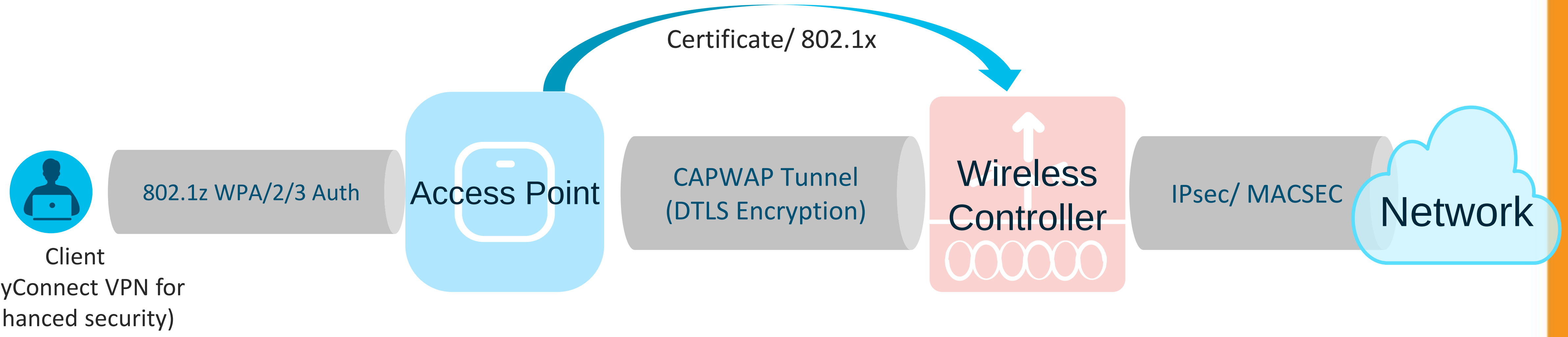
- CAPWAP: **C**ontrol **A**nd **P**rovisioning of **W**ireless **A**ccess **P**oints is used between APs and Wireless controller and based on Cisco’s LWAPP over IPv4 or IPv6
- CAPWAP carries both control and data traffic between AP and Wireless Controller
  - Control plane is DTLS encrypted
  - Data plane is DTLS encrypted (encryption optional)



SAMART
TELCOMS

ALERT
ADAPT
ACHIEVE

End-to-end Security/ Encryption



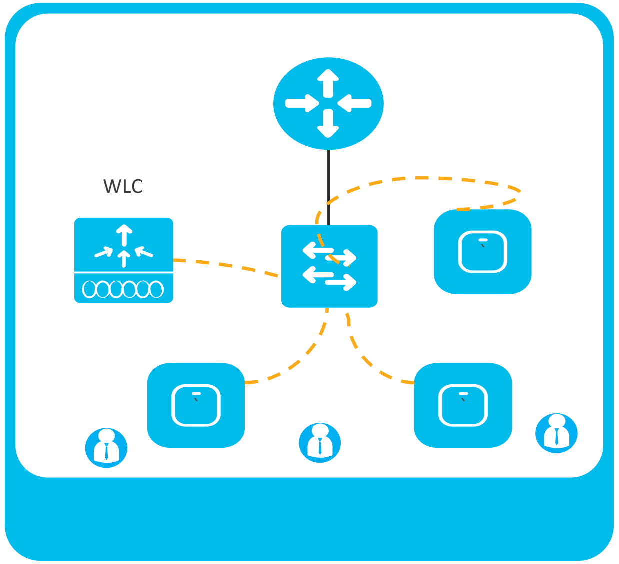
SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

Branch Wireless Deployment Options

BRANCH

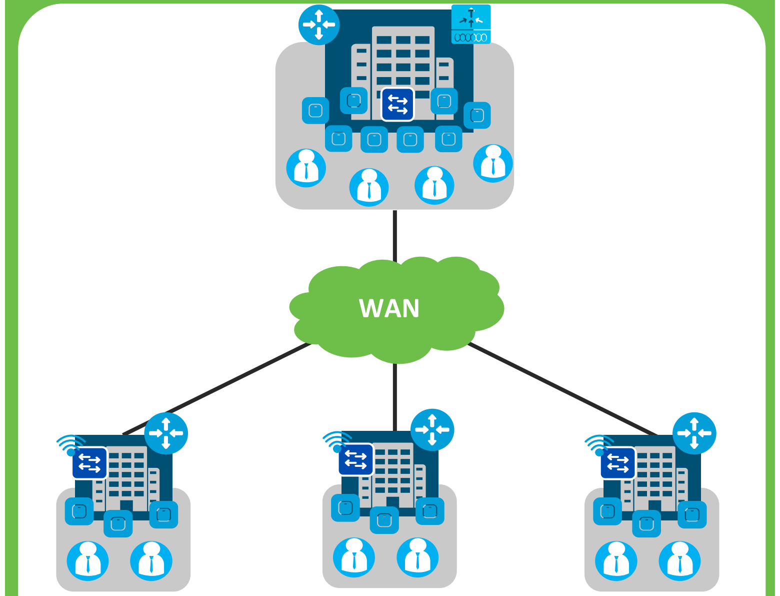
Local Controller



Local WLAN Controller

BRANCH

Flex Connect

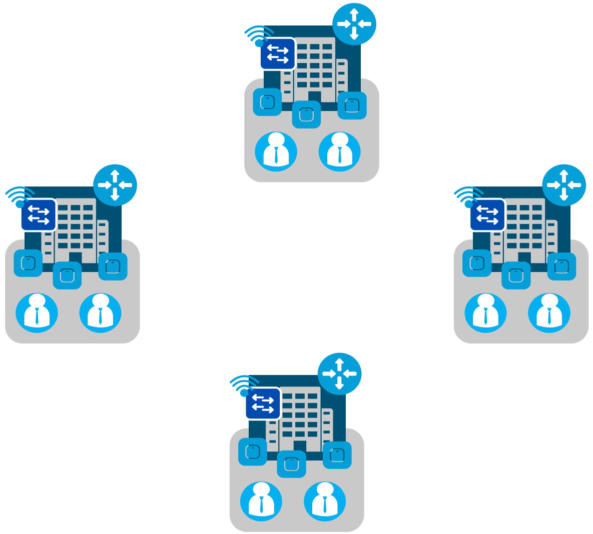


FlexConnect

Distributed Network
Highly Scalable

BRANCH

Mobility Express



Single or Multi-Site

Cisco DNA Center

Policy **Automation** **Assurance** **Security** **ISE** **CMX**

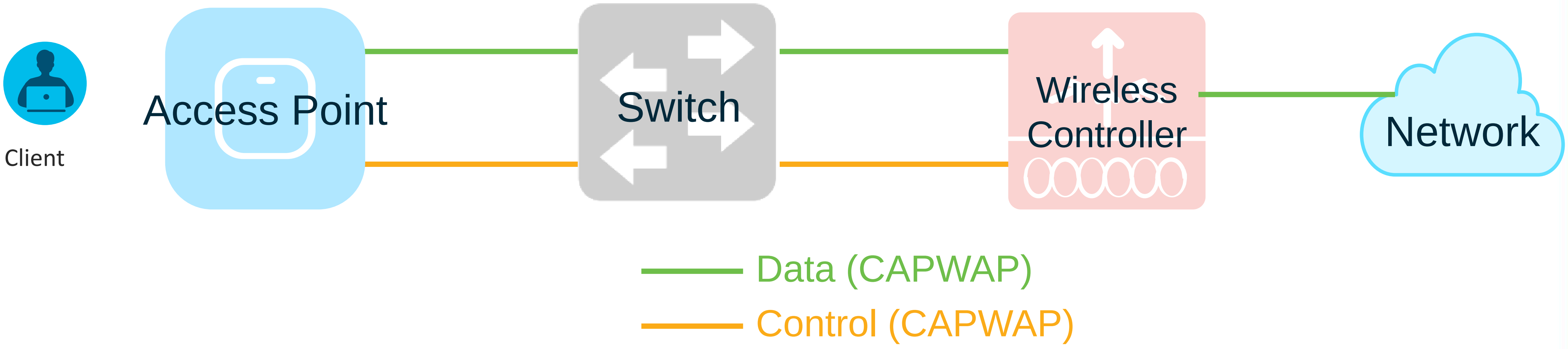
SAMART
TELCOMS

Central Mode

You make security **possible**

Central Mode

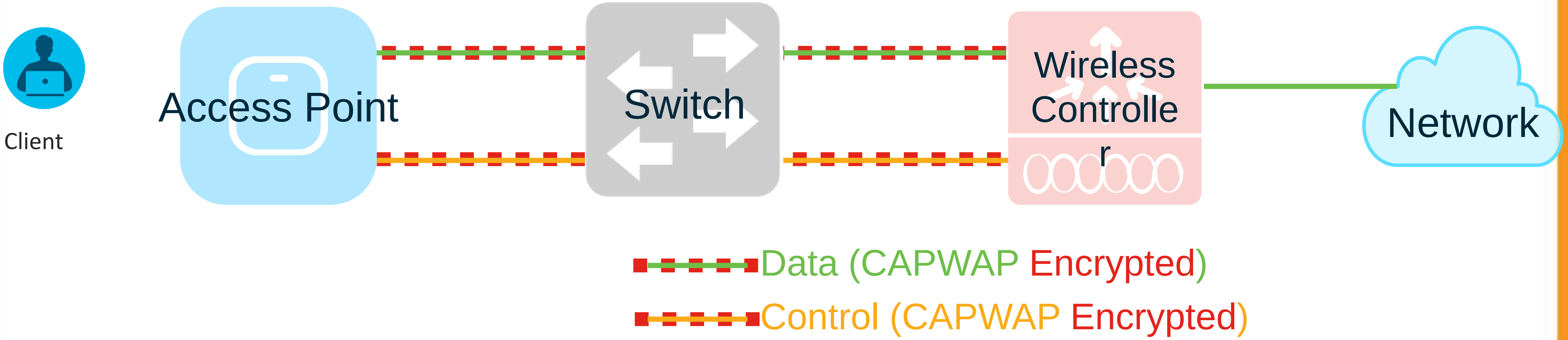
- Control Traffic run through the controller (Centralized Control Plane)
- Data Traffic run through the controller (Centralized Data Plane)



ALERT
ADAPT
ACHIEVE

Central Mode

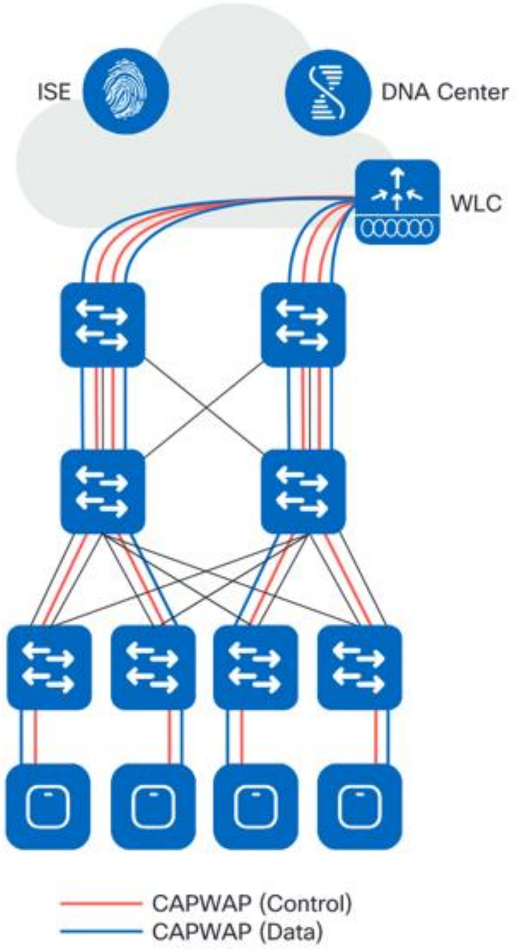
- Control Traffic run through the controller (Centralized Control Plane)
- Data Traffic run through the controller (Centralized Data Plane)



SAMART
TELCOMS

ALERT
ADAPT
ACHIEVE

Why Centralized Wireless Deployment?



- Simple IP Addressing and mobility
  - All wireless client traffic is switched at the WLC
  - Client IP addressing & VLAN(s) defined on the WLC
  - Client Layer 3 roaming without reassigning an address
- Single point of connection to the wired network
  - Easier to apply security & QoS policies for wireless users
- Simplified Overlay Design
  - Traffic is tunnelled (using CAPWAP Protocol) from AP to WLC
  - Can be deployed on top of *any* wired infrastructure
- Throughput governed by WLC capabilities

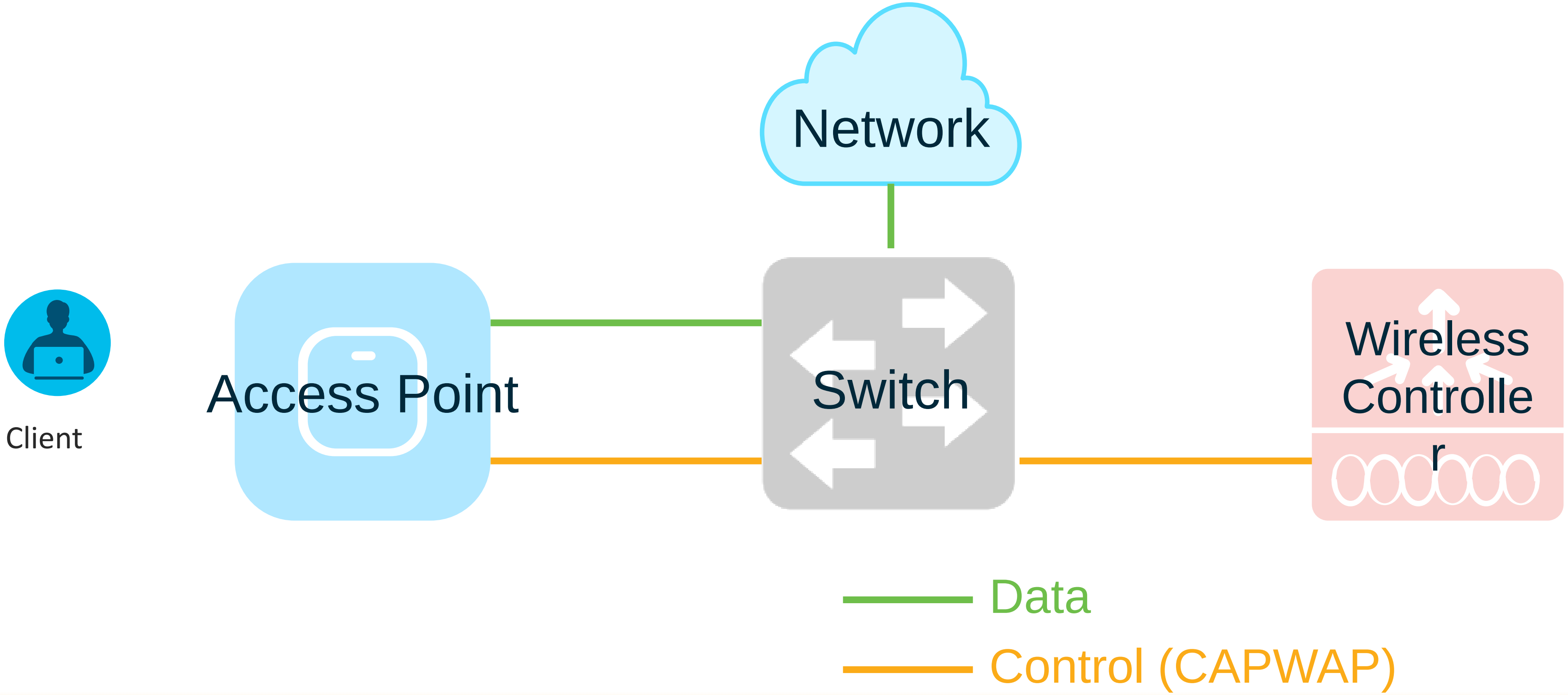
FlexConnect

You make security **possible**

ALERT
ADAPT
ACHIEVE

FlexConnect Deployment

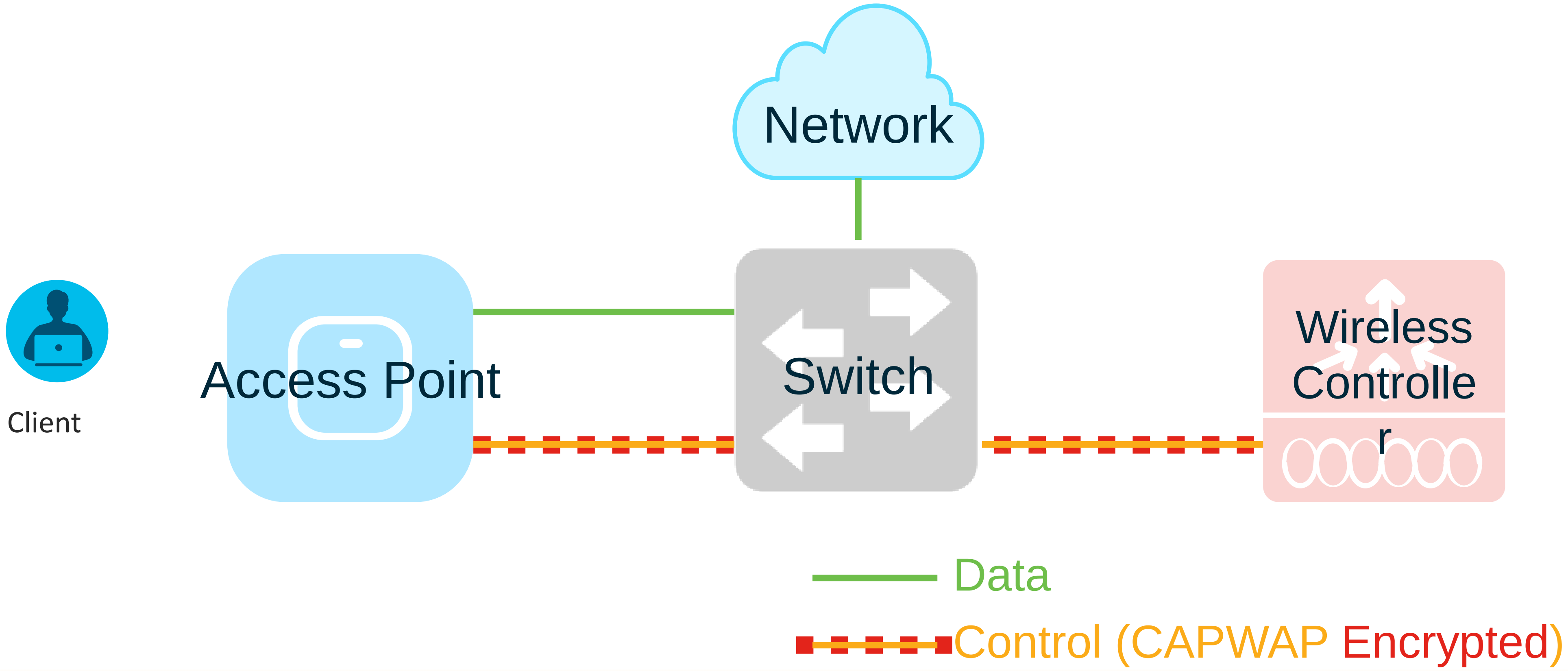
- Control Traffic run through the controller (Centralized Control Plane)
- Data Traffic bypasses controller and directly forwarded from switch (Distributed Data Plane)



SAMART TELCOMS

FlexConnect Deployment

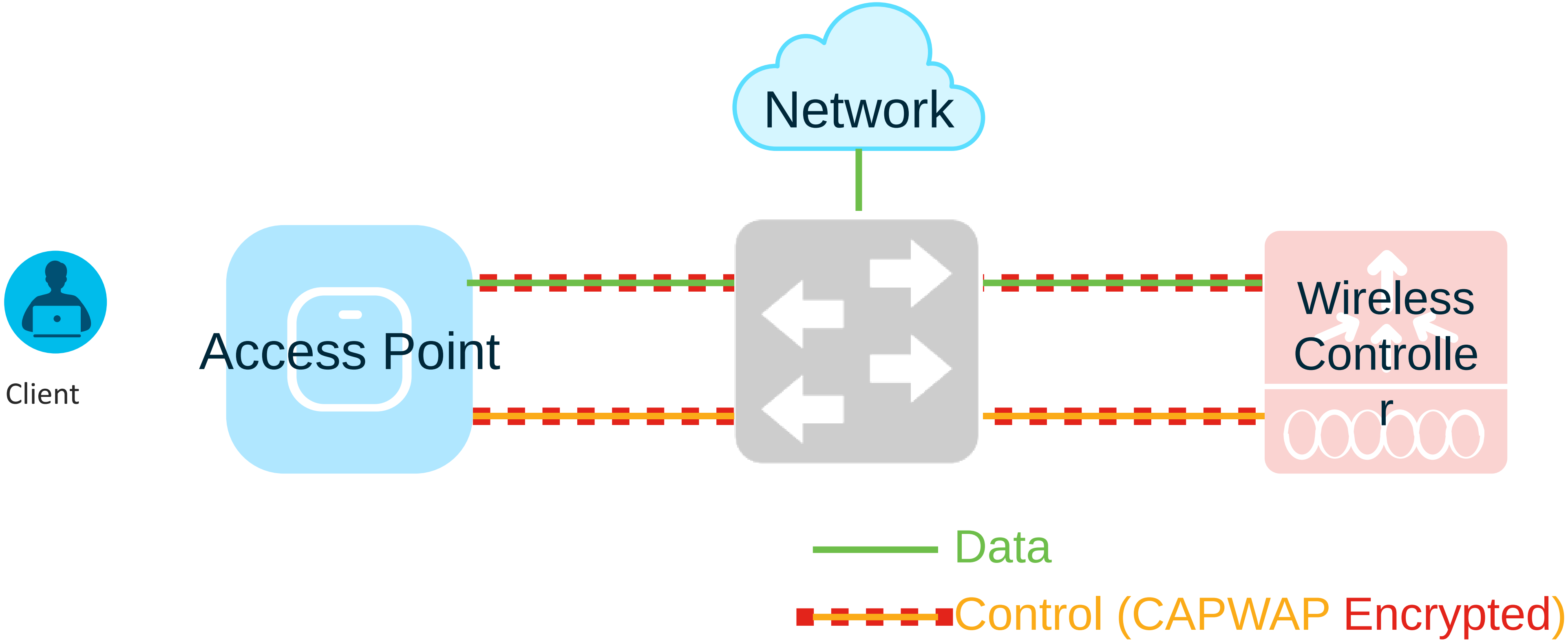
- Control Traffic run through the controller (Centralized Control Plane)
- Data Traffic bypasses controller and directly forwarded from switch (Distributed Data Plane)



ALERT
ADAPT
ACHIEVE

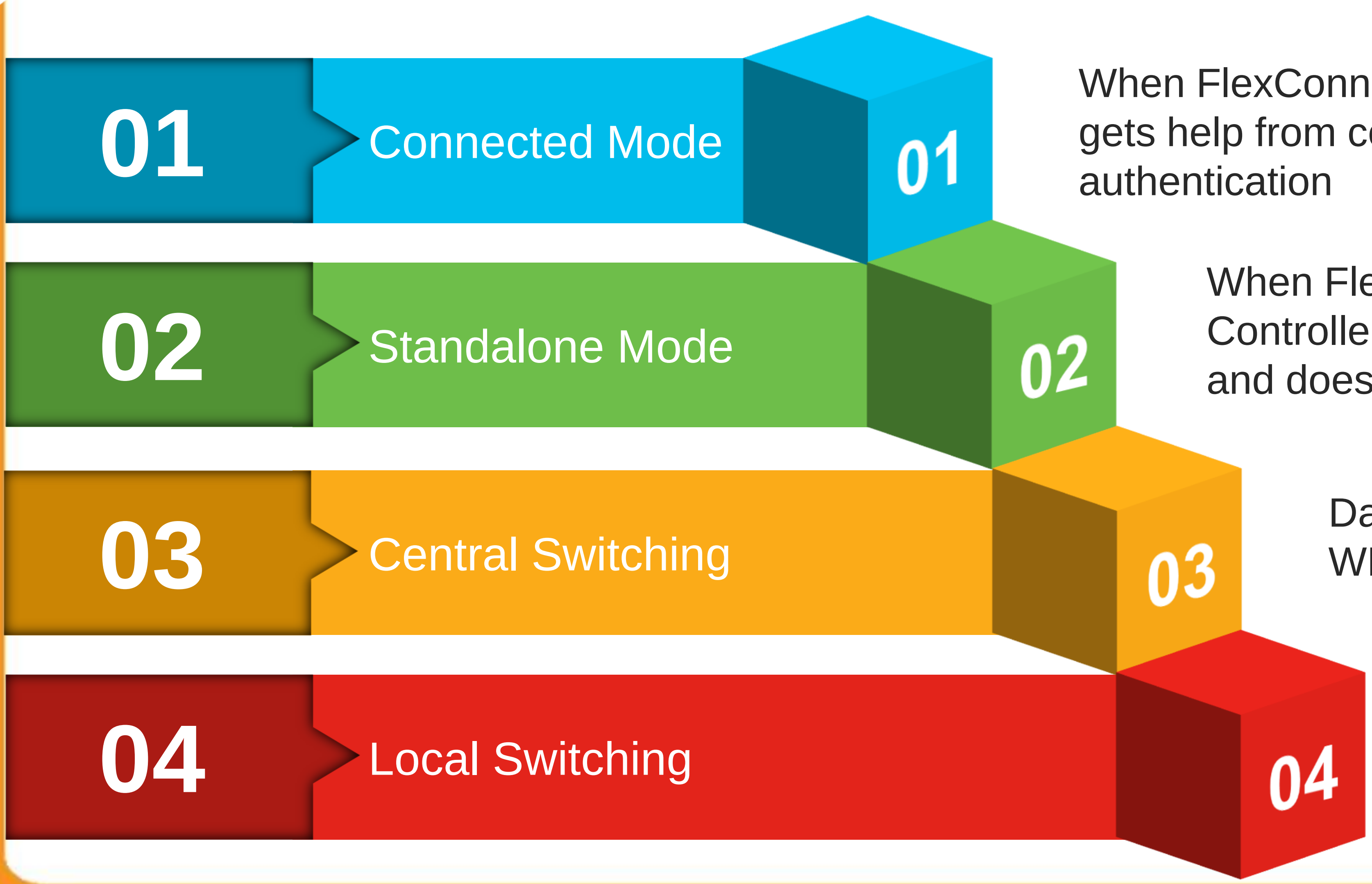
FlexConnect Deployment

- Control Traffic run through the controller (Centralized Control Plane)
- Data Traffic bypasses controller and directly forwarded from switch (Distributed Data Plane)
  - *Data Traffic run though controller (ACL/ AAA Override for Centralized Data Traffic)*



SAMART
TELCOMS

FlexConnect Terminology/Glossary



01 Connected Mode

When FlexConnect AP **can reach** Controller, it gets help from controller to complete client authentication

02 Standalone Mode

When FlexConnect AP **cannot reach** Controller, it goes into standalone mode and does client authentication by itself

03 Central Switching

Data traffic i**s tunneled back** to WLC for an SSID

04 Local Switching

Data traffic **is switched onto local VLANs** for an SSID

ALERT
ADAPT
ACHIEVE

Flex Connect Design Considerations

WAN Limitation Apply

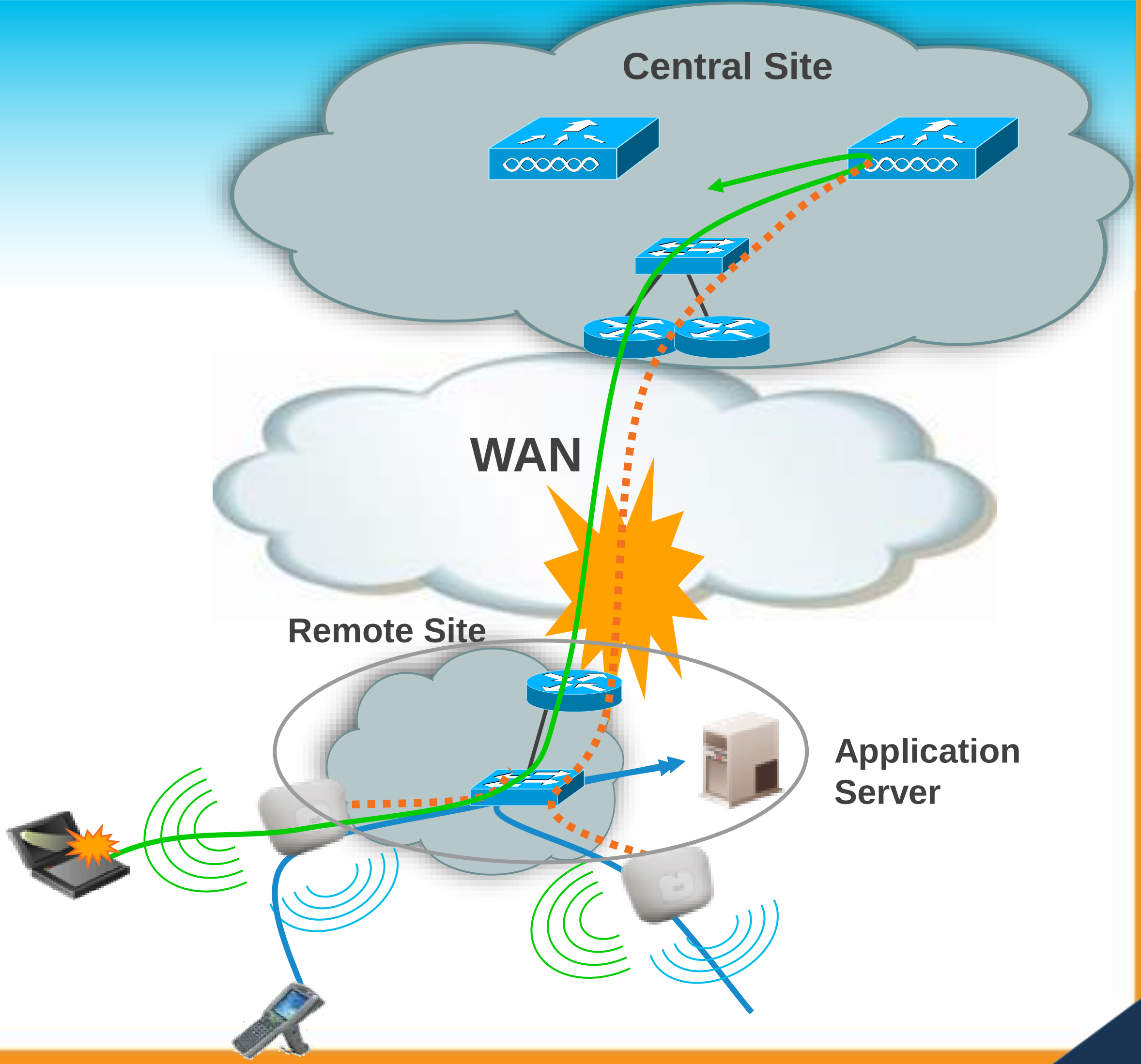
Deployment Type	WAN Bandwidth (Min)	WAN RTT Latency (Max)	Max APs per Branch	Max Clients per Branch
Data	64 kbps	300 ms	5	25
Data	640 kbps	300 ms	50	1000
Data	1.44 Mbps	1 sec	50	1000
Data+Voice	128 kbps	100 ms	5	25
Data+Voice	1.44 Mbps	100 ms	50	1000
Monitor	64 kbps	2 sec	5	N/A
Monitor	640 kbps	2 sec	50	N/A

It is highly recommended that the minimum bandwidth restriction remains 24 Kbps per AP with the round trip latency no greater than 300 ms for data deployments and 100 ms for Data + Voice deployments.

FlexConnect Resiliency - WAN Failure

WAN Failure

- FlexConnect APs will go to Standalone mode
  - No impact for locally switched SSIDs
  - Disconnection of centrally switched SSIDs clients
- Static authentication keys are locally stored in FlexConnect AP
- Lost Features
  - RRM, WIDS, location, other AP modes
  - Web authentication, NAC



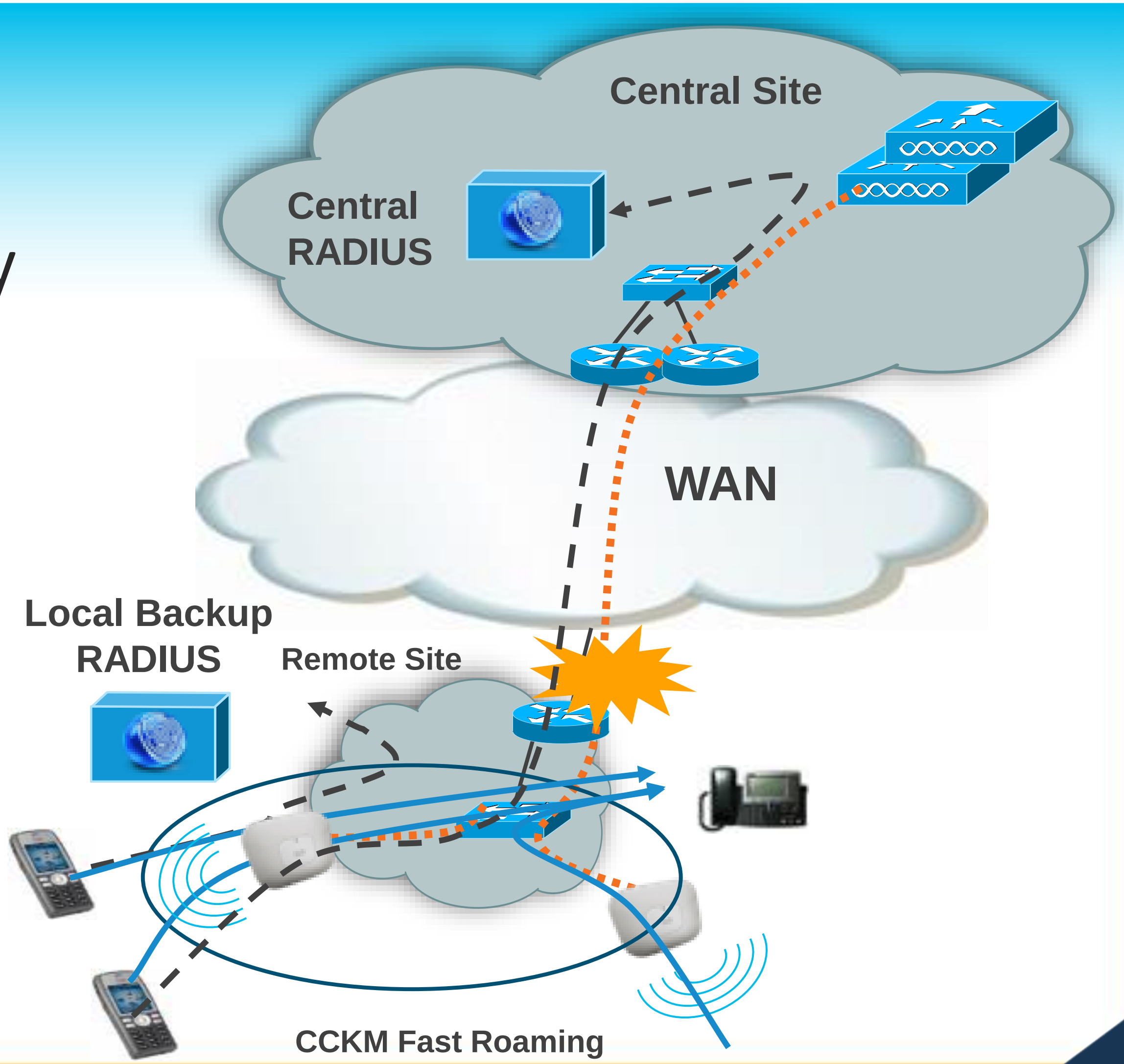
ALERT
ADAPT
ACHIEVE

FlexConnect – AAA Survivability

Local Backup RADIUS

Local Backup RADIUS

- Normal authentication is done centrally
- On WAN failure, AP goes to Standalone mode and authenticates new clients with locally defined RADIUS server
- Existing connected clients stay connected
- Clients can roam with
  - CCKM fast roaming, or
  - Re-authentication

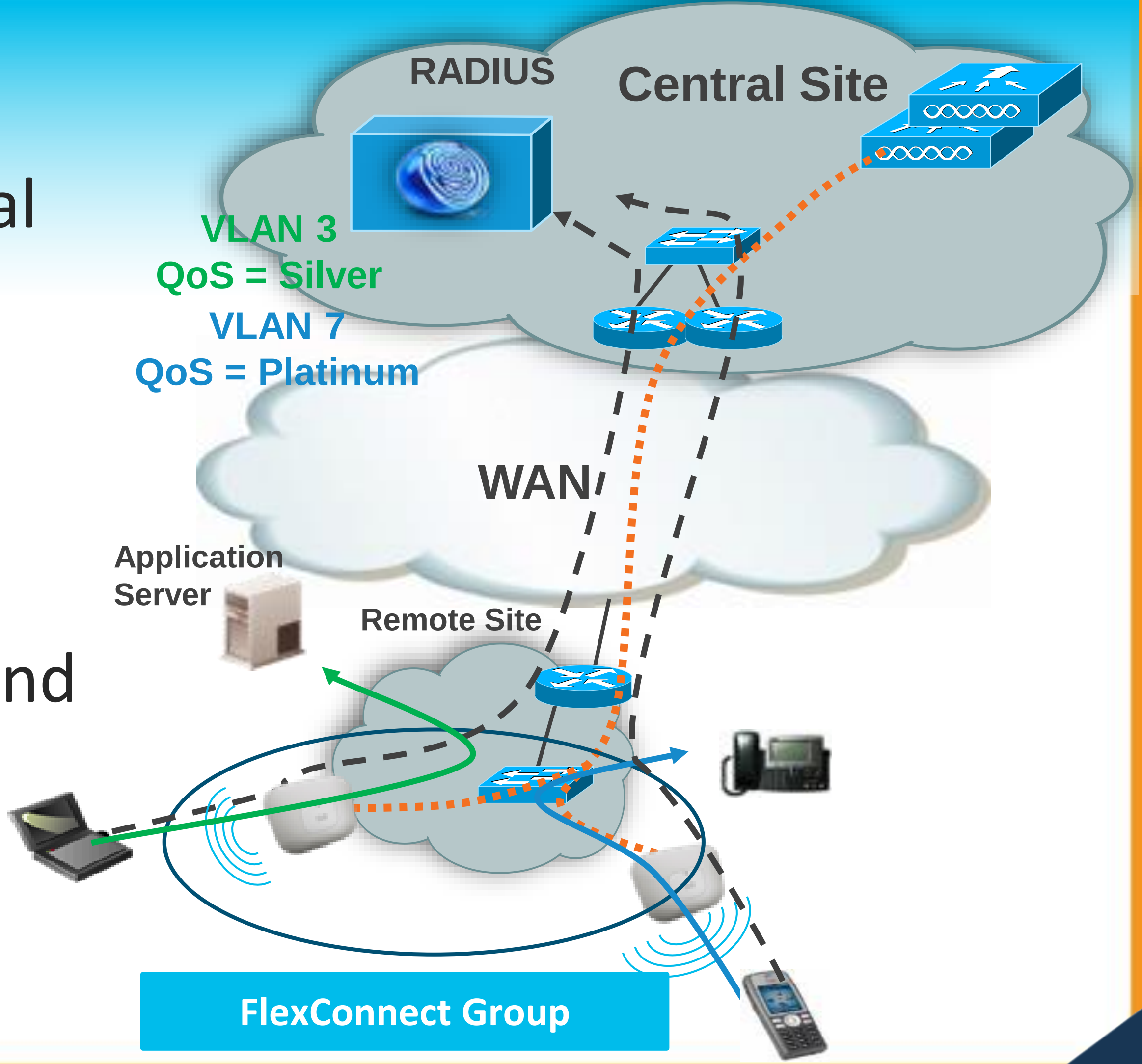


SAMART TELCOMS

FlexConnect AAA VLAN Override

Description

- AAA VLAN Override with local or central authentication
- Up to 16 VLANs per FlexConnect AP
- VLAN ID must be enabled per AP or FlexConnect Group
- Consistent configuration between AP and switch port required

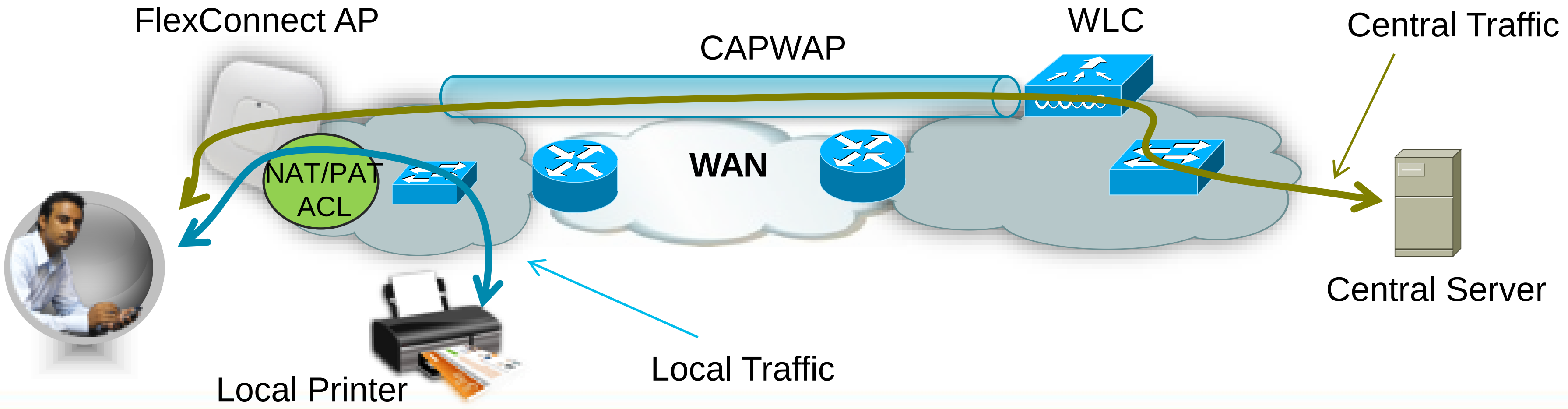


ALERT
ADAPT
ACHIEVE

FlexConnect ACL – Split Tunneling

Overview

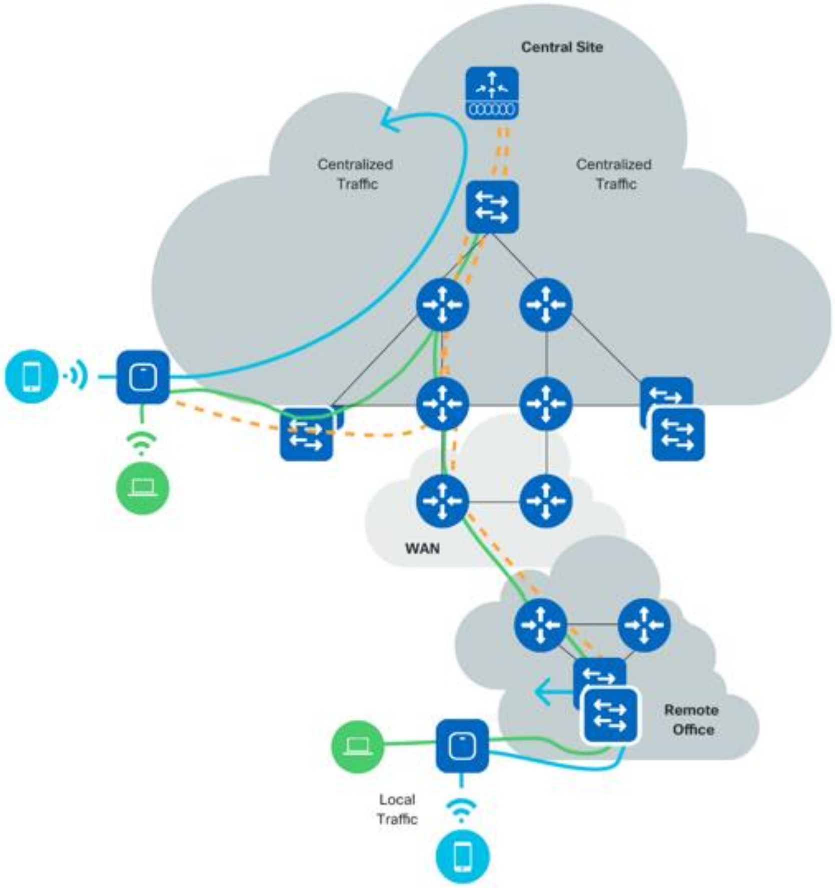
- Split tunneling allow some traffic to be locally switched although the WLAN is defined as centrally switched
- Split tunneling is using a NAT/PAT feature with ACL to perform the local switching
- Split tunneling is using the AP IP address for the NAT/PAT feature



SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

Why FlexConnect Wireless Deployment?



- WAN Distributed Branch Offices, with resiliency
  - Survivability across WAN for small, medium & large sites (client data & authentication)
- Optimized Control and Data Planes
  - Client data traffic can be switched locally, while APs are managed centrally
  - Throughput not governed by central WLC
- Efficient AP Upgrade across WAN
  - With the Smart Image Upgrade, software only sent to Master AP, reducing WAN bandwidth requirements

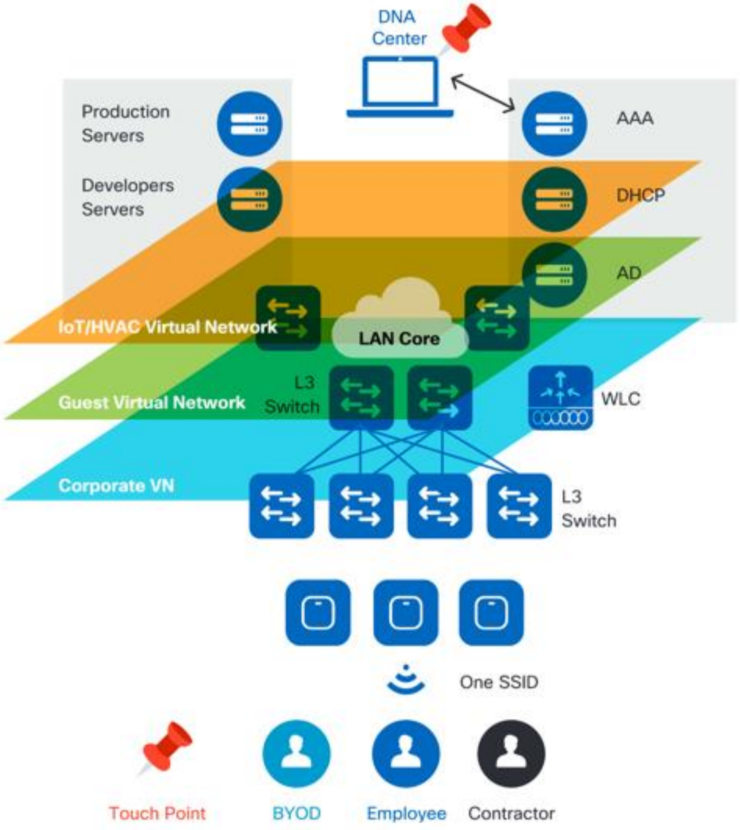
SAMART TELCOMS

SD Access

(SDA, Campus Fabric)

You make security **possible**

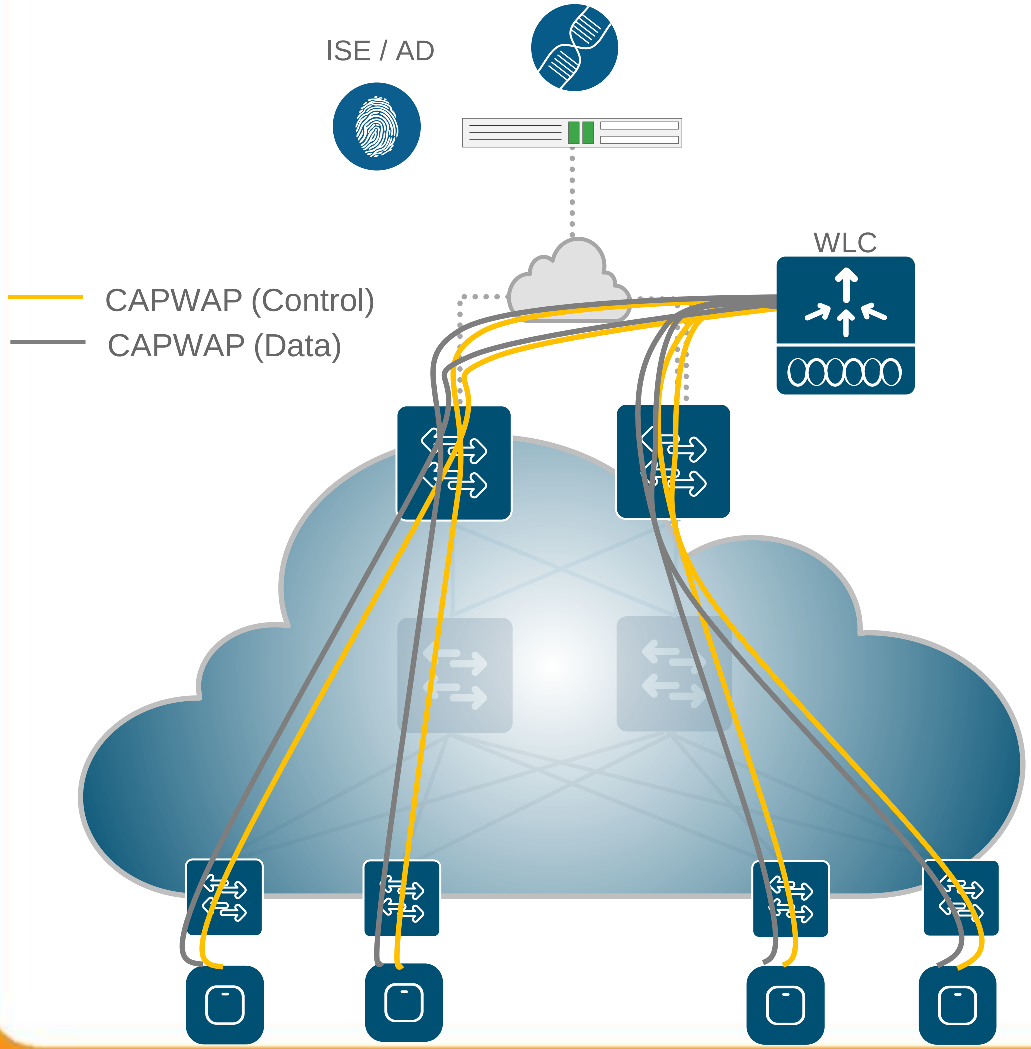
Software Defined Access (SDA)



- Simplifying Data, Control and Management Planes
  - Control Plane centralized at WLC
  - Forwarding (Data) Plane separated from services plane (reside in different fabrics)
    - Data plane is distributed
  - Cisco DNA Center single management touchpoint
- Simplified Policy
  - Separation of policy (QoS, security etc.) from client IP address / location
- Seamless Roaming Domain
  - Stretch client subnet without extending same VLAN everywhere

ALERT
ADAPT
ACHIEVE

Centralized Wireless Network Strengths



Simplified operations?	Yes with WLC
Network Overlay?	CAPWAP
L3 roaming across Campus?	WLC as Mobility Anchor
Simplified IP addressing?	WLC as mobility Anchor
Guest traffic segmentation?	Foreign-Anchor

SAMART TELCOMS

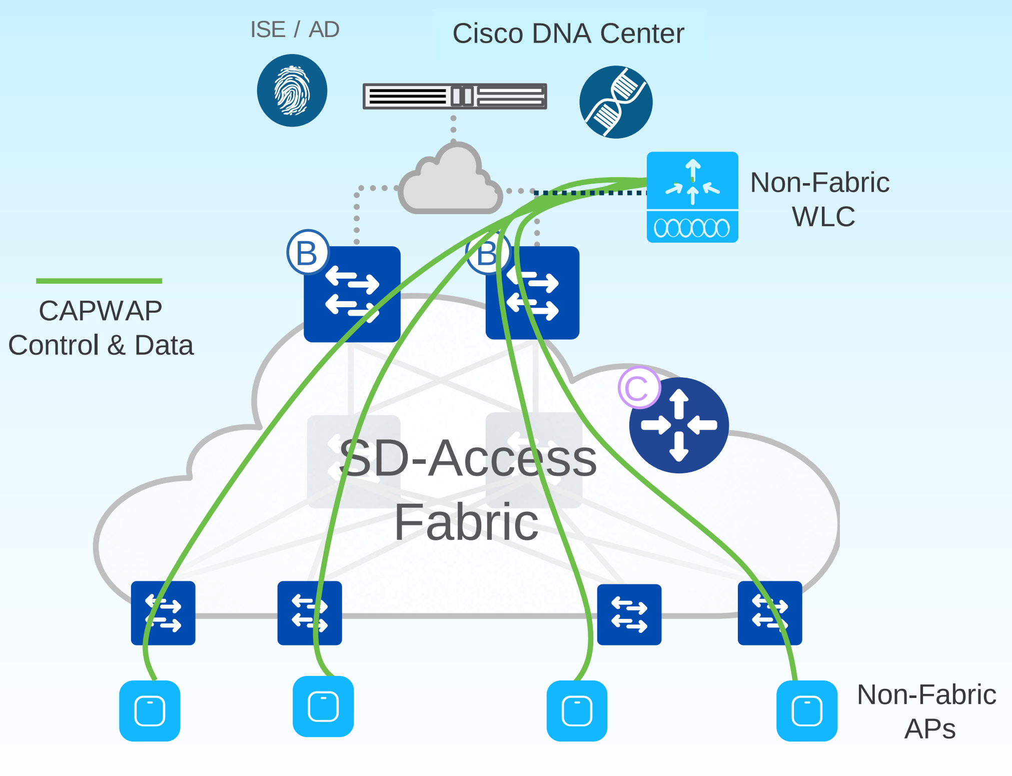
Wireless in SDA

You make security **possible**

ALERT
ADAPT
ACHIEVE

Wireless on top of SDA Fabric

CUWN wireless Over The Top (OTT)

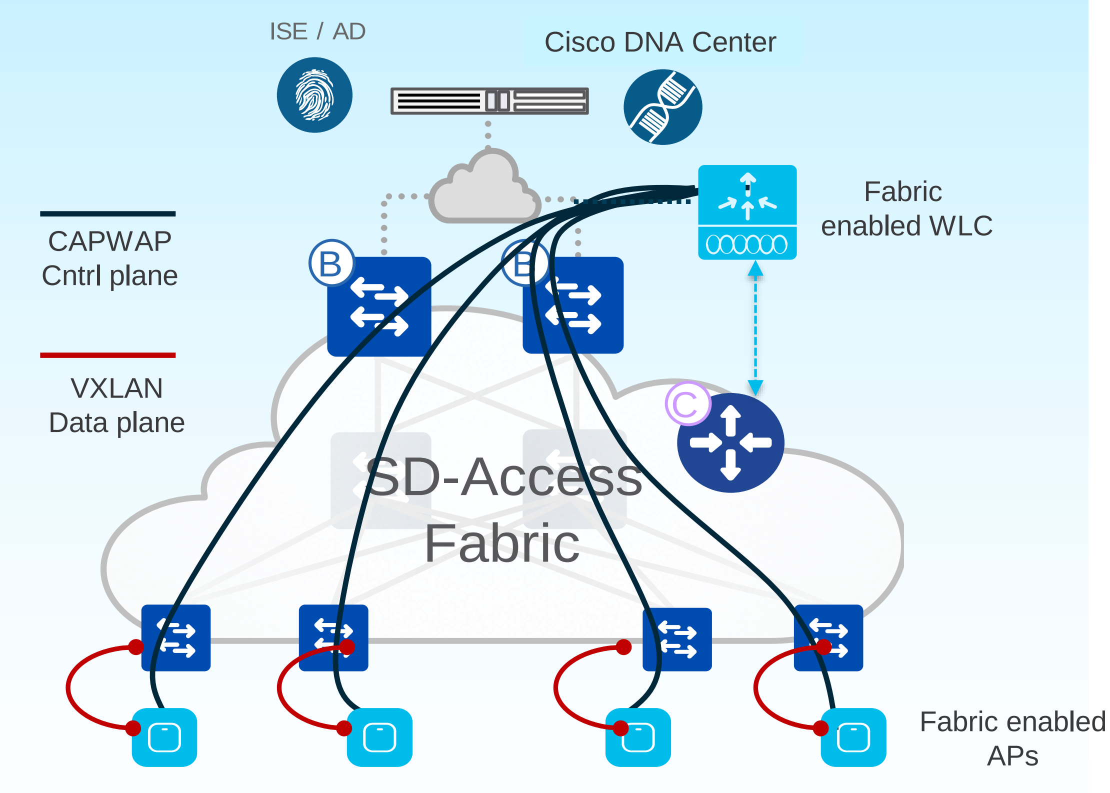


- CAPWAP for Control Plane and Data Plane
- SDA Fabric is just a transport
- Supported on any WLC/AP software and hardware
- **Only Centralized mode was supported at FCS**

- **No SDA advantages for wireless**
- Migration step to full SD-Access
- Customer wants/need to first migrate wired (different Ops teams managing wired and wireless, get familiar with Fabric, different buying cycles, etc.) and leave wireless “as it is”
- Customer cannot migrate to Fabric yet (older APs, need to certify the new software, etc.)

SD-Access Wireless: True integration in Fabric

SD-Access Wireless

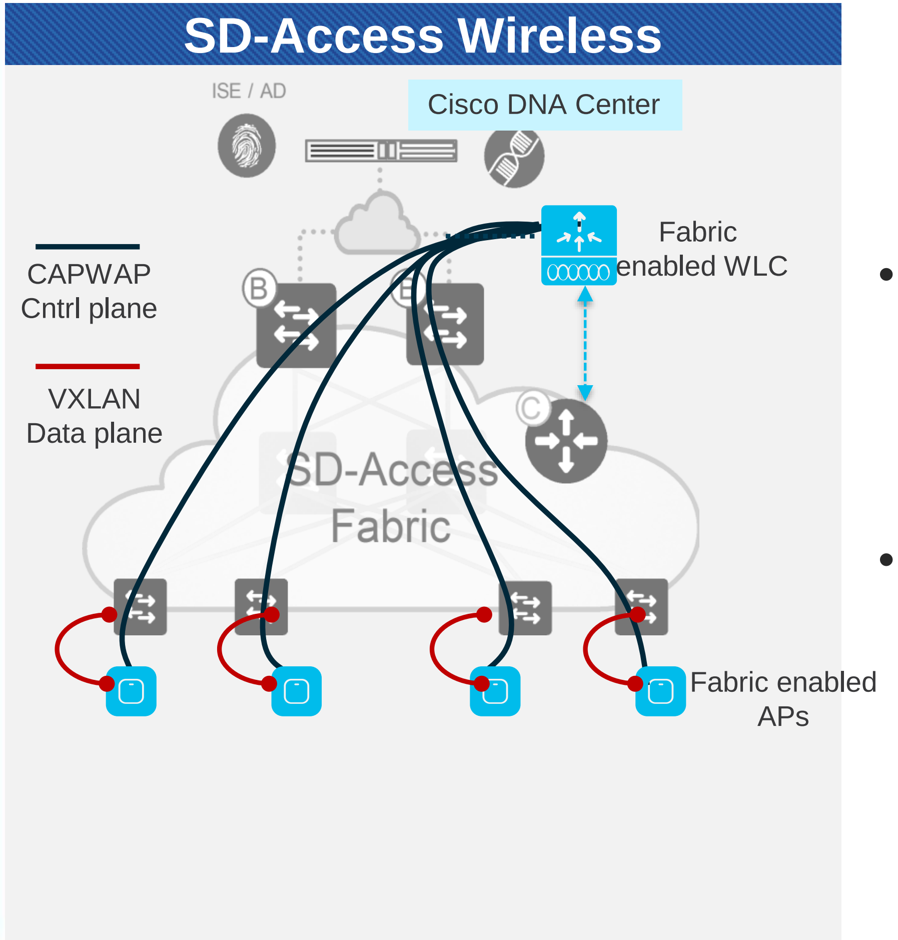


- CAPWAP Control Plane, VXLAN Data plane
- WLC/APs integrated in Fabric, SD-Access advantages
- Requires software upgrade (8.5+)
- Optimized for 802.11ac Wave 2 APs

- True wireless integration with Fabric
- Provides all the advantages of SDA for wireless clients:
  - Full automation with Cisco DNA Center
  - Hierarchical segmentation (VRF and SGT)
  - Same policy as wired
  - Distributed Data Plane with no drawbacks
  - Optimized traffic path for Guest
- Recommended option

ALERT
ADAPT
ACHIEVE

Why use SD-Acess?



- Automation
  - Unified Wired-Wireless automation for design and deployment
- Segmentation
  - Macro-Micro Segmentation for enhanced security (Common policies for Wired-Wireless)
- Scale
  - Distributed data plane for Wireless (No restriction with Wireless Controller Data throughput)

SAMART TELCOMS

AP Groups

You make multicloud **possible**

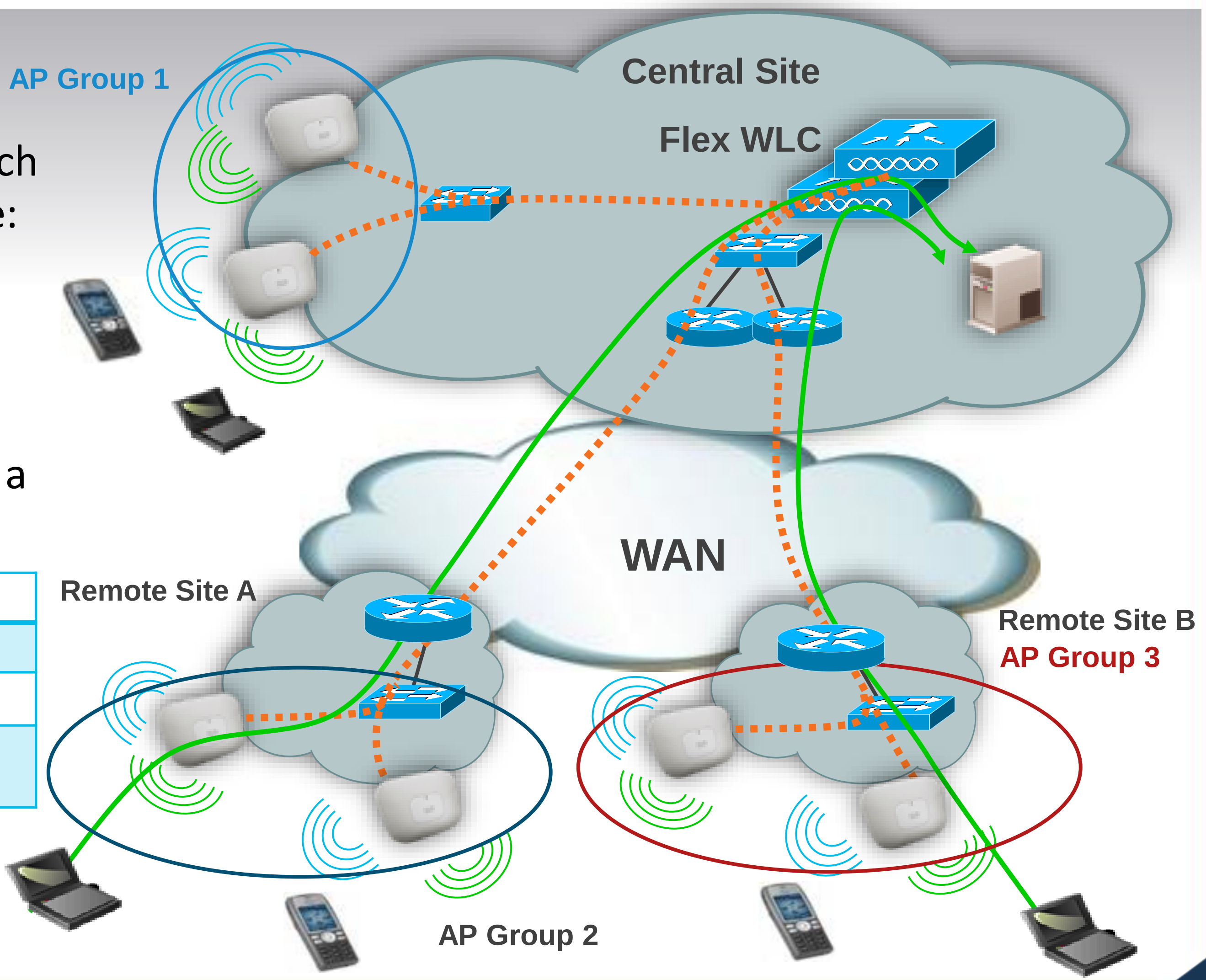
ALERT
ADAPT
ACHIEVE

Understanding AP Groups

Overview

- AP Groups is a logical concept of grouping APs which deliver similar Wi-Fi services; these services can be:
  - By physical location, and/or
  - By functional services (data, voice, guest, …)
- Same AP groups need to be defined in all WLC's of a mobility group

Scaling	8540	5520	9800-40	9800-80	3504
#AP Groups	6000	1500	2000	6000	150
#WLAN (SSID)	512	512	4096	4096	64
#VLAN Interfaces	4096	4096	4096	4096	64



SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

AP Groups Usage

Per Location SSID

AP groups give the ability to enable Wi-Fi Services (WLAN) based on physical location

Central Site

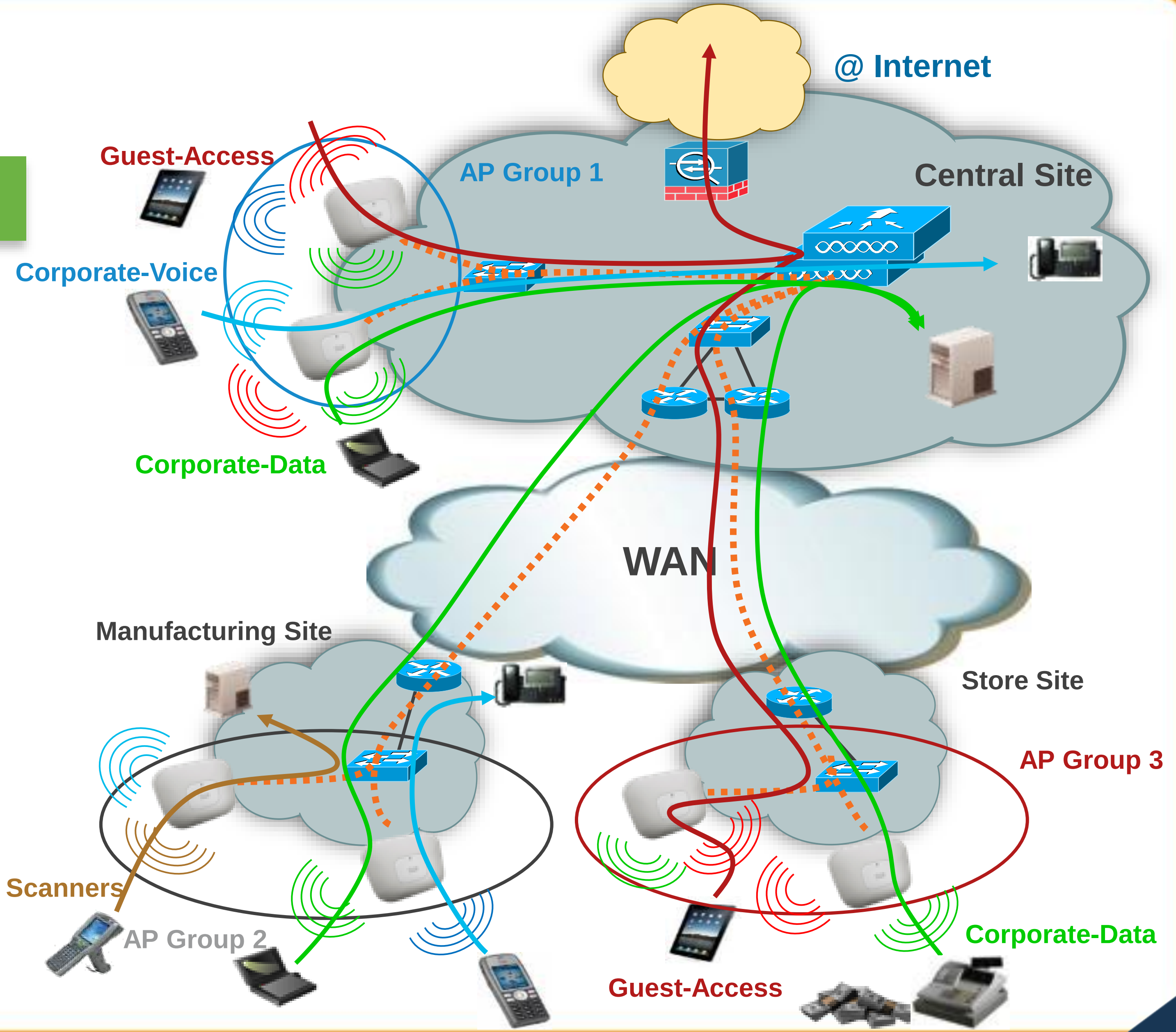
Corporate-Voice, Corporate-Data, Guest-Access

Manufacturing Site

Corporate-Voice, Corporate-Data, Scanners

Store

Corporate-Data, Guest-Access

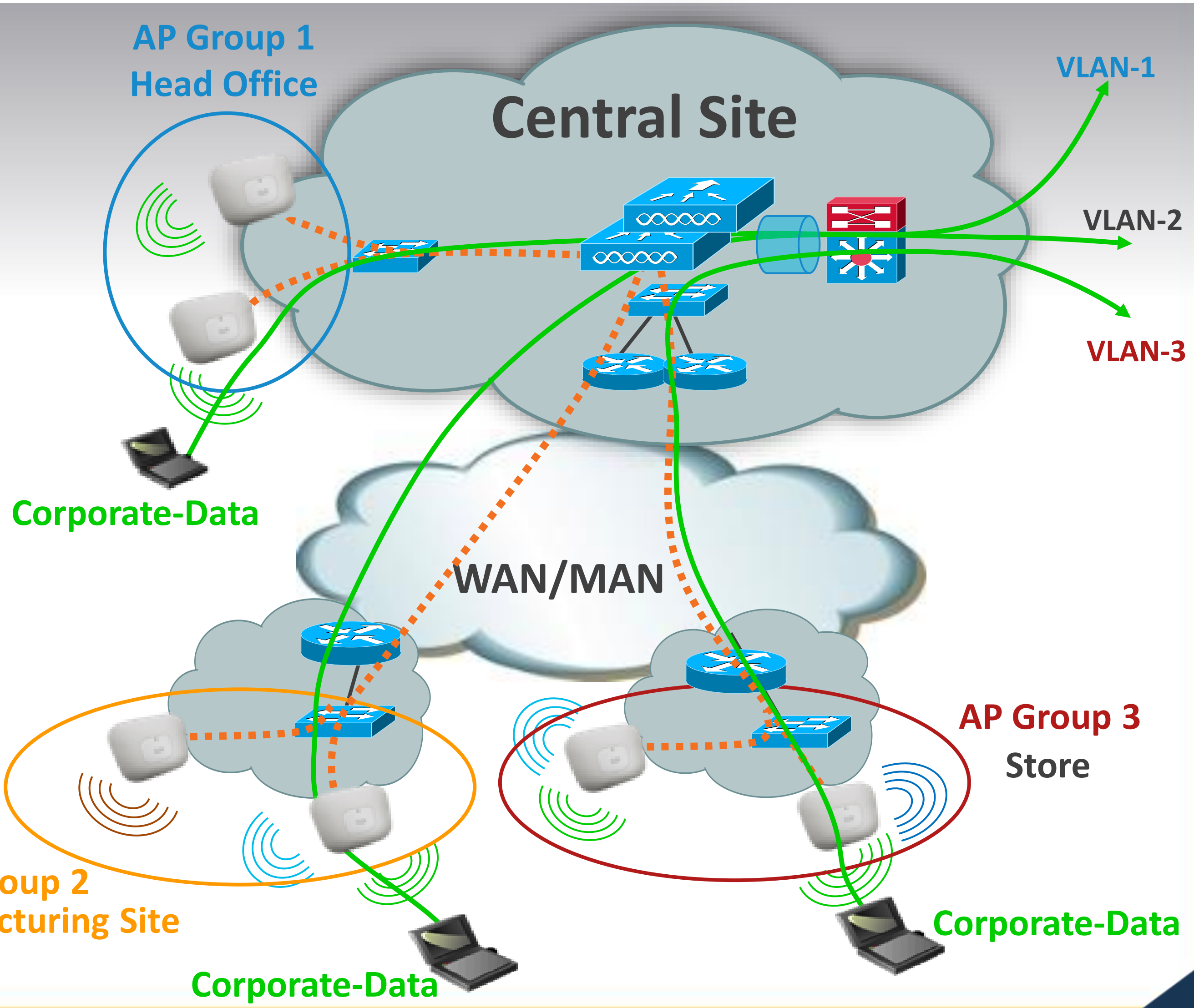


SAMART TELCOMS

AP Groups Usage

Per AP Group SSID to VLAN Mapping

- AP groups give the ability to statically map Wi-Fi service (WLAN) to VLAN based on physical location
- Users see the same Wi-Fi service on all sites.
- Admin can monitor and filter based on different IP@ each site
- Can also be used to have smaller Wi-Fi subnets
  - For example per floor subnets in a building.

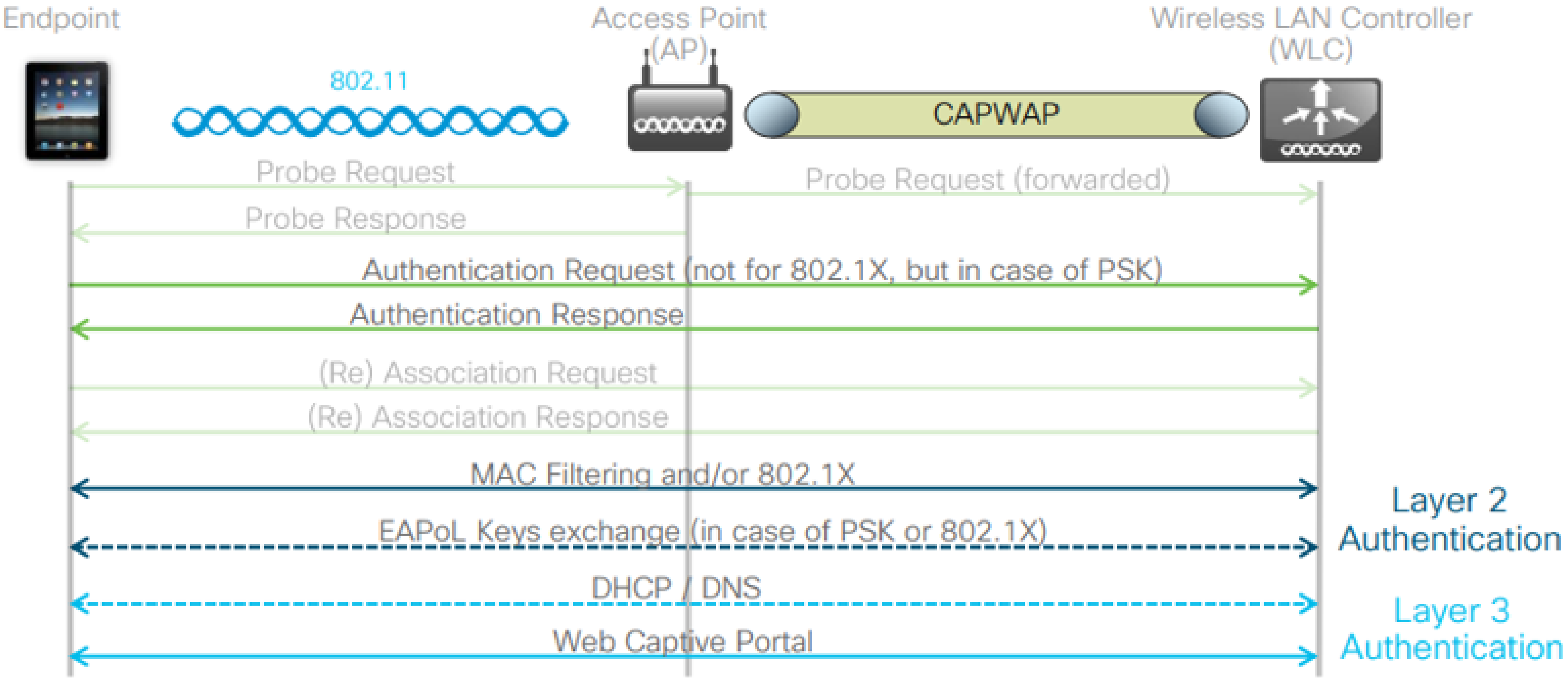


Wi-Fi Security

You make security **possible**

ALERT
ADAPT
ACHIEVE

Wireless connection workflow



Endpoint

Access Point (AP)

Wireless LAN Controller (WLC)

Probe Request

Probe Request (forwarded)

Probe Response

Authentication Request (not for 802.1X, but in case of PSK)

Authentication Response

(Re) Association Request

(Re) Association Response

MAC Filtering and/or 802.1X

EAPoL Keys exchange (in case of PSK or 802.1X)

Layer 2 Authentication

DHCP / DNS

Web Captive Portal

Layer 3 Authentication

SAMART TELCOMS

Secure or open SSID?

- Secure SSID
- Open SSID

- A secure SSID cannot fall back to open.
  - Example: guests not supporting 802.1X cannot fall back to web portal authentication on the same SSID as corporate users.
- Pre-shared keys (PSK) and keys derived from 802.1X are not supported together.
- We can have a secure SSID (PSK or 802.1X) followed by web portal authentication.

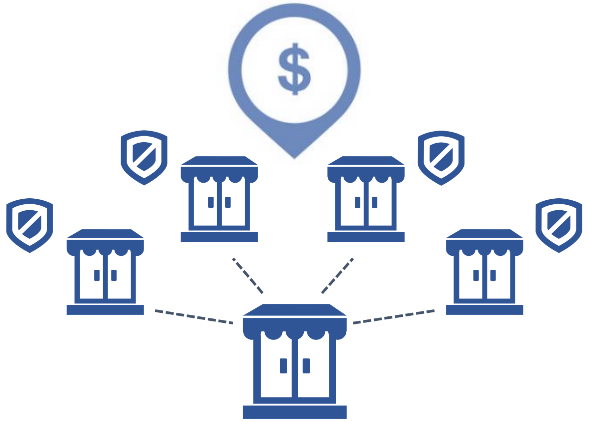
Identity PSK

You make security **possible**

Challenges for Enterprises: Advanced security encryption across all devices

Increased demand for IoT devices

Identity security without 802.1x



Simple Operations

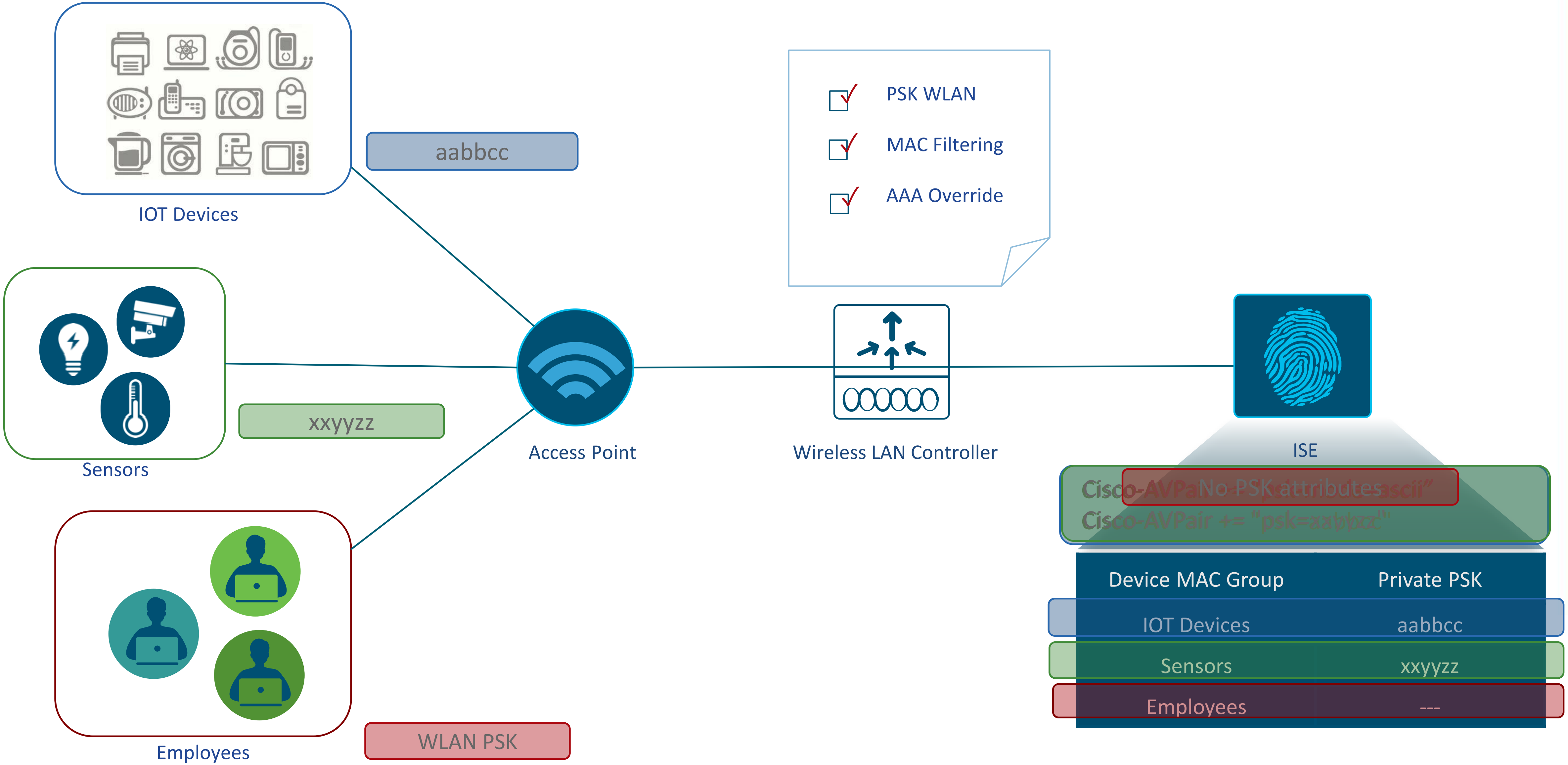
High Scale

Cost Effective

Keys Solution Asks:
Private PSK with RADIUS integration; Per client AAA override (VLAN / ACL, QoS etc)

Cisco Advantage:
Highly scalable identity PSK solution designed for a large multi controller network

Identity PSK



☑ PSK WLAN

☑ MAC Filtering

☑ AAA Override

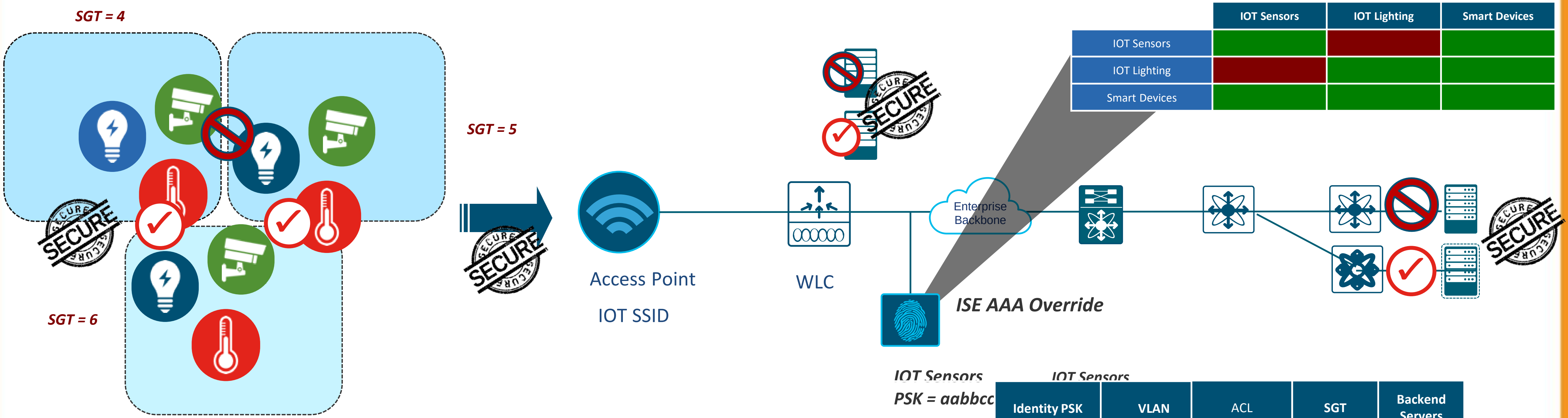
Cisco-AVPair += "psk-mode=ascii"

Cisco-AVPair += "psk=xxyyzz"

No PSK attributes

Device MAC Group	Private PSK
IOT Devices	aabbcc
Sensors	xxyyzz
Employees	---

IOT SSID Security and Segmentation



	IOT Sensors	IOT Lighting	Smart Devices
IOT Sensors	🟩	🟥	🟩
IOT Lighting	🟥	🟩	🟩
Smart Devices	🟩	🟩	🟩

IOT Sensors
PSK = aabbcc

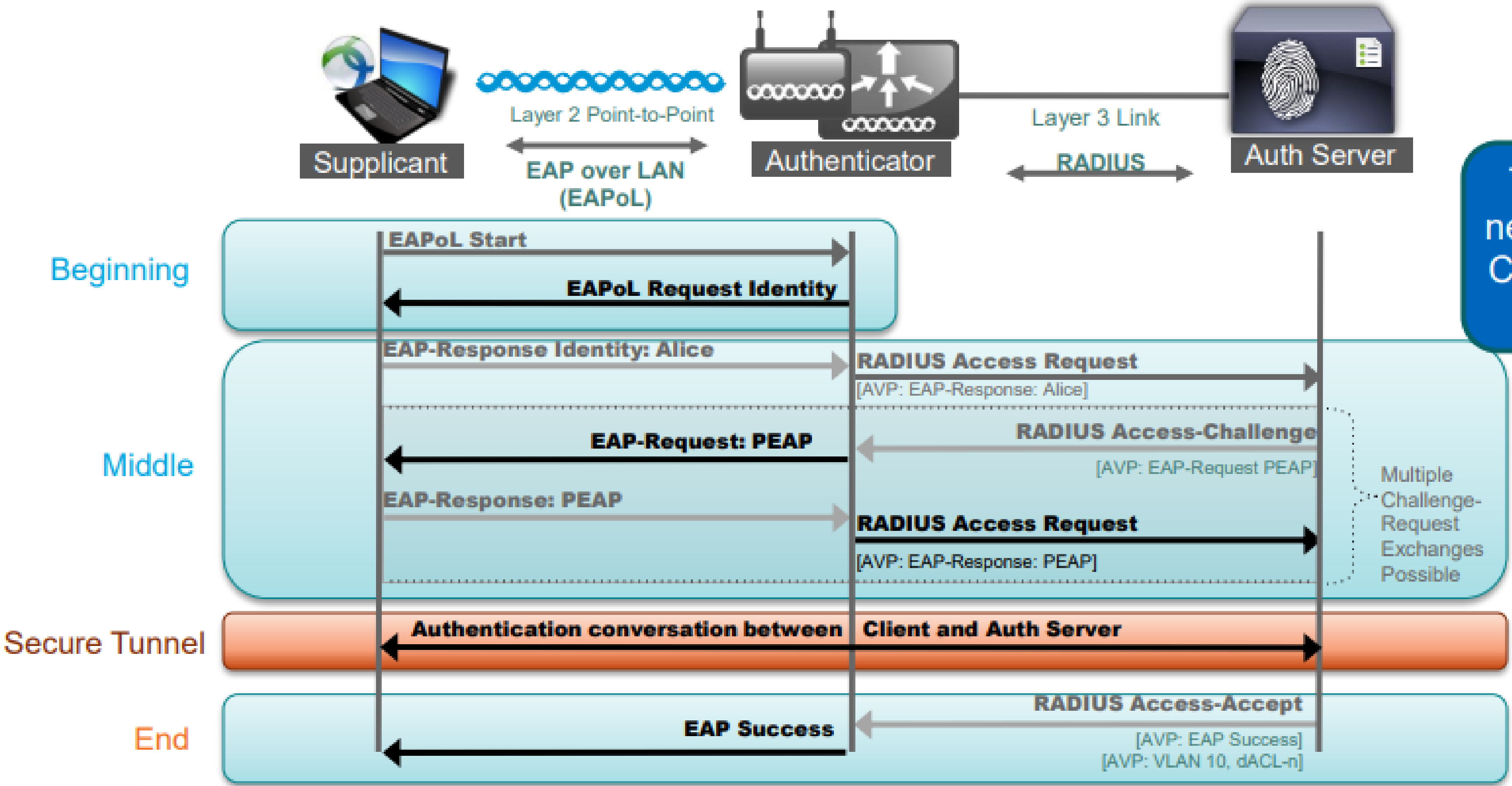
IOT Sensors

	Identity PSK	VLAN	ACL	SGT	Backend Servers
IOT Sensors	aabbcc	10	PERMIT	4	PERMIT
IOT Lighting	*eeffgg*	10	PERMIT	5	DENY
Smart Devices	*xxyyzz*	20	DENY	6	DENY

802.1x

You make security **possible**

Extensible Authentication Protocol (EAP) — Protocol Flow



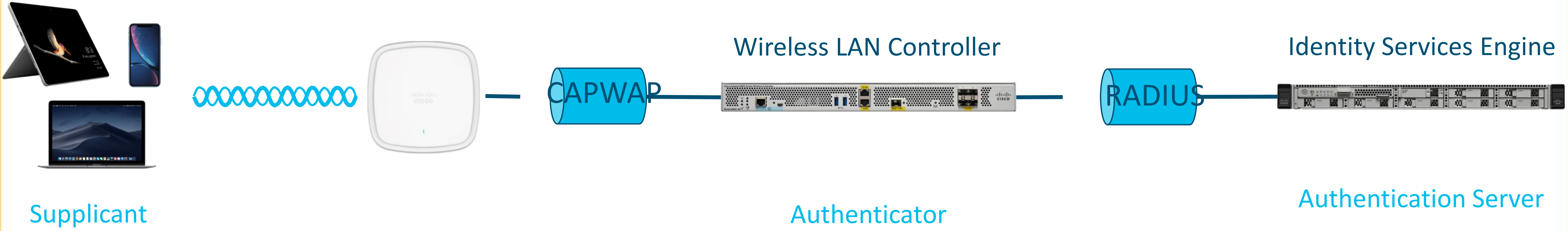
The EAP Type is negotiated between Client and RADIUS Server

- 802.1X (EAPoL) is a **delivery mechanism** and it doesn't provide the actual authentication mechanisms.
- When utilizing 802.1X, you need to choose an **EAP type**, such as Transport Layer Security (EAP-TLS) or PEAP, which defines how the authentication takes place.

ALERT
ADAPT
ACHIEVE

802.11 Fundamentals

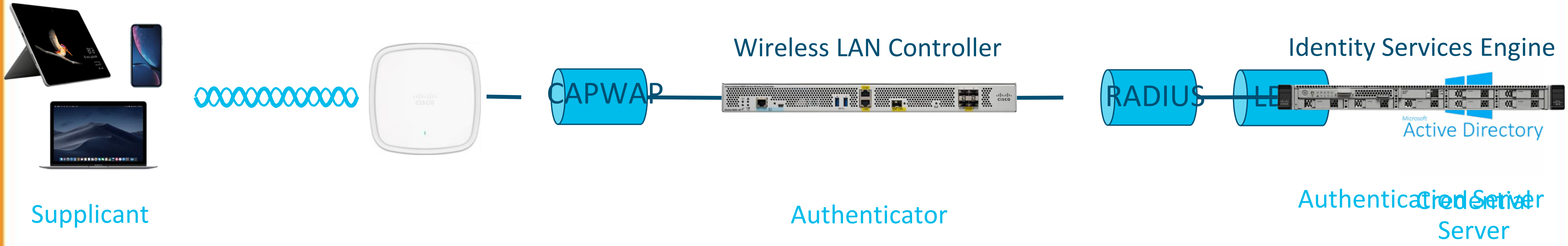
Authentication



SAMART TELCOMS

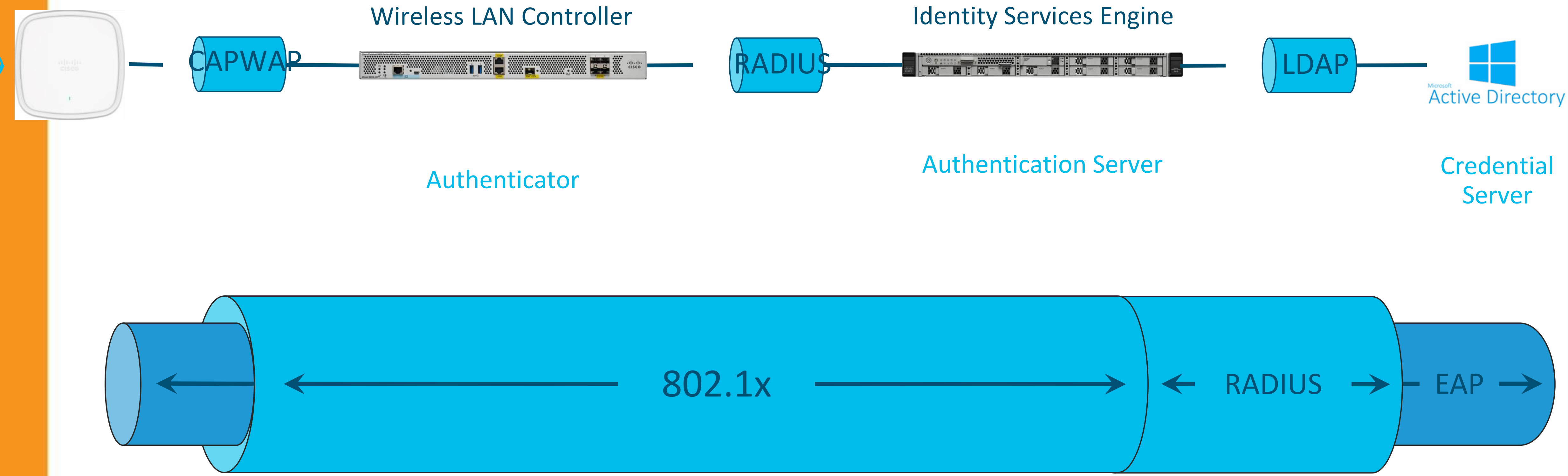
802.11 Fundamentals

Authentication



802.11 Fundamentals

Authentication



Wireless LAN Controller

Identity Services Engine

CAPWAP

RADIUS

LDAP

Microsoft Active Directory

Authenticator

Authentication Server

Credential Server

802.1x

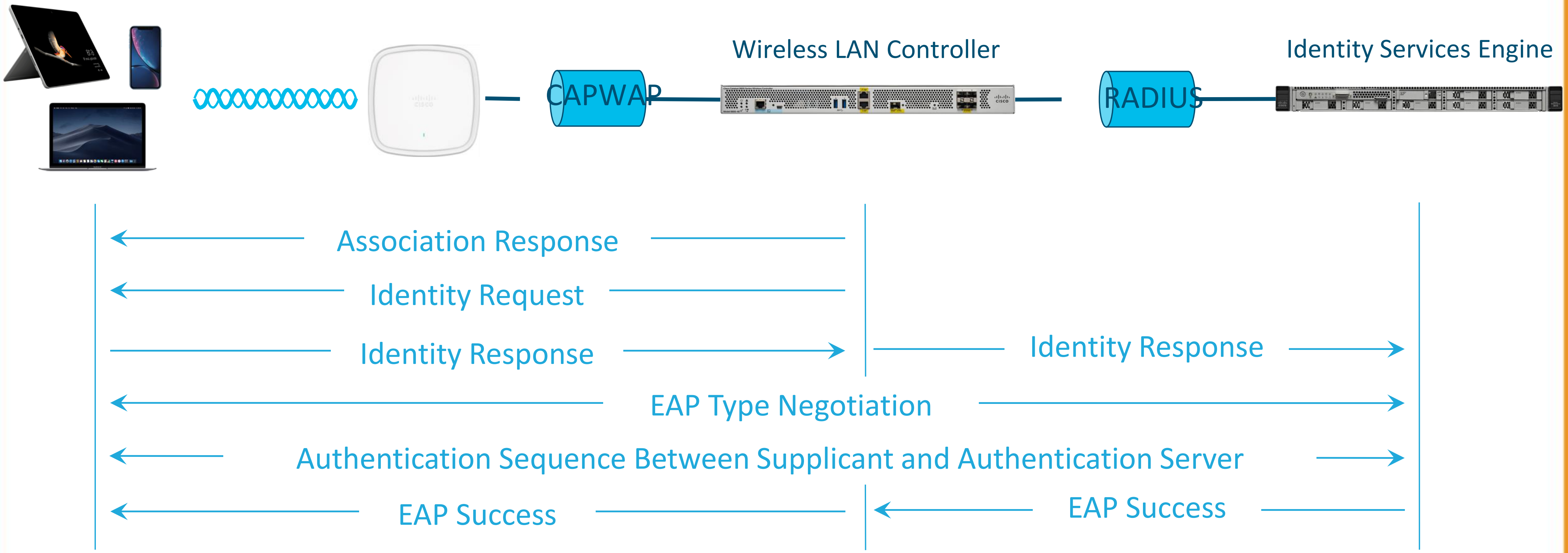
RADIUS

EAP

ALERT
ADAPT
ACHIEVE

802.11 Fundamentals

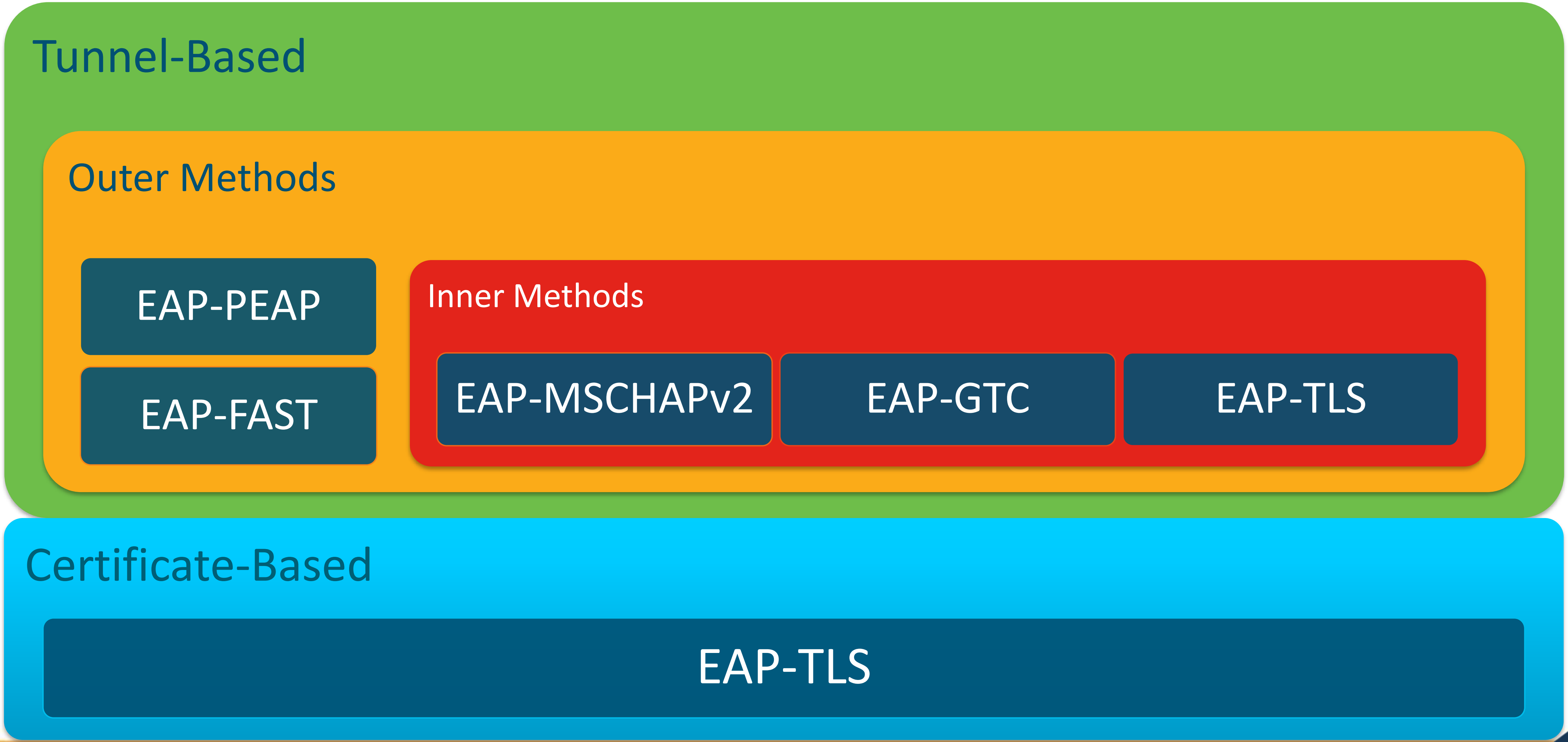
Authentication



SAMART
TELCOMS

WPA-Enterprise

802.1 and Extensible Authentication Protocols



Tunnel-Based

Outer Methods

EAP-PEAP

EAP-FAST

Inner Methods

EAP-MSCHAPv2

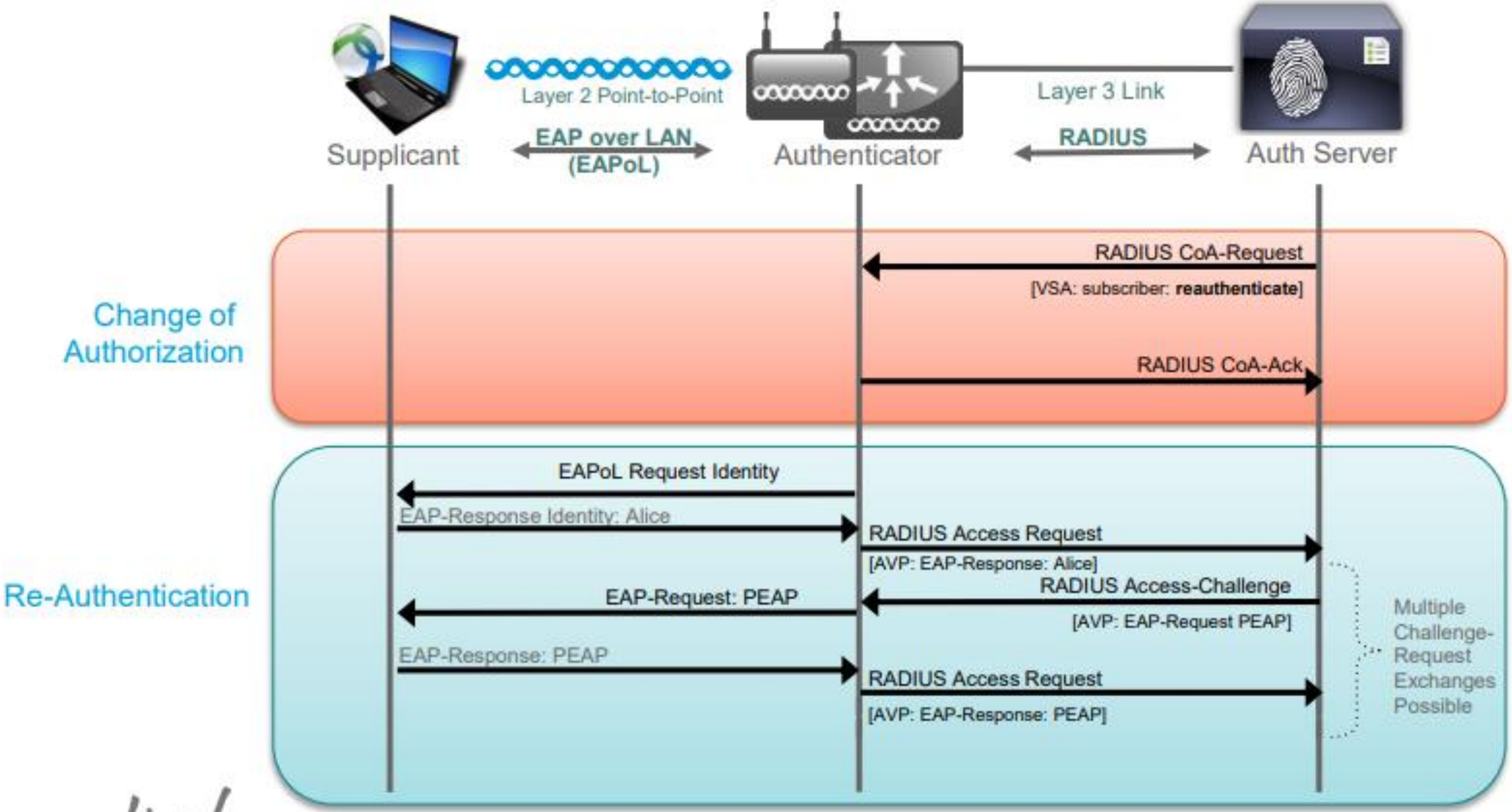
EAP-GTC

EAP-TLS

Certificate-Based

EAP-TLS

IEEE 802.1X with Change of Authorization (CoA)



Supplicant

Layer 2 Point-to-Point

EAP over LAN (EAPoL)

Authenticator

Layer 3 Link

RADIUS

Auth Server

Change of Authorization

RADIUS CoA-Request

[VSA: subscriber: **reauthenticate**]

RADIUS CoA-Ack

Re-Authentication

EAPoL Request Identity

EAP-Response Identity: Alice

RADIUS Access Request

[AVP: EAP-Response: Alice]

RADIUS Access-Challenge

[AVP: EAP-Request PEAP]

EAP-Request: PEAP

EAP-Response: PEAP

RADIUS Access Request

[AVP: EAP-Response: PEAP]

Multiple Challenge-Request Exchanges Possible

Cisco live!

Web Auth

You make networking **possible**

Agenda

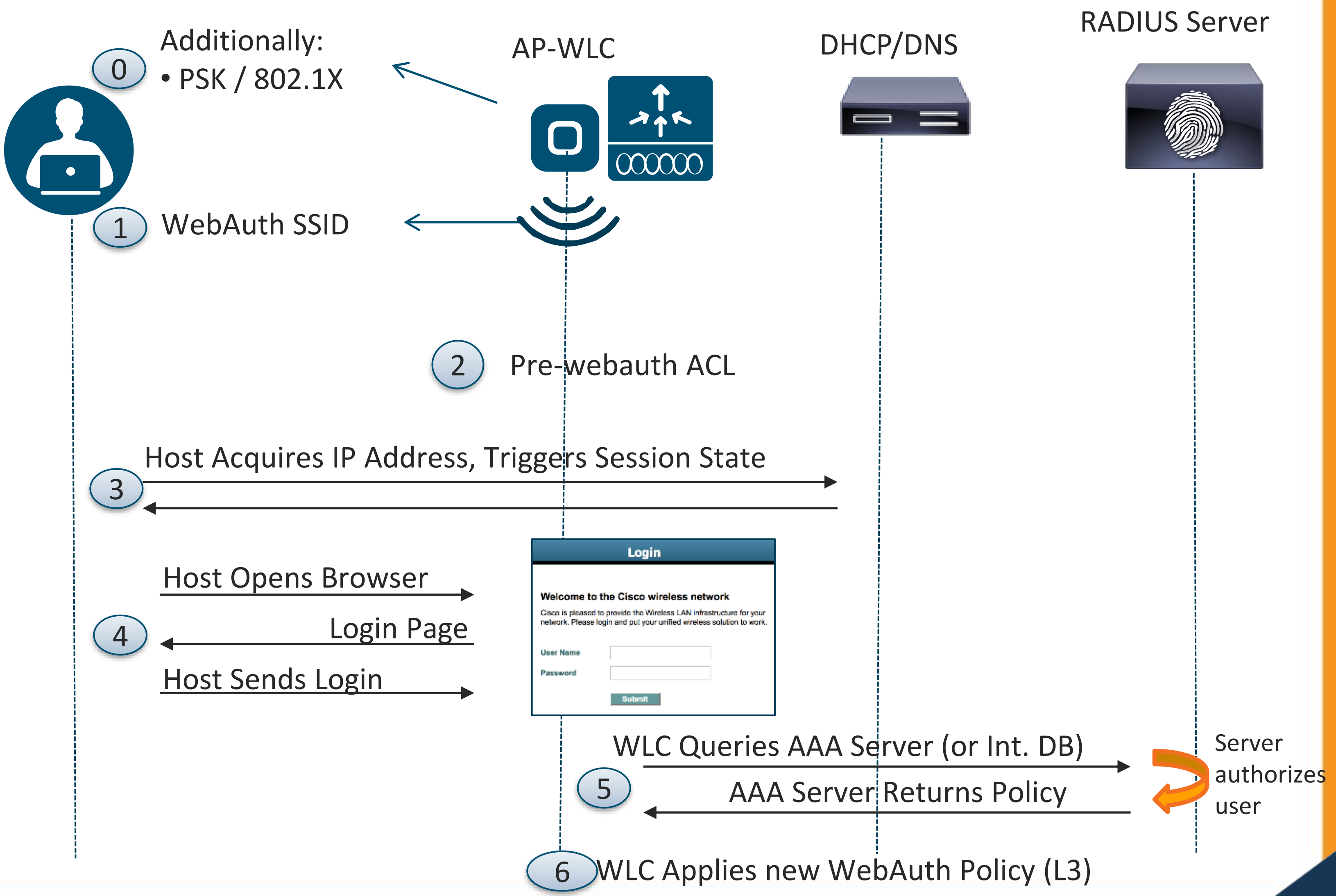
This session covers the configuration steps to setup Guest solution with the C9800, including:

- Local Web Authentication (LWA) with C9800
  - With internal portal
  - With internal custom portal
  - With an external portal
- Central Web authentication (CWA) with C9800 and ISE
- Setting up a Foreign – Anchor guest solution

Local Web Authentication (LWA)

PSK / 802.1X
Local
Web Auth

LOCAL because the redirection URL and the pre-webauth ACL are **locally** configured on the Wireless Controller.



Login

Welcome to the Cisco wireless network

Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work.

User Name

Password

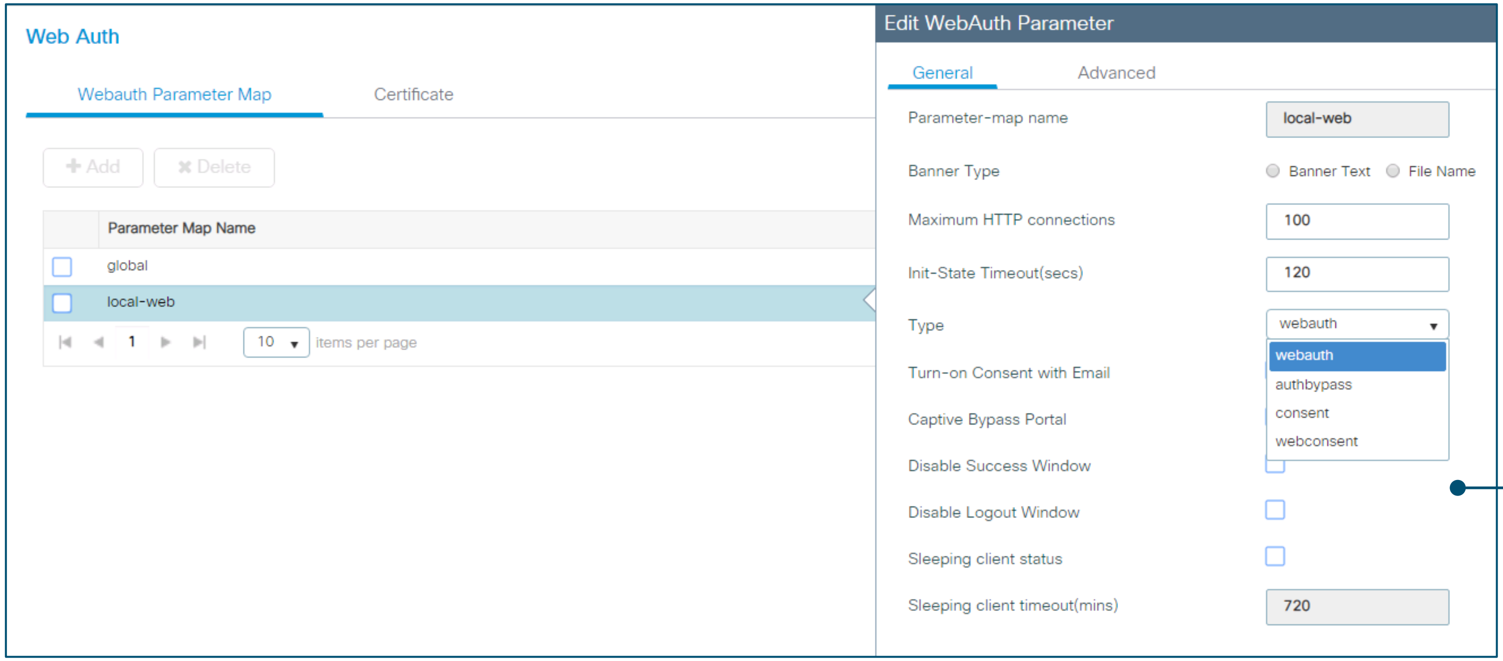
Submit

ALERT
ADAPT
ACHIEVE

Configuring Local Webauth

Webauth Parameter Map

- Navigate to **Configuration > Security > Web Auth** and either modify the existing Parameter map or create a new one.
- Configure the General settings first. Here is where you choose the type of webauth



Web Auth

Webauth Parameter Map | Certificate

+ Add ✖ Delete

	Parameter Map Name
□	global
□	local-web

1 | 10 items per page

Edit WebAuth Parameter

General | Advanced

Parameter-map name: local-web

Banner Type: ○ Banner Text ○ File Name

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: webauth
- webauth
- authbypass
- consent
- webconsent

Turn-on Consent with Email

Captive Bypass Portal

Disable Success Window □

Disable Logout Window □

Sleeping client status □

Sleeping client timeout(mins): 720

choose the desired webauth type (see next slide)

You can disable Success and Logout popup windows. By default these are enabled

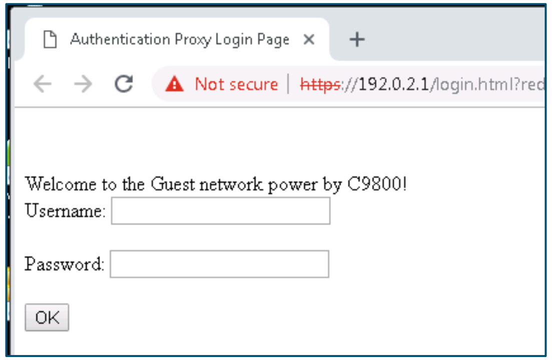
SAMART TELCOMS

Configuring Local Webauth

Webauth Parameter Map

Different webauth type determines a different user login experience:

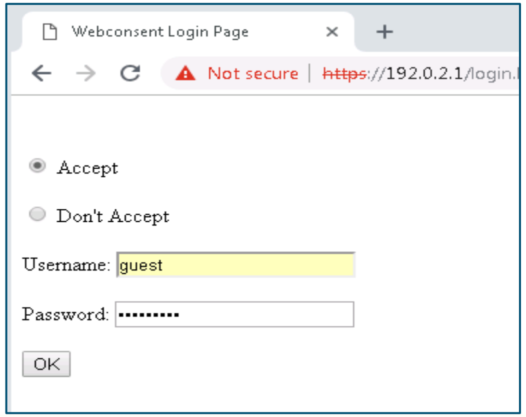
- Webauth:



Authentication Proxy Login Page
Not secure | https://192.0.2.1/login.html?red

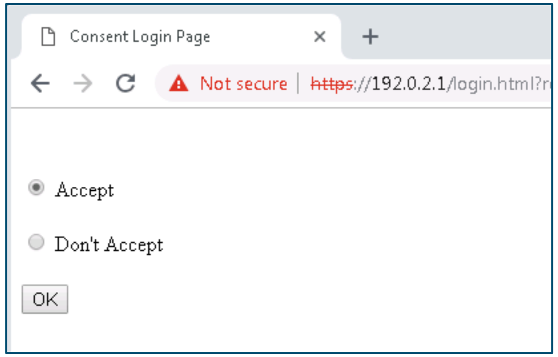
Welcome to the Guest network power by C9800!
Username:
Password:
OK

- Webconsent:



● Accept
○ Don't Accept
Username: guest
Password: ••••••••••
OK

- Consent:



● Accept
○ Don't Accept
OK

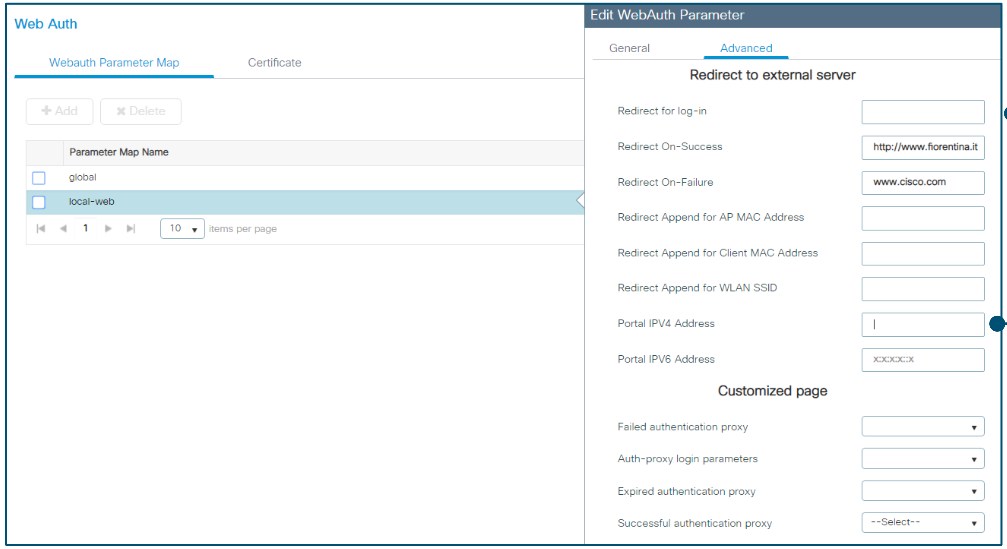
- Authbypass:

Client connects to the SSID and gets an IP address, but the client goes to RUN state only if the MAC address is allowed either locally or in AAA. If not, the client it is not allowed to join.

Configuring Local Webauth

Webauth Parameter Map for Internal Portal

- Configure the desired advanced parameter for the Parameter Map



	Parameter Map Name
□	global
□	local-web

Redirect to external server

Redirect for log-in	
Redirect On-Success	http://www.fiorentina.it
Redirect On-Failure	www.cisco.com
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	|
Portal IPV6 Address	X:X:X:X::X

Customized page

Failed authentication proxy	▾
Auth-proxy login parameters	▾
Expired authentication proxy	▾
Successful authentication proxy	--Select-- ▾

Leave this blank if using the internal portal

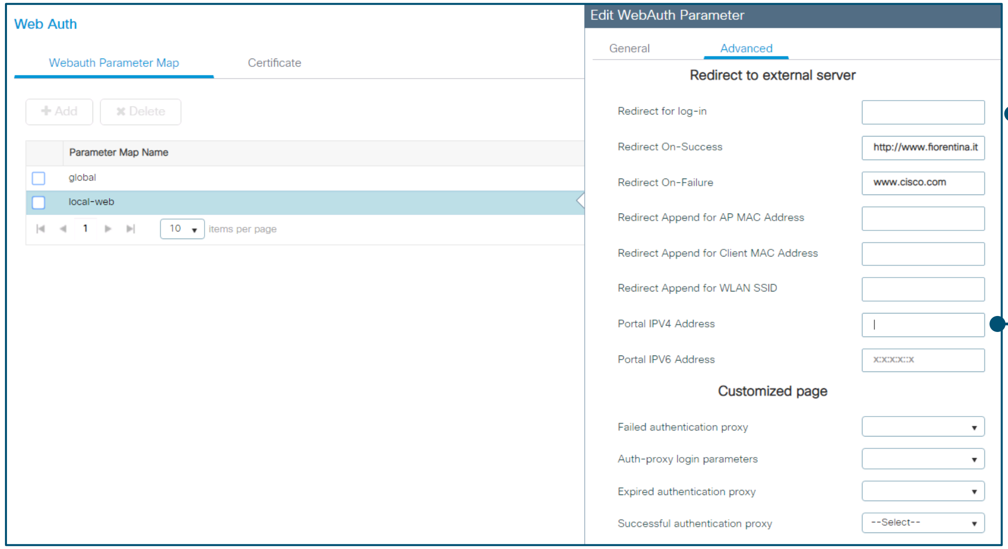
Set the other optional settings like (success page, redirect page on failure, etc

Leave this blank if using the internal portal

Configuring Local Webauth

Webauth Parameter Map for Internal Portal

- Configure the desired advanced parameter for the Parameter Map



	Parameter Map Name
□	global
□	local-web

Redirect to external server

Redirect for log-in	
Redirect On-Success	http://www.fiorentina.it
Redirect On-Failure	www.cisco.com
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	|
Portal IPV6 Address	X:X:X:X::X

Customized page

Failed authentication proxy	
Auth-proxy login parameters	
Expired authentication proxy	
Successful authentication proxy	--Select--

Leave this blank if using the internal portal

Set the other optional settings like (success page, redirect page on failure, etc

Leave this blank if using the internal portal

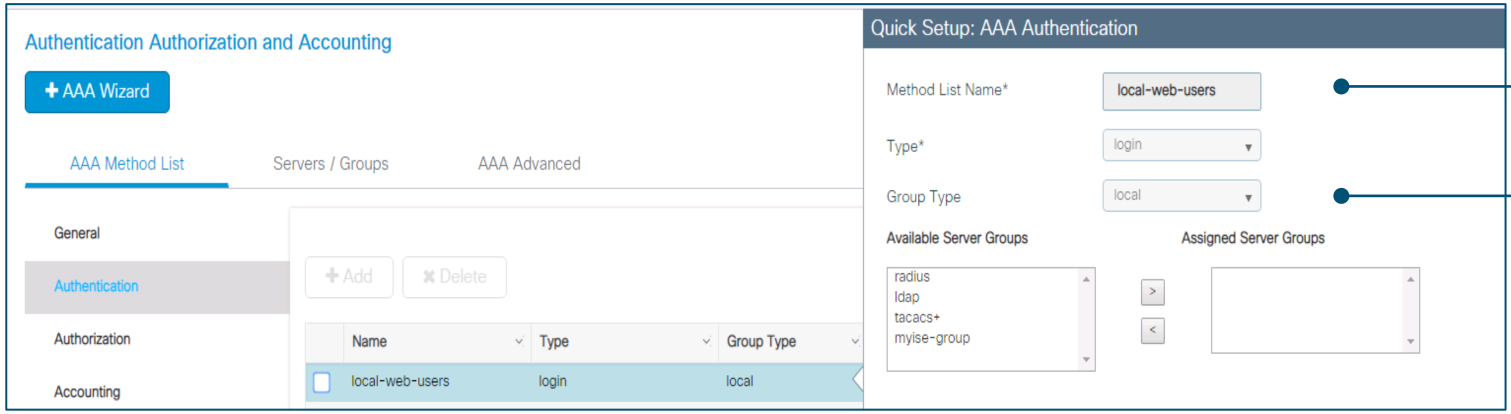
- If using the internal portal, a pre-auth ACL to allow DNS, DHCP, and HTTP/HTTPs client traffic before the user is authenticated, it is automatically created by the wireless controller

ALERT
ADAPT
ACHIEVE

Configuring Local Webauth

AAA settings – AAA Authentication method list - internal DB

- Configure the AAA settings. Go to Configuration > Security > AAA > AAA Method List > Authentication and add a Login Authentication method:



Name	Type	Group Type
local-web-users	login	local

Method List Name*: local-web-users

Type*: login

Group Type: local

Make sure you select type “login”

- Choose “local” if you want to authenticate the users locally on the C9800
- Choose “Group” and then select and available AAA group

- **Note #1**: If you are going to authenticate clients with credentials configured locally on the C9800, login to CLI and run this config command: `aaa authorization network default local`
- **Note #2**: internal guest users are configured under Administration > User Administration. Create a new user and select privilege “no access”(see next slide)

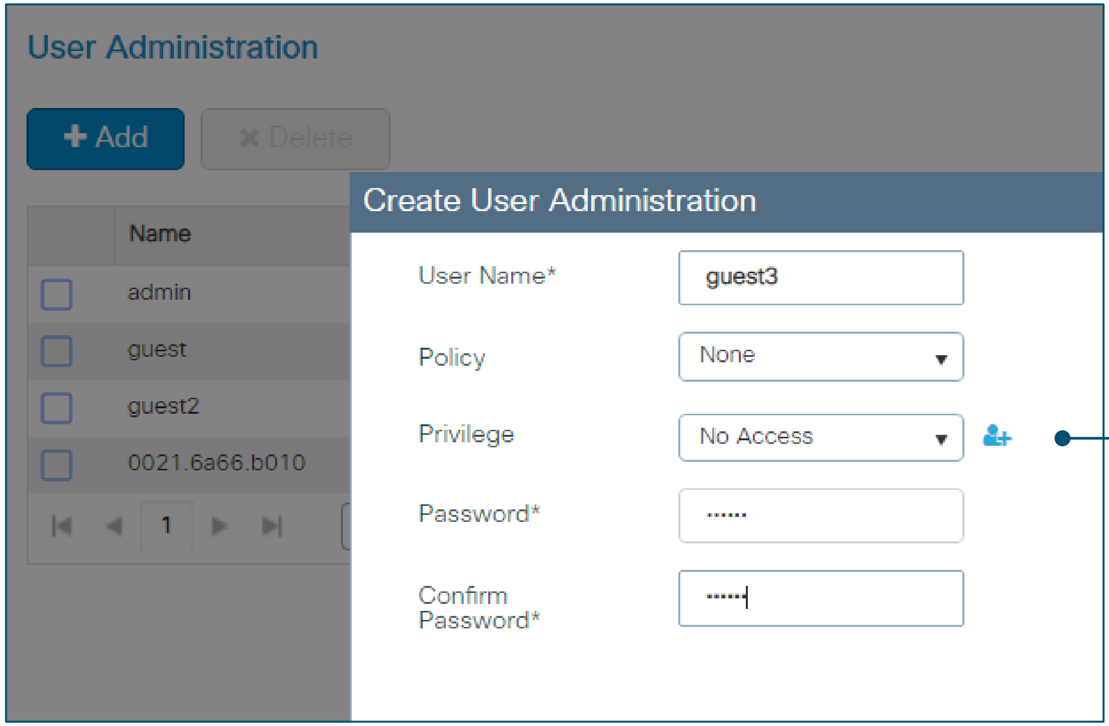
SAMART
TELCOMS

ALERT
ADAPT
ACHIEVE

Configuring Local Webauth

AAA settings – AAA Authentication method list - internal DB

- **TIP:** If you want to use local database users, go to Administration > User Administration and create a guest credentials:



User Administration

	Name
□	admin
□	guest
□	guest2
□	0021.6a66.b010

Create User Administration

User Name*	guest3
Policy	None
Privilege	No Access
Password*	······
Confirm Password*	······

Set the privilege to "no access" so the user will just be able to login to the network but not to the controller

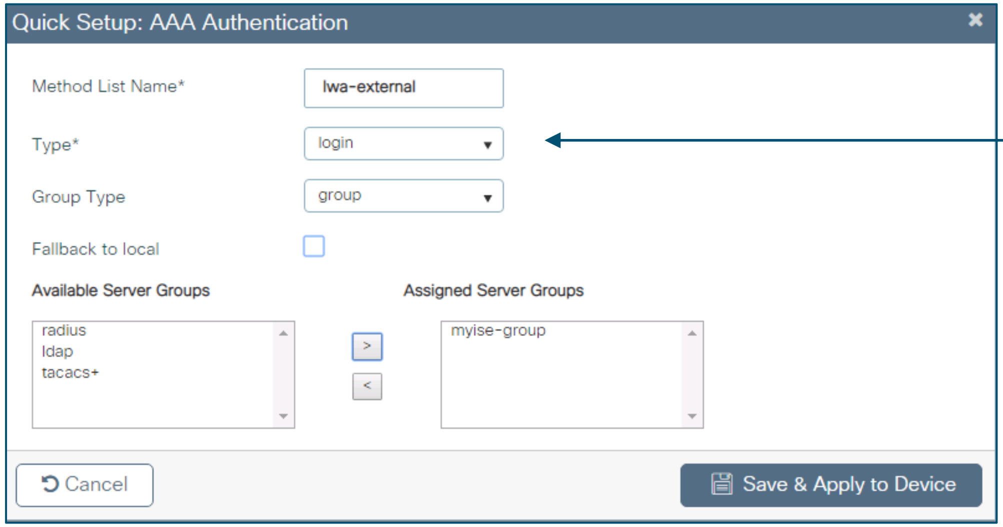
SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

Configuring Local Webauth

AAA settings – AAA Authentication method list – external AAA

- Customers may want to use an external repository for guest users and use RADIUS for authentication.
- In this case the user needs to add a server and a server group to C9800 under Configuration > Security > AAA > Server / Group (same as when using AAA for dot1x)
- Go to Configuration > Security > AAA > AAA Method List > Authentication and add a Login Authentication method list. The only difference vs. an authentication list for dot1x is the the type that has to be “login” (instead of dot1x):



Quick Setup: AAA Authentication

Method List Name* lwa-external

Type* login

Group Type group

Fallback to local □

Available Server Groups: radius, ldap, tacacs+

Assigned Server Groups: myise-group

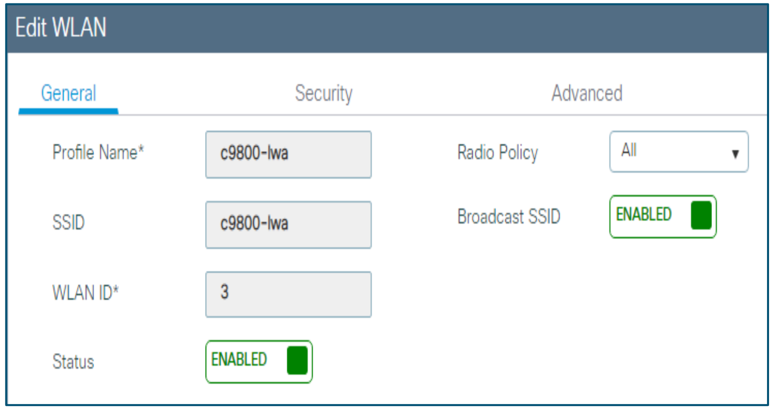
Choose Type = login

SAMART TELCOMS

Configuring Local Webauth

SSID (WLAN profile) configuration

- Configure the WLAN. Go to Configuration > Wireless > WLANs > and add and configure the SSID for webauth:



Edit WLAN

Profile Name* c9800-lwa

SSID c9800-lwa

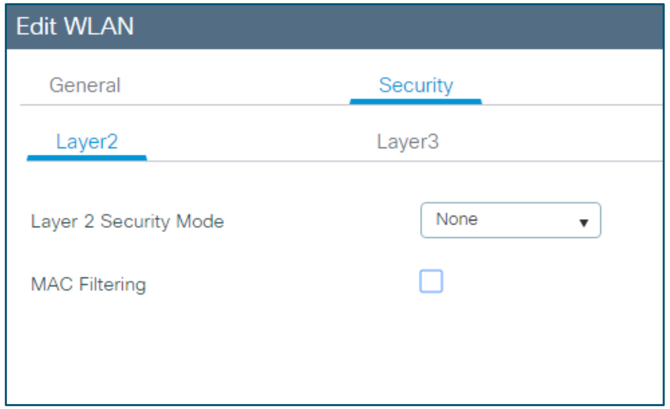
WLAN ID* 3

Status ENABLED

Radio Policy All

Broadcast SSID ENABLED

- Configure the name and enable the SSID

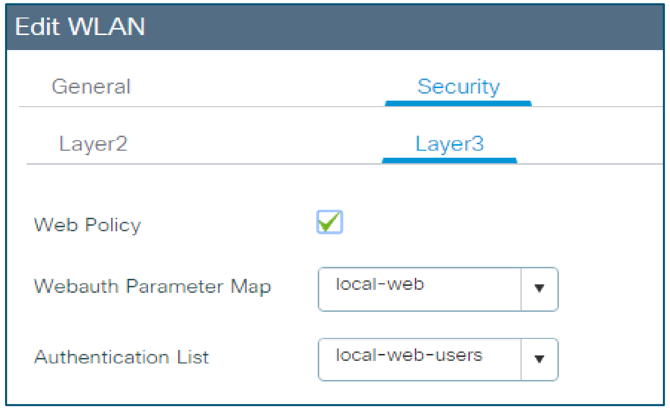


Edit WLAN

Layer 2 Security Mode None

MAC Filtering □

- Set the L2 security to none



Edit WLAN

Web Policy ☑

Webauth Parameter Map local-web

Authentication List local-web-users

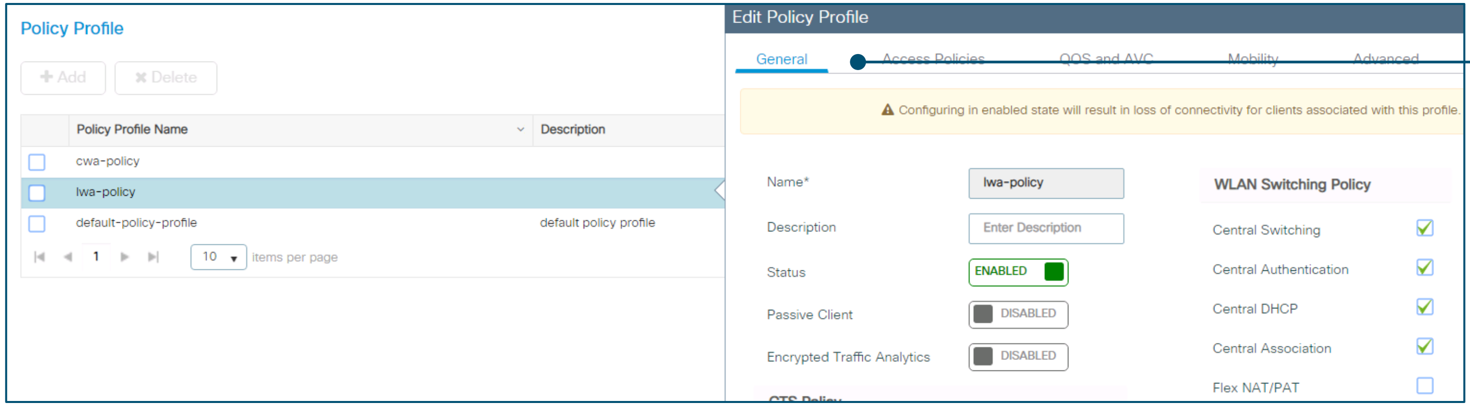
- check “Web policy” and select the Parameter map and Authentication list defined earlier

Configuring Local Webauth

Policy profile configuration

- Create a new policy profile or modify the default one

1



Policy Profile

+ Add ✖ Delete

	Policy Profile Name	Description
□	cwa-policy	
□	lwa-policy	
□	default-policy-profile	default policy profile

◀ 1 ▶ 10 ▾ items per page

Edit Policy Profile

General | Access Policies | QOS and AVC | Mobility | Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*	lwa-policy
Description	Enter Description
Status	ENABLED
Passive Client	DISABLED
Encrypted Traffic Analytics	DISABLED

CTS Policy

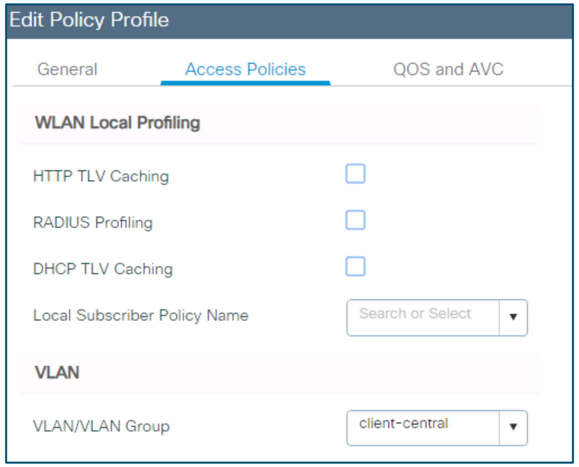
WLAN Switching Policy

Central Switching	☑
Central Authentication	☑
Central DHCP	☑
Central Association	☑
Flex NAT/PAT	□

Under General tab:

- Enable the profile
- Verify Central Auth is checked
- Anything else can be left to default

2



Edit Policy Profile

General | Access Policies | QOS and AVC

WLAN Local Profiling

HTTP TLV Caching	□
RADIUS Profiling	□
DHCP TLV Caching	□
Local Subscriber Policy Name	Search or Select ▾

VLAN

VLAN/VLAN Group	client-central ▾

Under Access Policy tab:

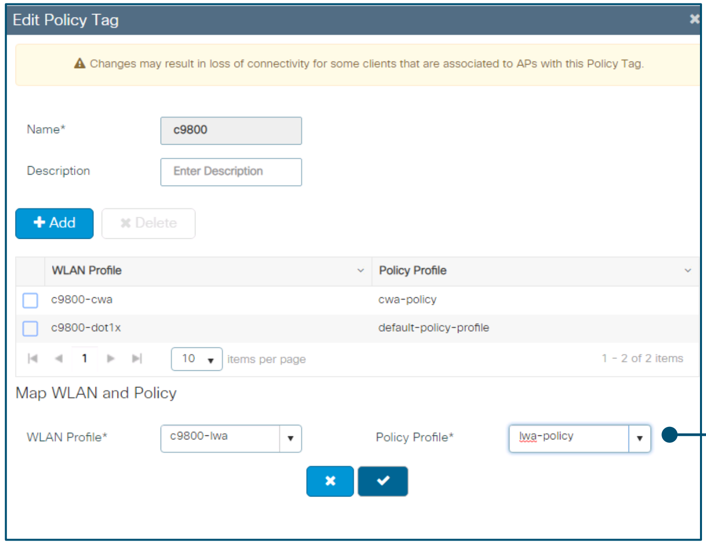
- Select the VLAN you want the guest users to use
- Anything else can be left to default

ALERT
ADAPT
ACHIEVE

Configuring Local Webauth

Policy Tag and AP assignment

- Define a policy tag and assign it to the APs. Go to Configuration > Tags & Profiles > Tags > Policy and edit the policy tag or create a new one. Associate the WLAN to the Policy profile configured



⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name* c9800

Description Enter Description

	WLAN Profile	Policy Profile
□	c9800-cwa	cwa-policy
□	c9800-dot1x	default-policy-profile

1 - 2 of 2 items

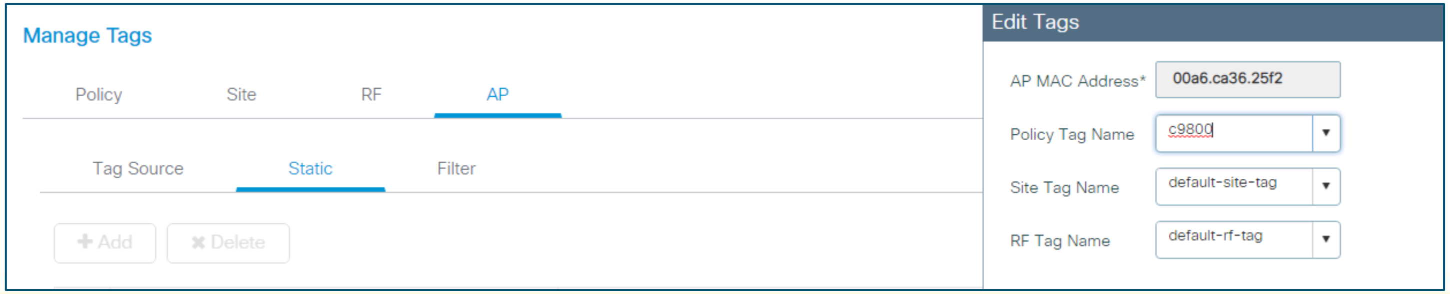
Map WLAN and Policy

WLAN Profile* c9800-lwa

Policy Profile* lwa-policy

Associate the WLAN profile to the Policy profile

- Go to Configuration > Tags & Profiles > Tags > AP and assigned the Policy tag to the AP



AP MAC Address* 00a6.ca36.25f2

Policy Tag Name c9800

Site Tag Name default-site-tag

RF Tag Name default-rf-tag

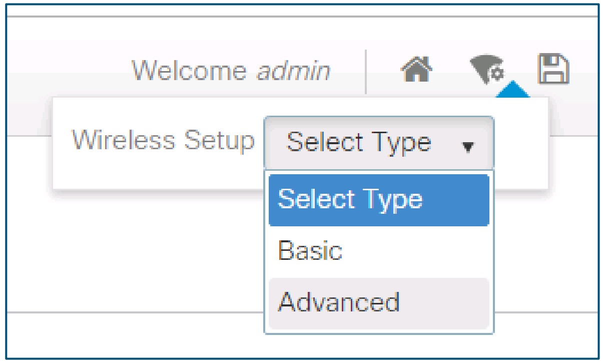
SAMART
TELCOMS

Configuring Local Webauth

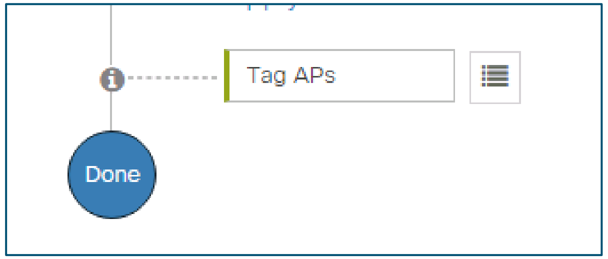
Tag to AP assignment

- **TIP**: how to assign the same TAG to multiple APs via the GUI? a simple way is the following:

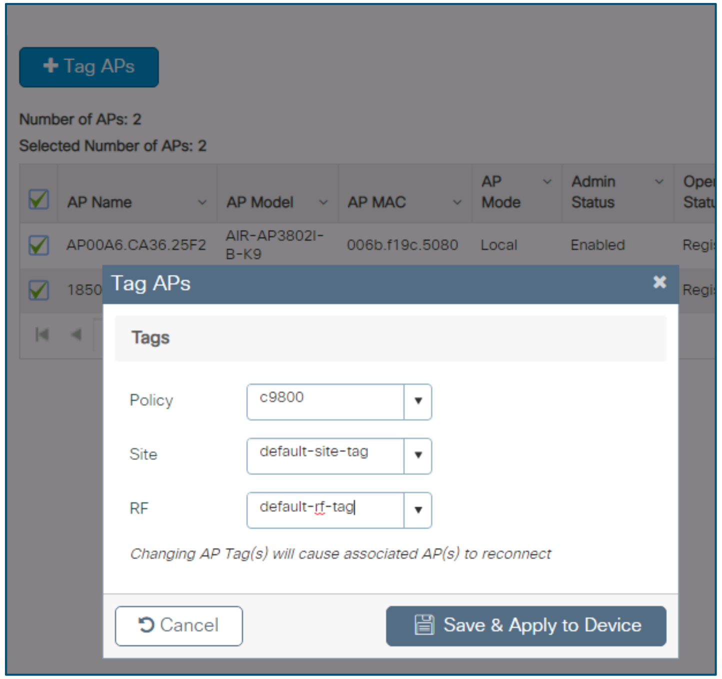
1 Select the Advanced setup and click on start now



2 Click on Tag the APs



3 Select the APs and click on +Tag APs



Number of APs: 2
Selected Number of APs: 2

☑	AP Name	AP Model	AP MAC	AP Mode	Admin Status	Oper Statu
☑	AP00A6.CA36.25F2	AIR-AP3802I-B-K9	006b.f19c.5080	Local	Enabled	Regi
☑	1850					Regi

Tag APs ✖

Tags

Policy: c9800 ▾
Site: default-site-tag ▾
RF: default-rf-tag ▾

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

(Optional) Local Webauth (LWA) with customized internal portal

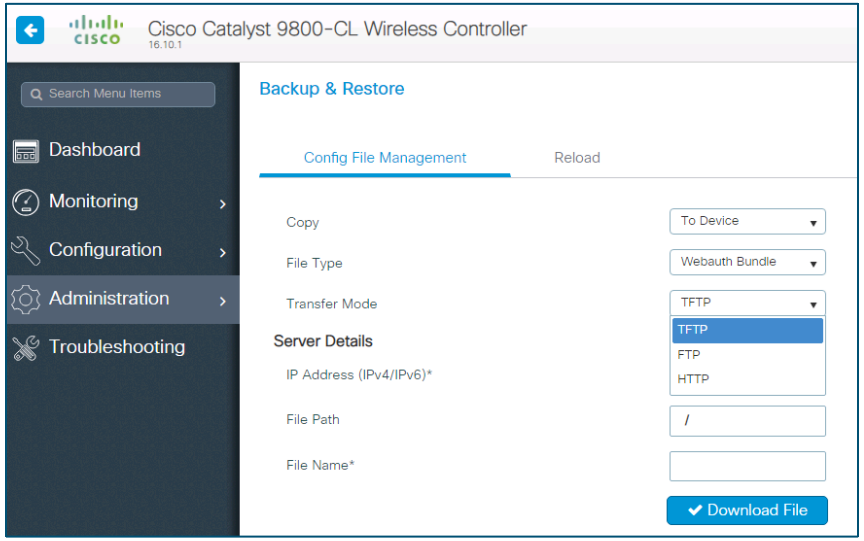
You make networking **possible**

ALERT
ADAPT
ACHIEVE

Configuring Local Webauth

Optional: customized internal portal

- User can download a WebAuth bundle to the controller and use customized page for Login, Success page, etc…
- Download the bundle to the C9800 in .tar format. Go to Administration > Backup & Restore > Config File Management and select WebAuth bundle as file type and the transfer mode



Copy: To Device
File Type: Webauth Bundle
Transfer Mode: TFTP

Server Details

IP Address (IPv4/IPv6)*:

File Path: /

File Name*:

Important NOTE:

- The downloaded bundle will get extracted in bootflash: in specific directories
- As of 16.10, the user will have to move the html files from the directories to bootflsh
- This is fixed in release 16.11

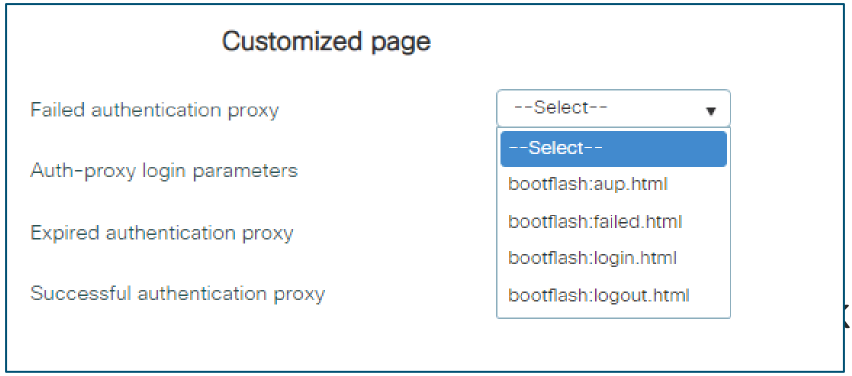
SAMART
TELCOMS

Configuring Local Webauth

Optional: customized internal portal

- Once the bundle has been installed, the user can select the customized web pages in the Configuration > Security > Webauth > Webauth Parameter Map > Advanced section under the Customized page configuration:

Release 16.10



Customized page

Failed authentication proxy: --Select--

- --Select--
- bootflash:aup.html
- bootflash:failed.html
- bootflash:login.html
- bootflash:logout.html

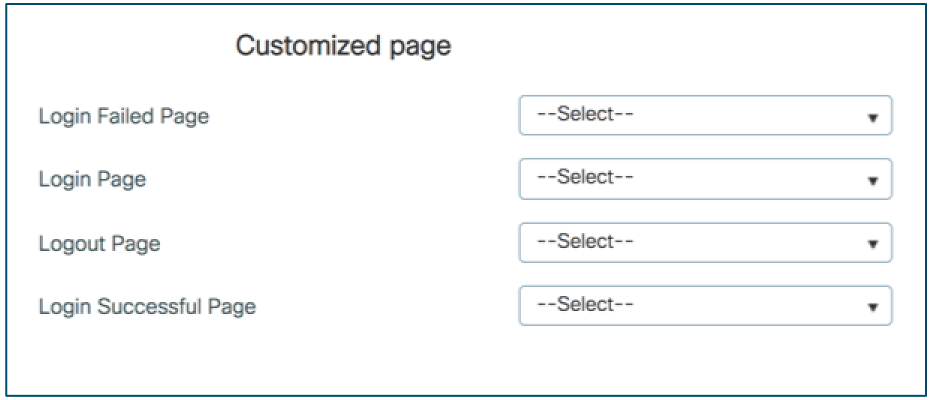
Auth-proxy login parameters

Expired authentication proxy

Successful authentication proxy

s like this:

Release 16.11



Customized page

Login Failed Page: --Select--

Login Page: --Select--

Logout Page: --Select--

Login Successful Page: --Select--

(Optional) Local Webauth (LWA) with with external portal

You make networking **possible**

Configuring Local Webauth

Webauth Parameter Map

- **Note #2**: when configuring an IP address for the portal a pre-auth ACL is automatically created to allow the HTTP and HTTPS traffic (TCP port 80 and 443) from the wireless clients to the external web authentication server. In the case of ISE, the portal is using port 8443, so an ACL has to be created to allow traffic to ISE, example:

```
c9800#sh ip access-lists ise-preauth-acl
Extended IP access list ise-preauth-acl
    10 permit udp any any eq domain (1188 matches)
    20 permit tcp any any eq domain
    30 permit udp any eq bootps any
    40 permit udp any any eq bootpc
    50 permit udp any eq bootpc any
    60 permit ip any host 172.16.3.4 (416 matches)
    70 permit ip host 172.16.3.4 any
    80 permit icmp any any (24 matches)
    90 deny ip any any (9369 matches)
```

Applied to the WLAN →

```
wlan c9800-lwa 3 c9800-lwa
 band-select
 ip access-group web ise-preauth-acl
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list local-web-users
 security web-auth parameter-map local-web
```

Configuring Central WebAuth (CWA)

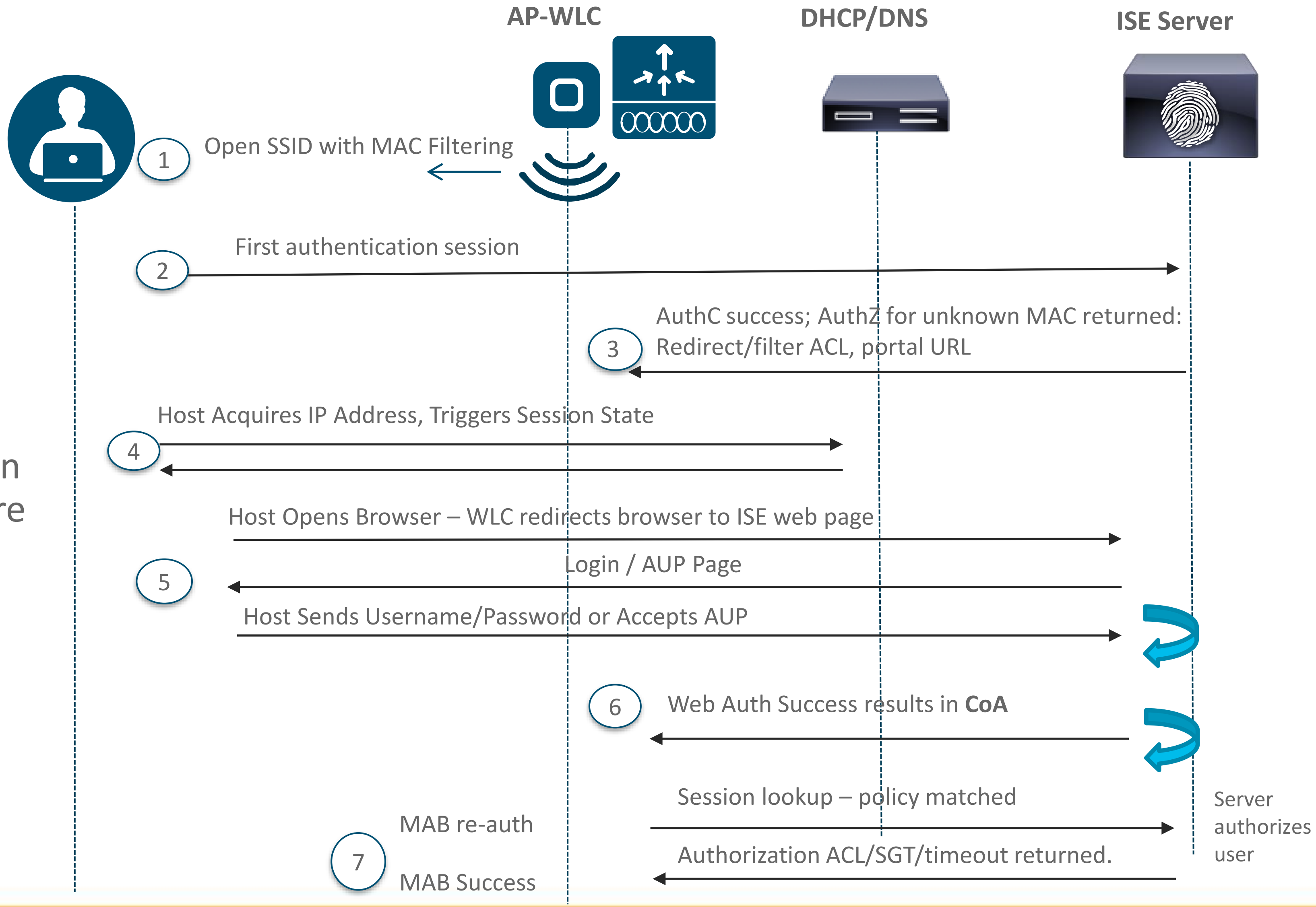
You make networking **possible**

ALERT
ADAPT
ACHIEVE

Central Web Authentication (CWA)

Central
Web Auth

CENTRAL because the redirection URL and the pre-webauth ACL are **centrally** configured on ISE and communicated to the WLC via RADIUS.



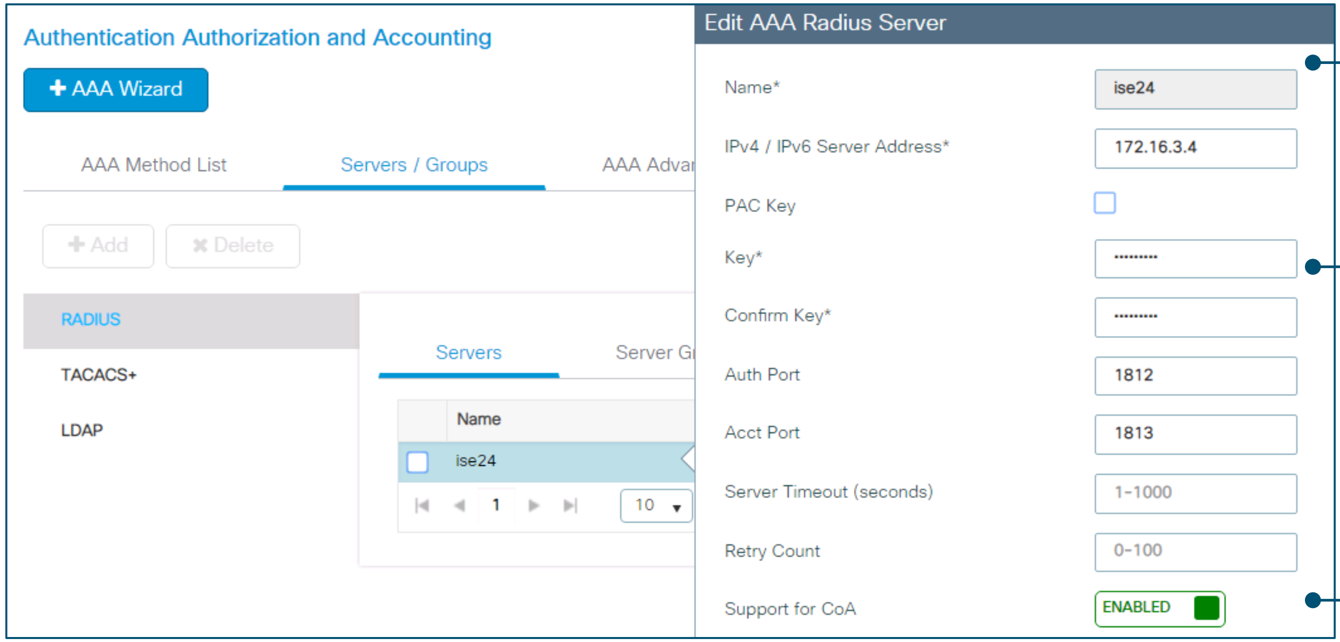
AP-WLC
DHCP/DNS
ISE Server
1
Open SSID with MAC Filtering
2
First authentication session
3
AuthC success; AuthZ for unknown MAC returned:
Redirect/filter ACL, portal URL
4
Host Acquires IP Address, Triggers Session State
5
Host Opens Browser – WLC redirects browser to ISE web page
Login / AUP Page
Host Sends Username/Password or Accepts AUP
6
Web Auth Success results in **CoA**
Session lookup – policy matched
Authorization ACL/SGT/timeout returned.
Server
authorizes
user
7
MAB re-auth
MAB Success

SAMART
TELCOMS

Configuring Central Webauth (CWA)

Adding a ISE as Radius Server

- Add ISE as AAA server to C9800. Navigate to Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > and click Add and enter the RADIUS server's information



Name	ise24

Edit AAA Radius Server

Name*	ise24
IPv4 / IPv6 Server Address*	172.16.3.4
PAC Key	□
Key*	·········
Confirm Key*	·········
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED

Enter all the mandatory information
Mandatory settings have a *

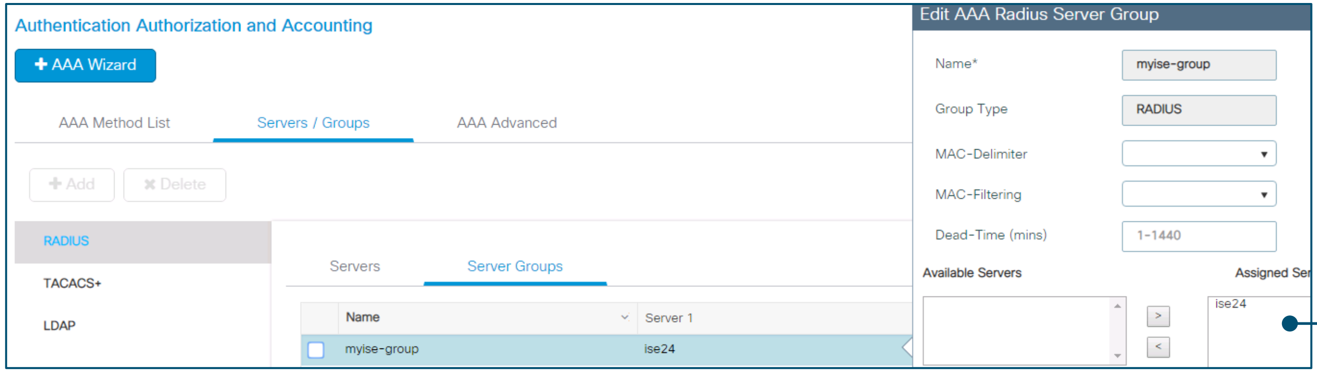
This is the shared secret that needs to configured on ISE as well

Enable support for CoA

Configuring Central Webauth (CWA)

Adding a Server Group and AAA Authentication method list

- Go to Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups, click Add and define a server group and add the defined AAA server:



Name	Server 1
myise-group	ise24

Name* myise-group

Group Type RADIUS

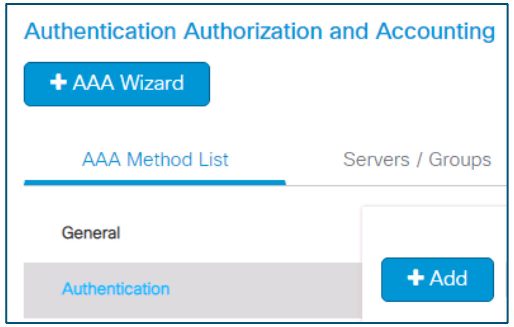
MAC-Delimiter

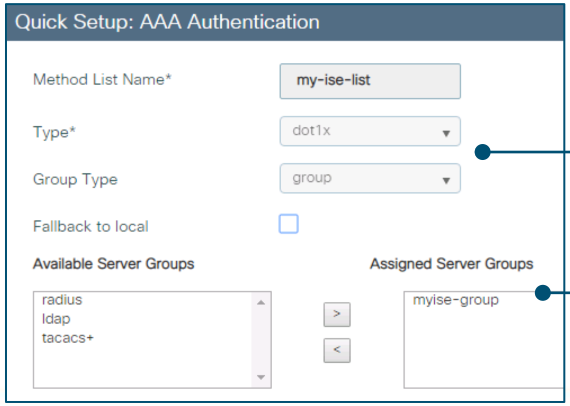
Dead-Time (mins) 1-1440

Assigned Se: ise24

Select the ISE server defined earlier

- Go to Configuration > Security > AAA > AAA Method List > Authentication and create a new method list by clicking Add:





Method List Name* my-ise-list

Type* dot1x

Group Type group

Fallback to local □

Assigned Server Groups: myise-group

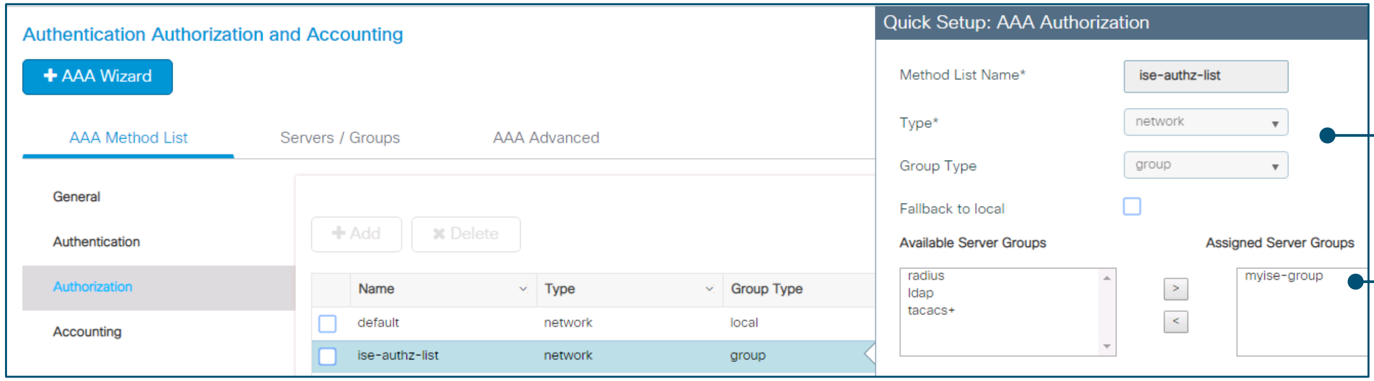
Choose type “dot1x” and group type “group”

Add the server group we have just defined

Configuring Central Webauth (CWA)

Adding Authorization and Accounting (optional) method list

- Create an authorization method list. Navigate to Configuration > Security > AAA > AAA Method List > Authorization and click Add



	Name	Type	Group Type
□	default	network	local
□	ise-authz-list	network	group

Method List Name* ise-authz-list

Type* network

Group Type group

Fallback to local □

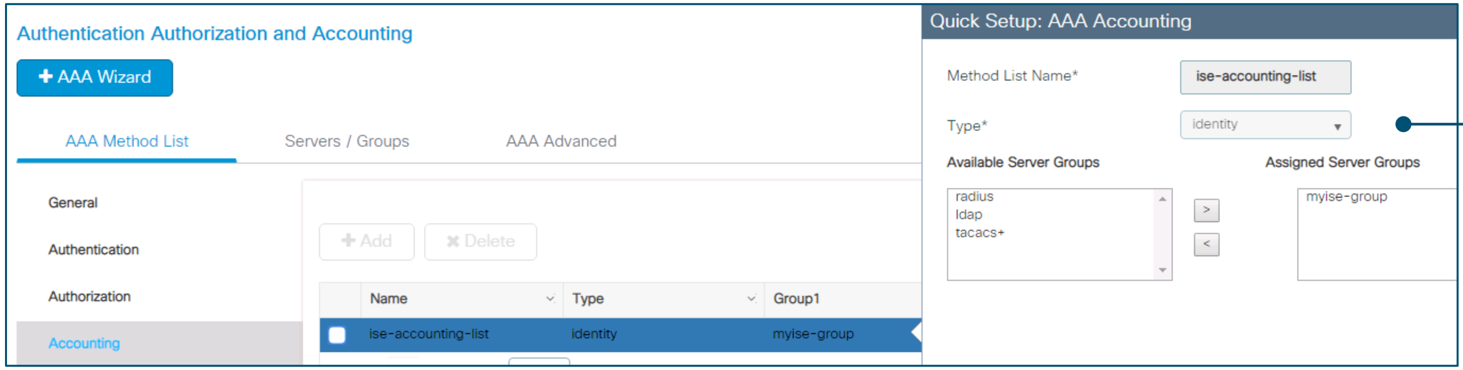
Available Server Groups: radius, ldap, tacacs+

Assigned Server Groups: myise-group

Select type “Network” and group type Group

Add the server group defined in previous step

- (Optional) create a Accounting method list



	Name	Type	Group1
□	ise-accounting-list	identity	myise-group

Method List Name* ise-accounting-list

Type* identity

Available Server Groups: radius, ldap, tacacs+

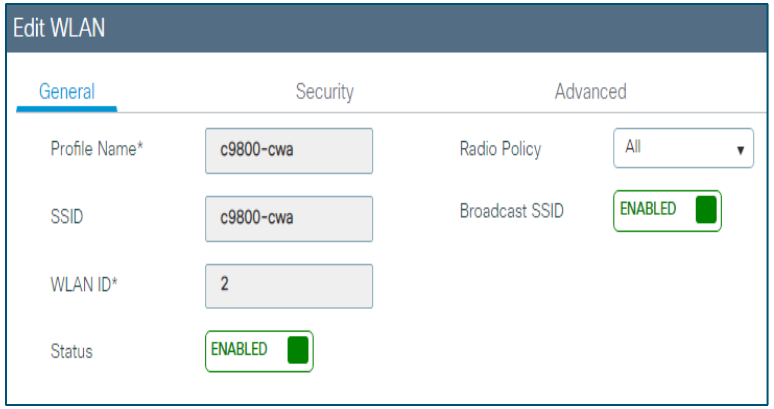
Assigned Server Groups: myise-group

Choose “identity” as type

Configuring Central Webauth (CWA)

Configuring the WLAN profile

- Configure the SSID. Go to Configuration > Wireless > WLANs > and add and configure the SSID for MAC filtering:



Profile Name* c9800-cwa

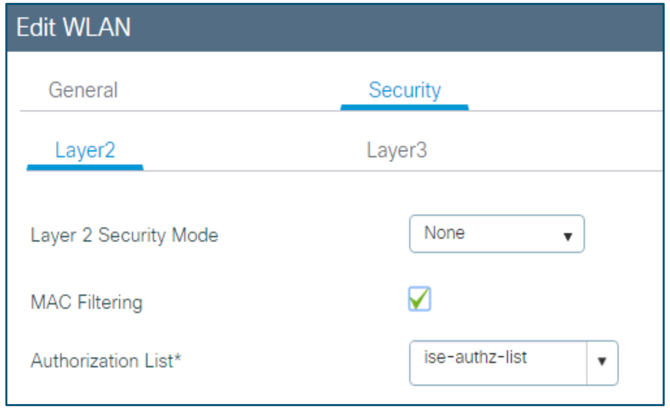
SSID c9800-cwa

WLAN ID* 2

Status ENABLED

Radio Policy All

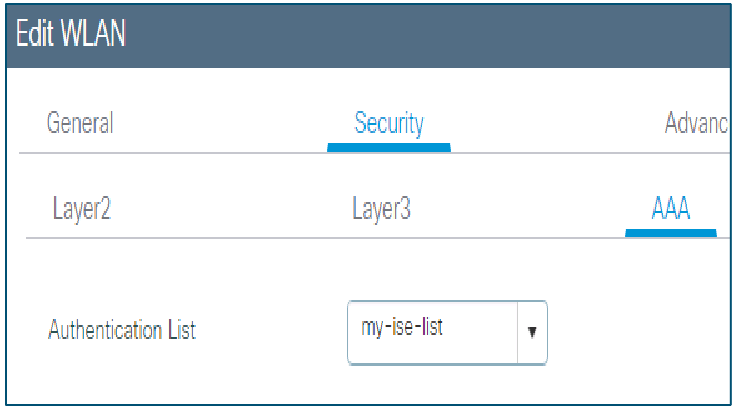
Broadcast SSID ENABLED



Layer 2 Security Mode None

MAC Filtering ☑

Authorization List* ise-authz-list



Authentication List my-ise-list

- Configure the name and enable the SSID
- Configure L2 security to use MAC filtering and select the authorization list defined earlier
- Under AAA tab, select the authentication list defined ealier

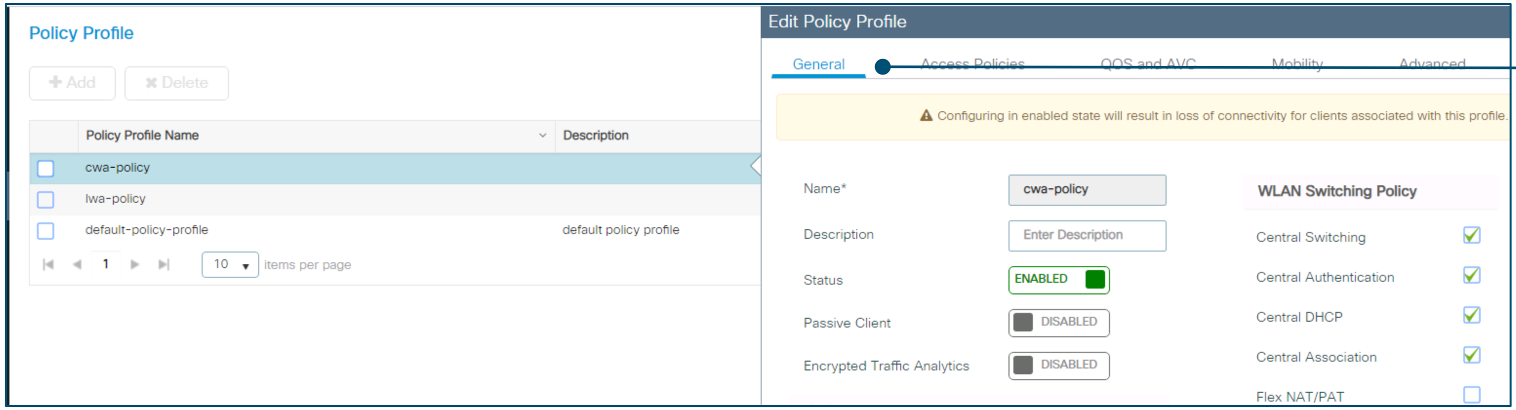
ALERT ADAPT ACHIEVE

Configuring Central Webauth (CWA)

Configuring the Policy profile

- Create a new policy profile or modify the default one:

1



Policy Profile

✚ Add ✖ Delete

	Policy Profile Name	Description
□	cwa-policy	
□	lwa-policy	
□	default-policy-profile	default policy profile

1 10 items per page

Edit Policy Profile

General Access Policies QOS and AVC Mobility Advanced

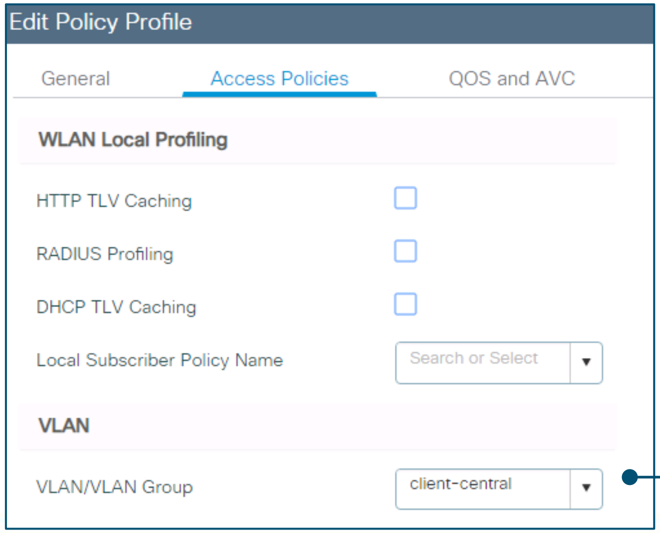
⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name* cwa-policy
Description Enter Description
Status ENABLED
Passive Client DISABLED
Encrypted Traffic Analytics DISABLED

WLAN Switching Policy
Central Switching ☑
Central Authentication ☑
Central DHCP ☑
Central Association ☑
Flex NAT/PAT □

- Enable the profile
- Verify Central Auth is checked
- Anything else can be left to default

2



Edit Policy Profile

General Access Policies QOS and AVC

WLAN Local Profiling
HTTP TLV Caching □
RADIUS Profiling □
DHCP TLV Caching □
Local Subscriber Policy Name Search or Select ▾

VLAN
VLAN/VLAN Group client-central ▾

Under Access Policy tab:

- Select the VLAN you want the guest users to use
- Anything else can be left to default

SAMART TELCOMS

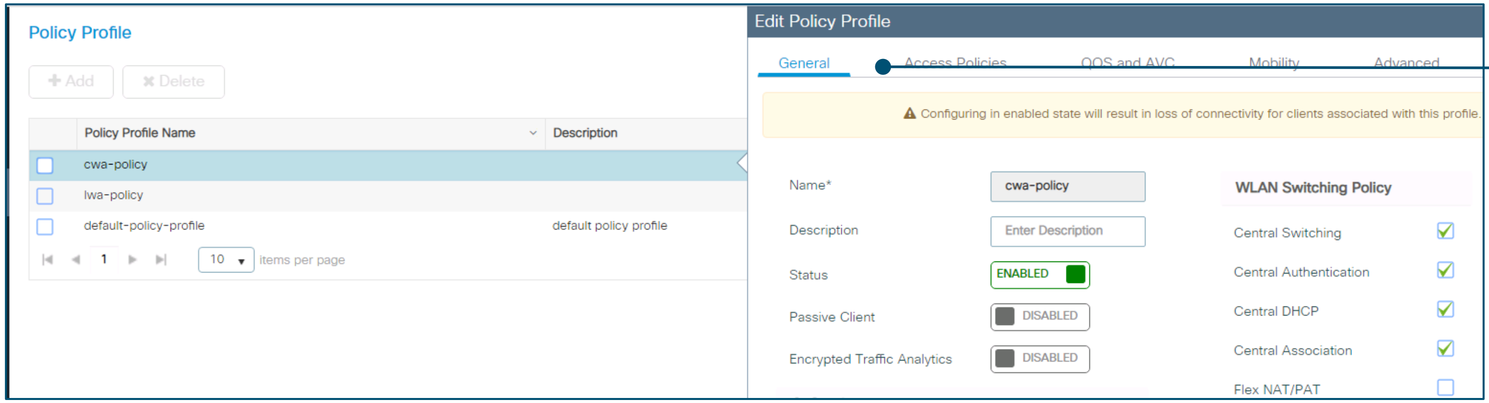
ALERT
ADAPT
ACHIEVE

Configuring Central Webauth (CWA)

Configuring the Policy profile

- Create a new policy profile or modify the default one:

1



Policy Profile

+ Add ✖ Delete

Policy Profile Name	Description
cwa-policy	
lwa-policy	
default-policy-profile	default policy profile

1 10 items per page

Edit Policy Profile

General Access Policies QOS and AVC Mobility Advanced

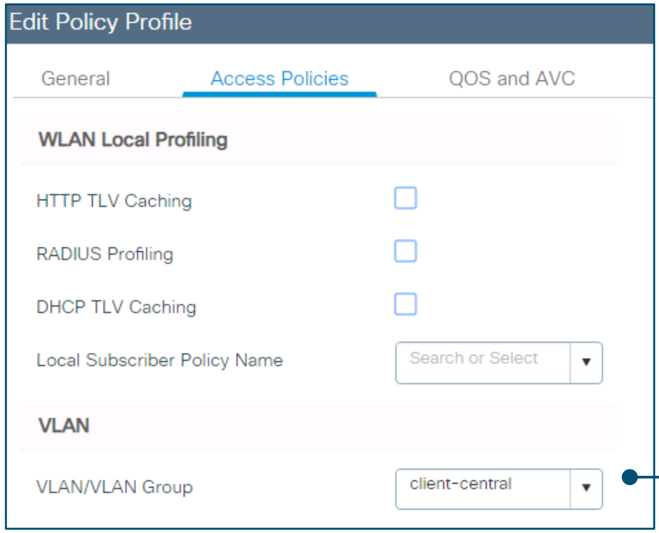
⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name* cwa-policy
Description Enter Description
Status ENABLED
Passive Client DISABLED
Encrypted Traffic Analytics DISABLED

WLAN Switching Policy
Central Switching ☑
Central Authentication ☑
Central DHCP ☑
Central Association ☑
Flex NAT/PAT □

Under **General tab**
- Enable the profile
- Verify Central Auth is checked
- Anything else can be left to default

2



Edit Policy Profile

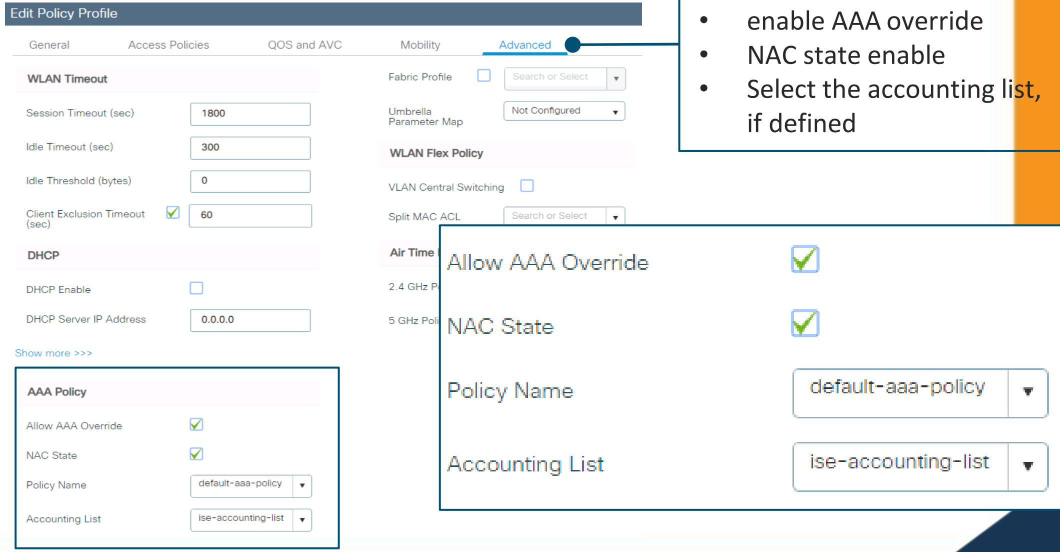
General Access Policies QOS and AVC

WLAN Local Profiling
HTTP TLV Caching □
RADIUS Profiling □
DHCP TLV Caching □
Local Subscriber Policy Name Search or Select

VLAN
VLAN/VLAN Group client-central

Under **Access Policy tab**:
- Select the VLAN you want the guest users to use
- Anything else can be left to default

3



Edit Policy Profile

General Access Policies QOS and AVC Mobility Advanced

WLAN Timeout
Session Timeout (sec) 1800
Idle Timeout (sec) 300
Idle Threshold (bytes) 0
Client Exclusion Timeout (sec) ☑ 60

DHCP
DHCP Enable □
DHCP Server IP Address 0.0.0.0

Show more >>>

AAA Policy
Allow AAA Override ☑
NAC State ☑
Policy Name default-aaa-policy
Accounting List ise-accounting-list

Fabric Profile □ Search or Select
Umbrella Parameter Map Not Configured

WLAN Flex Policy
VLAN Central Switching □
Split MAC ACL Search or Select

Air Time
2.4 GHz P
5 GHz Pol

Allow AAA Override ☑
NAC State ☑
Policy Name default-aaa-policy
Accounting List ise-accounting-list

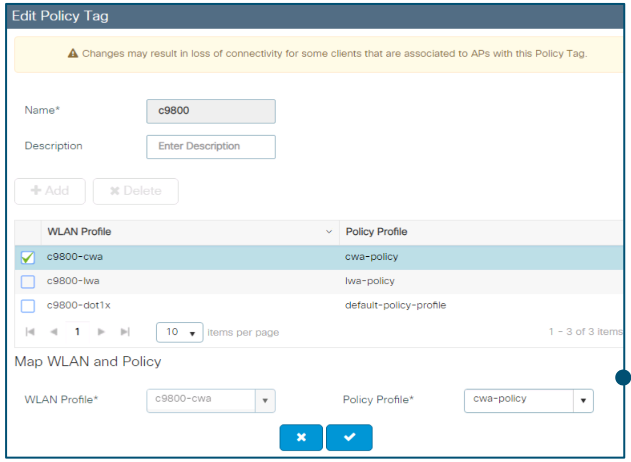
Under **Advanced tab**:
- enable AAA override
- NAC state enable
- Select the accounting list, if defined

SAMART TELCOMS

Configuring Central Webauth (CWA)

Policy Tag and AP assignment

- Define a policy tag and assign it to the APs. Go to Configuration > Tags & Profiles > Tags > Policy and edit the policy tag or create a new one. Associate the WLAN to the Policy profile configured



⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*: c9800

Description: Enter Description

	WLAN Profile	Policy Profile
☑	c9800-cwa	cwa-policy
□	c9800-lwa	lwa-policy
□	c9800-dot1x	default-policy-profile

1 | 10 items per page | 1 - 3 of 3 items

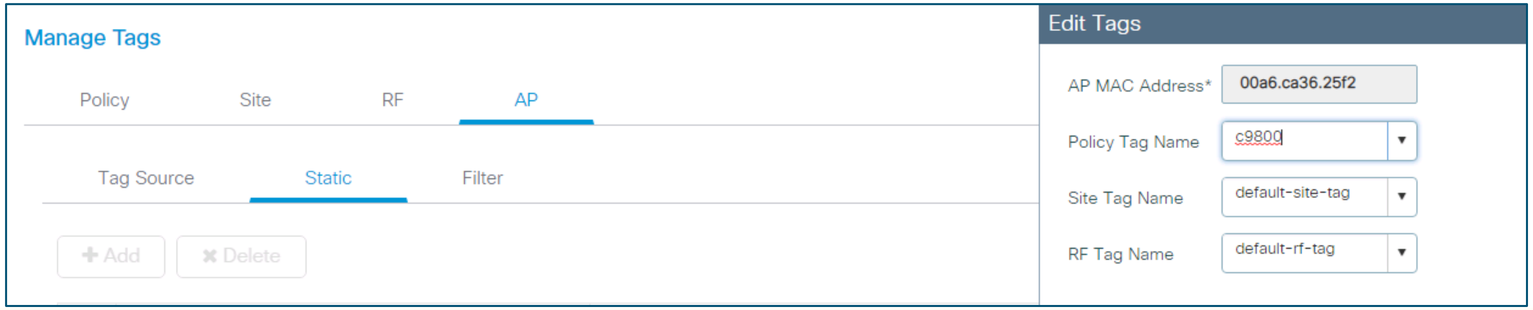
Map WLAN and Policy

WLAN Profile*: c9800-cwa

Policy Profile*: cwa-policy

Associate the WLAN profile c9800-cwa to the corresponding Policy profile configured in the previous step

- Go to Configuration > Tags & Profiles > Tags > AP and assigned the Policy tag to the AP



AP MAC Address*: 00a6.ca36.25f2

Policy Tag Name: c9800

Site Tag Name: default-site-tag

RF Tag Name: default-rf-tag

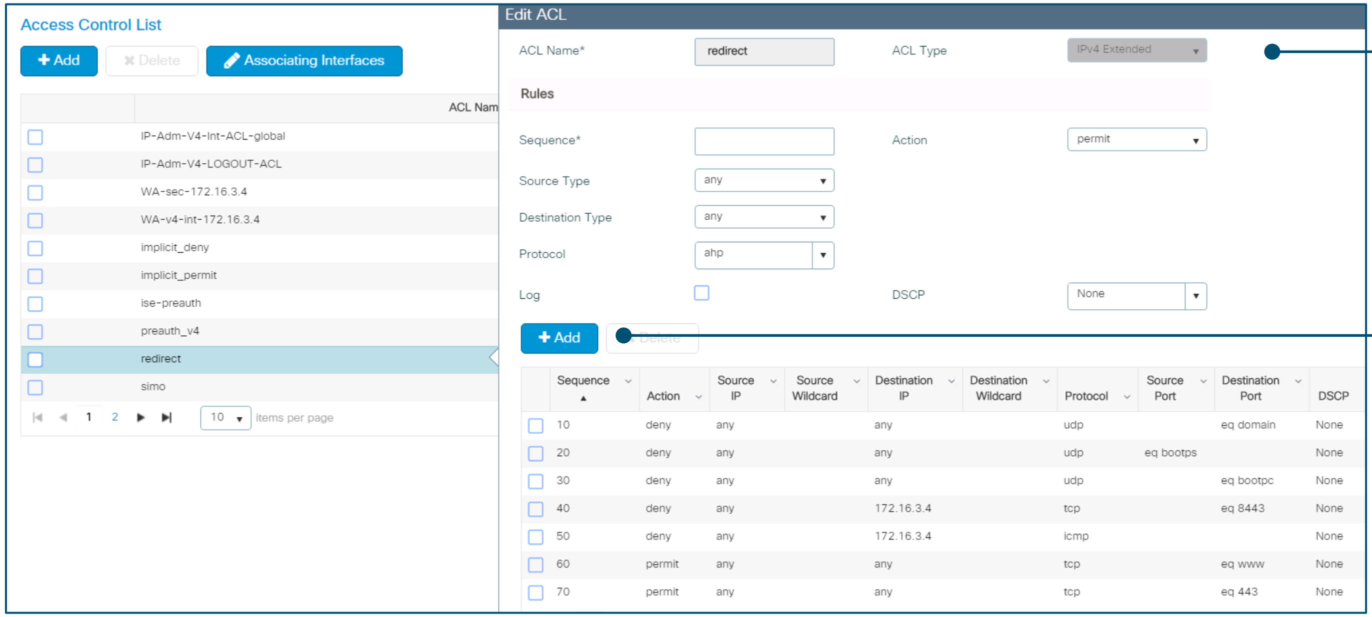
CWA – ISE related configuration

You make networking **possible**

ALERT
ADAPT
ACHIEVE

CWA – ISE related configuration

- The first time, user will be redirected to the ISE Portal for authentication. For the redirection to work, ISE pushes a **redirect ACL**. This needs to be configured on the wireless controller.
- Go to Configuration > Security > ACL and click +Add to create a new ACL:



	ACL Name
□	IP-Adm-V4-Int-ACL-global
□	IP-Adm-V4-LOGOUT-ACL
□	WA-sec-172.16.3.4
□	WA-v4-int-172.16.3.4
□	implicit_deny
□	implicit_permit
□	ise-preauth
□	preauth_v4
□	redirect
□	simo

ACL Name* redirect
ACL Type IPv4 Extended

Rules

Sequence*
Action permit
Source Type any
Destination Type any
Protocol ahp
Log □
DSCP None

	Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP
□	10	deny	any		any		udp		eq domain	None
□	20	deny	any		any		udp	eq bootps		None
□	30	deny	any		any		udp		eq bootpc	None
□	40	deny	any		172.16.3.4		tcp		eq 8443	None
□	50	deny	any		172.16.3.4		icmp			None
□	60	permit	any		any		tcp		eq www	None
□	70	permit	any		any		tcp		eq 443	None

Give it a name and choose type “**ipv4-Extended**”

Click Add to enter the ACL entries:
- Use “**deny**” for traffic you don’t want to redirect (DNS, DHC, ISE portal on port TCP 8443, etc.)
- “**permit**” for traffic that needs redirection (HTTP, HTTPs)

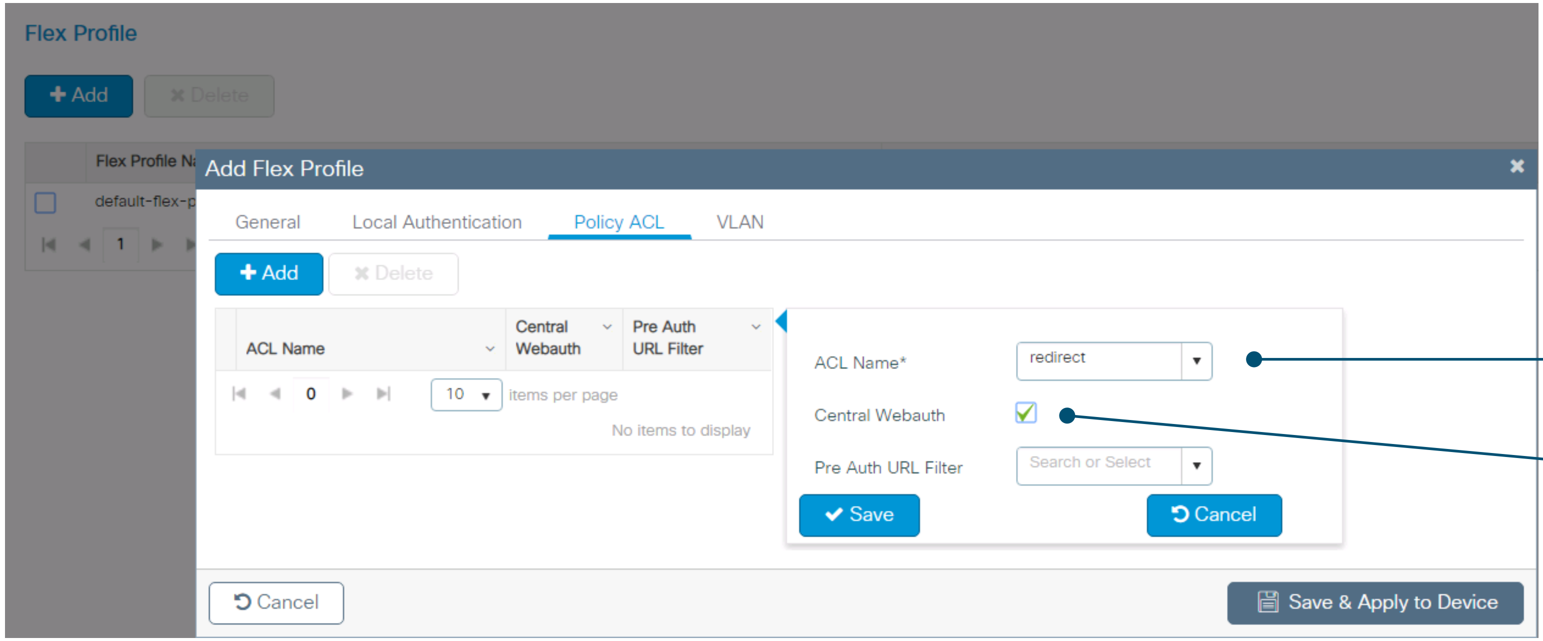
```
c9800#sh access-list redirect

Extended IP access list redirect
10 deny udp any any eq domain
20 deny udp any eq bootps any
30 deny udp any any eq bootpc
40 deny tcp any host 172.16.3.4 eq 8443
50 deny icmp any host 172.16.3.4
60 permit tcp any any eq www
70 permit tcp any any eq 443
```

Replace “172.16.3.4” with your ISE PSN IP address
ICMP is optional, good for testing reachability

SAMART TELCOMS

CWA – ISE related configuration

- If using Flex local switching the redirect ACL needs to be pushed to the APs. Go to Configuration > Tags & Profiles > Flex and click on the Flex profile. Go to the Policy ACL tab.



ACL Name*: redirect

Central Webauth: ☑

Pre Auth URL Filter: Search or Select

Choose the same ACL name defined previously

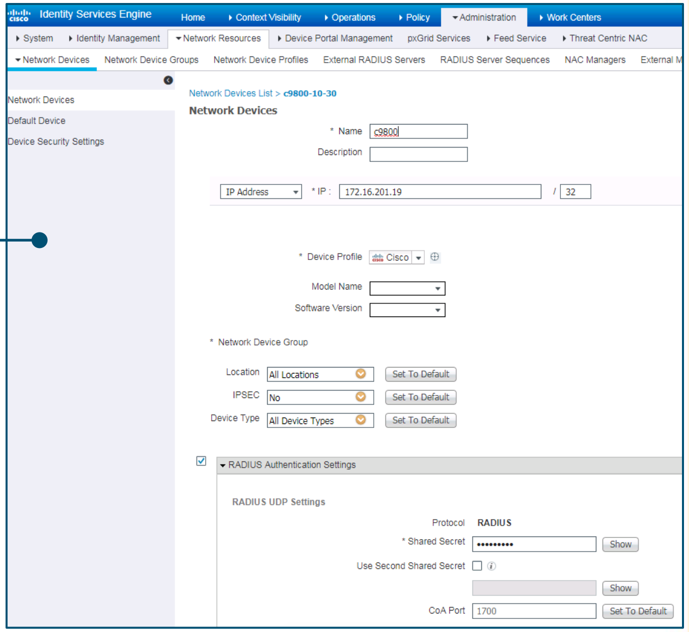
Select Central Webauth (*)

(*) This checkbox automatically inverts the ACL entries on the AP. This is because a "deny" statement means "do not redirect" on the C9800 IOS-XE, however on the AP the "deny" statement means the opposite, so this checkbox automatically swaps all permits and deny when pushing to the AP. You can verify this with a "show ip access list" form the AP CLI)

CWA – ISE related configuration

- On ISE, add the C9800 wireless controller as a network device. Go to Administration > Network Resources > Network Devices and click on +Add. Fill in the required info
- Create a authorization profile to redirect users. Go to Policy > Policy Elements > Results > Authorization > Authorization Profiles > and click +Add:

1



Network Devices List > **c9800-10-30**

Network Devices

* Name: c9800

Description:

IP Address * IP : 172.16.201.19 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations

IPSEC: No

Device Type: All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

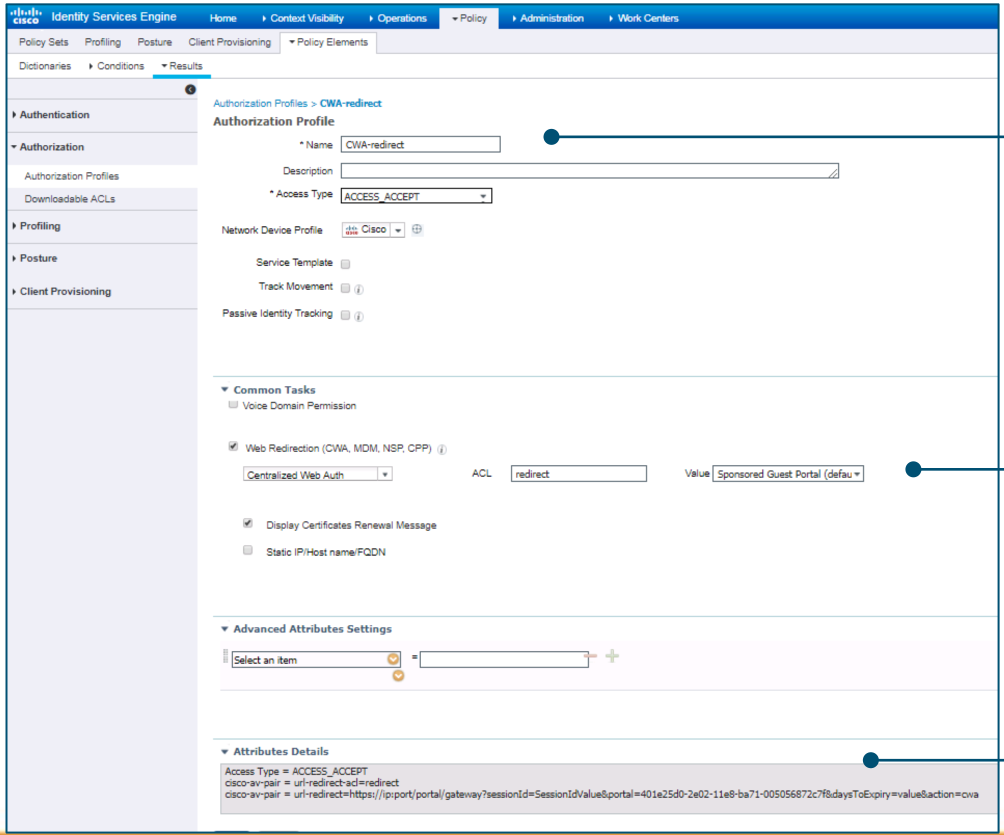
Protocol: **RADIUS**

* Shared Secret: ••••••••••

Use Second Shared Secret ☐

CoA Port: 1700

2



Authorization Profiles > **CWA-redirect**

Authorization Profile

* Name: CWA-redirect

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

Common Tasks

☐ Voice Domain Permission

☑ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth — ACL: redirect — Value: Sponsored Guest Portal (defau

☑ Display Certificates Renewal Message

☐ Static IP/Host name/FQDN

Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=401e25d0-2e02-11e8-ba71-005056872c7f&daysToExpiry=value&action=cwa
```

Pick a name

Under Common tasks:

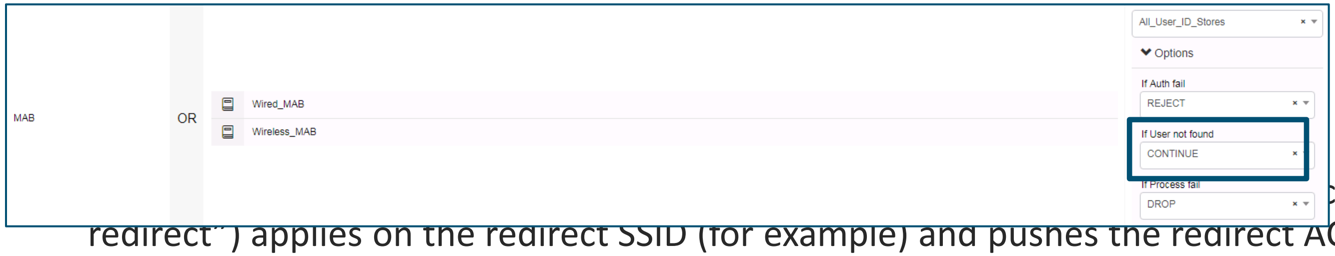
- Scroll down and select Web Redirection
- ACL = acl name previously configured (“redirect” in this case)
- Value can be left as default (Sponsored Guest Portal)

This is what will be pushed to the Wireless controller

ALERT
ADAPT
ACHIEVE

CWA – ISE related configuration

- Configure the Authentication rule. Go to Policy > Policy Set > Authentication Policy and modify the MAB policy to continue if user not found



MAB OR

Wired_MAB

Wireless_MAB

All_User_ID_Stores

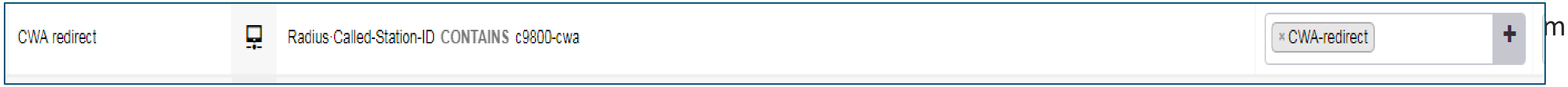
Options

If Auth fail: REJECT

If User not found: CONTINUE

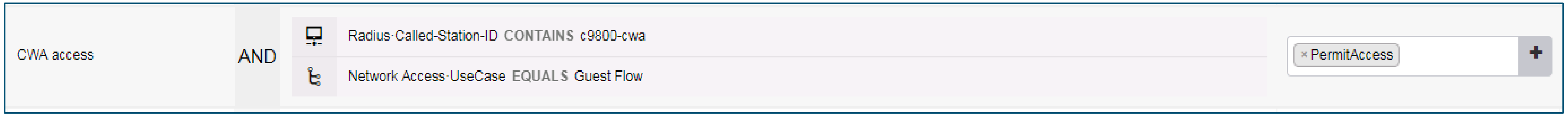
If Process fail: DROP

cy and add two rules for CWA. The first rule (called here “CWA redirect”) applies on the redirect SSID (for example) and pushes the redirect ACL.



CWA redirect	Radius·Called-Station-ID CONTAINS c9800-cwa	CWA-redirect

mit access.

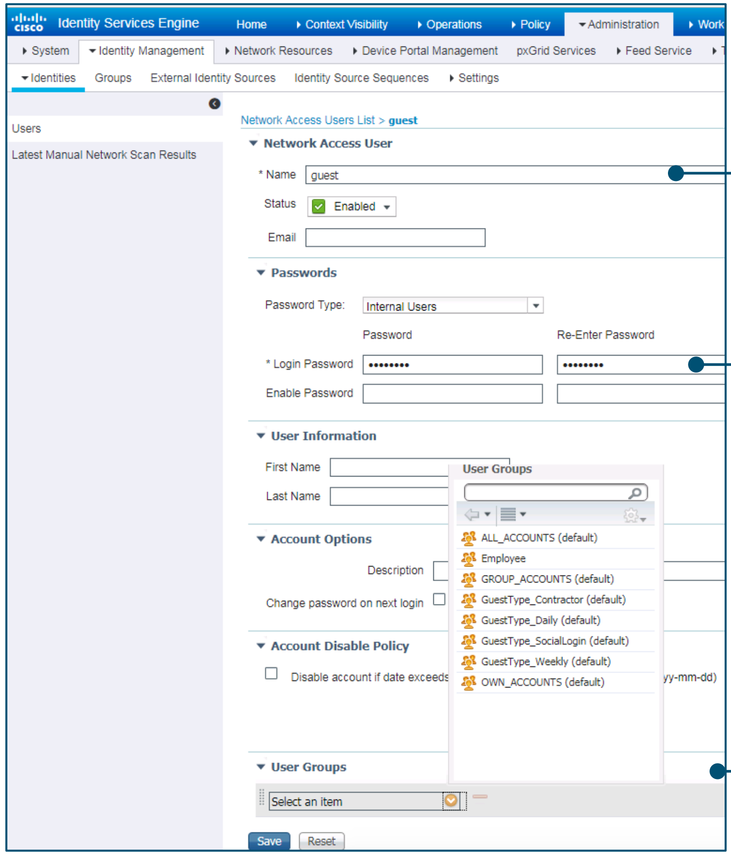


CWA access	AND	Radius·Called-Station-ID CONTAINS c9800-cwa Network Access·UseCase EQUALS Guest Flow	PermitAccess

SAMART
TELCOMS

CWA – ISE related configuration

- Finally you would need to define a Guest user. Go to Administration > Identity and configure and click on +Add:



Network Access Users List > guest

Network Access User

* Name: guest

Status: ☑ Enabled

Email:

Passwords

Password Type: Internal Users

	Password	Re-Enter Password
* Login Password	••••••••	••••••••
Enable Password		

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login □

Account Disable Policy

□ Disable account if date exceeds ... yy-mm-dd)

User Groups

Select an item

User Groups

- ALL_ACCOUNTS (default)
- Employee
- GROUP_ACCOUNTS (default)
- GuestType_Contractor (default)
- GuestType_Daily (default)
- GuestType_SocialLogin (default)
- GuestType_Weekly (default)
- OWN_ACCOUNTS (default)

Choose the username

Choose the password

Select a user group. You can choose ALL_Accounts or you can pick a more specific one

Catalyst 9800 Wireless Controller Configuration Model

You make customer experience **possible**

Benefits of New Configuration Model

Reusability
Config modularized as objects

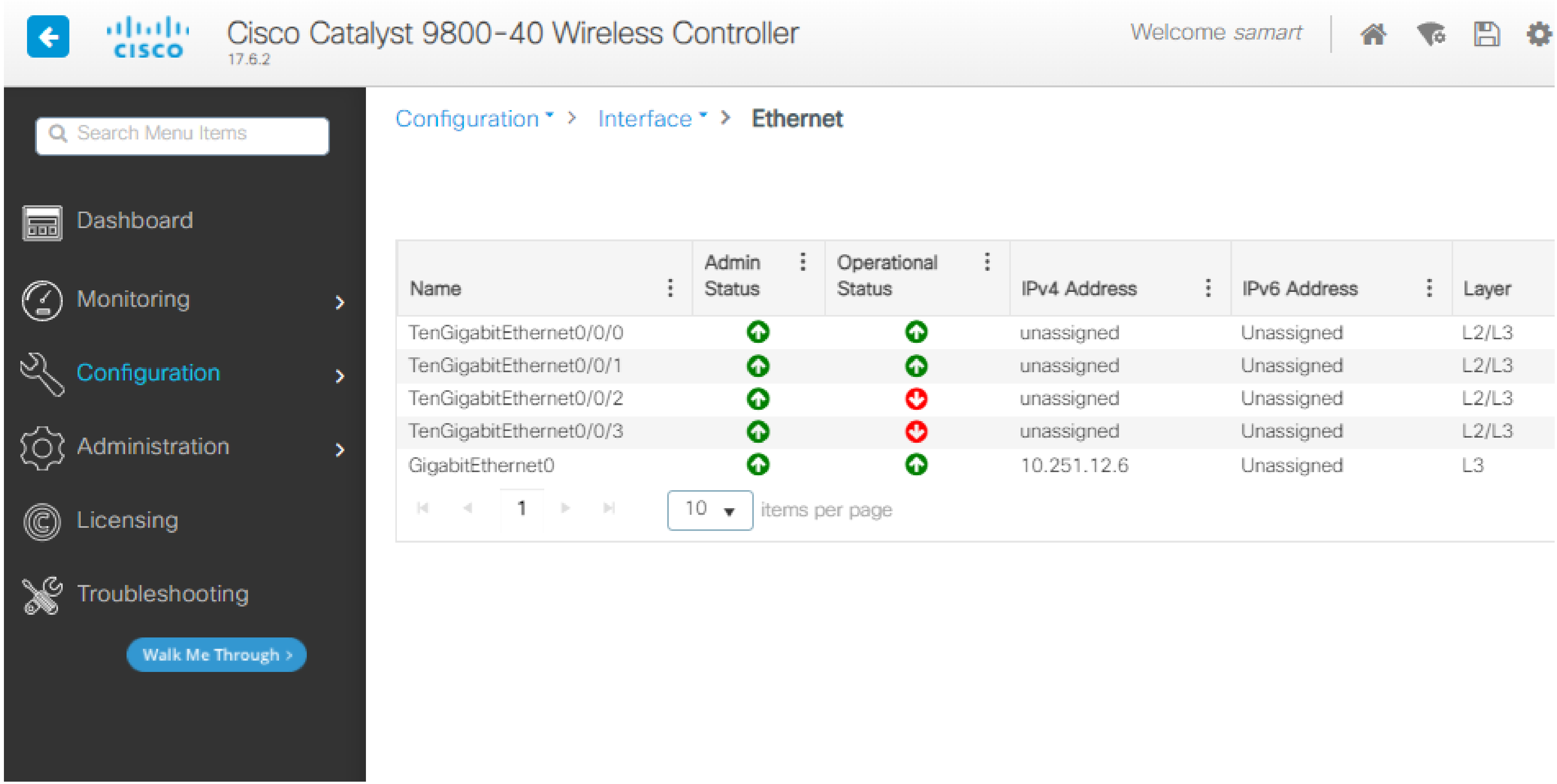
Simplicity
No inheritance or containers

Easy Provisioning
With AP attribute Tagging

Rule-based Tagging
For easy Day 1 configuration

Change Management
Site based filtering

Config Interface

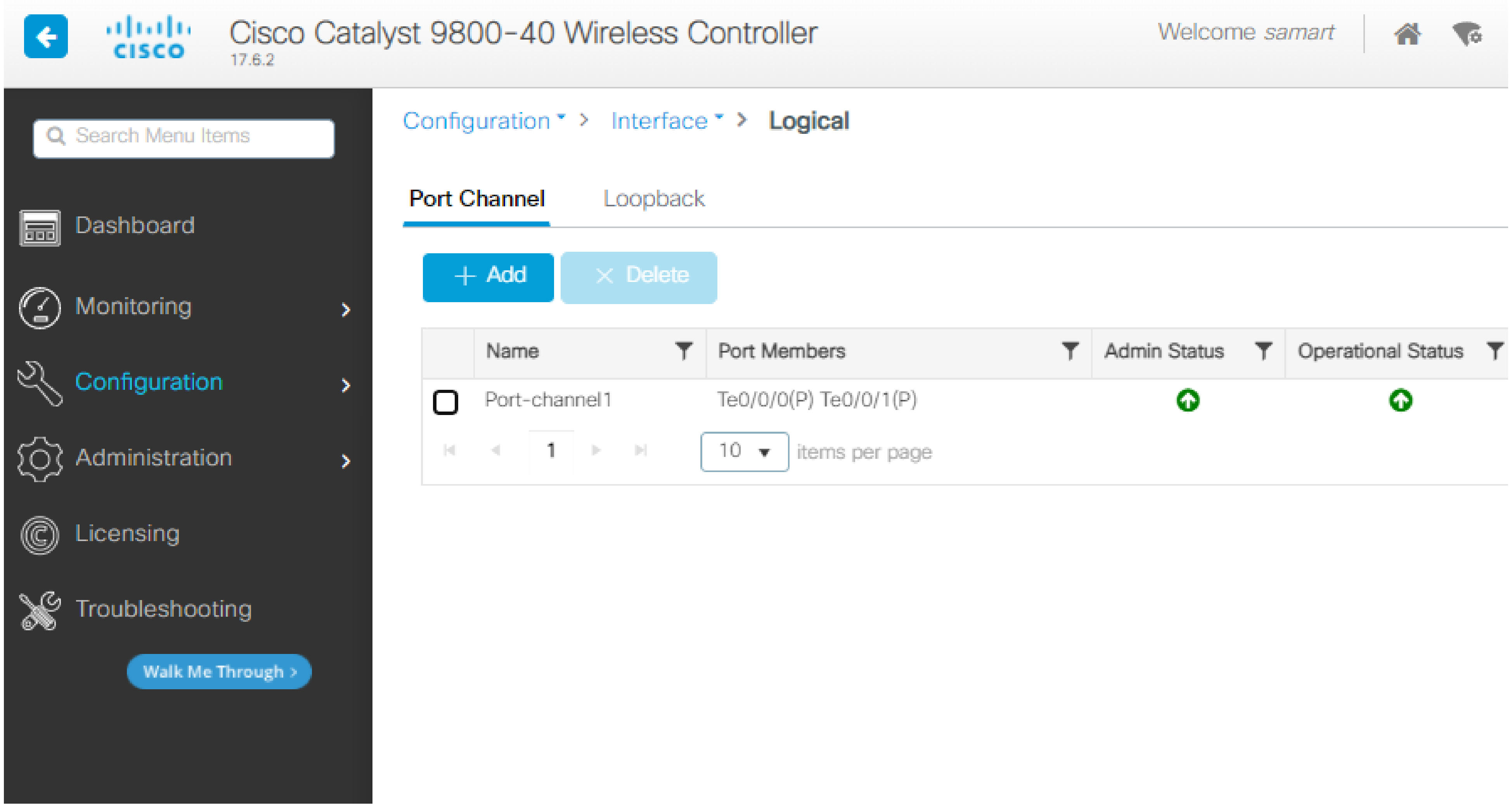


Configuration › Interface › Ethernet

Name	Admin Status	Operational Status	IPv4 Address	IPv6 Address	Layer
TenGigabitEthernet0/0/0	↑	↑	unassigned	Unassigned	L2/L3
TenGigabitEthernet0/0/1	↑	↑	unassigned	Unassigned	L2/L3
TenGigabitEthernet0/0/2	↑	↓	unassigned	Unassigned	L2/L3
TenGigabitEthernet0/0/3	↑	↓	unassigned	Unassigned	L2/L3
GigabitEthernet0	↑	↑	10.251.12.6	Unassigned	L3

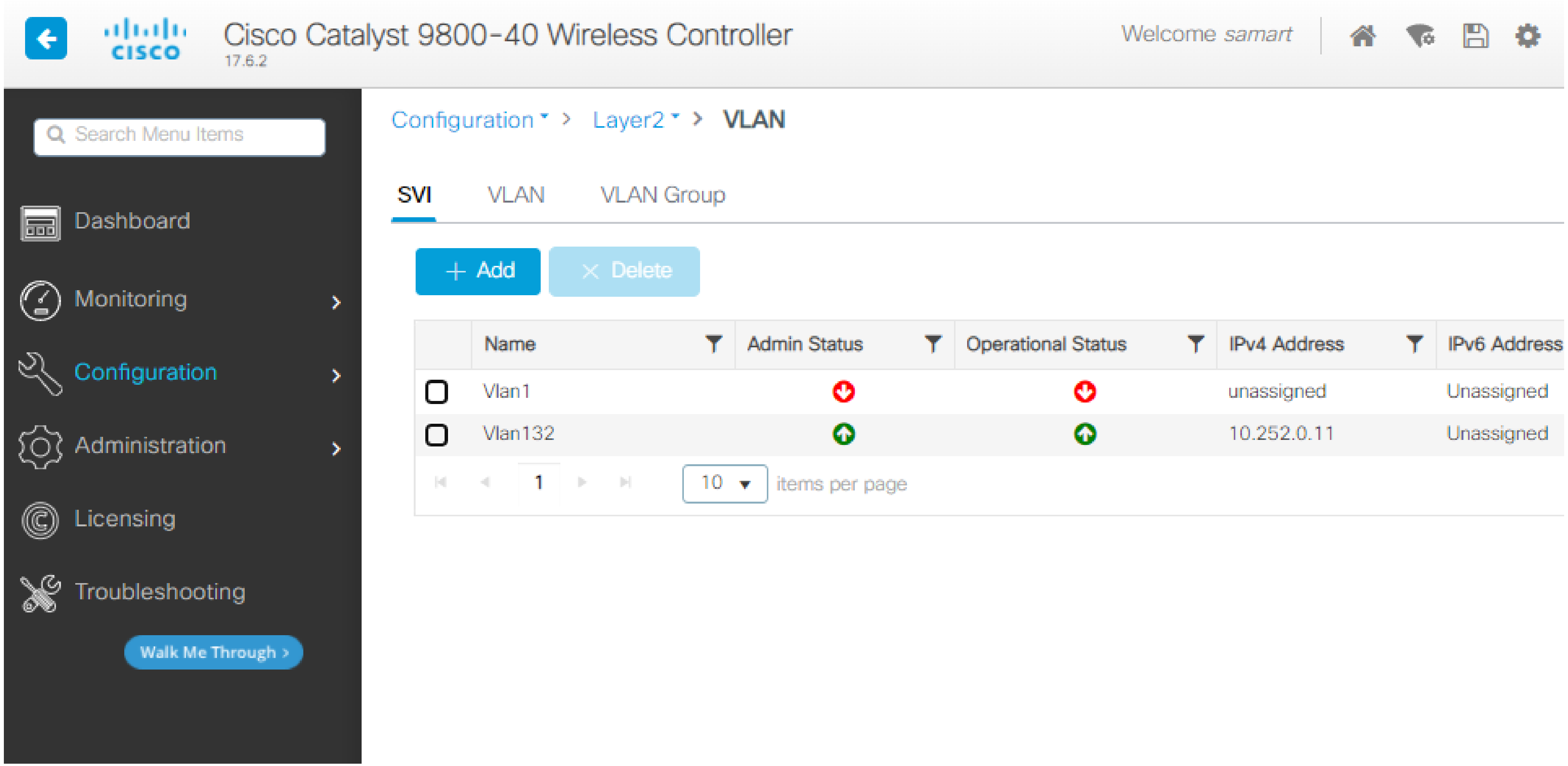
1 — 10 items per page

Config Interface



☐	Name	Port Members	Admin Status	Operational Status
☐	Port-channel1	Te0/0/0(P) Te0/0/1(P)	↑	↑

Config Vlan



Configuration › Layer2 › VLAN

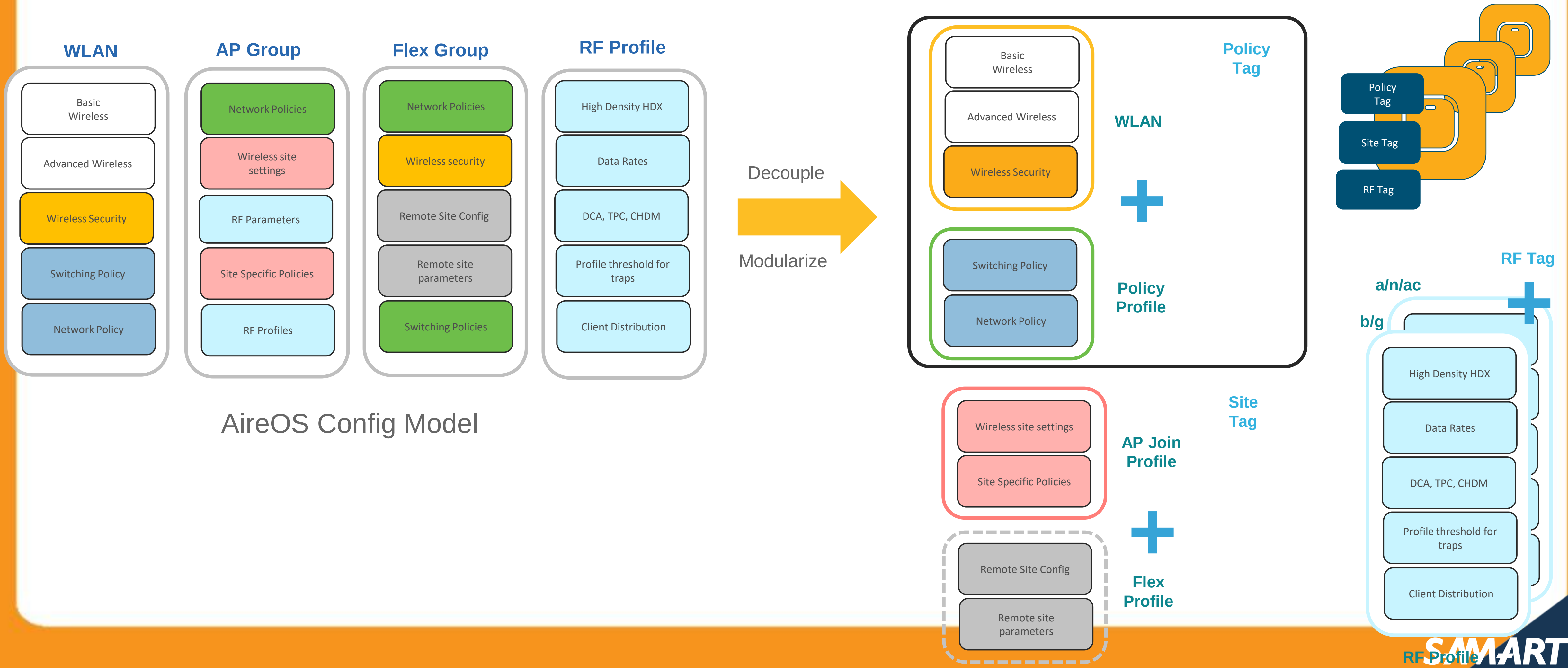
	Name	Admin Status	Operational Status	IPv4 Address	IPv6 Address
□	Vlan1	↓	↓	unassigned	Unassigned
□	Vlan132	↑	↑	10.252.0.11	Unassigned

1 | 10 items per page

AireOS vs. Catalyst 9800 Config Model

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

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



WLAN
- Basic Wireless
- Advanced Wireless
- Wireless Security
- Switching Policy
- Network Policy

AP Group
- Network Policies
- Wireless site settings
- RF Parameters
- Site Specific Policies
- RF Profiles

Flex Group
- Network Policies
- Wireless security
- Remote Site Config
- Remote site parameters
- Switching Policies

RF Profile
- High Density HDX
- Data Rates
- DCA, TPC, CHDM
- Profile threshold for traps
- Client Distribution

AireOS Config Model

Decouple

Modularize

Policy Tag

WLAN
- Basic Wireless
- Advanced Wireless
- Wireless Security

+

Policy Profile
- Switching Policy
- Network Policy

Site Tag

AP Join Profile
- Wireless site settings
- Site Specific Policies

+

Flex Profile
- Remote Site Config
- Remote site parameters

Policy Tag

Site Tag

RF Tag

RF Tag

a/n/ac

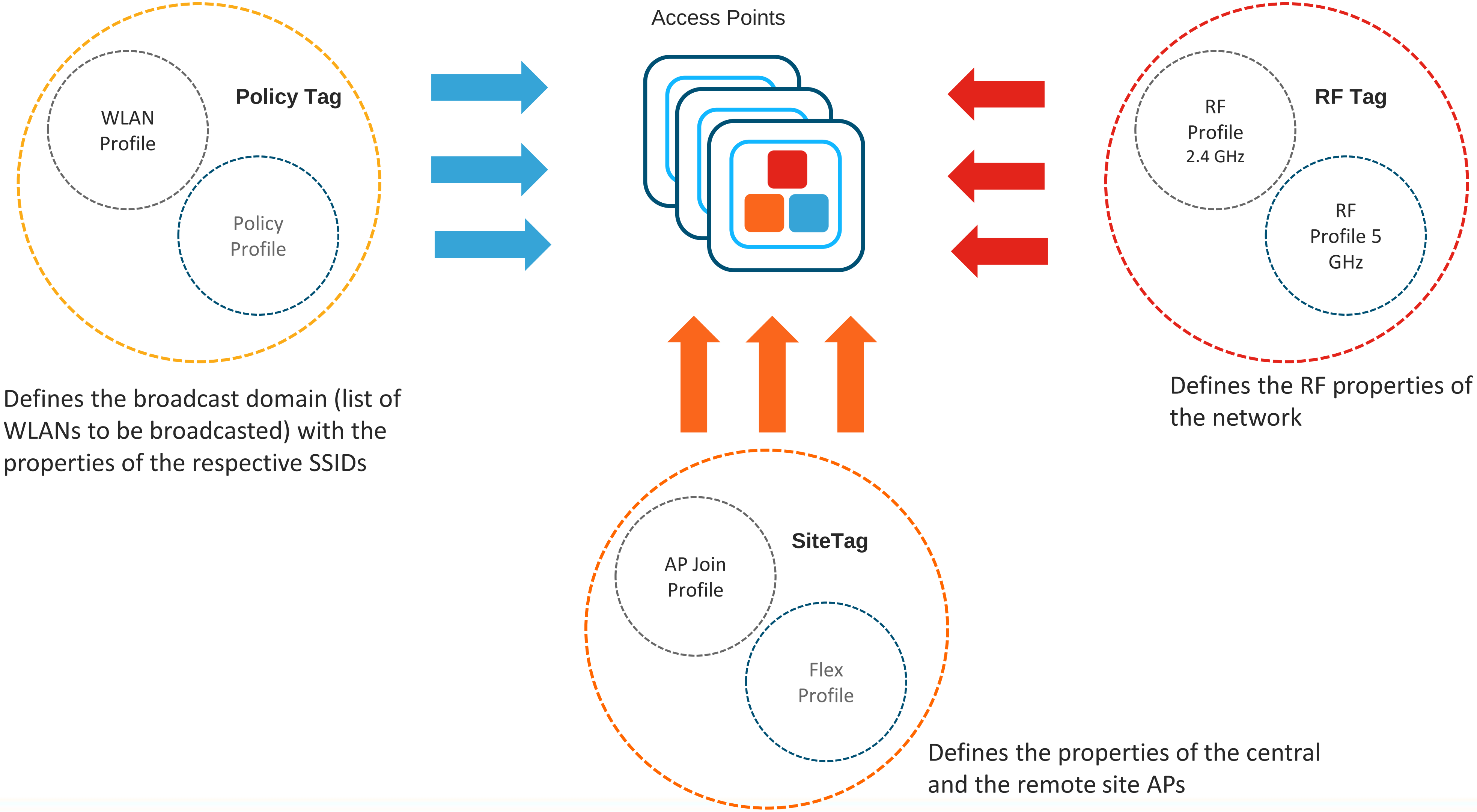
b/g

+

RF Profile
- High Density HDX
- Data Rates
- DCA, TPC, CHDM
- Profile threshold for traps
- Client Distribution

ALERT
ADAPT
ACHIEVE

Cisco 9800 Catalyst 9800 Config Model



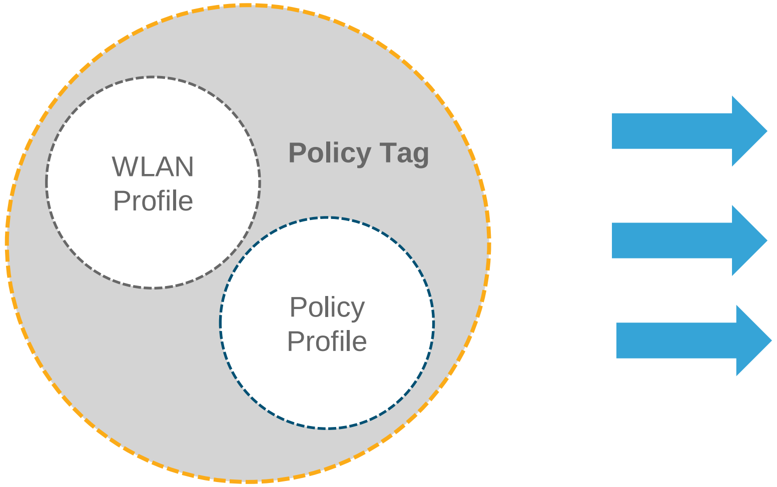
Defines the broadcast domain (list of WLANs to be broadcasted) with the properties of the respective SSIDs

Defines the RF properties of the network

Defines the properties of the central and the remote site APs

SAMART
TELCOMS

Components of Policy Tag



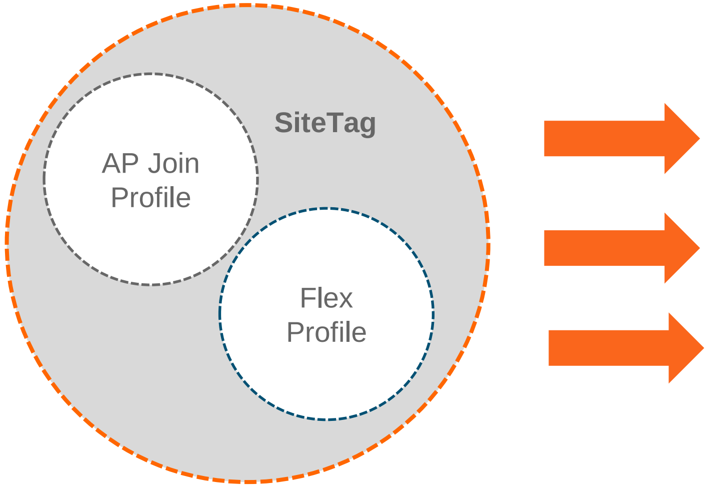
Components of WLAN Profile

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”

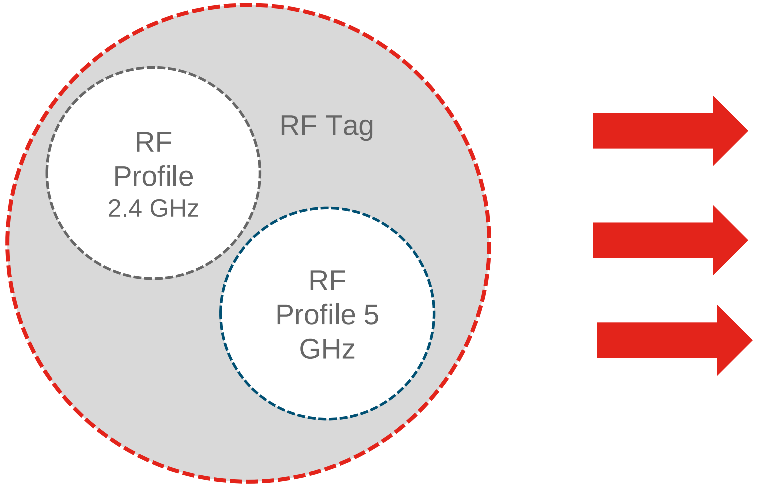
Syslog - “current default”

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

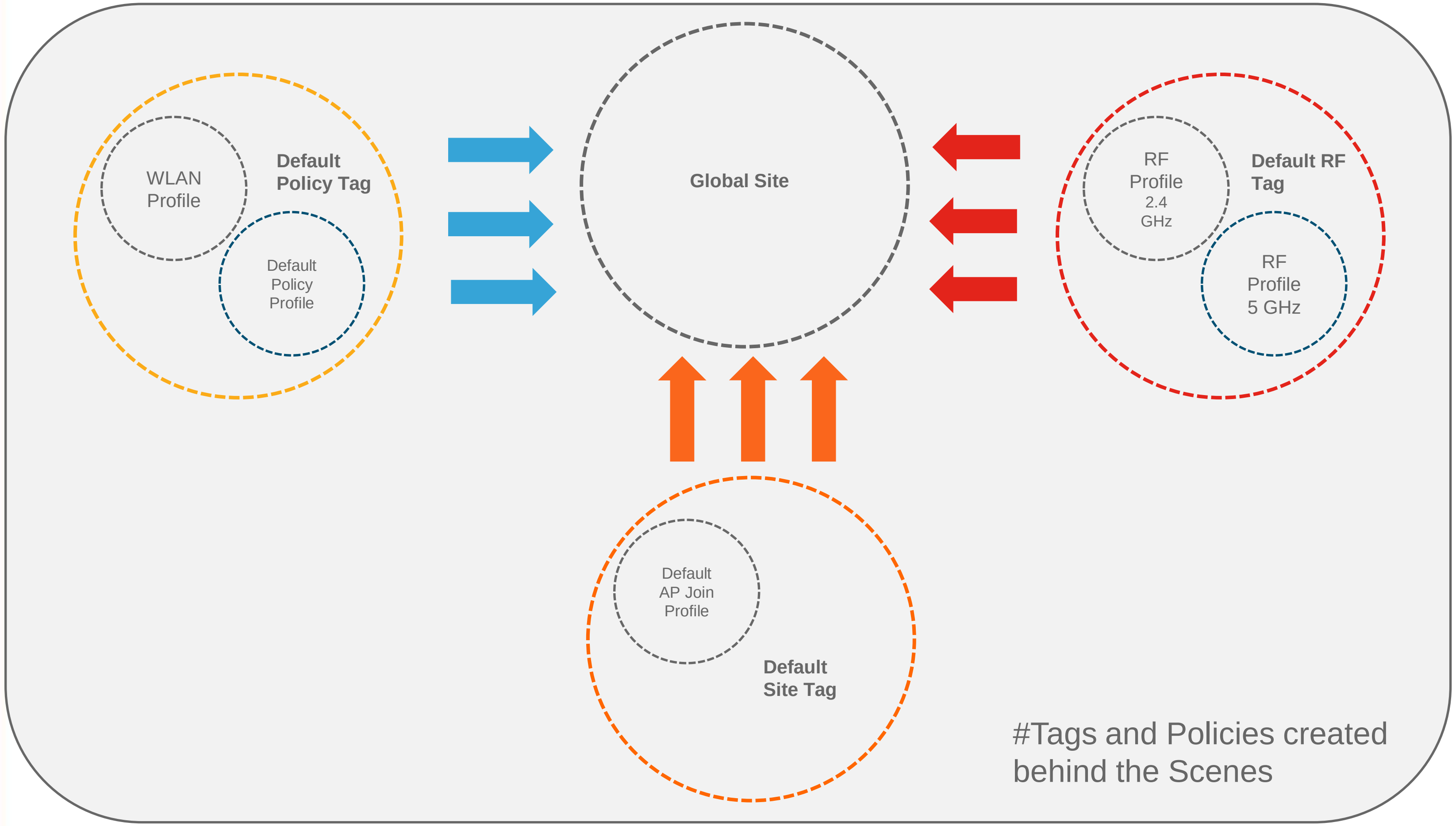
Multicast Data Rates

Rx Sop Threshold

Load Balancing (window & denial)

Band Select Parameters (Applicable only for 802.11bg)

Day 0 - Backend Constructs



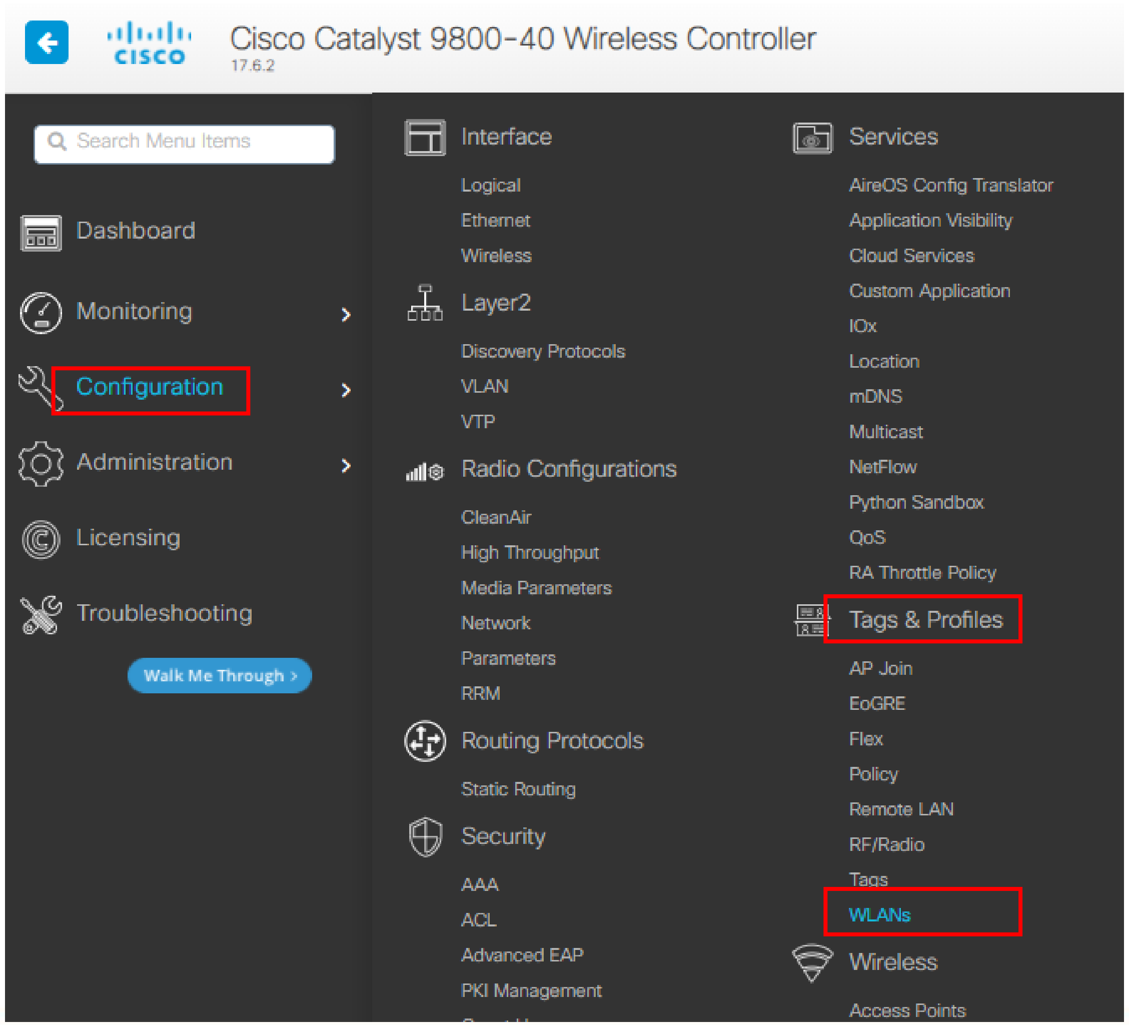
#Tags and Policies created behind the Scenes

- Creation of WLAN profiles
- Pre-provisioned Default Policy Profile
- Mapping of WLAN profiles to Default Policy Tag
- Pre-provisioned default RF Tag and Profiles
- Pre-provisioned Default Site Tag and AP Join Profile

ALERT
ADAPT
ACHIEVE

การสร้าง WLAN

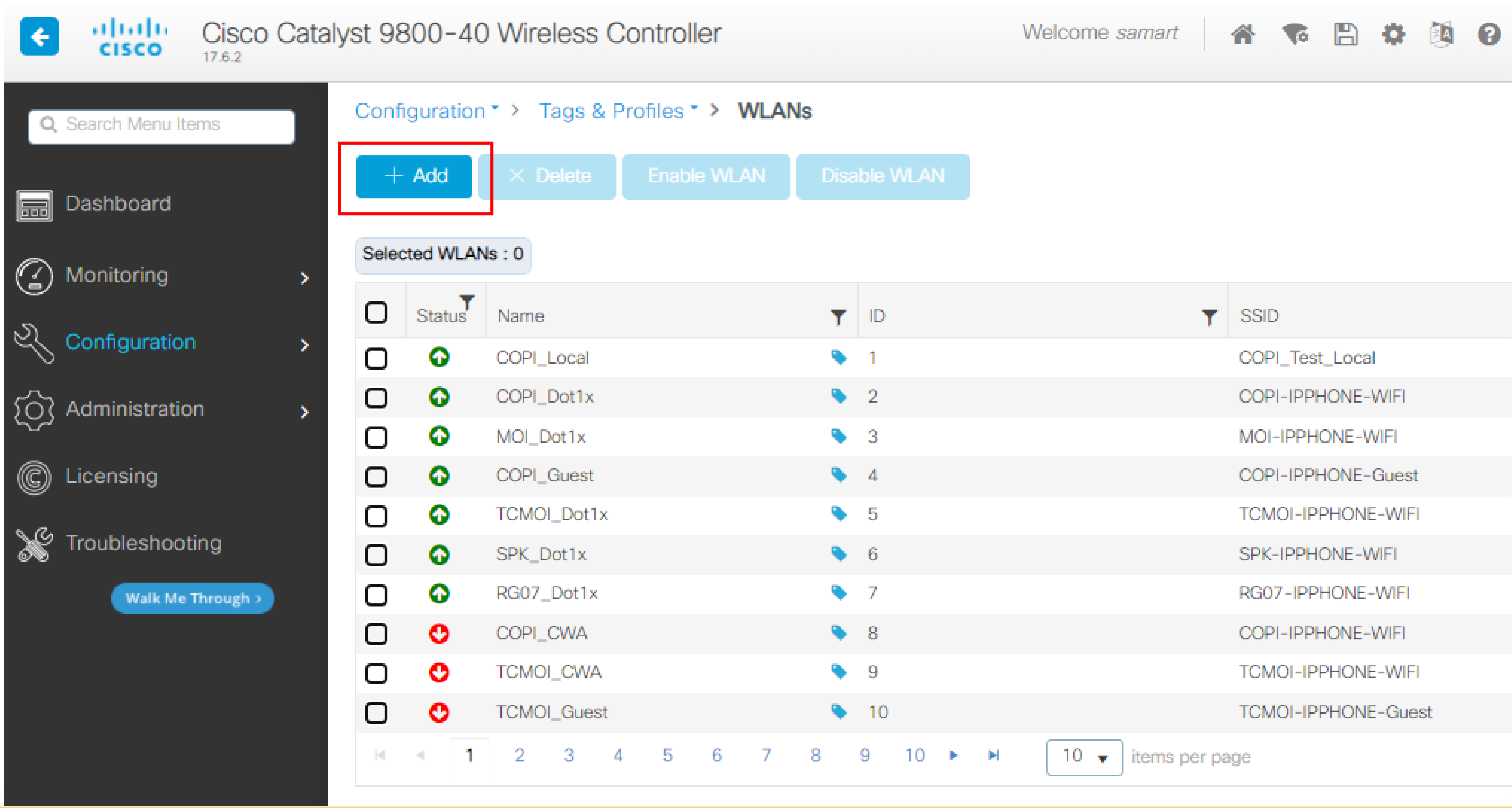
Step 1. Select Configuration > Tag & Profiles > WLANs



SAMART TELCOMS

การสร้าง WLAN

Step 2. Select Add

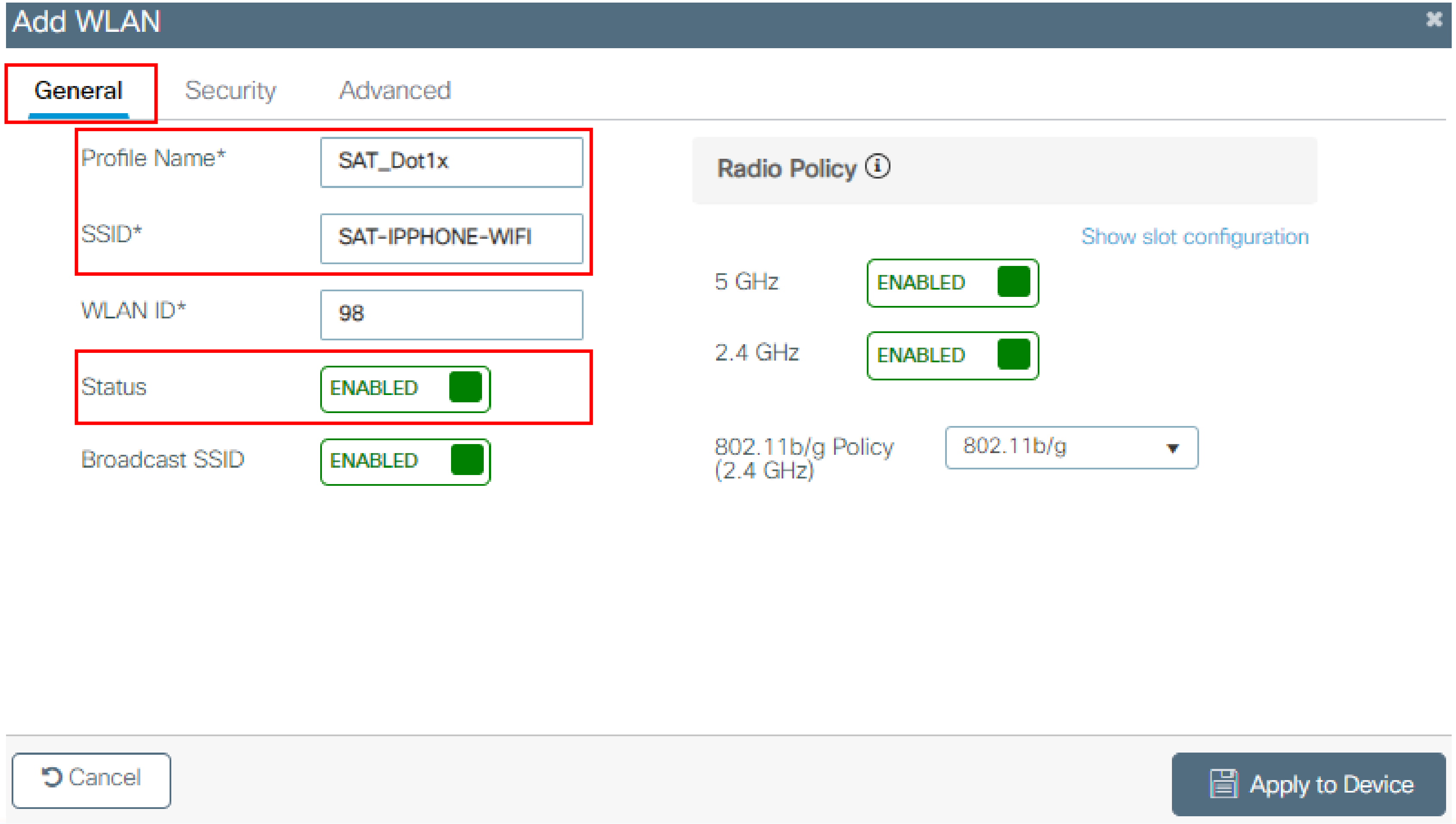


Selected WLANs : 0

□	Status	Name	ID	SSID
□	⬆	COPI_Local	1	COPI_Test_Local
□	⬆	COPI_Dot1x	2	COPI-IPPHONE-WIFI
□	⬆	MOI_Dot1x	3	MOI-IPPHONE-WIFI
□	⬆	COPI_Guest	4	COPI-IPPHONE-Guest
□	⬆	TCMOI_Dot1x	5	TCMOI-IPPHONE-WIFI
□	⬆	SPK_Dot1x	6	SPK-IPPHONE-WIFI
□	⬆	RG07_Dot1x	7	RG07-IPPHONE-WIFI
□	⬇	COPI_CWA	8	COPI-IPPHONE-WIFI
□	⬇	TCMOI_CWA	9	TCMOI-IPPHONE-WIFI
□	⬇	TCMOI_Guest	10	TCMOI-IPPHONE-Guest

การสร้าง WLAN

Step 3. Select General



Add WLAN

General | Security | Advanced

Profile Name* SAT_Dot1x

SSID* SAT-IPPHONE-WIFI

WLAN ID* 98

Status ENABLED

Broadcast SSID ENABLED

Radio Policy ⓘ

Show slot configuration

5 GHz ENABLED

2.4 GHz ENABLED

802.11b/g Policy (2.4 GHz) 802.11b/g ▾

Cancel

Apply to Device

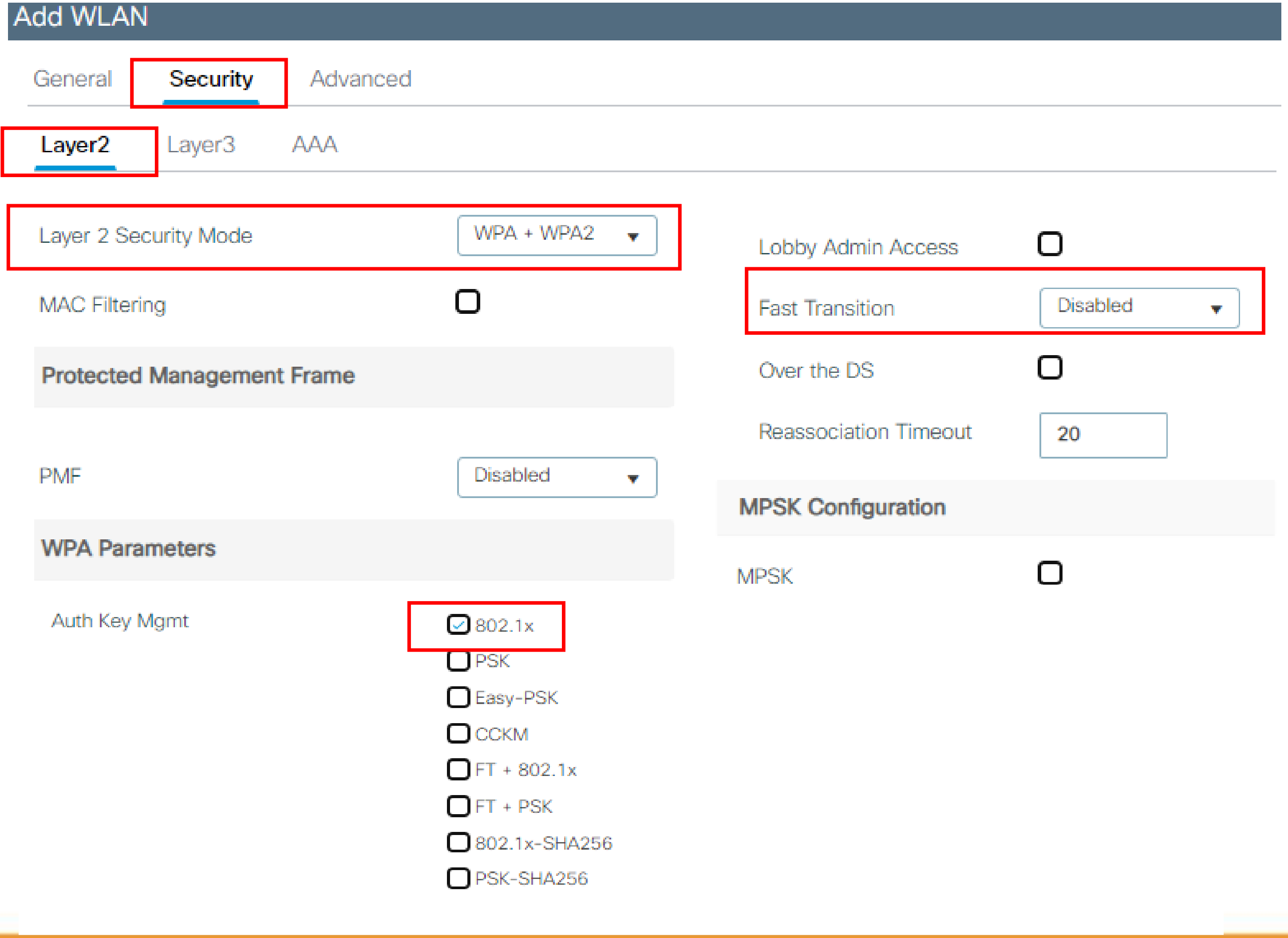
ทำการใส่ข้อมูลดังนี้

- Profile Name
- SSID
- Status Enable

ALERT
ADAPT
ACHIEVE

การสร้าง WLAN

Step 4. Select Security > Layer2



Add WLAN

General | **Security** | Advanced

Layer2 | Layer3 | AAA

Layer 2 Security Mode: WPA + WPA2 ▾

MAC Filtering □

Protected Management Frame

PMF: Disabled ▾

WPA Parameters

Auth Key Mgmt:
☑ 802.1x
□ PSK
□ Easy-PSK
□ CCKM
□ FT + 802.1x
□ FT + PSK
□ 802.1x-SHA256
□ PSK-SHA256

Lobby Admin Access □

Fast Transition: Disabled ▾

Over the DS □

Reassociation Timeout: 20

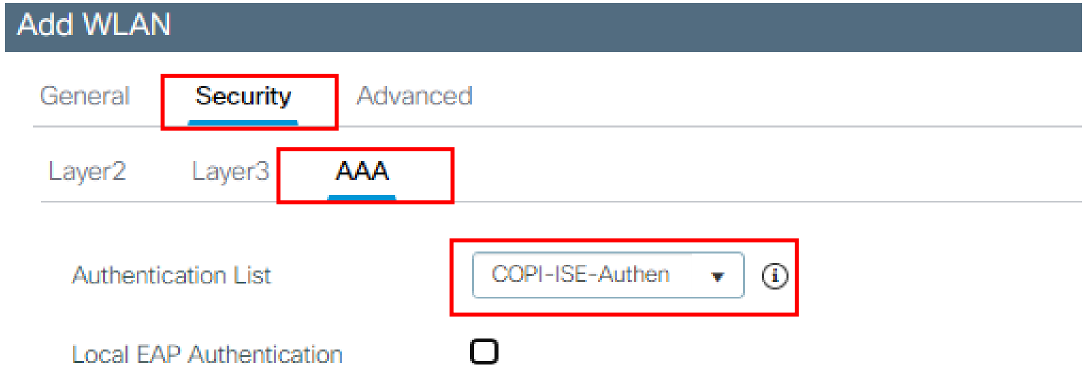
MPSK Configuration

MPSK □

ทำการเลือกข้อมูลดังนี้
- Layer 2 Security Mode = WPA+WPA2
- Fast Transition = Disable
- Auth Key Mgmt = 802.1x

การสร้าง WLAN

Step 5. Select Security > AAA > Authentication List



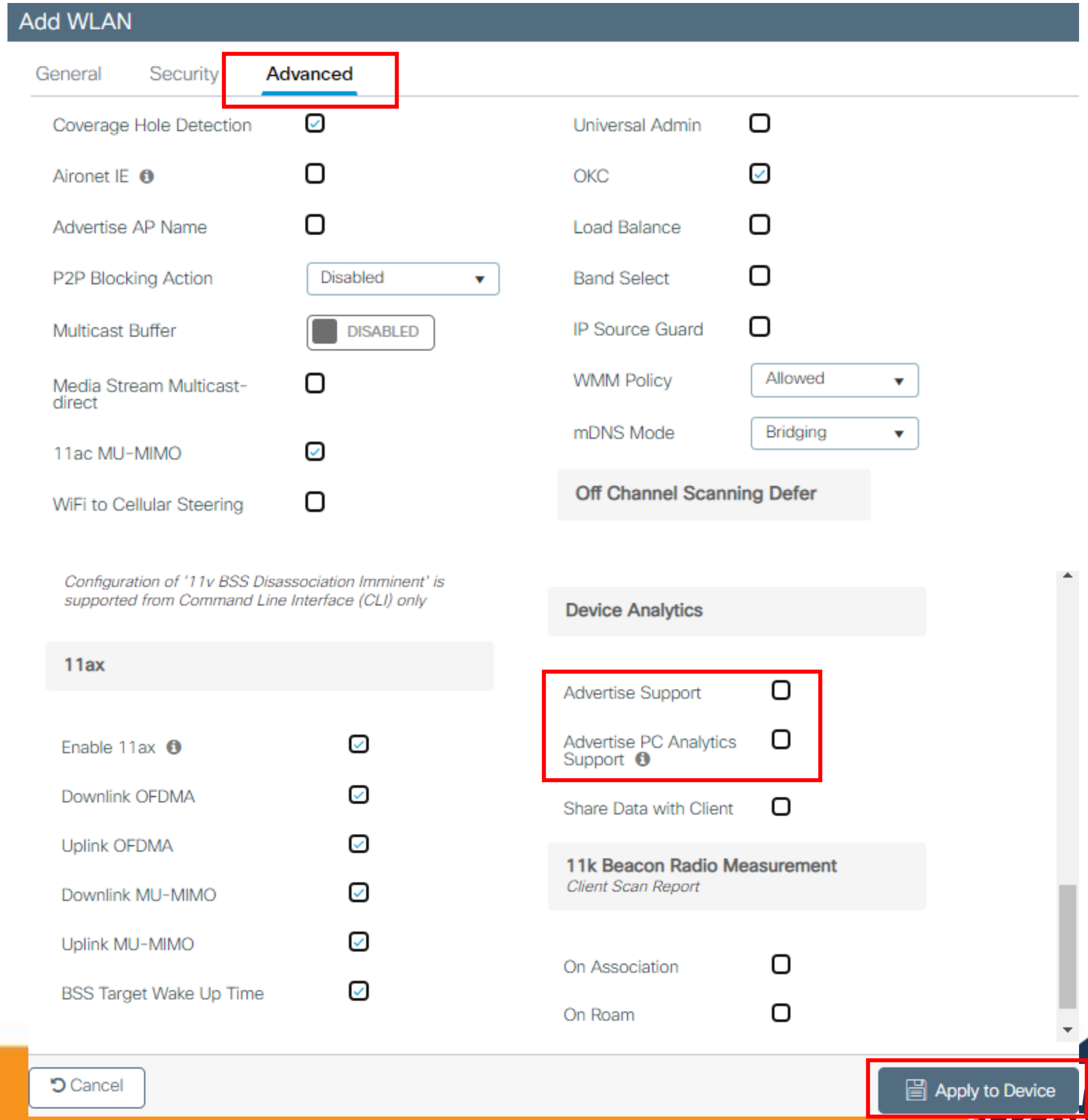
Add WLAN

Authentication List: COPI-ISE-Authen ▾

Local EAP Authentication □

Authentication List ให้เลือก
“COPI-ISE-Authen”

Step 6. Select Advanced > Device Analytics



Add WLAN

Coverage Hole Detection ☑

Aironet IE □

Advertise AP Name □

P2P Blocking Action: Disabled ▾

Multicast Buffer: DISABLED

Media Stream Multicast-direct □

11ac MU-MIMO ☑

WiFi to Cellular Steering □

Universal Admin □

OKC ☑

Load Balance □

Band Select □

IP Source Guard □

WMM Policy: Allowed ▾

mDNS Mode: Bridging ▾

Off Channel Scanning Defer

Configuration of '11v BSS Disassociation Imminent' is supported from Command Line Interface (CLI) only

11ax

Enable 11ax ☑

Downlink OFDMA ☑

Uplink OFDMA ☑

Downlink MU-MIMO ☑

Uplink MU-MIMO ☑

BSS Target Wake Up Time ☑

Device Analytics

Advertise Support □

Advertise PC Analytics Support □

Share Data with Client □

11k Beacon Radio Measurement
Client Scan Report

On Association □

On Roam □

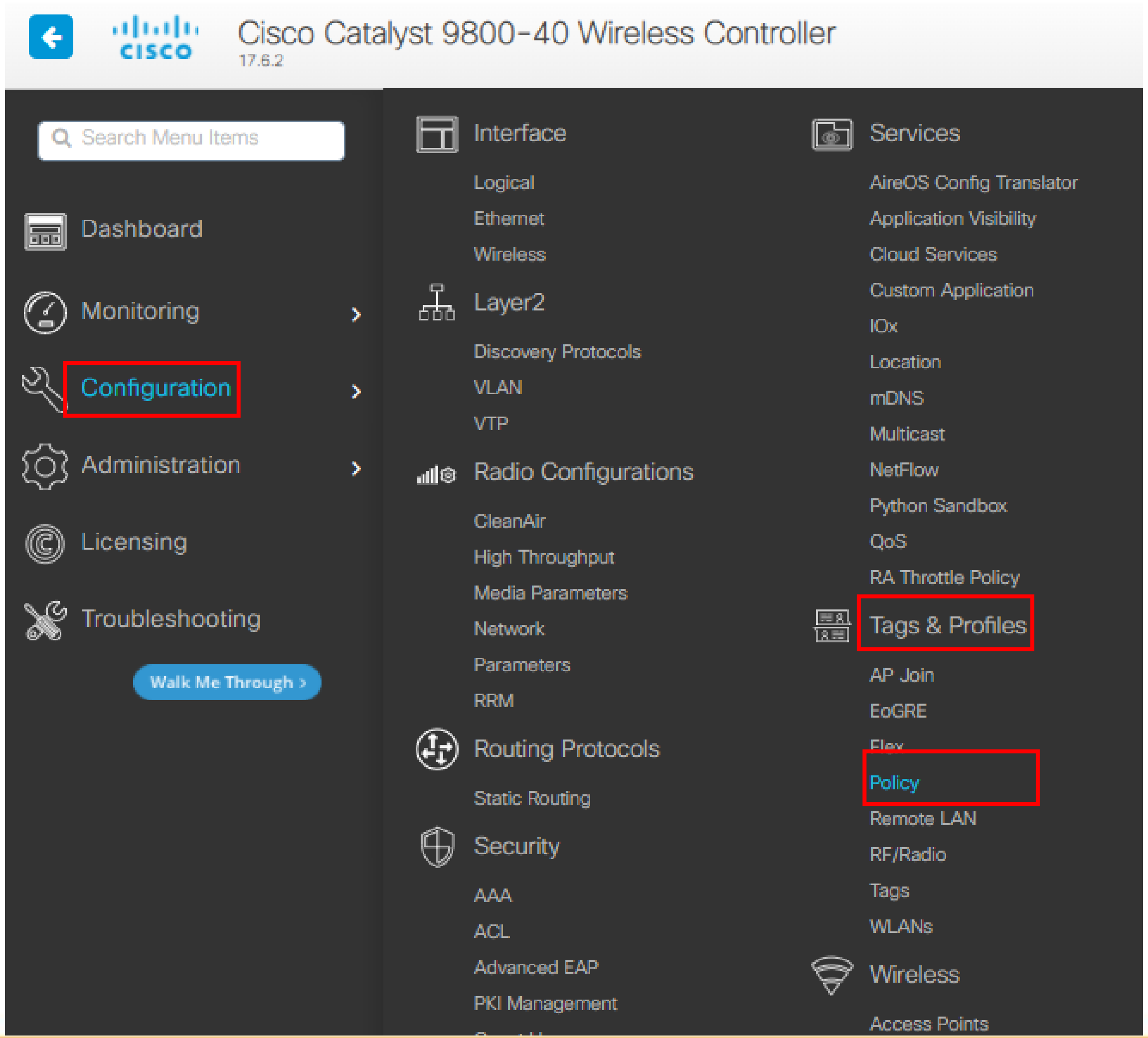
Device Analytics ให้เอาเครื่องหมายถูก ออก

- Advertise Support
- Advertise PC Analytics Support

จากนั้นทำการกด Apply to Device

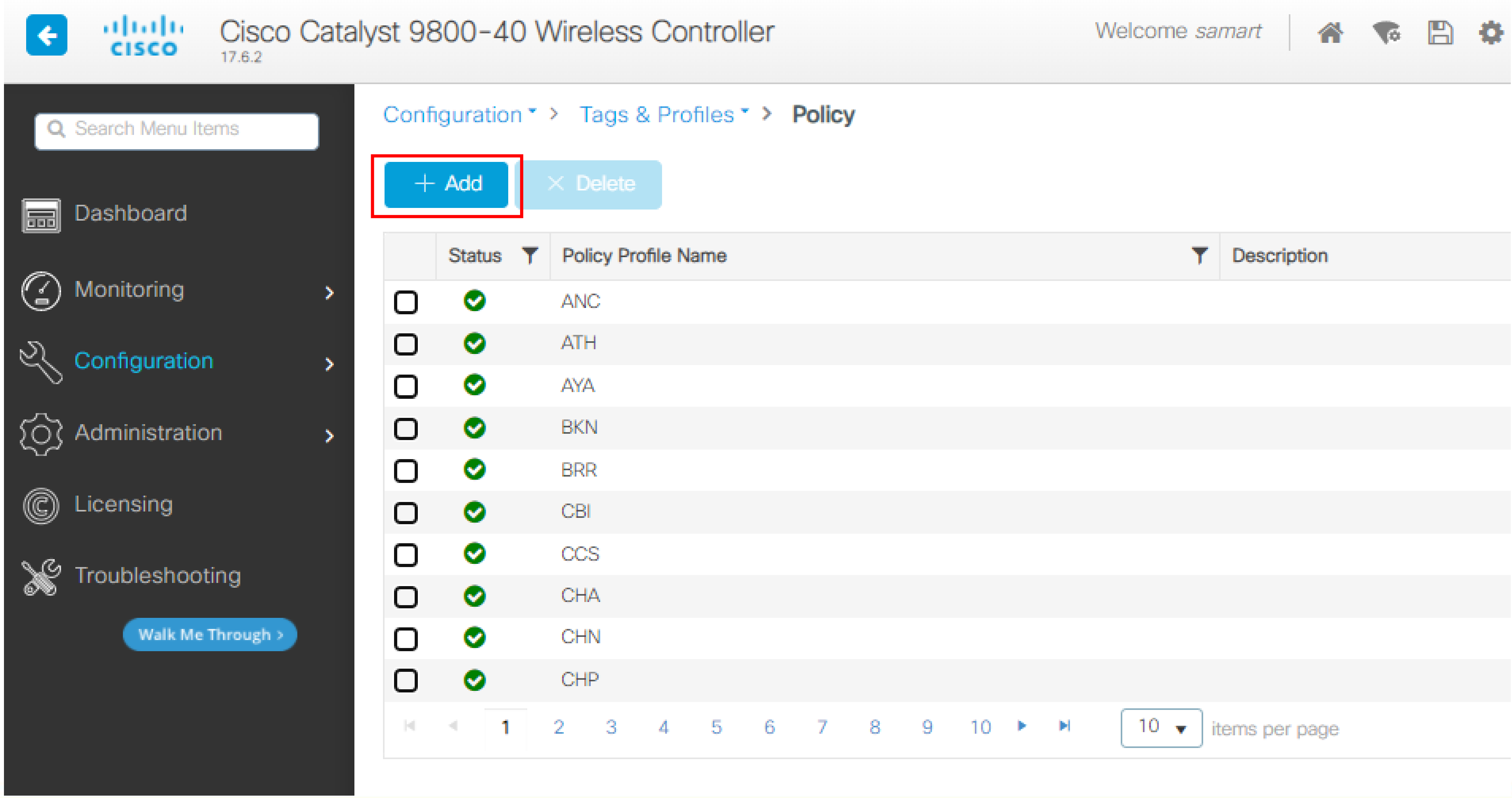
การสร้าง Policy

Step 1. Select Configuration > Tag & Profiles > Policy



การสร้าง Policy

Step 2. Select Add



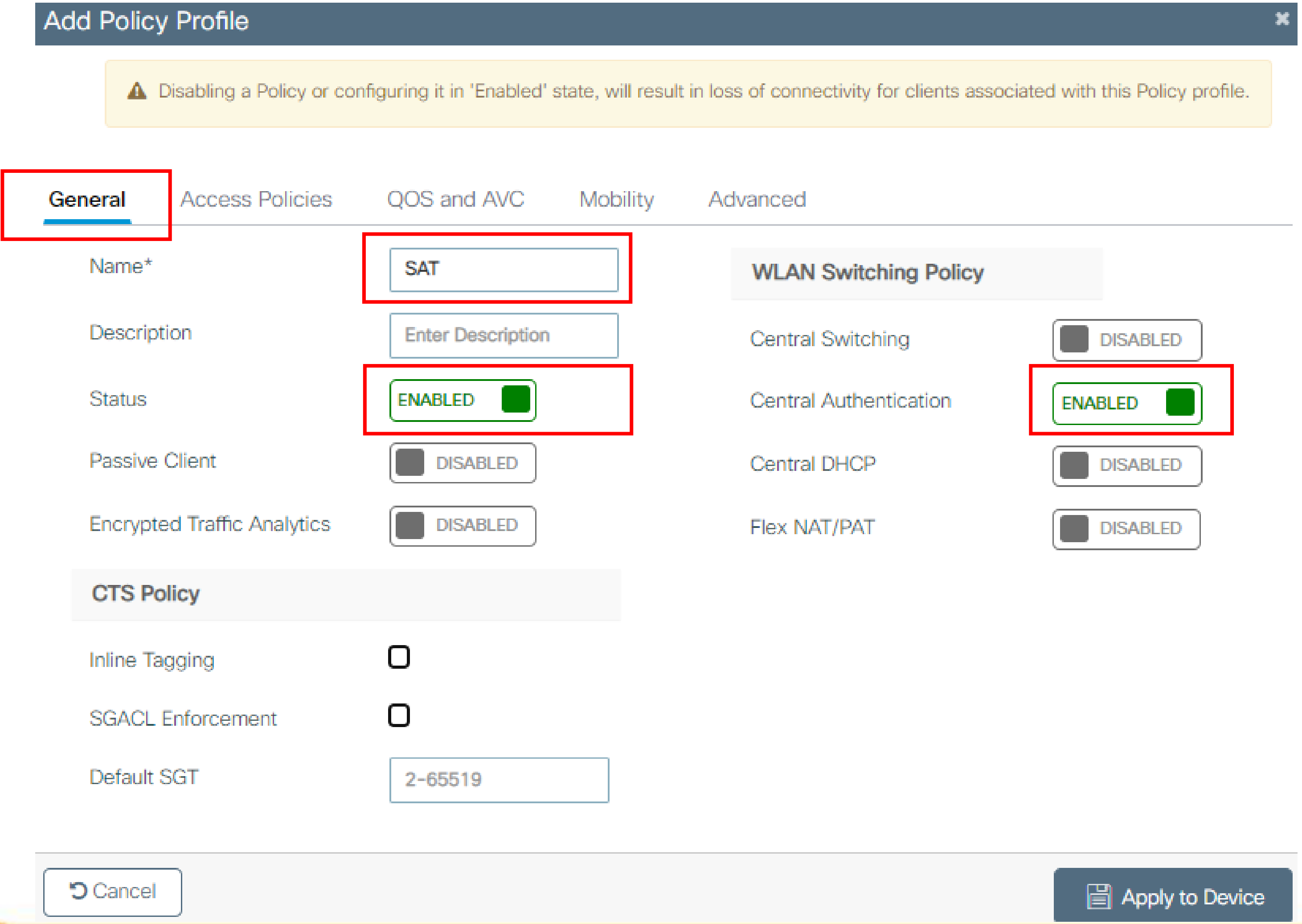
	Status	Policy Profile Name	Description
□	✓	ANC	
□	✓	ATH	
□	✓	AYA	
□	✓	BKN	
□	✓	BRR	
□	✓	CBI	
□	✓	CCS	
□	✓	CHA	
□	✓	CHN	
□	✓	CHP	

1 2 3 4 5 6 7 8 9 10 ▸ ▸| 10 ▾ items per page

ALERT
ADAPT
ACHIEVE

การสร้าง Policy

Step 3. Select General



Add Policy Profile ✖

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

Name*	SAT
Description	Enter Description
Status	ENABLED
Passive Client	DISABLED
Encrypted Traffic Analytics	DISABLED

CTS Policy

Inline Tagging	□
SGACL Enforcement	□
Default SGT	2-65519

WLAN Switching Policy

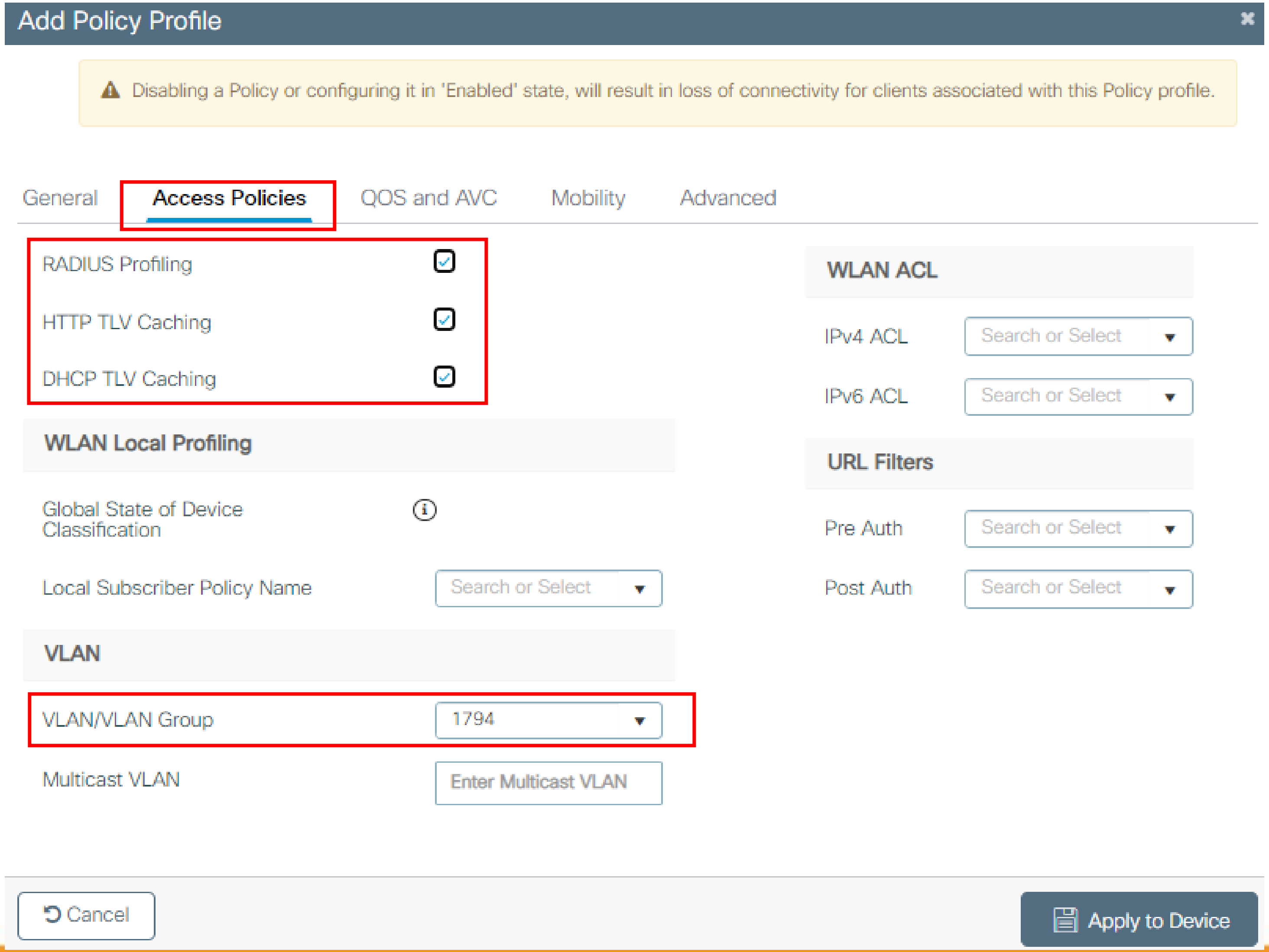
Central Switching	DISABLED
Central Authentication	ENABLED
Central DHCP	DISABLED
Flex NAT/PAT	DISABLED

ทำการใส่ข้อมูลดังนี้
- Name = ชื่อ Site นั้นๆ
- Status = Enable
- Central Authentication = Enable

SAMART
TELCOMS

การสร้าง Policy

Step 4. Select Access Policies



Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

RADIUS Profiling ☑

HTTP TLV Caching ☑

DHCP TLV Caching ☑

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name: Search or Select ▾

VLAN

VLAN/VLAN Group: 1794 ▾

Multicast VLAN: Enter Multicast VLAN

WLAN ACL

IPv4 ACL: Search or Select ▾

IPv6 ACL: Search or Select ▾

URL Filters

Pre Auth: Search or Select ▾

Post Auth: Search or Select ▾

ทำการใส่เครื่องหมายถูก ดังนี้

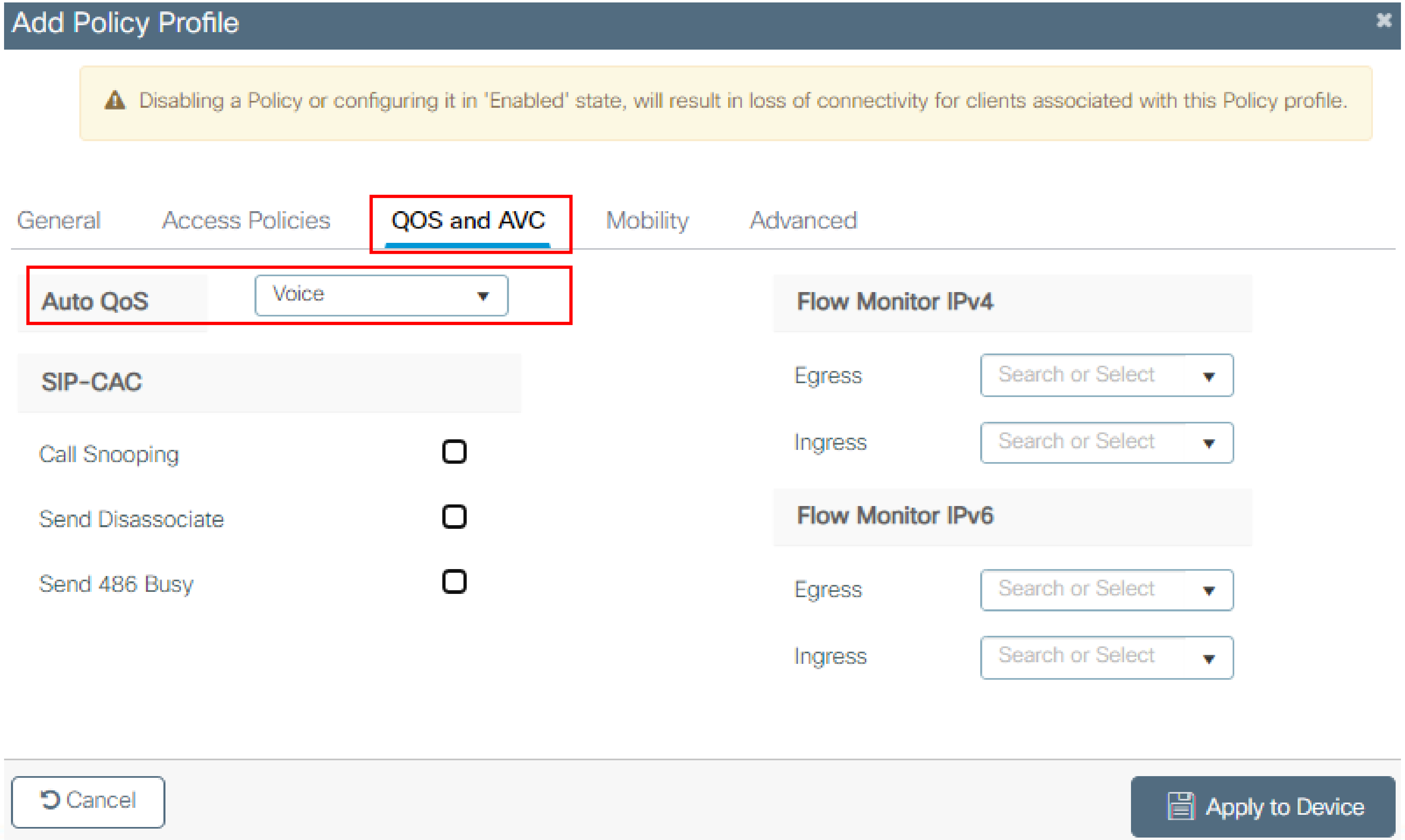
- RADIUS Profiling
- HTTP TLV Caching
- DHCP TLV Caching

ทำการใส่ค่า หมายเลข Vlan ที่จะใช้งาน ในช่อง VLAN/VLAN Group

ALERT
ADAPT
ACHIEVE

การสร้าง Policy

Step 5. Select QOS and AVC > Auto QoS > Voice



Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

Auto QoS: Voice

SIP-CAC

Call Snooping □

Send Disassociate □

Send 486 Busy □

Flow Monitor IPv4

Egress: Search or Select

Ingress: Search or Select

Flow Monitor IPv6

Egress: Search or Select

Ingress: Search or Select

SAMART TELCOMS

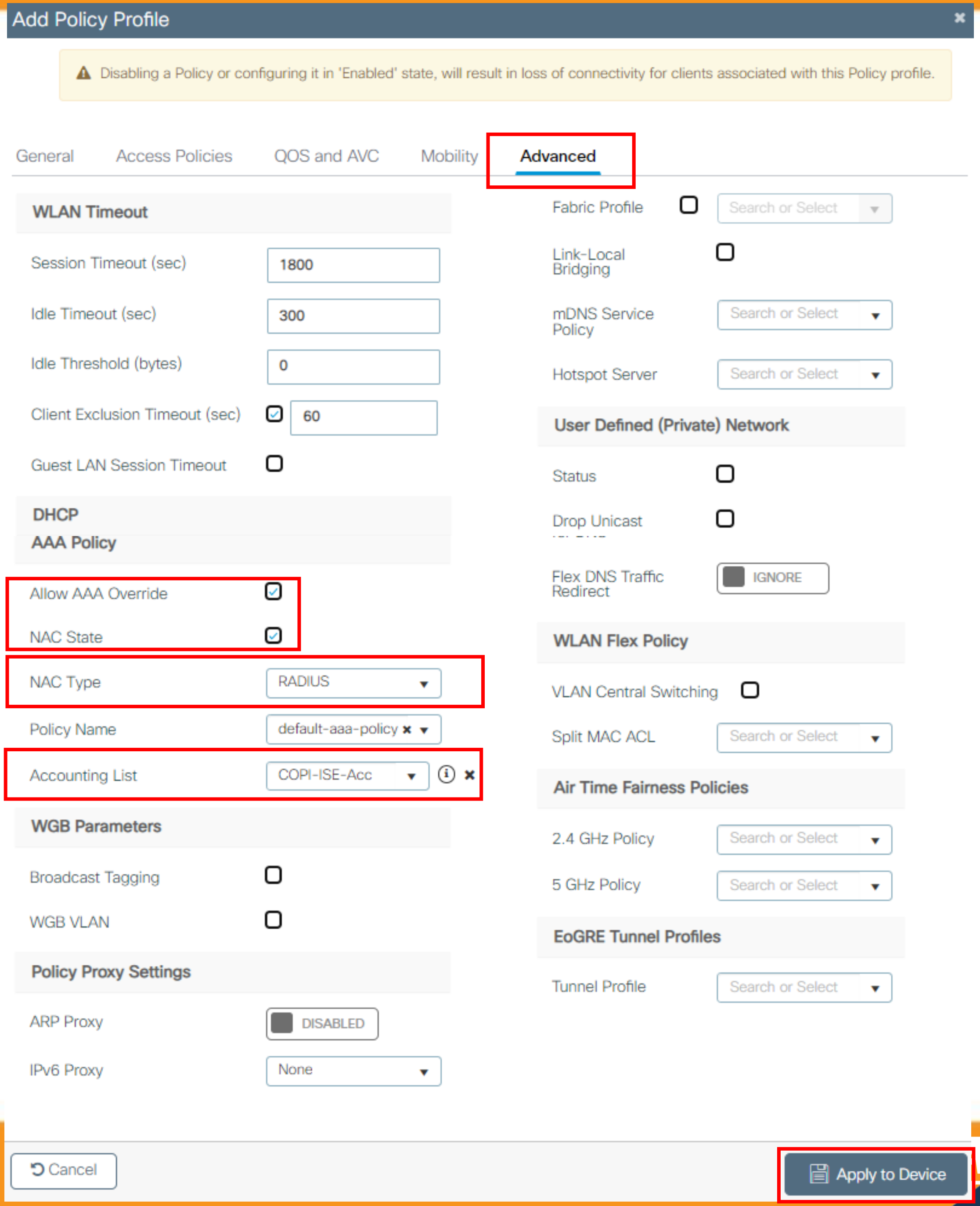
การสร้าง Policy

Step 6. Select Advanced > AAA Policy

AAA Policy ให้ใส่เครื่องหมายถูก ที่
- Allow AAA Override
- NAC State

NAC Type เลือก RADIUS
Accounting List เลือก COPI-ISE-Acc

จากนั้นทำการกด Apply to Device



Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General | Access Policies | QOS and AVC | Mobility | **Advanced**

WLAN Timeout

Session Timeout (sec): 1800

Idle Timeout (sec): 300

Idle Threshold (bytes): 0

Client Exclusion Timeout (sec): ☑ 60

Guest LAN Session Timeout: □

DHCP

AAA Policy

Allow AAA Override: ☑

NAC State: ☑

NAC Type: RADIUS

Policy Name: default-aaa-policy

Accounting List: COPI-ISE-Acc

WGB Parameters

Broadcast Tagging: □

WGB VLAN: □

Policy Proxy Settings

ARP Proxy: DISABLED

IPv6 Proxy: None

Fabric Profile: □ Search or Select

Link-Local Bridging: □

mDNS Service Policy: Search or Select

Hotspot Server: Search or Select

User Defined (Private) Network

Status: □

Drop Unicast: □

Flex DNS Traffic Redirect: IGNORE

WLAN Flex Policy

VLAN Central Switching: □

Split MAC ACL: Search or Select

Air Time Fairness Policies

2.4 GHz Policy: Search or Select

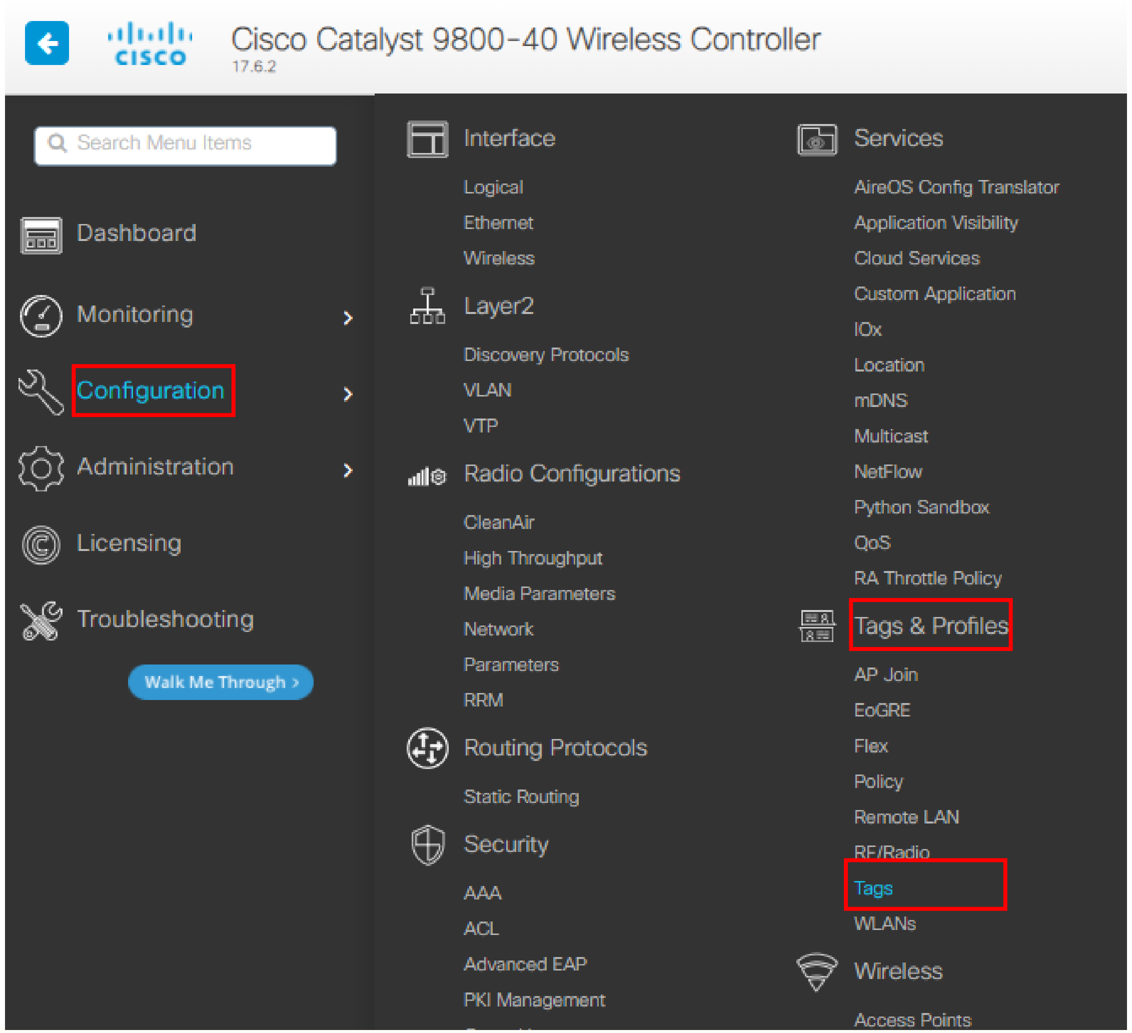
5 GHz Policy: Search or Select

EoGRE Tunnel Profiles

Tunnel Profile: Search or Select

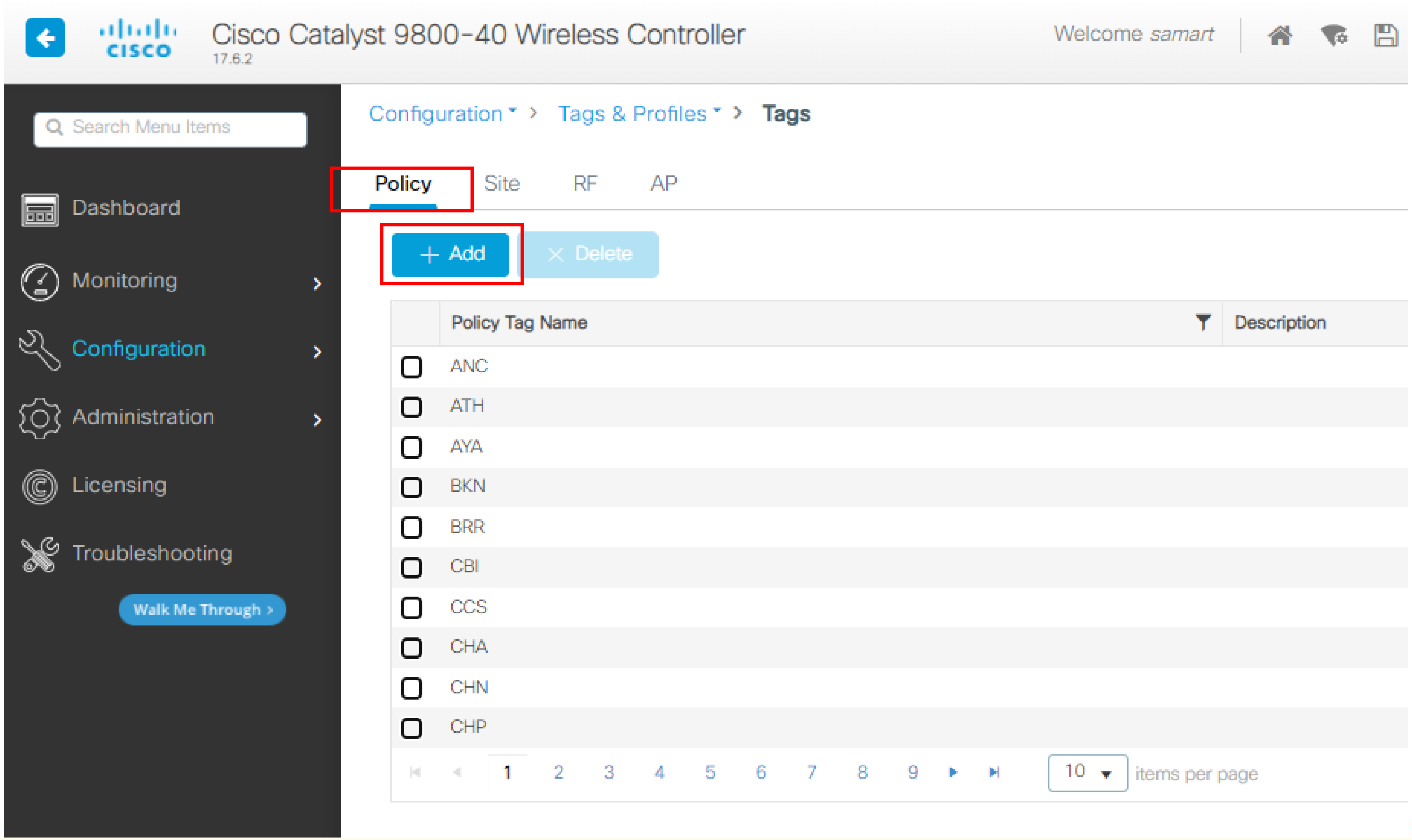
การสร้าง Policy Tags

Step 1. Select Configuration > Tags & Profiles > Tags



การสร้าง Policy Tags

Step 2. Select Policy > Add

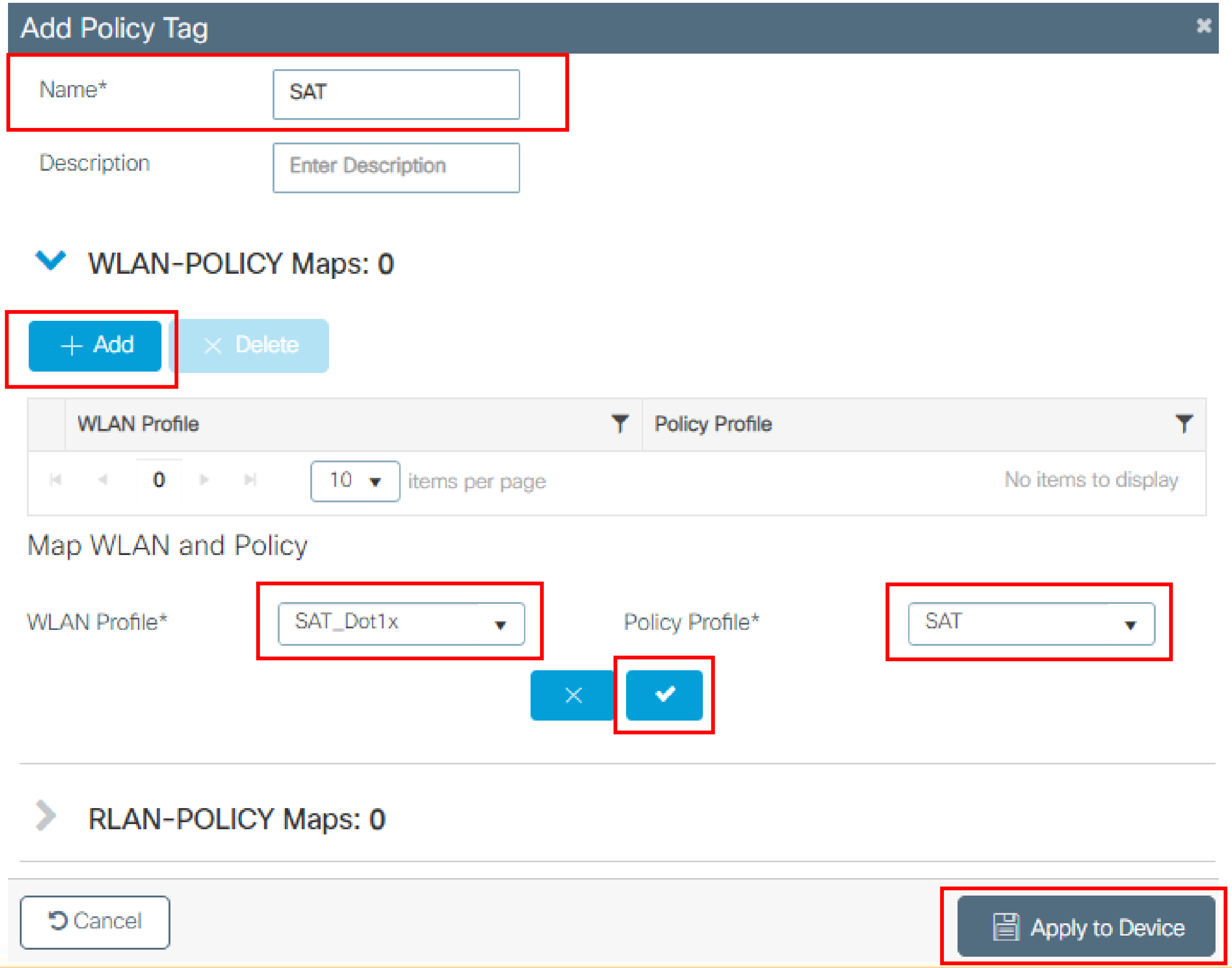


Policy Tag Name	Description
ANC	
ATH	
AYA	
BKN	
BRR	
CBI	
CCS	
CHA	
CHN	
CHP	

ALERT
ADAPT
ACHIEVE

การสร้าง Policy Tags

Step 3. Select Add Policy Tag



Add Policy Tag

Name* SAT

Description Enter Description

WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
0 · 10 items per page	No items to display

Map WLAN and Policy

WLAN Profile* SAT_Dot1x

Policy Profile* SAT

RLAN-POLICY Maps: 0

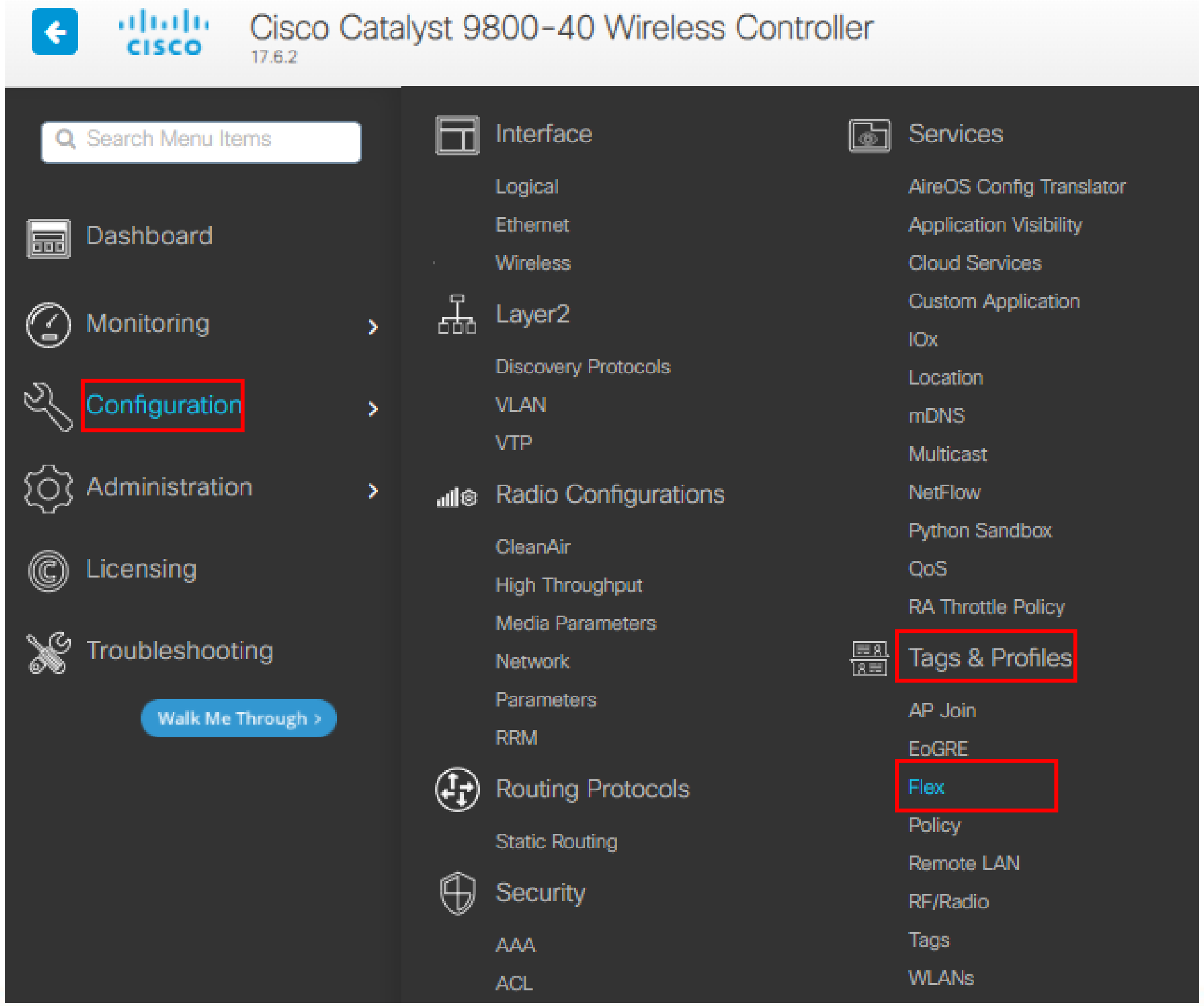
- ทำการใส่ชื่อ Name
- ทำการกด Add WLAN-Policy MAP
- เลือก WLAN Profiles และ Policy Profile
- ทำการกด เครื่องหมายถูก

จากนั้นทำการกด Apply to Device

SAMART
TELCOMS

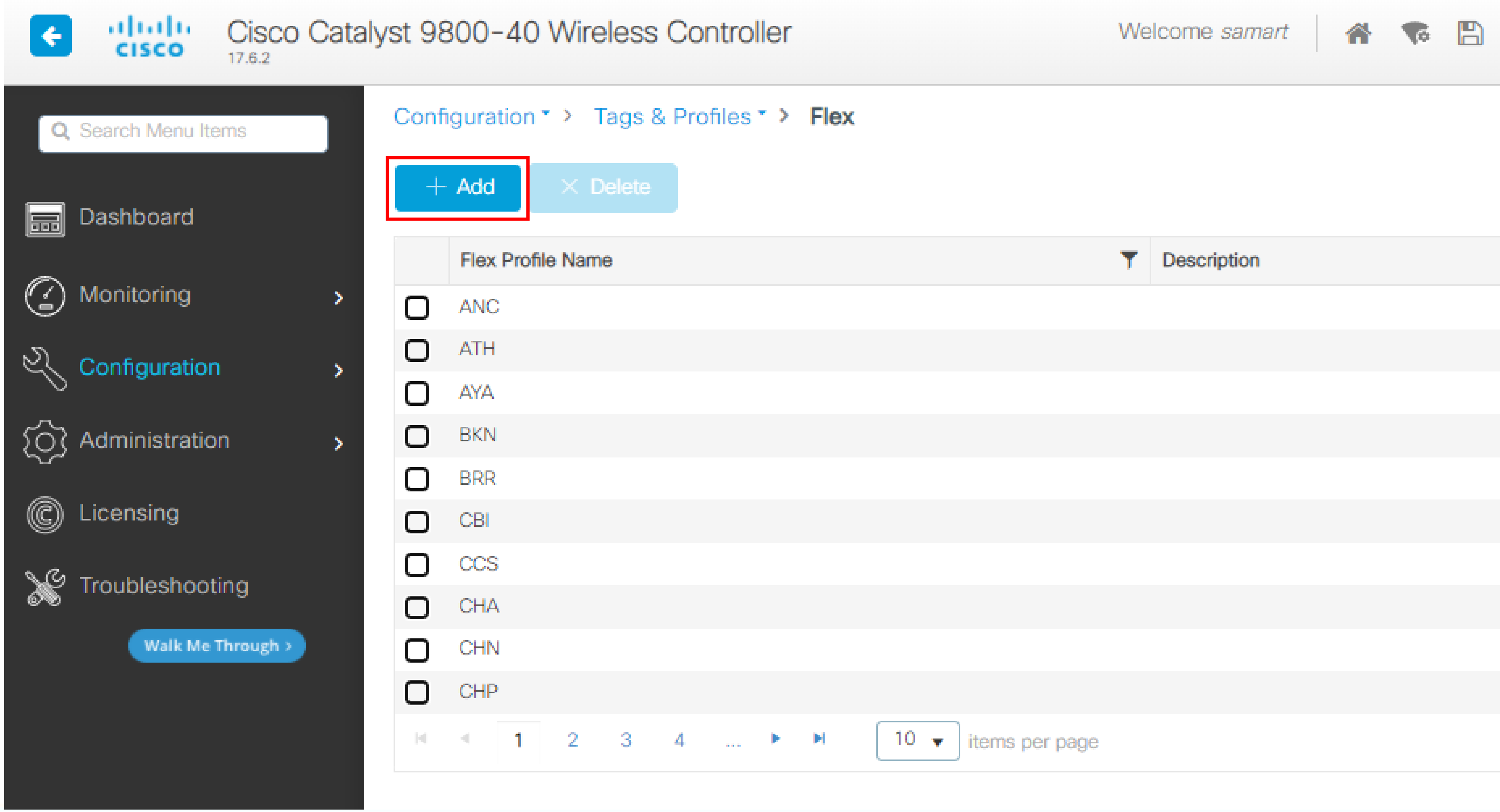
การสร้าง Flex

Step 1. Select Configuration > Tags & Profiles > Flex



การสร้าง Flex

Step 2. Select Add



Cisco Catalyst 9800-40 Wireless Controller
17.6.2

Welcome *samart*

Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Licensing
- Troubleshooting

Walk Me Through ›

Configuration › Tags & Profiles › Flex

+ Add   × Delete

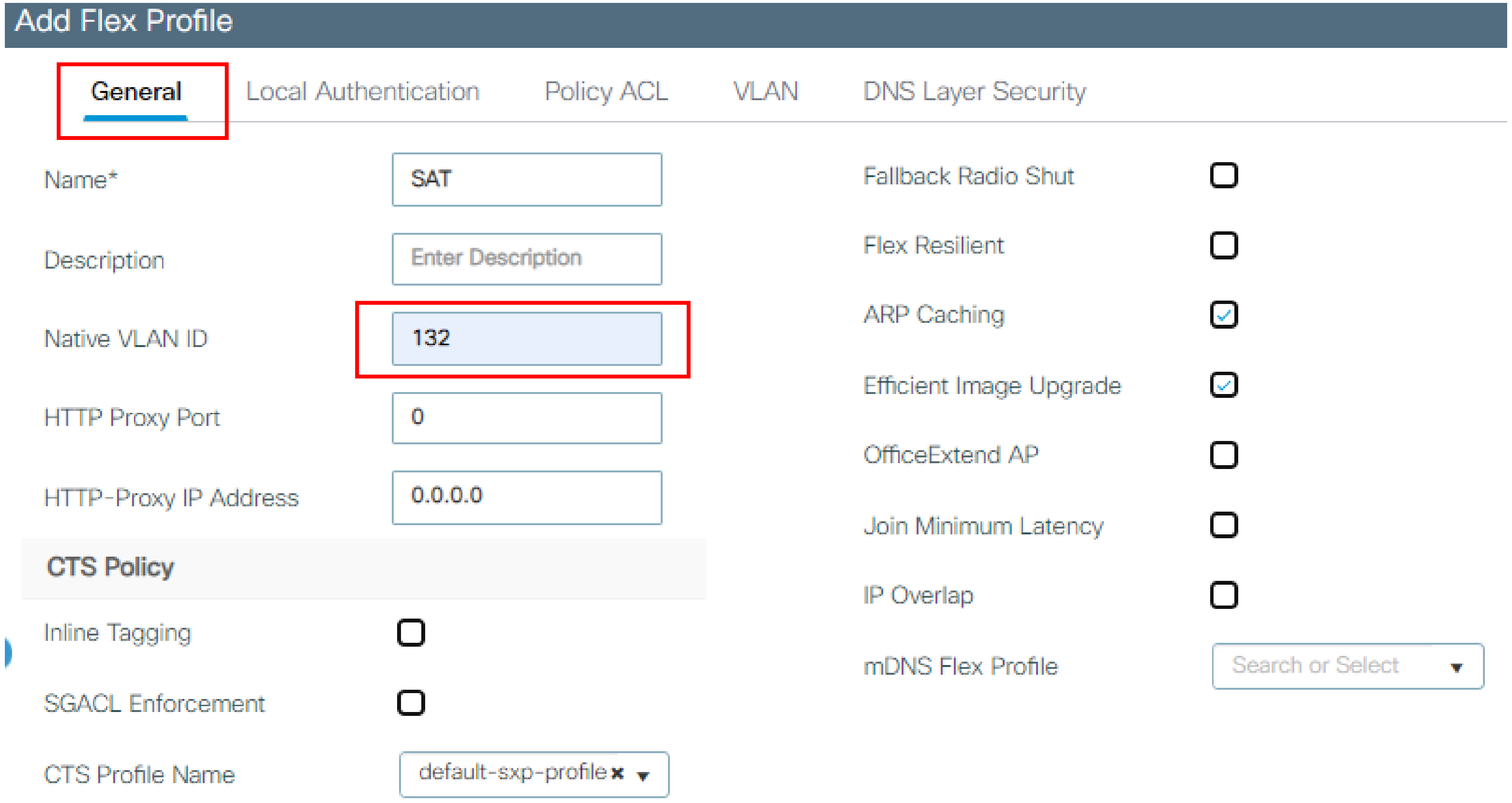
	Flex Profile Name	Description
□	ANC	
□	ATH	
□	AYA	
□	BKN	
□	BRR	
□	CBI	
□	CCS	
□	CHA	
□	CHN	
□	CHP	

1 2 3 4 ... 10 items per page

ALERT
ADAPT
ACHIEVE

การสร้าง Flex

Step 3. Select General



Add Flex Profile

Name*	SAT
Description	Enter Description
Native VLAN ID	132
HTTP Proxy Port	0
HTTP-Proxy IP Address	0.0.0.0

CTS Policy

Inline Tagging	□
SGACL Enforcement	□
CTS Profile Name	default-sxp-profile ✖ ▾

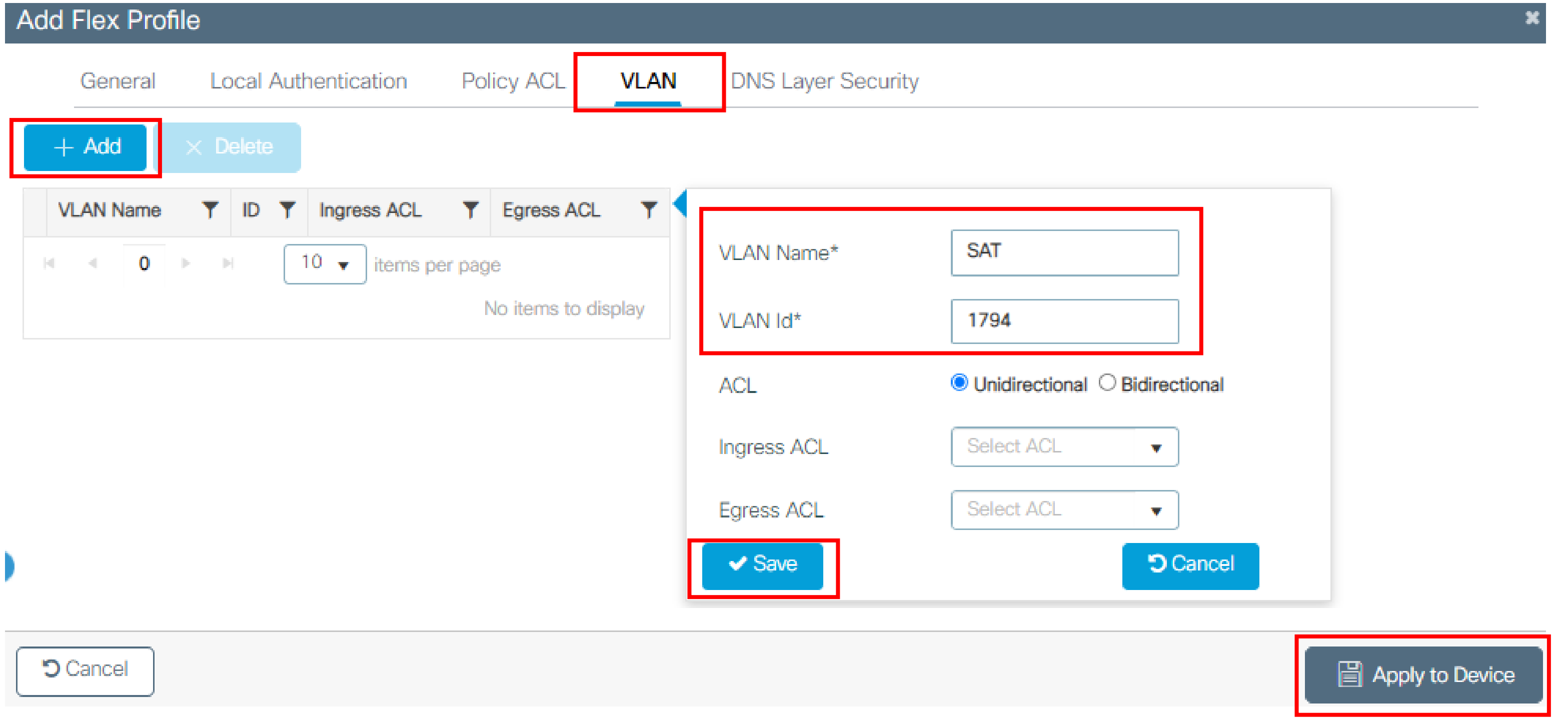
Fallback Radio Shut	□
Flex Resilient	□
ARP Caching	☑
Efficient Image Upgrade	☑
OfficeExtend AP	□
Join Minimum Latency	□
IP Overlap	□
mDNS Flex Profile	Search or Select ▾

ทำการใส่ค่า หมายเลข Vlan ของ Access Point ในช่อง Native VLAN ID

SAMART
TELCOMS

การสร้าง Flex

Step 4. Select VLAN > Add



VLAN Name* SAT

VLAN Id* 1794

ACL ● Unidirectional ○ Bidirectional

Ingress ACL Select ACL

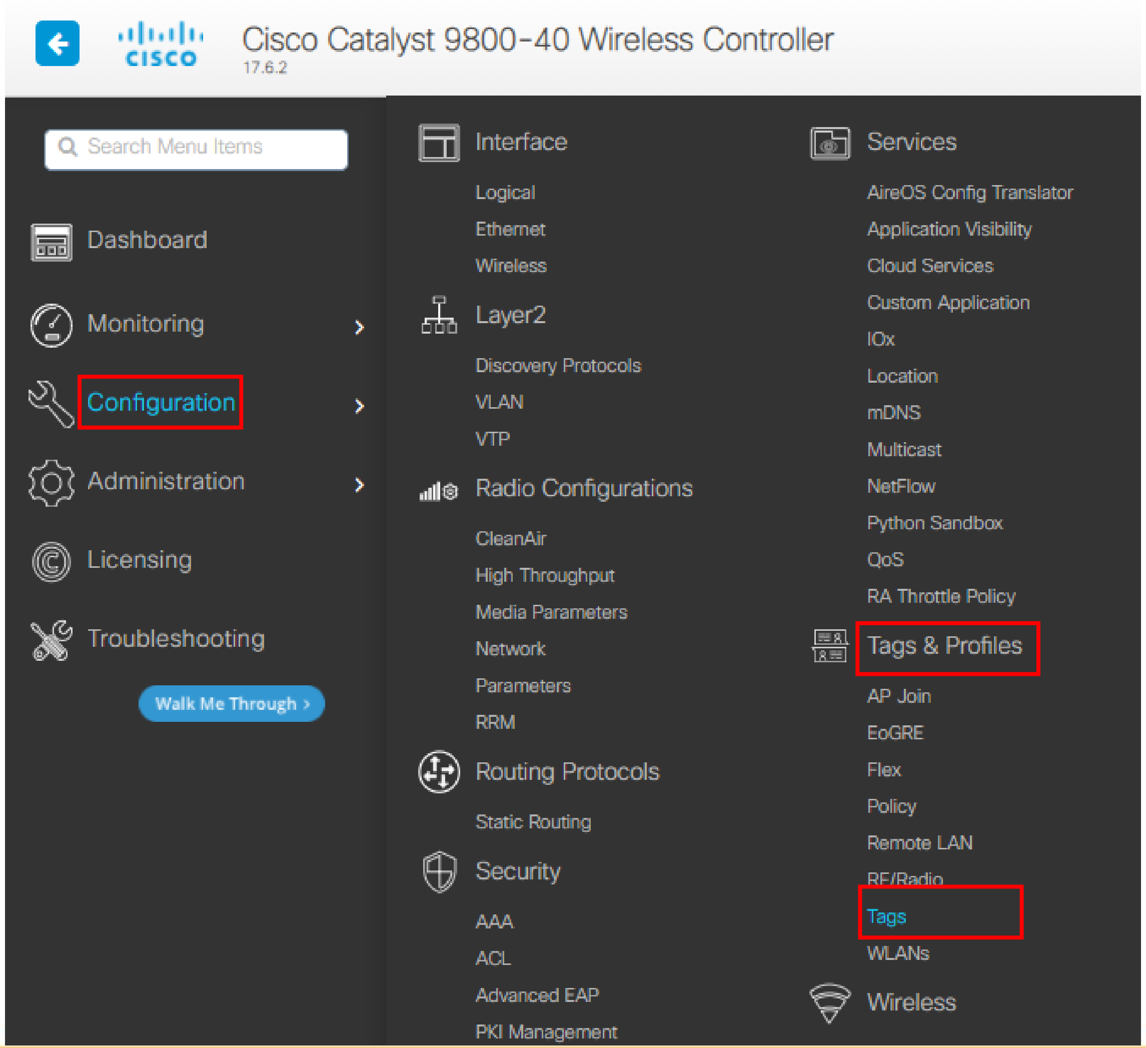
Egress ACL Select ACL

ทำการใส่ข้อมูลดังนี้
- VLAN Name
- VLAN ID

ทำการกด Save จากนั้นทำการกด Apply to Device

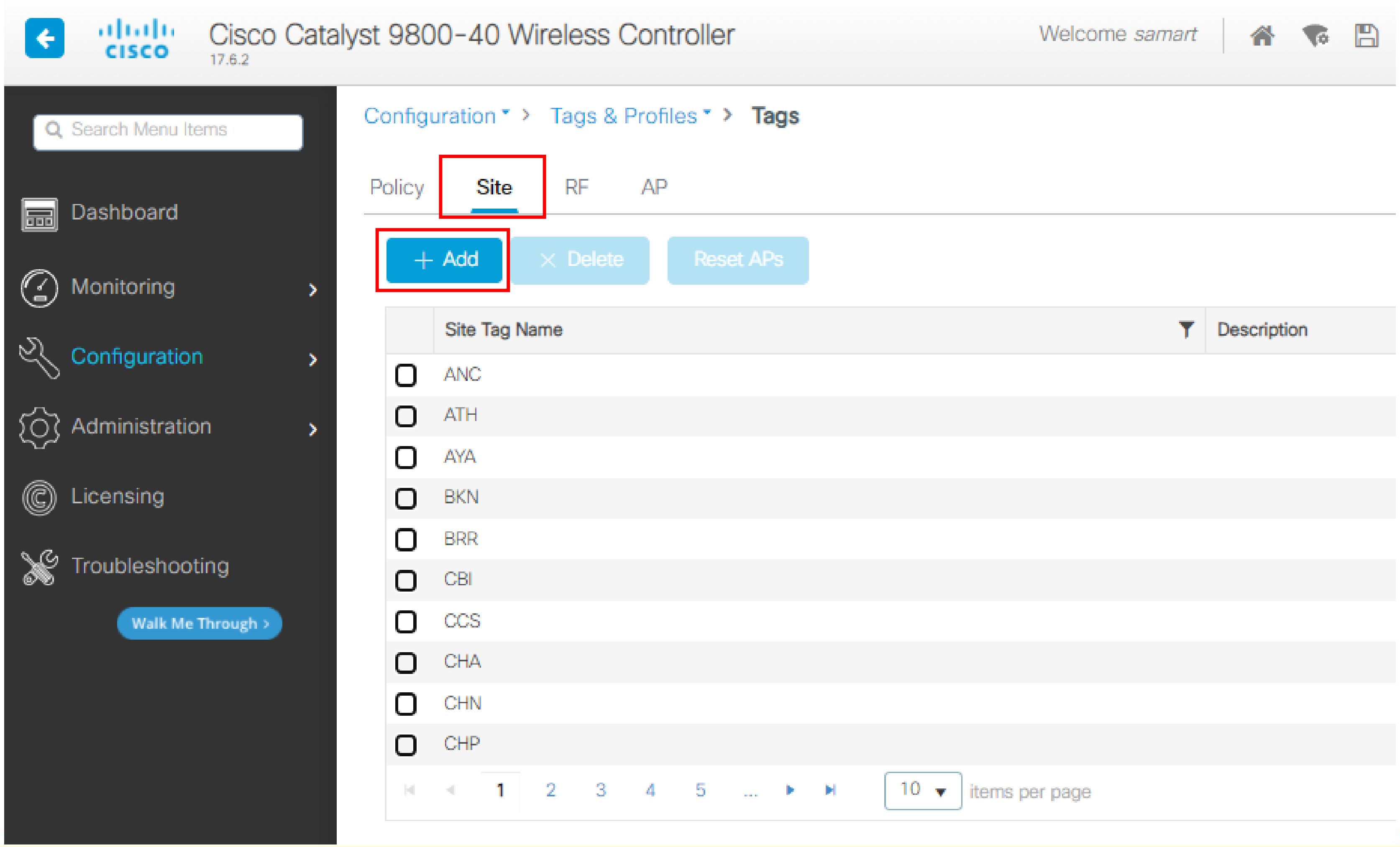
การสร้าง Site Tag

Step 1. Select Configuration > Tags & Profiles > Tags



การสร้าง Site Tag

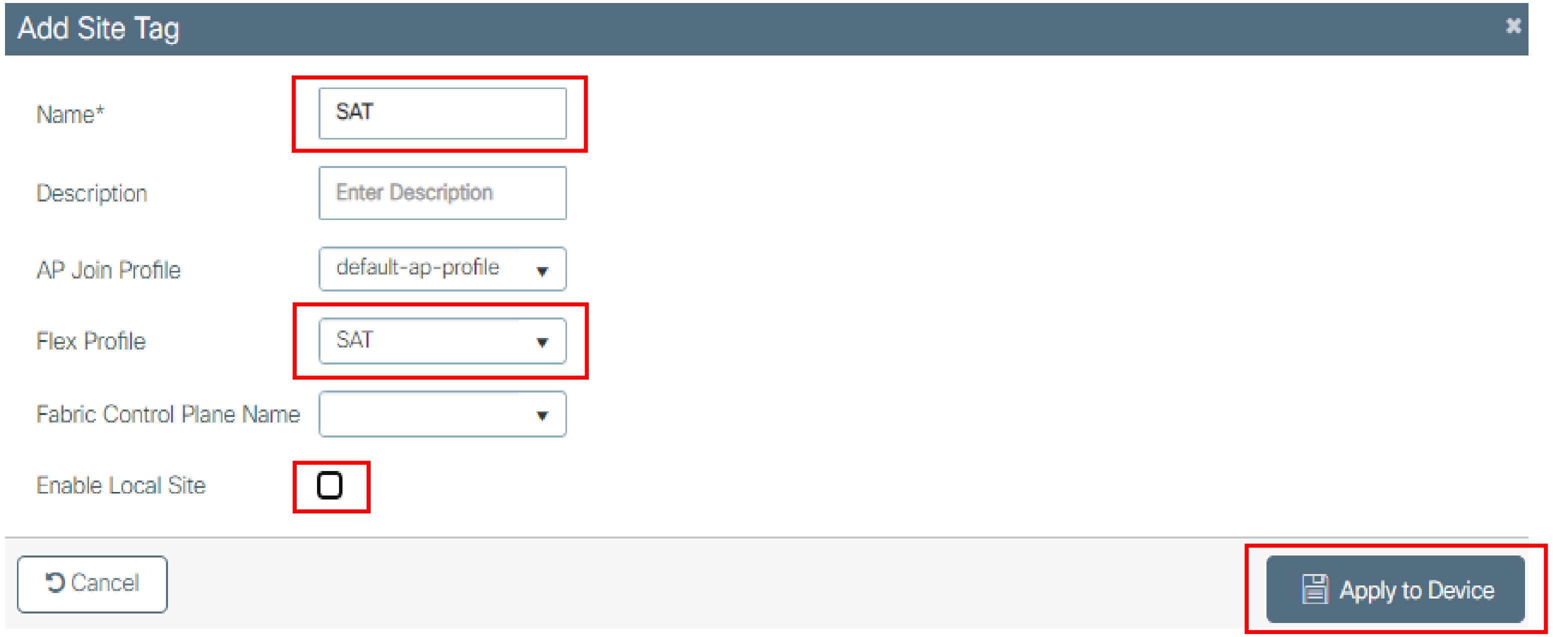
Step 2. Select Site > Add



	Site Tag Name	Description
□	ANC	
□	ATH	
□	AYA	
□	BKN	
□	BRR	
□	CBI	
□	CCS	
□	CHA	
□	CHN	
□	CHP	

การสร้าง Site Tag

Step 3. Select Add Site Tag



Add Site Tag

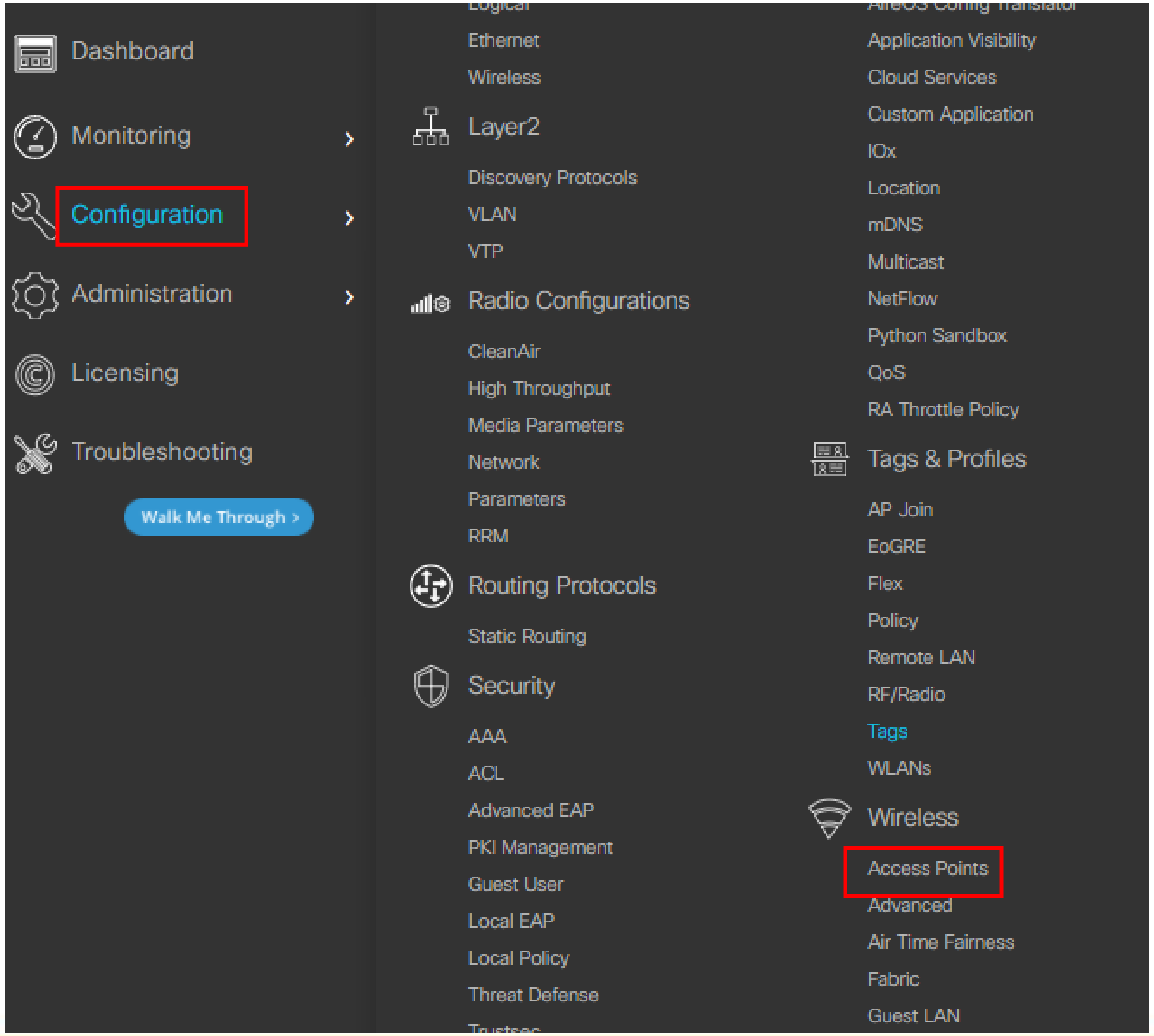
Name*	SAT
Description	Enter Description
AP Join Profile	default-ap-profile
Flex Profile	SAT
Fabric Control Plane Name	
Enable Local Site	□

- ทำการใส่ชื่อ Name
- ทำการเลือก Flex Profile
- Enable Local Site เอาเครื่องหมายถูกออก

จากนั้นทำการกด Apply to Device

การ Config Access Point

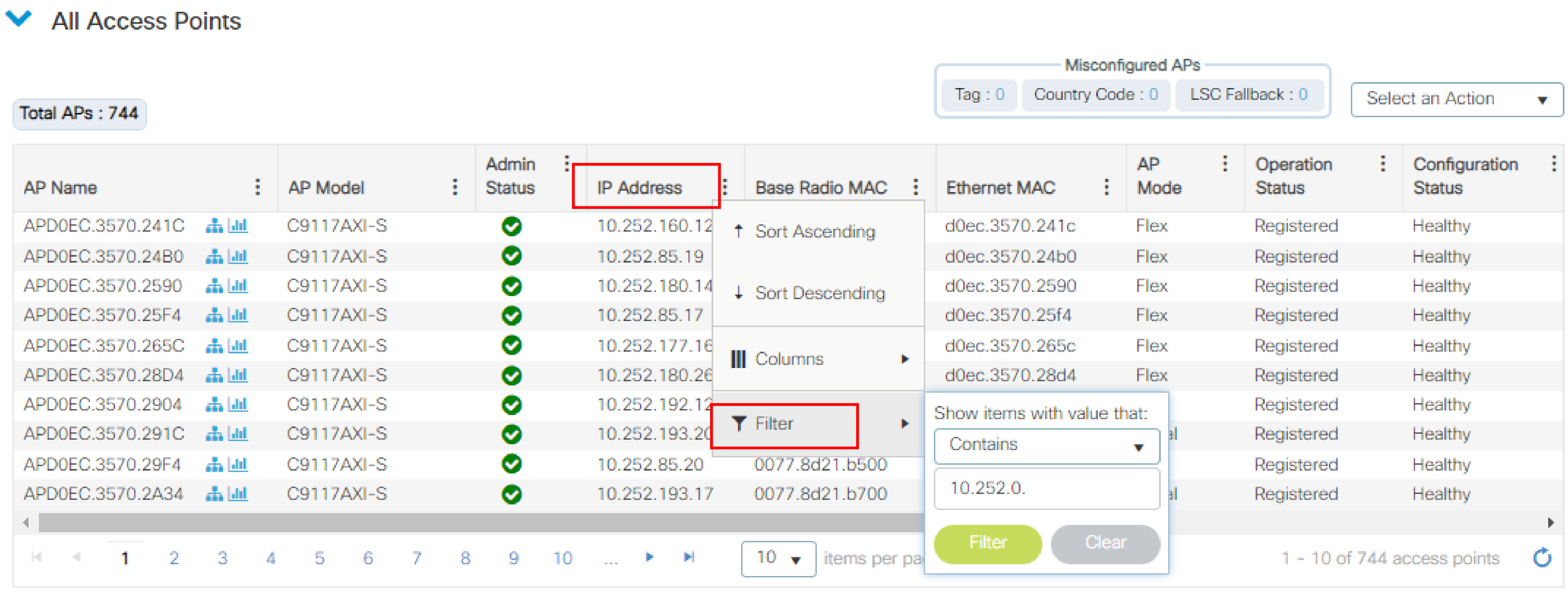
Step 1. Select Configuration > Wireless > Access Points



ALERT
ADAPT
ACHIEVE

การ Config Access Point

Step 2. Select IP Address > Filter



All Access Points

Total APs : 744

Misconfigured APs: Tag : 0 | Country Code : 0 | LSC Fallback : 0

AP Name	AP Model	Admin Status	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Operation Status	Configuration Status
APD0EC.3570.241C	C9117AXI-S	✓	10.252.160.12		d0ec.3570.241c	Flex	Registered	Healthy
APD0EC.3570.24B0	C9117AXI-S	✓	10.252.85.19		d0ec.3570.24b0	Flex	Registered	Healthy
APD0EC.3570.2590	C9117AXI-S	✓	10.252.180.14		d0ec.3570.2590	Flex	Registered	Healthy
APD0EC.3570.25F4	C9117AXI-S	✓	10.252.85.17		d0ec.3570.25f4	Flex	Registered	Healthy
APD0EC.3570.265C	C9117AXI-S	✓	10.252.177.16		d0ec.3570.265c	Flex	Registered	Healthy
APD0EC.3570.28D4	C9117AXI-S	✓	10.252.180.26		d0ec.3570.28d4	Flex	Registered	Healthy
APD0EC.3570.2904	C9117AXI-S	✓	10.252.192.12				Registered	Healthy
APD0EC.3570.291C	C9117AXI-S	✓	10.252.193.20				Registered	Healthy
APD0EC.3570.29F4	C9117AXI-S	✓	10.252.85.20	0077.8d21.b500			Registered	Healthy
APD0EC.3570.2A34	C9117AXI-S	✓	10.252.193.17	0077.8d21.b700			Registered	Healthy

Show items with value that: Contains

10.252.0.

1 2 3 4 5 6 7 8 9 10 ...

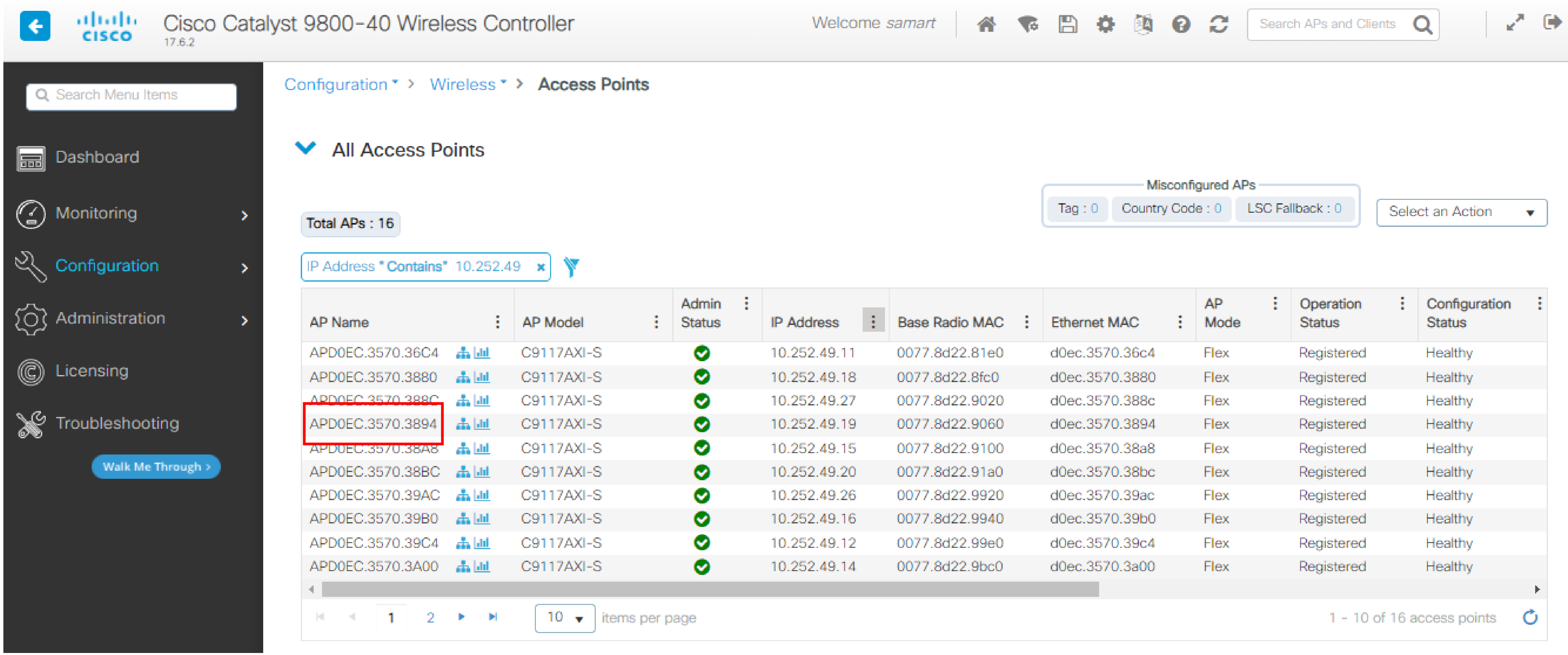
10 items per pa

1 - 10 of 744 access points

SAMART TELCOMS

การ Config Access Point

Step 3. Select AP Name

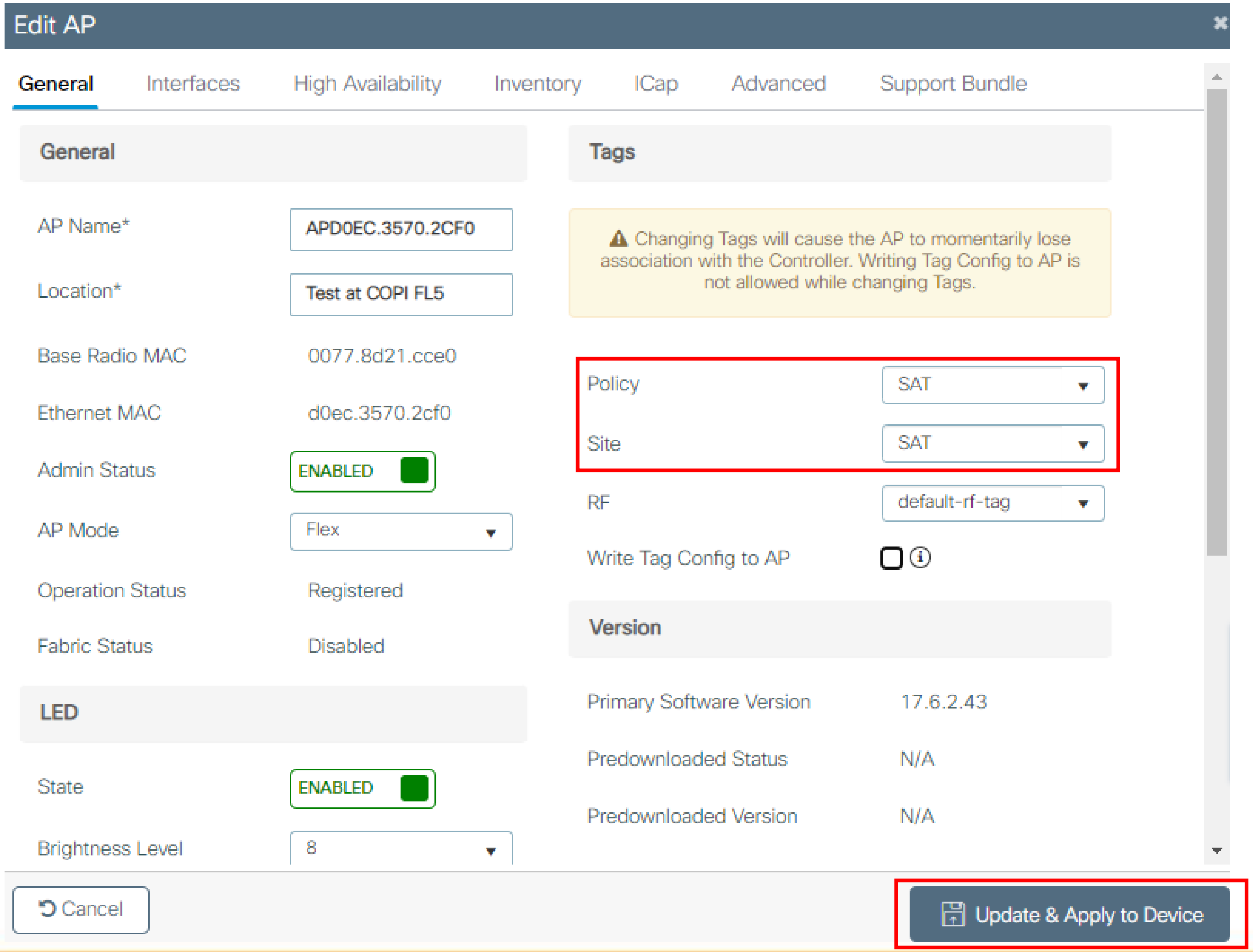


AP Name	AP Model	Admin Status	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Operation Status	Configuration Status
APD0EC.3570.36C4	C9117AXI-S	✓	10.252.49.11	0077.8d22.81e0	d0ec.3570.36c4	Flex	Registered	Healthy
APD0EC.3570.3880	C9117AXI-S	✓	10.252.49.18	0077.8d22.8fc0	d0ec.3570.3880	Flex	Registered	Healthy
APD0EC.3570.388C	C9117AXI-S	✓	10.252.49.27	0077.8d22.9020	d0ec.3570.388c	Flex	Registered	Healthy
APD0EC.3570.3894	C9117AXI-S	✓	10.252.49.19	0077.8d22.9060	d0ec.3570.3894	Flex	Registered	Healthy
APD0EC.3570.38A8	C9117AXI-S	✓	10.252.49.15	0077.8d22.9100	d0ec.3570.38a8	Flex	Registered	Healthy
APD0EC.3570.38BC	C9117AXI-S	✓	10.252.49.20	0077.8d22.91a0	d0ec.3570.38bc	Flex	Registered	Healthy
APD0EC.3570.39AC	C9117AXI-S	✓	10.252.49.26	0077.8d22.9920	d0ec.3570.39ac	Flex	Registered	Healthy
APD0EC.3570.39B0	C9117AXI-S	✓	10.252.49.16	0077.8d22.9940	d0ec.3570.39b0	Flex	Registered	Healthy
APD0EC.3570.39C4	C9117AXI-S	✓	10.252.49.12	0077.8d22.99e0	d0ec.3570.39c4	Flex	Registered	Healthy
APD0EC.3570.3A00	C9117AXI-S	✓	10.252.49.14	0077.8d22.9bc0	d0ec.3570.3a00	Flex	Registered	Healthy

ALERT
ADAPT
ACHIEVE

การ Config Access Point

Step 4. Select General



Edit AP

General

AP Name* APD0EC.3570.2CF0

Location* Test at COPI FL5

Base Radio MAC 0077.8d21.cce0

Ethernet MAC d0ec.3570.2cf0

Admin Status ENABLED

AP Mode Flex

Operation Status Registered

Fabric Status Disabled

LED

State ENABLED

Brightness Level 8

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.

Policy SAT

Site SAT

RF default-rf-tag

Write Tag Config to AP □ ⓘ

Version

Primary Software Version 17.6.2.43

Predownloaded Status N/A

Predownloaded Version N/A

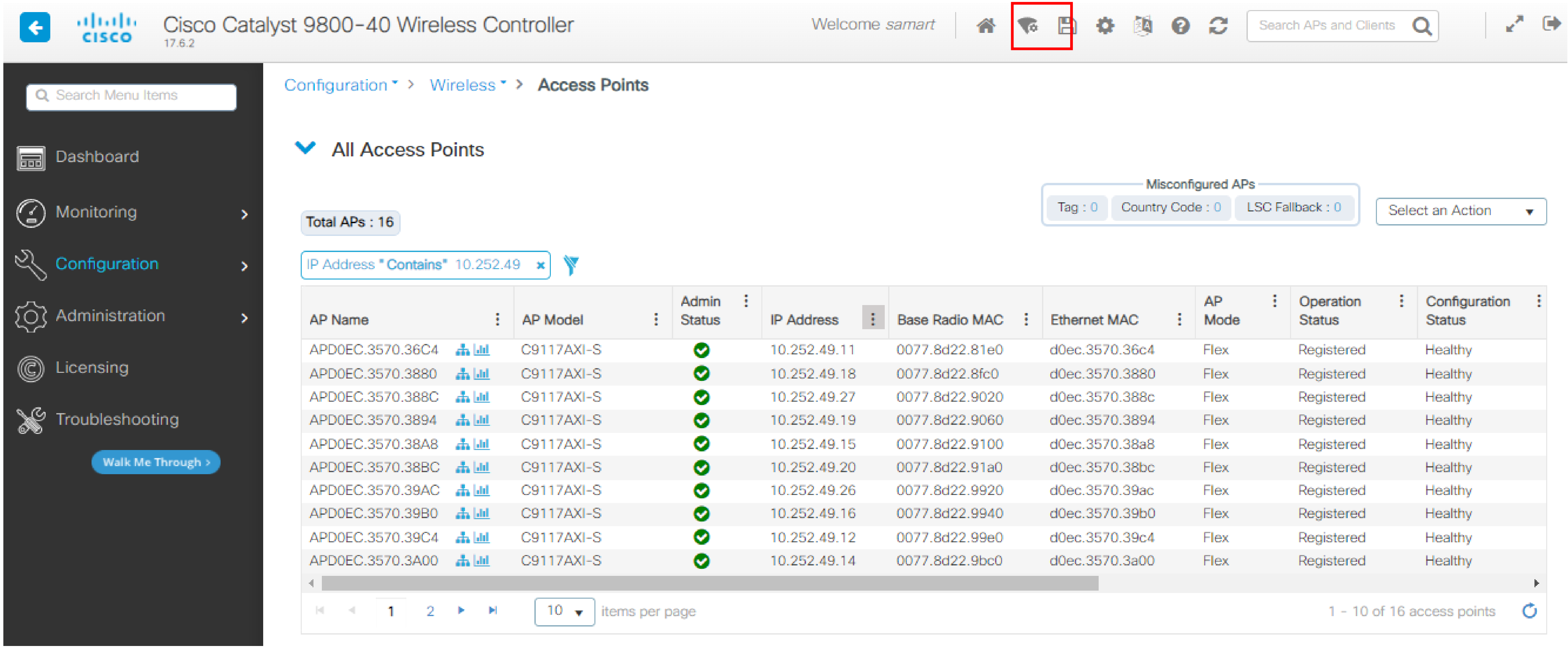
ทำการเลือก Policy และ Site ให้ตรงกับ Site นั้นๆ

จากนั้นทำการกด Update & Apply to Device

SAMART TELCOMS

การ Config Access Point

Step 5. Save



Configuration › Wireless › Access Points

All Access Points

Misconfigured APs: Tag : 0 | Country Code : 0 | LSC Fallback : 0

Select an Action

Total APs : 16

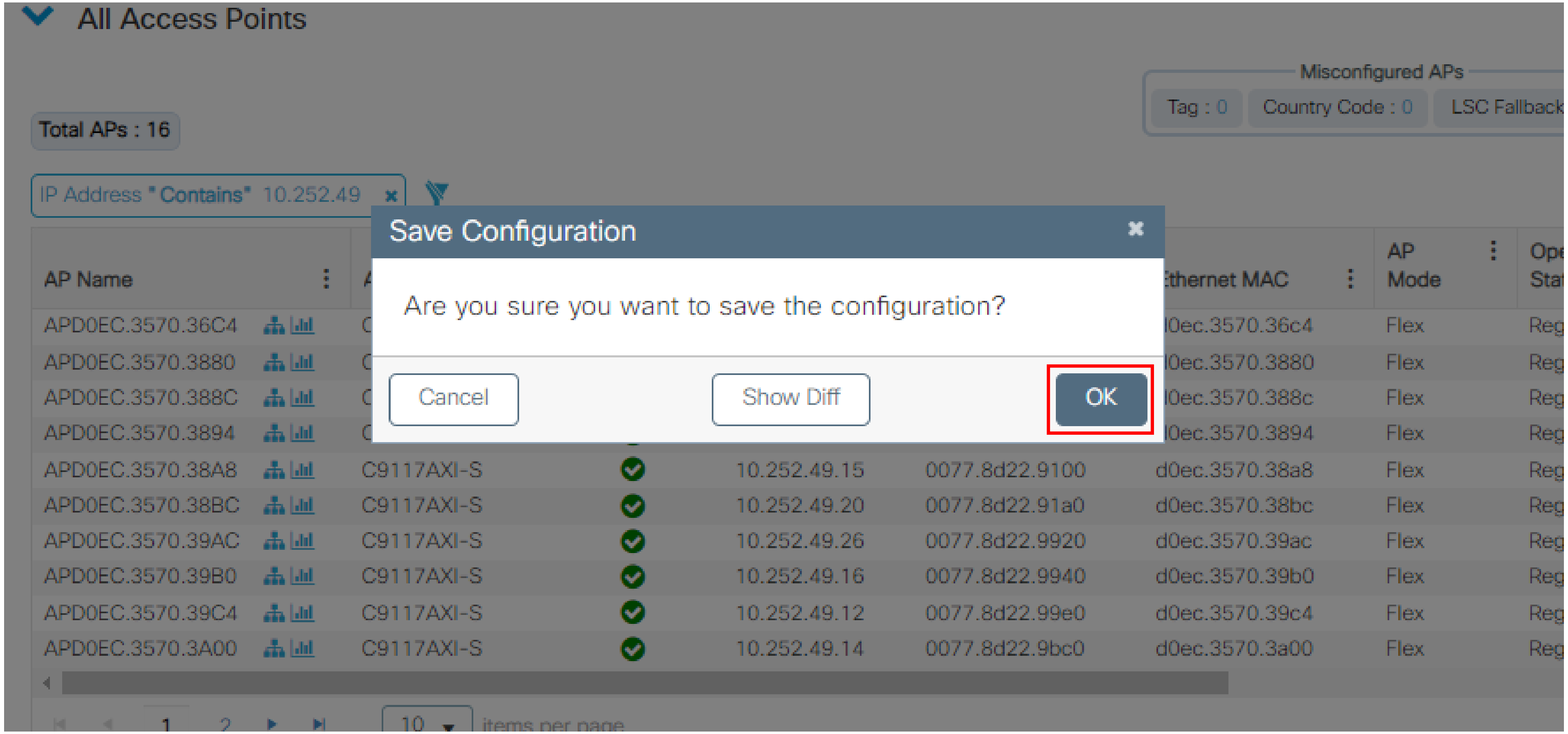
IP Address "Contains" 10.252.49

AP Name	AP Model	Admin Status	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Operation Status	Configuration Status
APD0EC.3570.36C4	C9117AXI-S	✓	10.252.49.11	0077.8d22.81e0	d0ec.3570.36c4	Flex	Registered	Healthy
APD0EC.3570.3880	C9117AXI-S	✓	10.252.49.18	0077.8d22.8fc0	d0ec.3570.3880	Flex	Registered	Healthy
APD0EC.3570.388C	C9117AXI-S	✓	10.252.49.27	0077.8d22.9020	d0ec.3570.388c	Flex	Registered	Healthy
APD0EC.3570.3894	C9117AXI-S	✓	10.252.49.19	0077.8d22.9060	d0ec.3570.3894	Flex	Registered	Healthy
APD0EC.3570.38A8	C9117AXI-S	✓	10.252.49.15	0077.8d22.9100	d0ec.3570.38a8	Flex	Registered	Healthy
APD0EC.3570.38BC	C9117AXI-S	✓	10.252.49.20	0077.8d22.91a0	d0ec.3570.38bc	Flex	Registered	Healthy
APD0EC.3570.39AC	C9117AXI-S	✓	10.252.49.26	0077.8d22.9920	d0ec.3570.39ac	Flex	Registered	Healthy
APD0EC.3570.39B0	C9117AXI-S	✓	10.252.49.16	0077.8d22.9940	d0ec.3570.39b0	Flex	Registered	Healthy
APD0EC.3570.39C4	C9117AXI-S	✓	10.252.49.12	0077.8d22.99e0	d0ec.3570.39c4	Flex	Registered	Healthy
APD0EC.3570.3A00	C9117AXI-S	✓	10.252.49.14	0077.8d22.9bc0	d0ec.3570.3a00	Flex	Registered	Healthy

1 2 | 10 items per page | 1 - 10 of 16 access points

การ Config Access Point

Step 6. OK



All Access Points

Total APs : 16

Misconfigured APs: Tag : 0 | Country Code : 0 | LSC Fallback

IP Address "Contains" 10.252.49

Save Configuration

Are you sure you want to save the configuration?

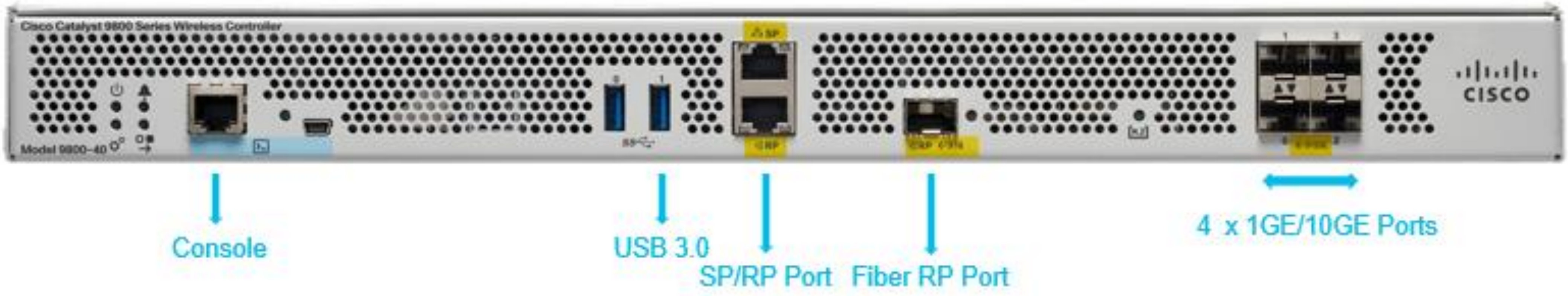
AP Name	A				Ethernet MAC	AP Mode	Ope Sta
APD0EC.3570.36C4	C				0ec.3570.36c4	Flex	Reg
APD0EC.3570.3880	C				0ec.3570.3880	Flex	Reg
APD0EC.3570.388C	C				0ec.3570.388c	Flex	Reg
APD0EC.3570.3894	C				0ec.3570.3894	Flex	Reg
APD0EC.3570.38A8	C9117AXI-S	✓	10.252.49.15	0077.8d22.9100	d0ec.3570.38a8	Flex	Reg
APD0EC.3570.38BC	C9117AXI-S	✓	10.252.49.20	0077.8d22.91a0	d0ec.3570.38bc	Flex	Reg
APD0EC.3570.39AC	C9117AXI-S	✓	10.252.49.26	0077.8d22.9920	d0ec.3570.39ac	Flex	Reg
APD0EC.3570.39B0	C9117AXI-S	✓	10.252.49.16	0077.8d22.9940	d0ec.3570.39b0	Flex	Reg
APD0EC.3570.39C4	C9117AXI-S	✓	10.252.49.12	0077.8d22.99e0	d0ec.3570.39c4	Flex	Reg
APD0EC.3570.3A00	C9117AXI-S	✓	10.252.49.14	0077.8d22.9bc0	d0ec.3570.3a00	Flex	Reg

Wireless Controller High Availability

You make customer experience **possible**

ALERT
ADAPT
ACHIEVE

Redundant Port (RP)



C9800-40-K9 Front Panel

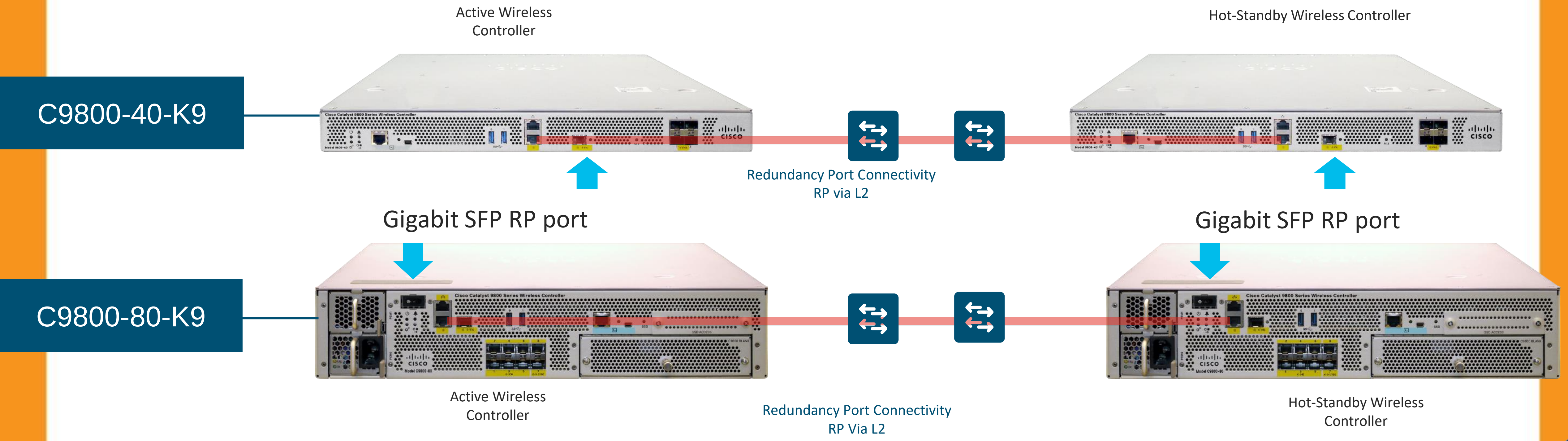
SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

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


Active Wireless Controller
Hot-Standby Wireless Controller
C9800-40-K9
Redundancy Port Connectivity RP via L2
Gigabit SFP RP port
Gigabit SFP RP port
C9800-80-K9
Active Wireless Controller
Redundancy Port Connectivity RP Via L2
Hot-Standby Wireless Controller

The only supported SFPs on Gigabit RP port are : GLC-SX-MMD and GLC-LH-SMD

SAMART TELCOMS

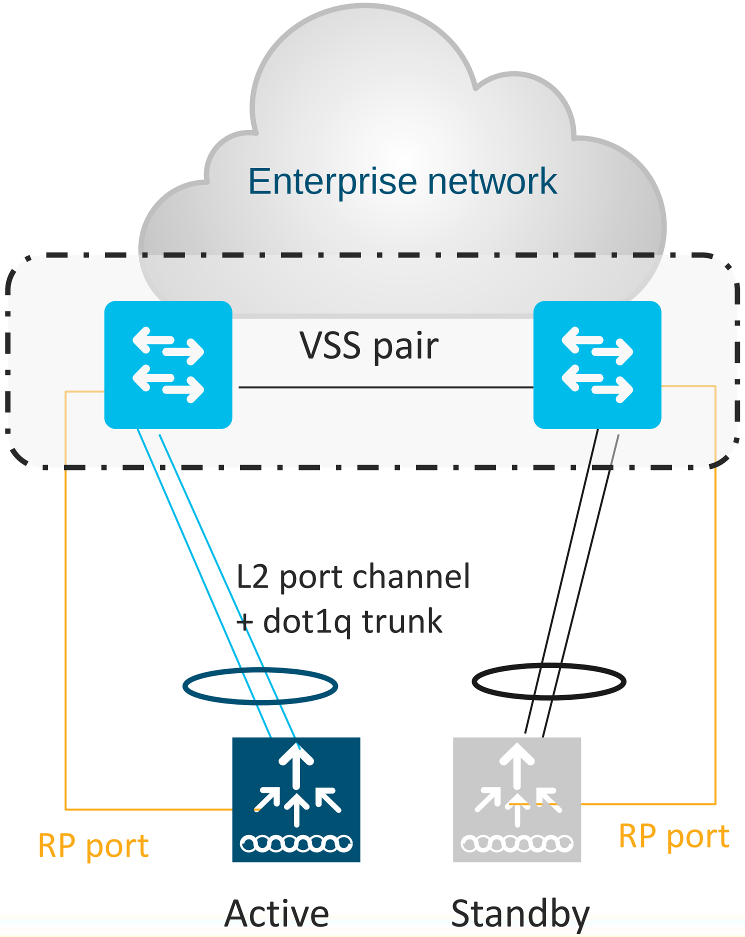
Controller Redundancy - Stateful Switchover (SSO)

- True Box to Box High Availability i.e. 1:1
  - One WLC in Active state and second WLC in Hot Standby state
  - Secondary continuously monitors the health of Active WLC via dedicated link
- Configuration on Active is synched to Standby WLC
  - This happens at startup and incrementally at each configuration change on the Active
- What else is synched between Active and Standby?
  - AP CAPWAP state in 7.3 and 7.4: APs will not restart upon failover, SSID stays UP – **AP SSO**
  - Active Client State in 8.0: client will not disconnect – **Client SSO**
- Downtime during failover reduced to 5 - 1000 msec depending on Failover
  - In the case of power failure on the Active WLC it may take 350-500 msec
  - In case of network failover it can take up to few seconds
- SSO is supported on 3504 /5520 / 8540 / 9800

ALERT
ADAPT
ACHIEVE

High Availability – supported topologies

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

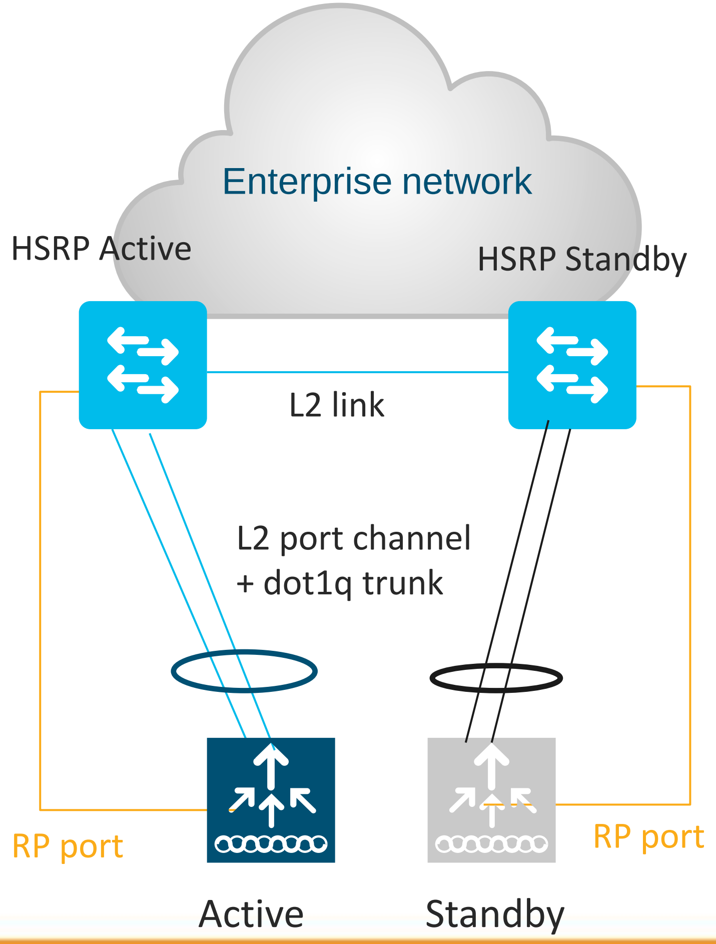


- For SSO HA, connect the Standby in the same way
- Single L2 port-channel on each box
- Enable dot1q to carry multiple VLANs
- IMPORTANT: only LAG with mode ON is supported
- **IMPORTANT: connect RP port to the same VSS/stack member as the uplinks and not back to back**
- Make sure that switch can scale in terms of ARP and MAC table entries
- **This is the recommended topology**

SAMART
TELCOMS

High Availability – supported topologies

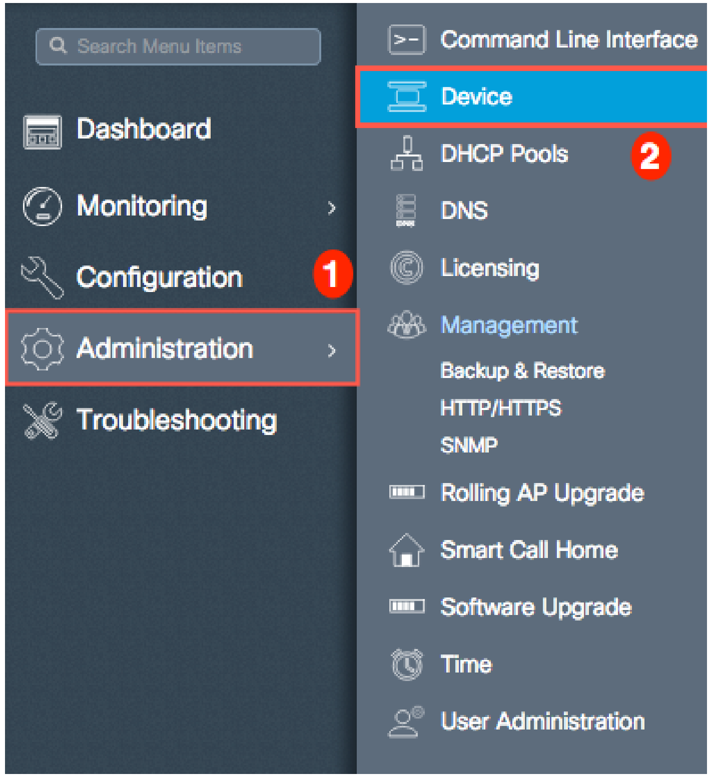
Dual distribution switch with HRSP

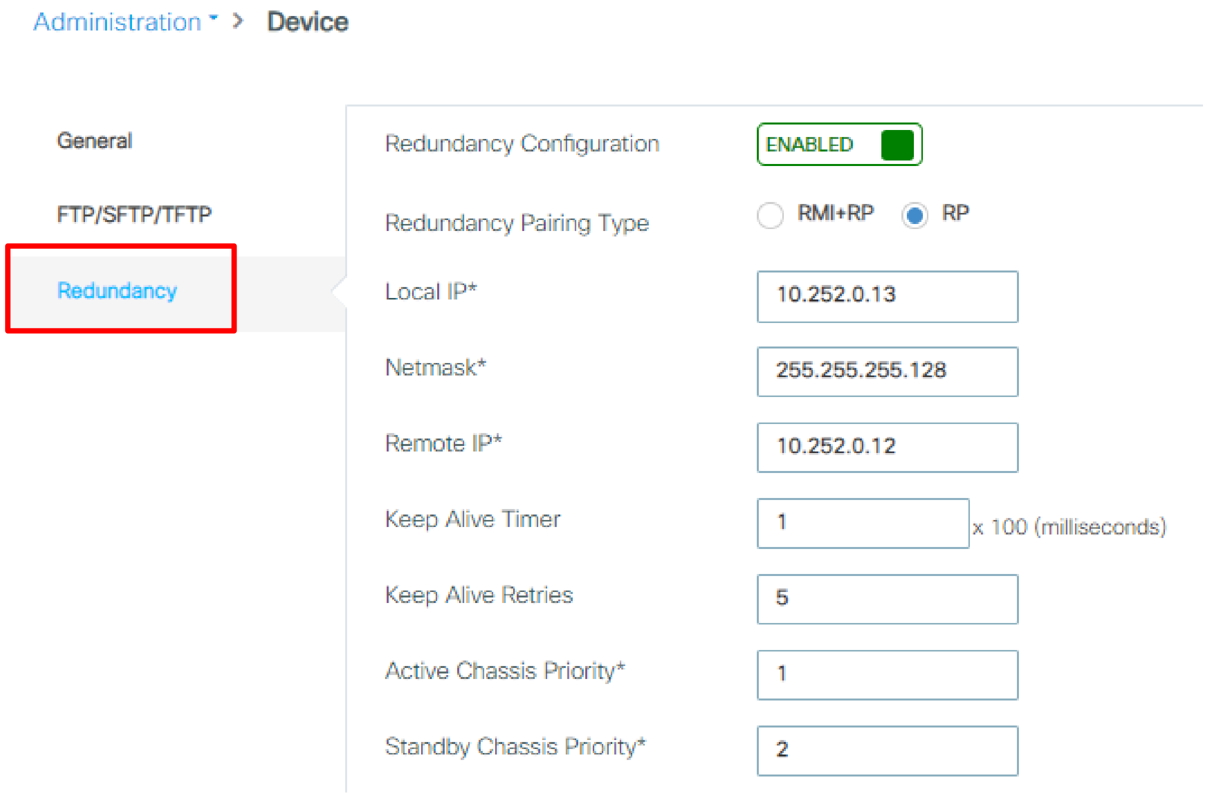


- For SSO HA, connect the Standby in the same way
- Single L2 port-channel on each box
- Enable dot1q to carry multiple VLANs
- IMPORTANT: only LAG with mode ON is supported
- **IMPORTANT: connect RP port to the same distribution switch as the uplinks and not back to back**
- Make sure that switch can scale in terms of ARP and MAC table entries
- **This is a supported topology**

HA SSO Configuration

Step1: Navigate to **Administration> Device** to configure a redundant device. Click on **Redundancy** and select IP address of existing WLC and an IP address for redundant WLC as shown below.





Administration > Device

Redundancy Configuration: ENABLED

Redundancy Pairing Type: ○ RMI+RP ● RP

Local IP*: 10.252.0.13

Netmask*: 255.255.255.128

Remote IP*: 10.252.0.12

Keep Alive Timer: 1 x 100 (milliseconds)

Keep Alive Retries: 5

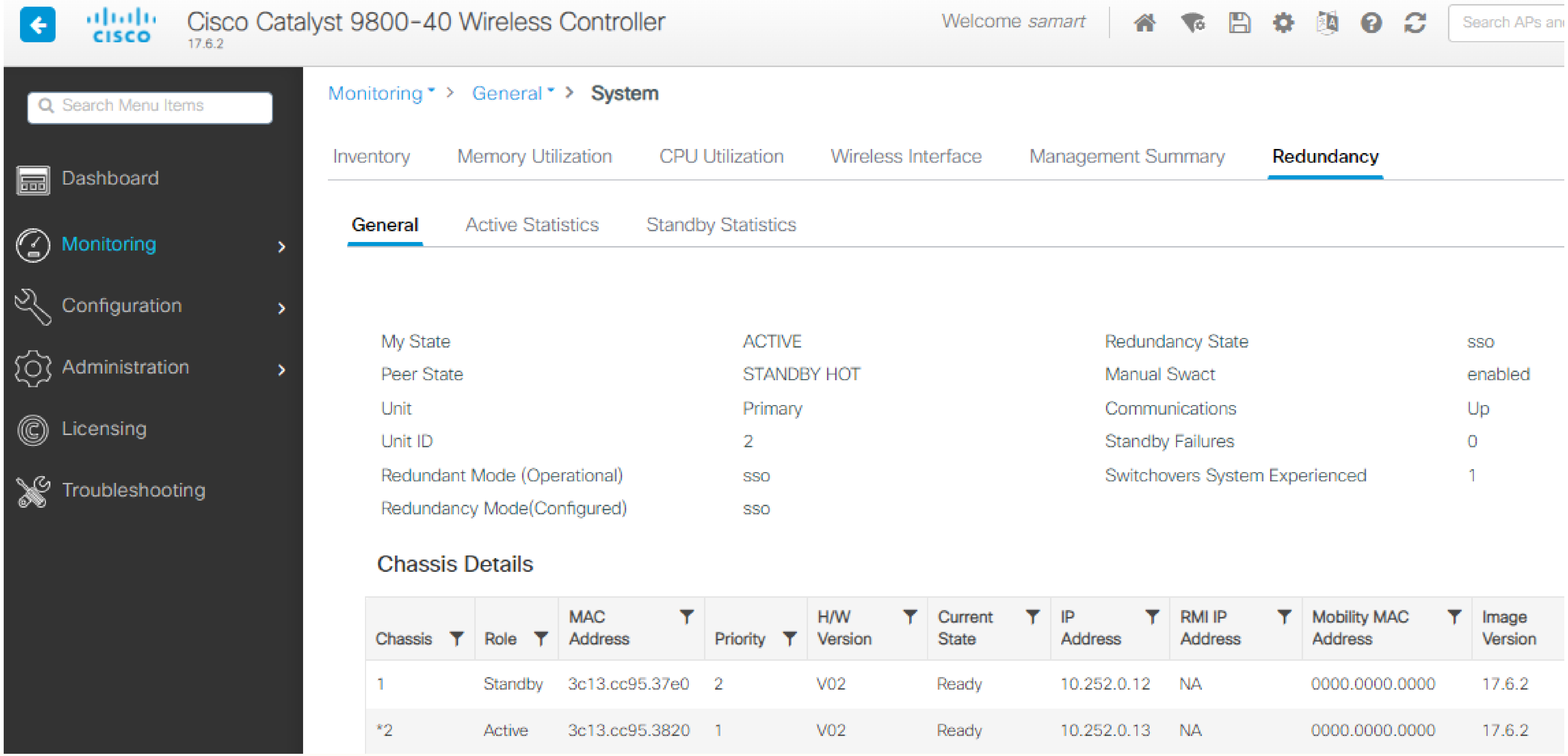
Active Chassis Priority*: 1

Standby Chassis Priority*: 2

ALERT
ADAPT
ACHIEVE

Redundancy on Cisco Catalyst 9800 Wireless Controller

Configuration and Verification



My State	ACTIVE	Redundancy State	sso
Peer State	STANDBY HOT	Manual Swact	enabled
Unit	Primary	Communications	Up
Unit ID	2	Standby Failures	0
Redundant Mode (Operational)	sso	Switchovers System Experienced	1
Redundancy Mode(Configured)	sso		

Chassis Details

Chassis	Role	MAC Address	Priority	H/W Version	Current State	IP Address	RMI IP Address	Mobility MAC Address	Image Version
1	Standby	3c13.cc95.37e0	2	V02	Ready	10.252.0.12	NA	0000.0000.0000	17.6.2
*2	Active	3c13.cc95.3820	1	V02	Ready	10.252.0.13	NA	0000.0000.0000	17.6.2

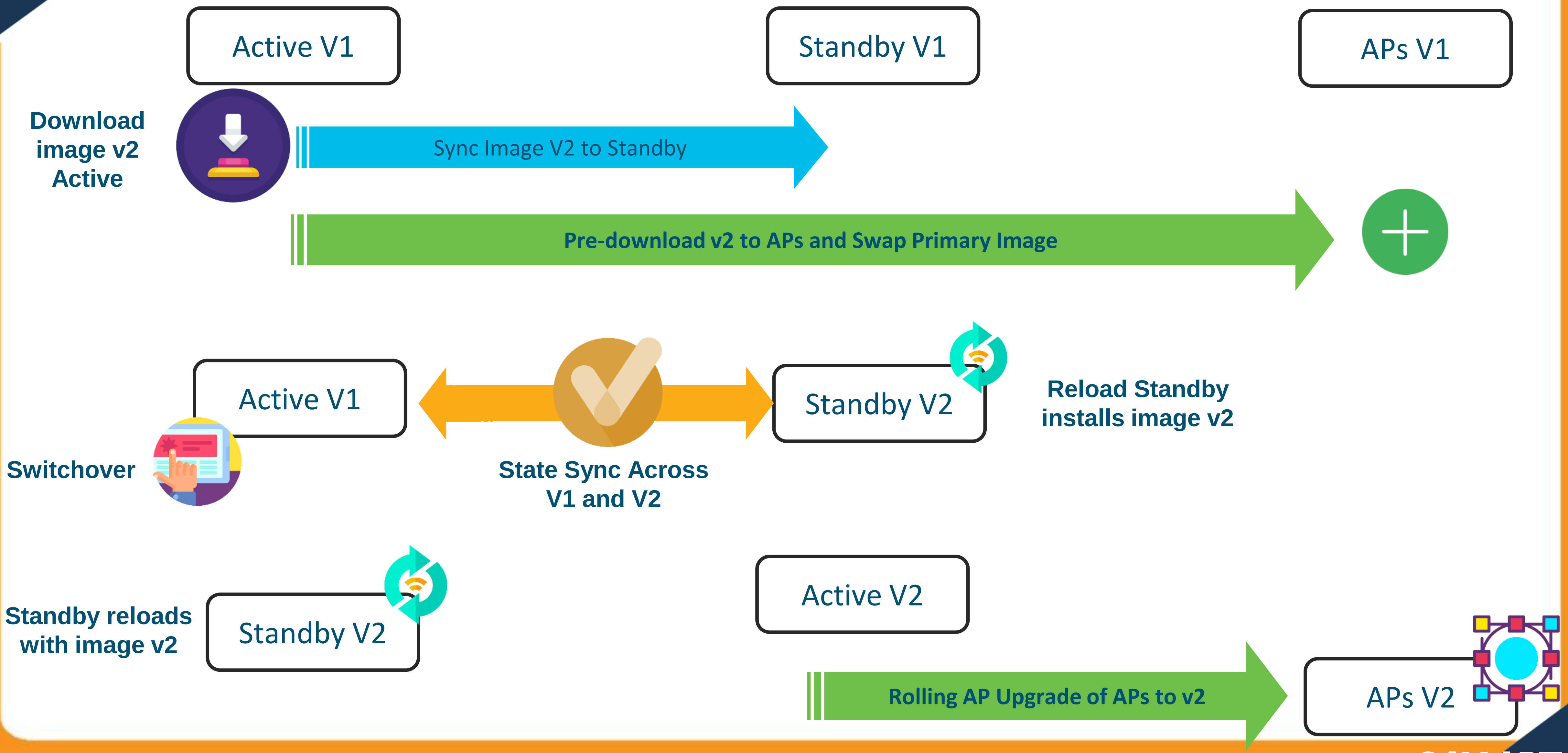
SAMART TELCOMS

ISSU*

You make networking **possible**

*Coming Soon

ISSU Workflow



Active V1

Standby V1

APs V1

Download image v2 Active

Sync Image V2 to Standby

Pre-download v2 to APs and Swap Primary Image

Active V1

Standby V2

Reload Standby installs image v2

Switchover

State Sync Across V1 and V2

Standby reloads with image v2

Standby V2

Active V2

Rolling AP Upgrade of APs to v2

APs V2

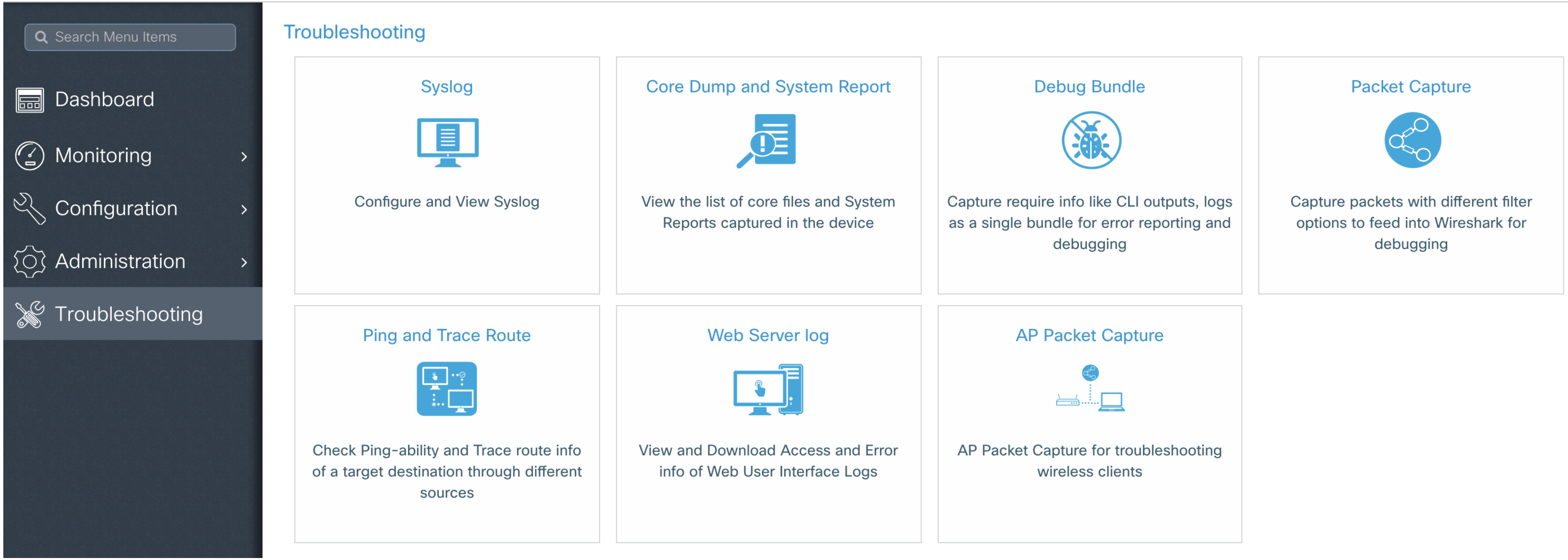
Troubleshooting Wireless Network

You make customer experience **possible**

ALERT
ADAPT
ACHIEVE

Troubleshooting tools

Troubleshooting page



Troubleshooting

Syslog

Configure and View Syslog

Core Dump and System Report

View the list of core files and System Reports captured in the device

Debug Bundle

Capture require info like CLI outputs, logs as a single bundle for error reporting and debugging

Packet Capture

Capture packets with different filter options to feed into Wireshark for debugging

Ping and Trace Route

Check Ping-ability and Trace route info of a target destination through different sources

Web Server log

View and Download Access and Error info of Web User Interface Logs

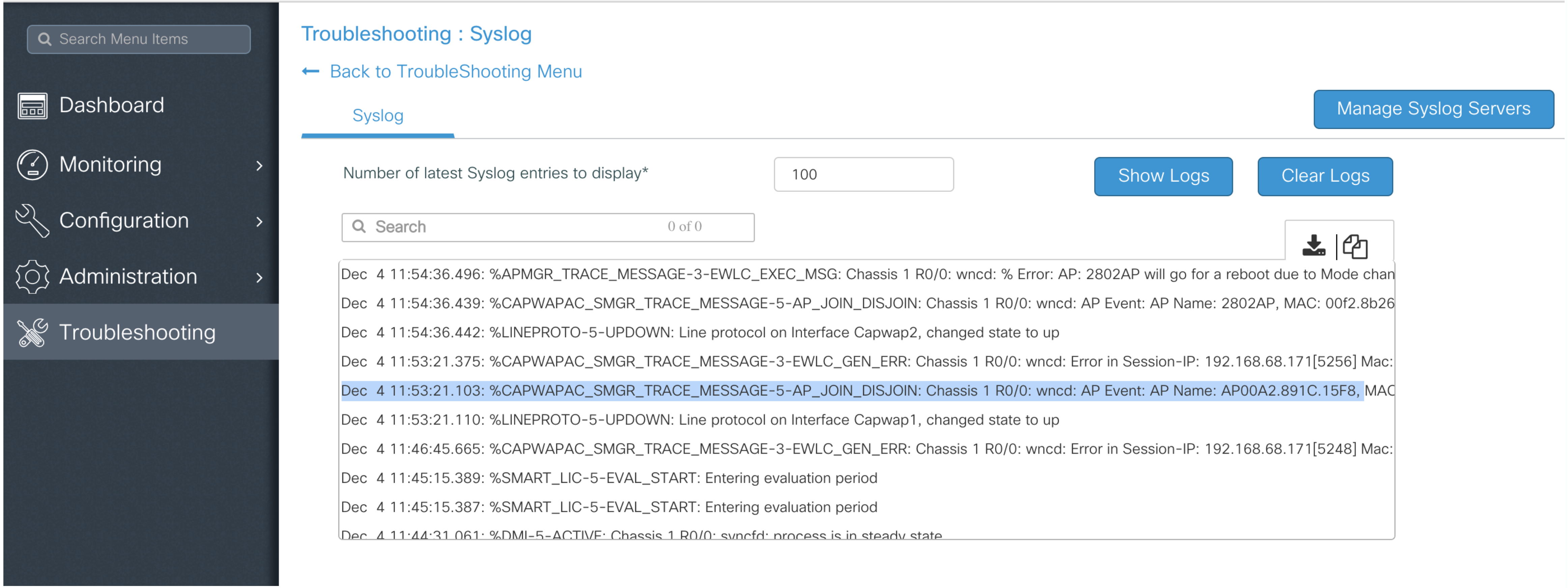
AP Packet Capture

AP Packet Capture for troubleshooting wireless clients

SAMART
TELCOMS

Troubleshooting tools

Syslog page



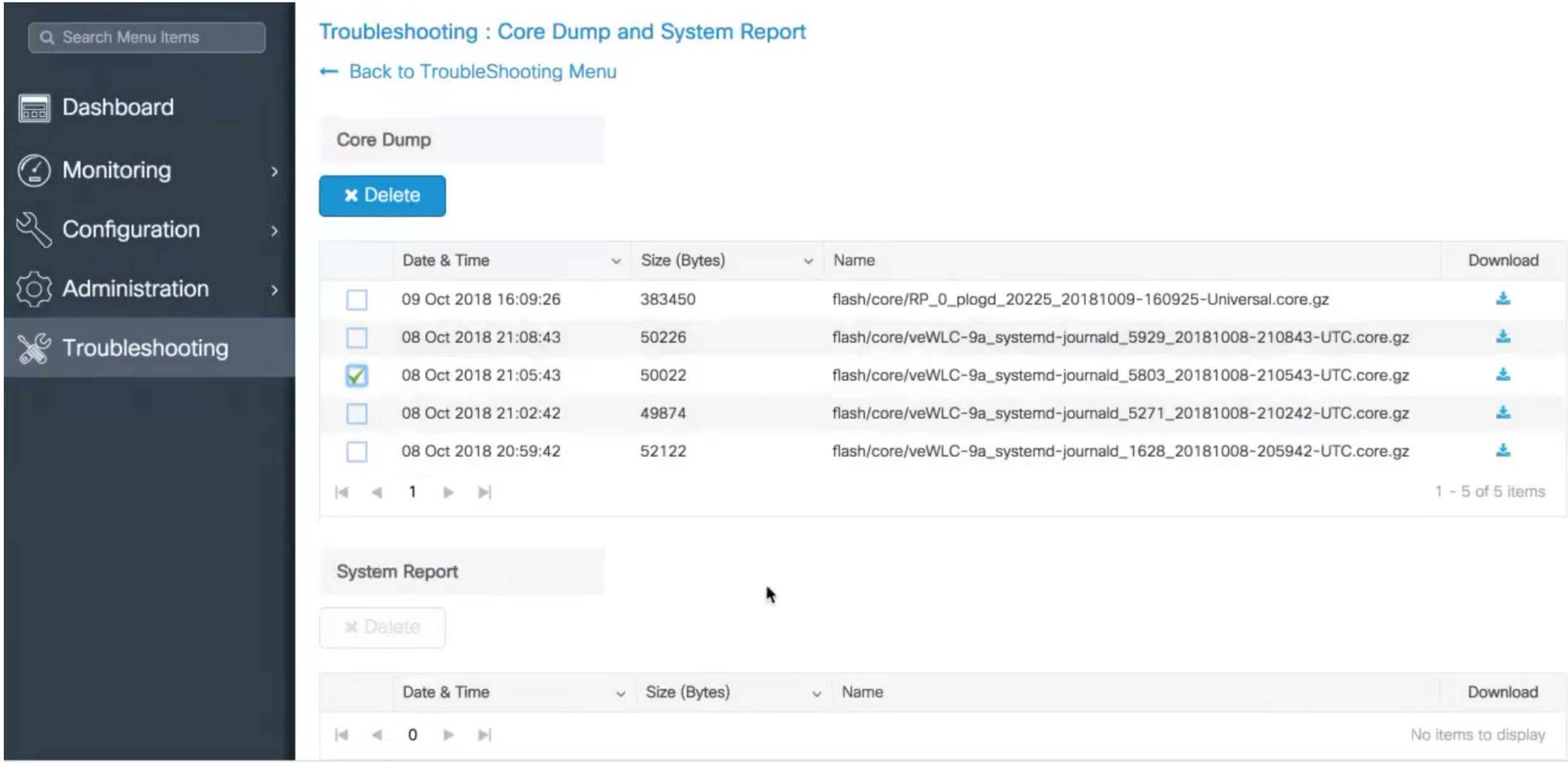
Number of latest Syslog entries to display* 100

```
Dec  4 11:54:36.496: %APMGR_TRACE_MESSAGE-3-EWLC_EXEC_MSG: Chassis 1 R0/0: wncd: % Error: AP: 2802AP will go for a reboot due to Mode chan
Dec  4 11:54:36.439: %CAPWAPAC_SMGR_TRACE_MESSAGE-5-AP_JOIN_DISJOIN: Chassis 1 R0/0: wncd: AP Event: AP Name: 2802AP, MAC: 00f2.8b26
Dec  4 11:54:36.442: %LINEPROTO-5-UPDOWN: Line protocol on Interface Capwap2, changed state to up
Dec  4 11:53:21.375: %CAPWAPAC_SMGR_TRACE_MESSAGE-3-EWLC_GEN_ERR: Chassis 1 R0/0: wncd: Error in Session-IP: 192.168.68.171[5256] Mac:
Dec  4 11:53:21.103: %CAPWAPAC_SMGR_TRACE_MESSAGE-5-AP_JOIN_DISJOIN: Chassis 1 R0/0: wncd: AP Event: AP Name: AP00A2.891C.15F8, MAC
Dec  4 11:53:21.110: %LINEPROTO-5-UPDOWN: Line protocol on Interface Capwap1, changed state to up
Dec  4 11:46:45.665: %CAPWAPAC_SMGR_TRACE_MESSAGE-3-EWLC_GEN_ERR: Chassis 1 R0/0: wncd: Error in Session-IP: 192.168.68.171[5248] Mac:
Dec  4 11:45:15.389: %SMART_LIC-5-EVAL_START: Entering evaluation period
Dec  4 11:45:15.387: %SMART_LIC-5-EVAL_START: Entering evaluation period
Dec  4 11:44:31.061: %DMI-5-ACTIVE: Chassis 1 R0/0: syncfd: process is in steady state
```

ALERT
ADAPT
ACHIEVE

Troubleshooting tools

Core Dump page



Troubleshooting : Core Dump and System Report

← Back to TroubleShooting Menu

Core Dump

✖ Delete

	Date & Time	Size (Bytes)	Name	Download
□	09 Oct 2018 16:09:26	383450	flash/core/RP_0_plogd_20225_20181009-160925-Universal.core.gz	⭳
□	08 Oct 2018 21:08:43	50226	flash/core/veWLC-9a_systemd-journald_5929_20181008-210843-UTC.core.gz	⭳
☑	08 Oct 2018 21:05:43	50022	flash/core/veWLC-9a_systemd-journald_5803_20181008-210543-UTC.core.gz	⭳
□	08 Oct 2018 21:02:42	49874	flash/core/veWLC-9a_systemd-journald_5271_20181008-210242-UTC.core.gz	⭳
□	08 Oct 2018 20:59:42	52122	flash/core/veWLC-9a_systemd-journald_1628_20181008-205942-UTC.core.gz	⭳

1

1 - 5 of 5 items

System Report

✖ Delete

	Date & Time	Size (Bytes)	Name	Download

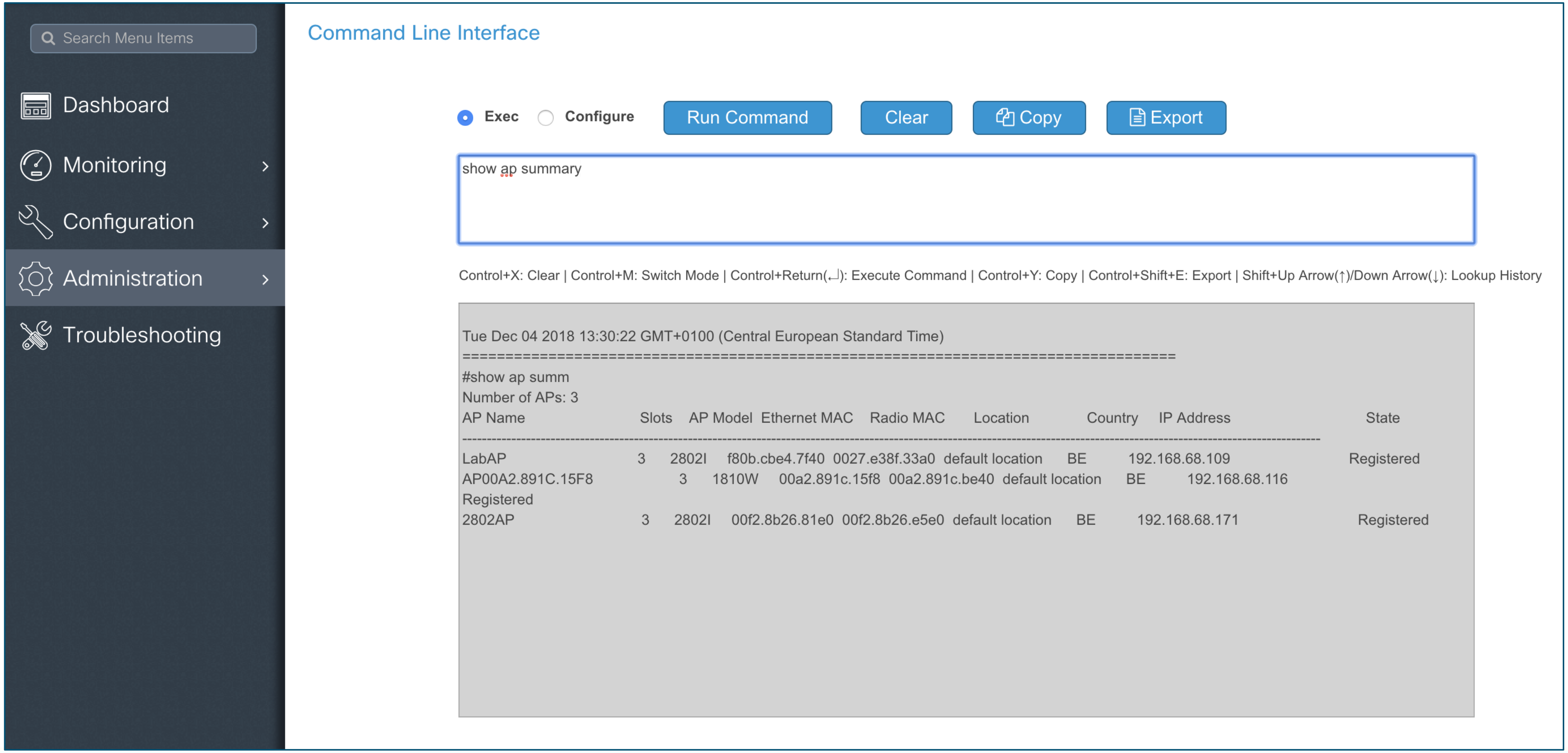
0

No items to display

SAMART
TELCOMS

Troubleshooting tools

Administration -> Command line interface page



```
show ap summary
```

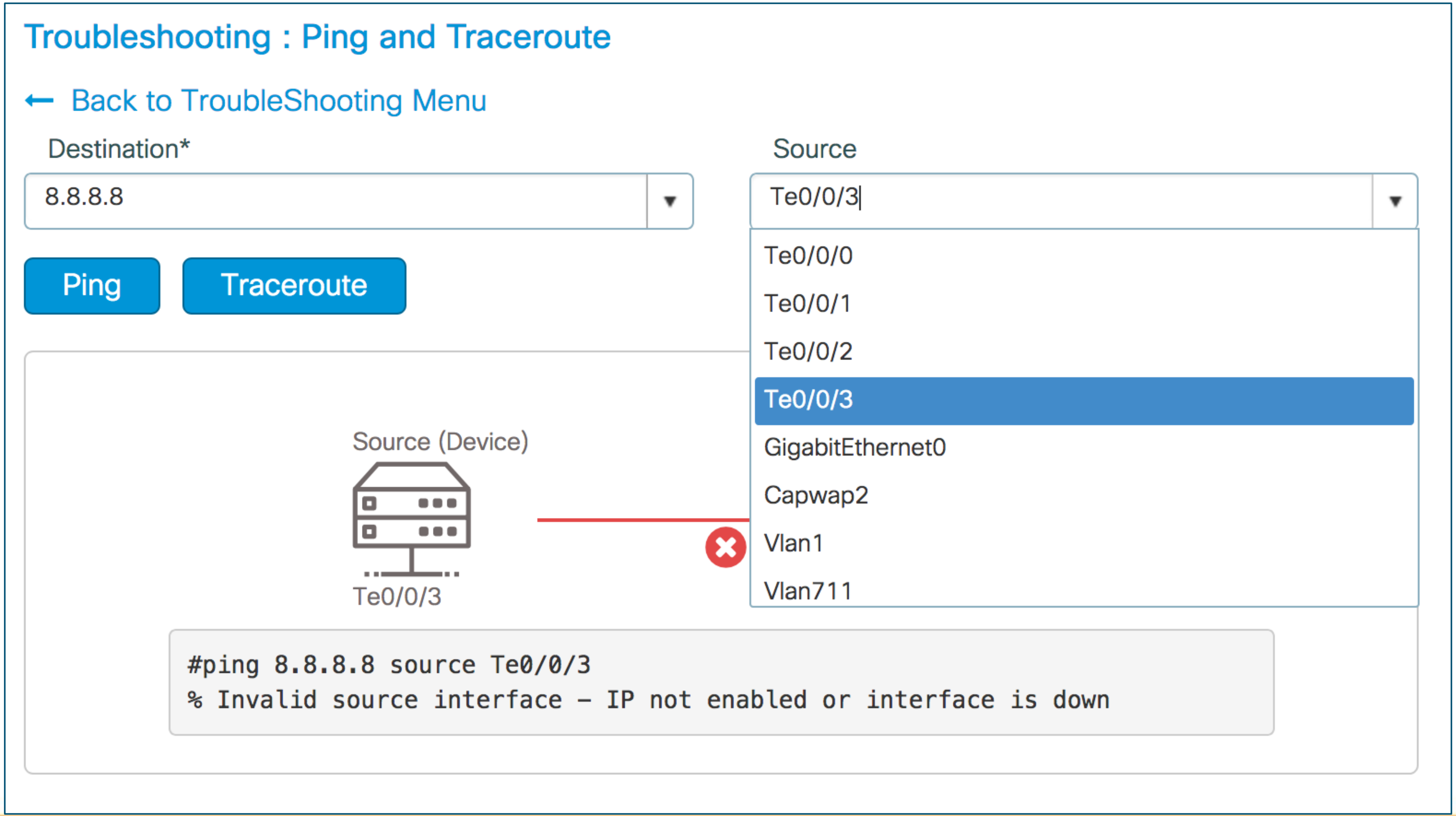
Control+X: Clear | Control+M: Switch Mode | Control+Return(↵): Execute Command | Control+Y: Copy | Control+Shift+E: Export | Shift+Up Arrow(↑)/Down Arrow(↓): Lookup History

```
Tue Dec 04 2018 13:30:22 GMT+0100 (Central European Standard Time)
===========================================================================
#show ap summ
Number of APs: 3
AP Name                    Slots   AP Model  Ethernet MAC    Radio MAC      Location           Country   IP Address                  State
-----------------------------------------------------------------------------------------------------------------------------------------------
LabAP                     3     2802I     f80b.cbe4.7f40  0027.e38f.33a0  default location     BE         192.168.68.109                  Registered
AP00A2.891C.15F8                3     1810W     00a2.891c.15f8  00a2.891c.be40  default location     BE         192.168.68.116
Registered
2802AP                    3     2802I     00f2.8b26.81e0  00f2.8b26.e5e0  default location     BE         192.168.68.171                  Registered
```

ALERT
ADAPT
ACHIEVE

Troubleshooting tools

Ping and Traceroute page



Troubleshooting : Ping and Traceroute

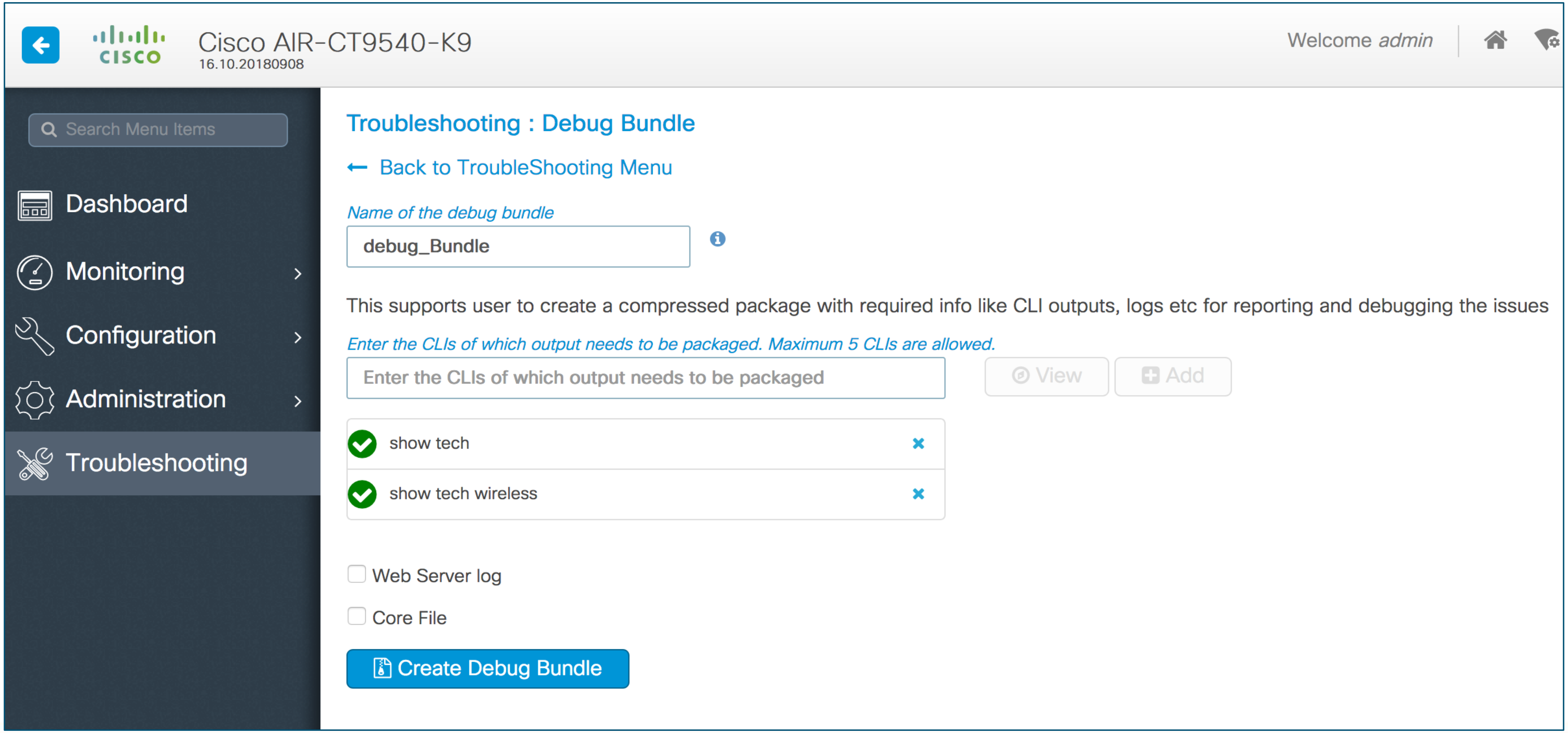
```
#ping 8.8.8.8 source Te0/0/3
% Invalid source interface - IP not enabled or interface is down
```

SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

Troubleshooting tools

Collecting outputs with the debug bundle (UI)



Troubleshooting : Debug Bundle

← Back to TroubleShooting Menu

Name of the debug bundle

debug_Bundle

This supports user to create a compressed package with required info like CLI outputs, logs etc for reporting and debugging the issues

Enter the CLIs of which output needs to be packaged. Maximum 5 CLIs are allowed.

Enter the CLIs of which output needs to be packaged View Add

✓ show tech ✖

✓ show tech wireless ✖

□ Web Server log

□ Core File

Create Debug Bundle

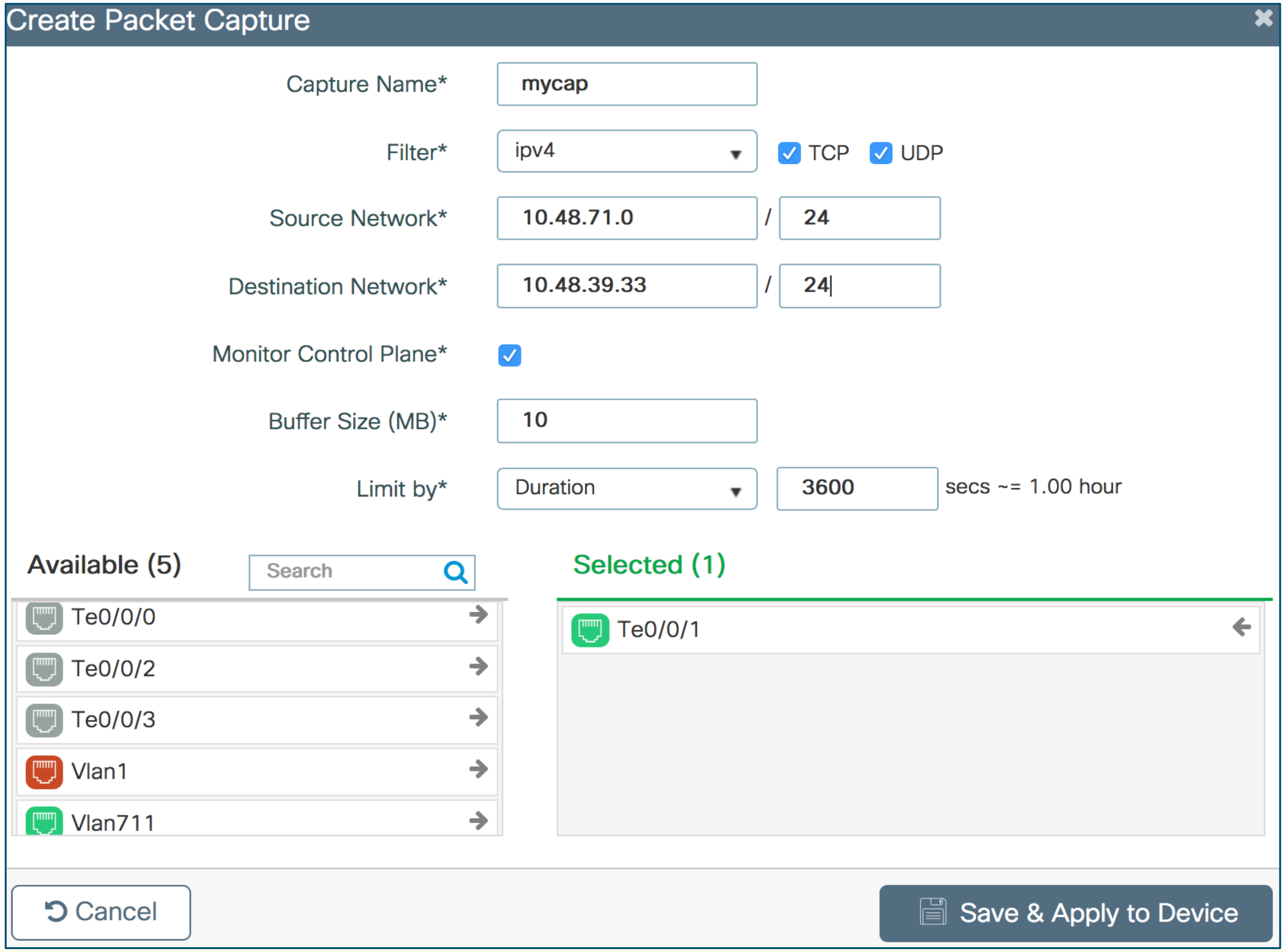
SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

Troubleshooting tools

Embedded Packet Capture web interface

- Web interface to the existing EPC CLI “monitor capture …”
- One click start/stop/download
- Physical and VLAN interfaces can be selected



Create Packet Capture

Capture Name*	mycap
Filter*	ipv4 ☑ TCP ☑ UDP
Source Network*	10.48.71.0 / 24
Destination Network*	10.48.39.33 / 24
Monitor Control Plane*	☑
Buffer Size (MB)*	10
Limit by*	Duration 3600 secs ~= 1.00 hour

Available (5)

- Te0/0/0
- Te0/0/2
- Te0/0/3
- Vlan1
- Vlan711

Selected (1)

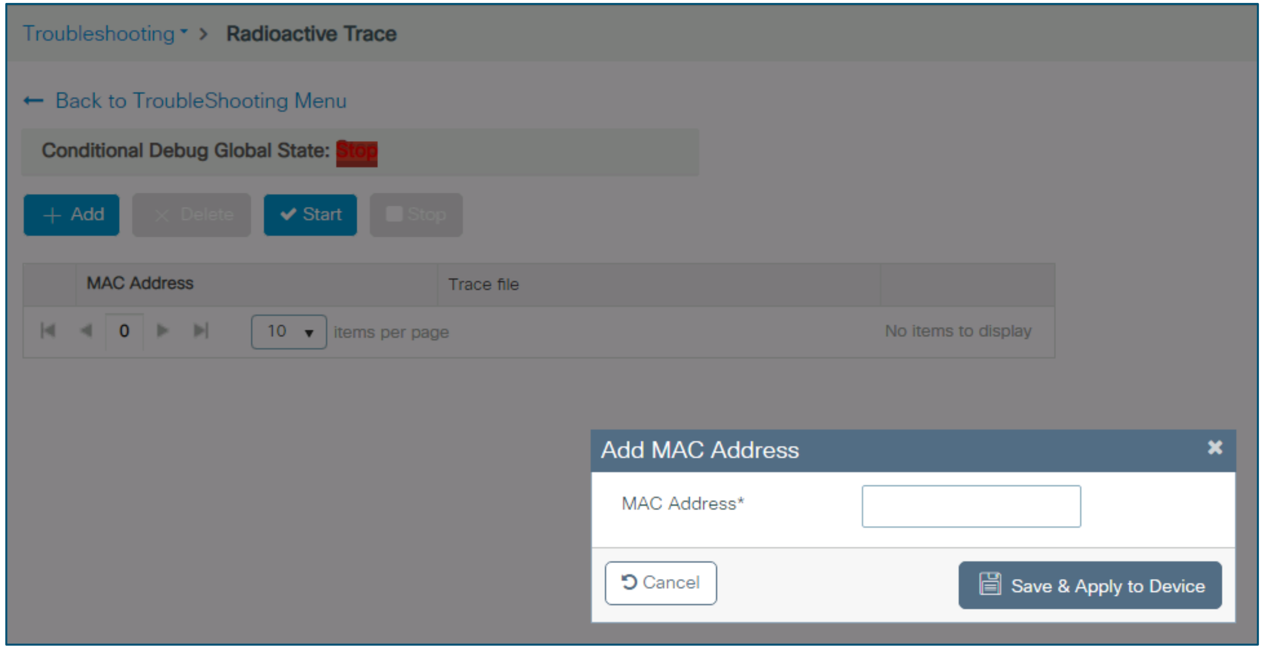
- Te0/0/1

SAMART TELCOMS

Radioactive tracing

Conditional debugging

- You define a condition: client MAC or AP MAC, for example
- Every entry process checks if the flow matches the conditional debugging
- If so, it sets a radioactive flag and passes it on with to all the functions called
- When the flow ends, the radioactive flag is reset
- All intermediate processes will be debugged at the same level without having to verify the original condition



Troubleshooting › Radioactive Trace

← Back to TroubleShooting Menu

Conditional Debug Global State: Stop

MAC Address	Trace file

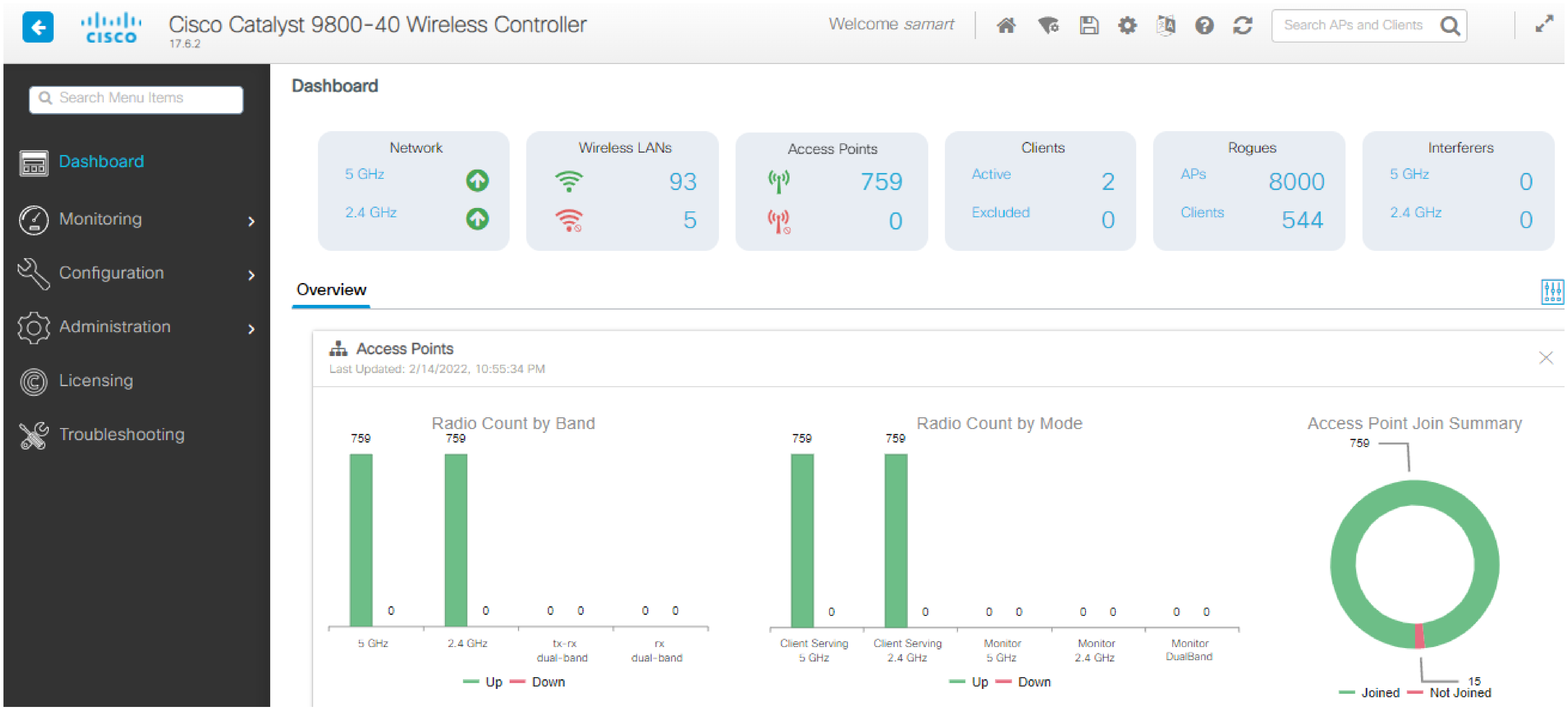
No items to display

Add MAC Address

MAC Address*

ALERT
ADAPT
ACHIEVE

Dashboard



Cisco Catalyst 9800-40 Wireless Controller
17.6.2

Welcome *samart*

Search APs and Clients

Search Menu Items

- Dashboard
- Monitoring ›
- Configuration ›
- Administration ›
- Licensing
- Troubleshooting

Dashboard

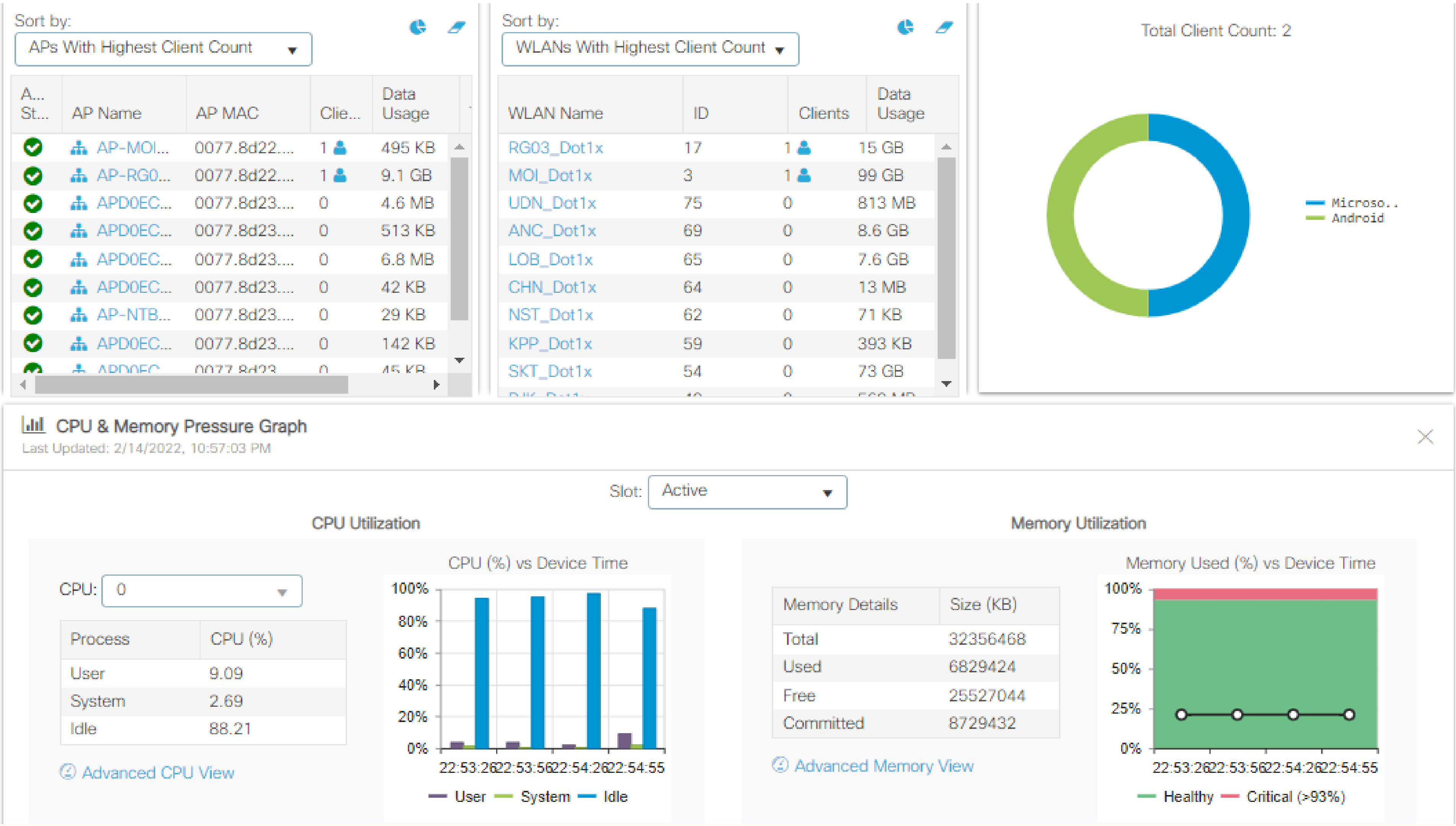
Network		Wireless LANs		Access Points		Clients		Rogues		Interferers	
5 GHz	↑		93		759	Active	2	APs	8000	5 GHz	0
2.4 GHz	↑		5		0	Excluded	0	Clients	544	2.4 GHz	0

Overview

Access Points
Last Updated: 2/14/2022, 10:55:34 PM

ALERT
ADAPT
ACHIEVE

Dashboard



Sort by: APs With Highest Client Count

A... St...	AP Name	AP MAC	Clie...	Data Usage
✓	AP-MOI...	0077.8d22....	1	495 KB
✓	AP-RG0...	0077.8d22....	1	9.1 GB
✓	APD0EC...	0077.8d23....	0	4.6 MB
✓	APD0EC...	0077.8d23....	0	513 KB
✓	APD0EC...	0077.8d23....	0	6.8 MB
✓	APD0EC...	0077.8d23....	0	42 KB
✓	AP-NTB...	0077.8d23....	0	29 KB
✓	APD0EC...	0077.8d23....	0	142 KB
✓	APD0EC...	0077.8d23....	0	45 KB

Sort by: WLANs With Highest Client Count

WLAN Name	ID	Clients	Data Usage
RG03_Dot1x	17	1	15 GB
MOI_Dot1x	3	1	99 GB
UDN_Dot1x	75	0	813 MB
ANC_Dot1x	69	0	8.6 GB
LOB_Dot1x	65	0	7.6 GB
CHN_Dot1x	64	0	13 MB
NST_Dot1x	62	0	71 KB
KPP_Dot1x	59	0	393 KB
SKT_Dot1x	54	0	73 GB

Total Client Count: 2

CPU & Memory Pressure Graph
Last Updated: 2/14/2022, 10:57:03 PM

Slot: Active

CPU Utilization

CPU: 0

Process	CPU (%)
User	9.09
System	2.69
Idle	88.21

Advanced CPU View

CPU (%) vs Device Time

Memory Utilization

Memory Details	Size (KB)
Total	32356468
Used	6829424
Free	25527044
Committed	8729432

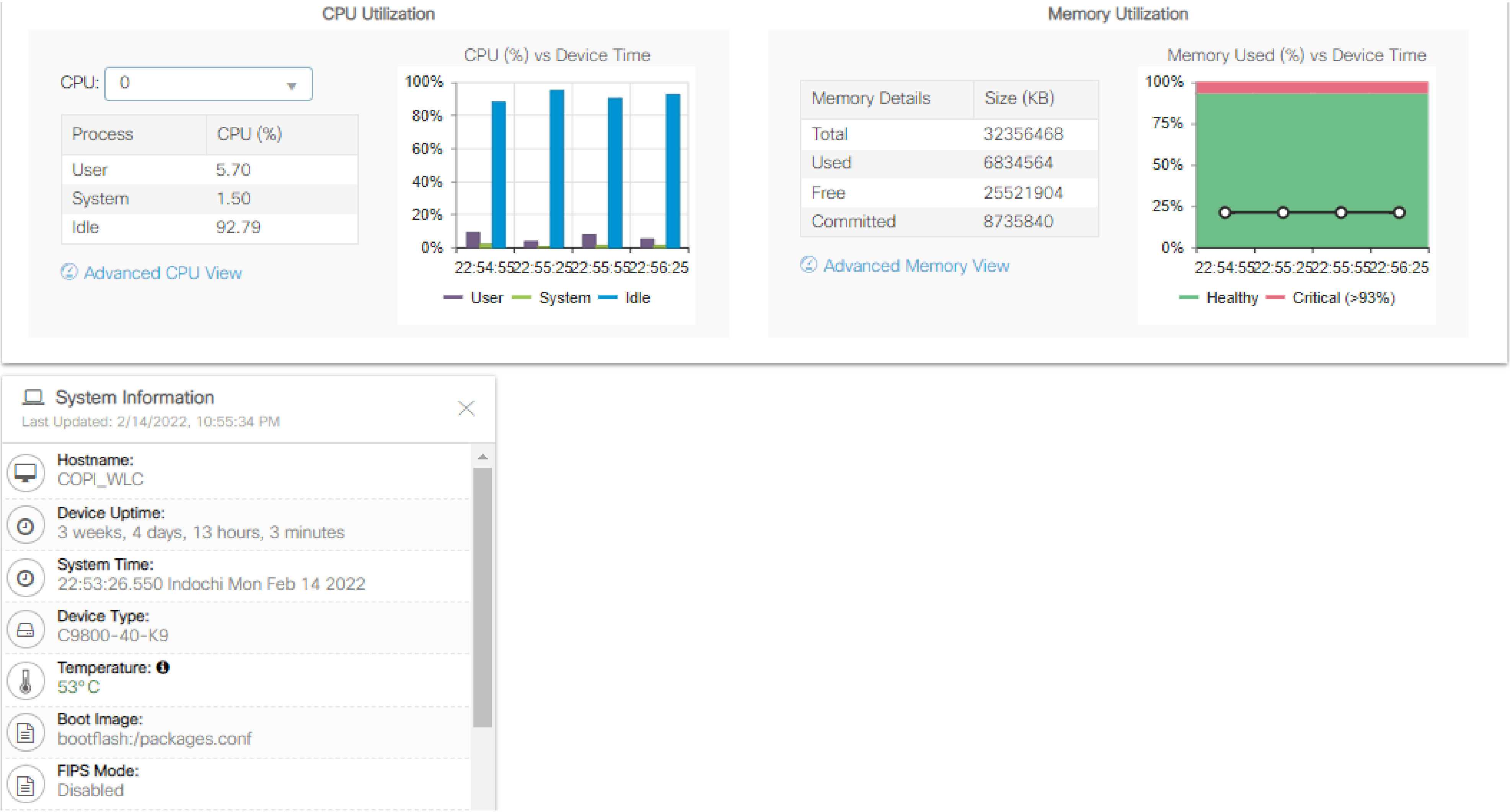
Advanced Memory View

Memory Used (%) vs Device Time

SAMART
TELCOMS

ALERT
ADAPT
ACHIEVE

Dashboard



CPU: 0

Process	CPU (%)
User	5.70
System	1.50
Idle	92.79

Memory Details	Size (KB)
Total	32356468
Used	6834564
Free	25521904
Committed	8735840

System Information
Last Updated: 2/14/2022, 10:55:34 PM

Hostname:
COPI_WLC

Device Uptime:
3 weeks, 4 days, 13 hours, 3 minutes

System Time:
22:53:26.550 Indochi Mon Feb 14 2022

Device Type:
C9800-40-K9

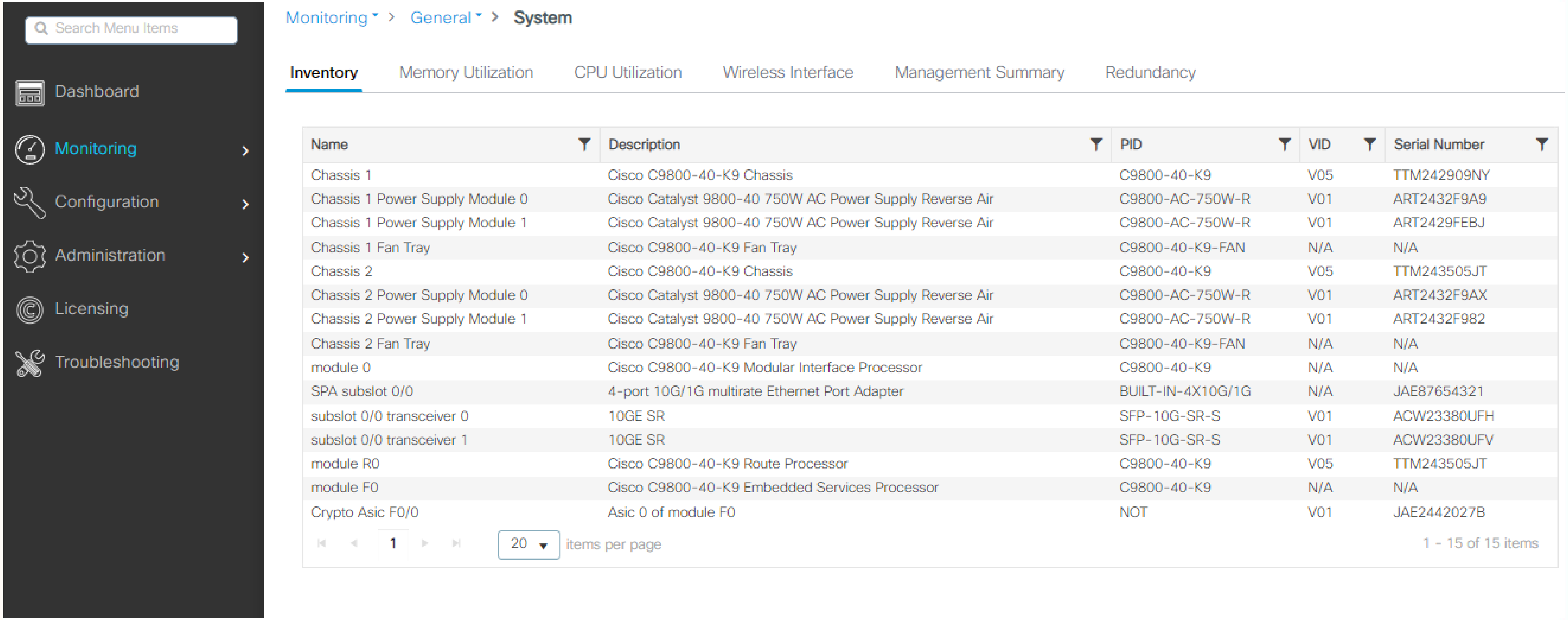
Temperature:
53° C

Boot Image:
bootflash:/packages.conf

FIPS Mode:
Disabled

SAMART TELCOMS

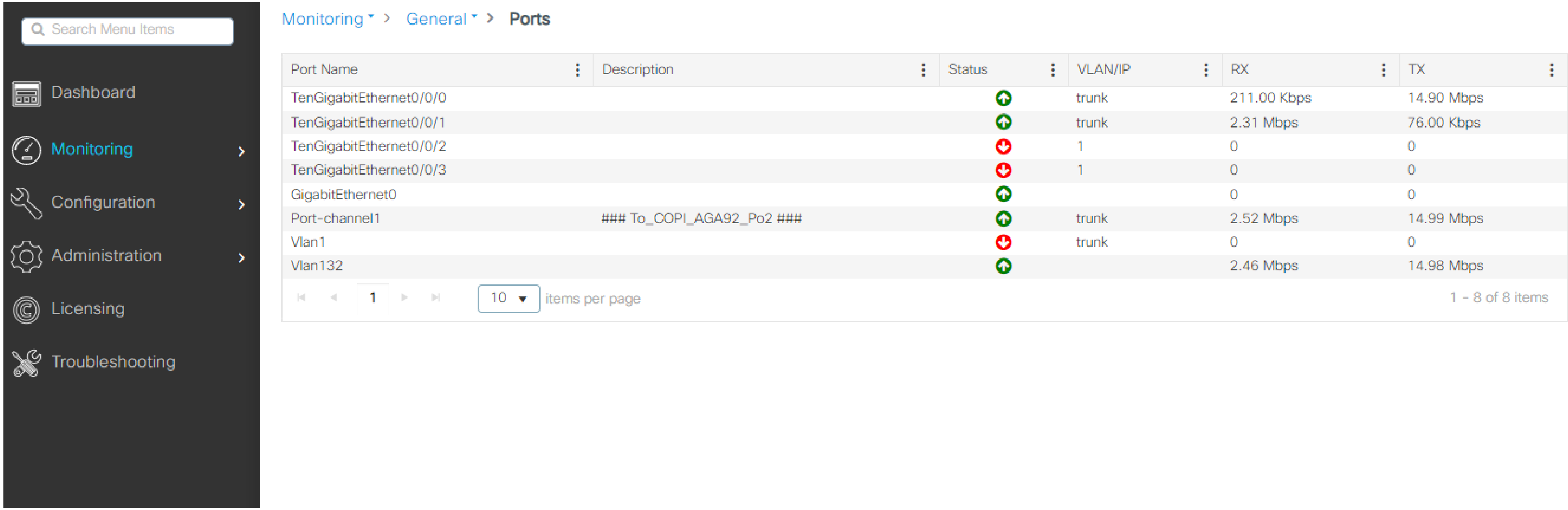
Monitoring System



Name	Description	PID	VID	Serial Number
Chassis 1	Cisco C9800-40-K9 Chassis	C9800-40-K9	V05	TTM242909NY
Chassis 1 Power Supply Module 0	Cisco Catalyst 9800-40 750W AC Power Supply Reverse Air	C9800-AC-750W-R	V01	ART2432F9A9
Chassis 1 Power Supply Module 1	Cisco Catalyst 9800-40 750W AC Power Supply Reverse Air	C9800-AC-750W-R	V01	ART2429FEBJ
Chassis 1 Fan Tray	Cisco C9800-40-K9 Fan Tray	C9800-40-K9-FAN	N/A	N/A
Chassis 2	Cisco C9800-40-K9 Chassis	C9800-40-K9	V05	TTM243505JT
Chassis 2 Power Supply Module 0	Cisco Catalyst 9800-40 750W AC Power Supply Reverse Air	C9800-AC-750W-R	V01	ART2432F9AX
Chassis 2 Power Supply Module 1	Cisco Catalyst 9800-40 750W AC Power Supply Reverse Air	C9800-AC-750W-R	V01	ART2432F982
Chassis 2 Fan Tray	Cisco C9800-40-K9 Fan Tray	C9800-40-K9-FAN	N/A	N/A
module 0	Cisco C9800-40-K9 Modular Interface Processor	C9800-40-K9	N/A	N/A
SPA subslot 0/0	4-port 10G/1G multirate Ethernet Port Adapter	BUILT-IN-4X10G/1G	N/A	JAE87654321
subslot 0/0 transceiver 0	10GE SR	SFP-10G-SR-S	V01	ACW23380UFH
subslot 0/0 transceiver 1	10GE SR	SFP-10G-SR-S	V01	ACW23380UFV
module R0	Cisco C9800-40-K9 Route Processor	C9800-40-K9	V05	TTM243505JT
module F0	Cisco C9800-40-K9 Embedded Services Processor	C9800-40-K9	N/A	N/A
Crypto Asic F0/0	Asic 0 of module F0	NOT	V01	JAE2442027B

1 | 20 items per page | 1 - 15 of 15 items

Monitoring Port

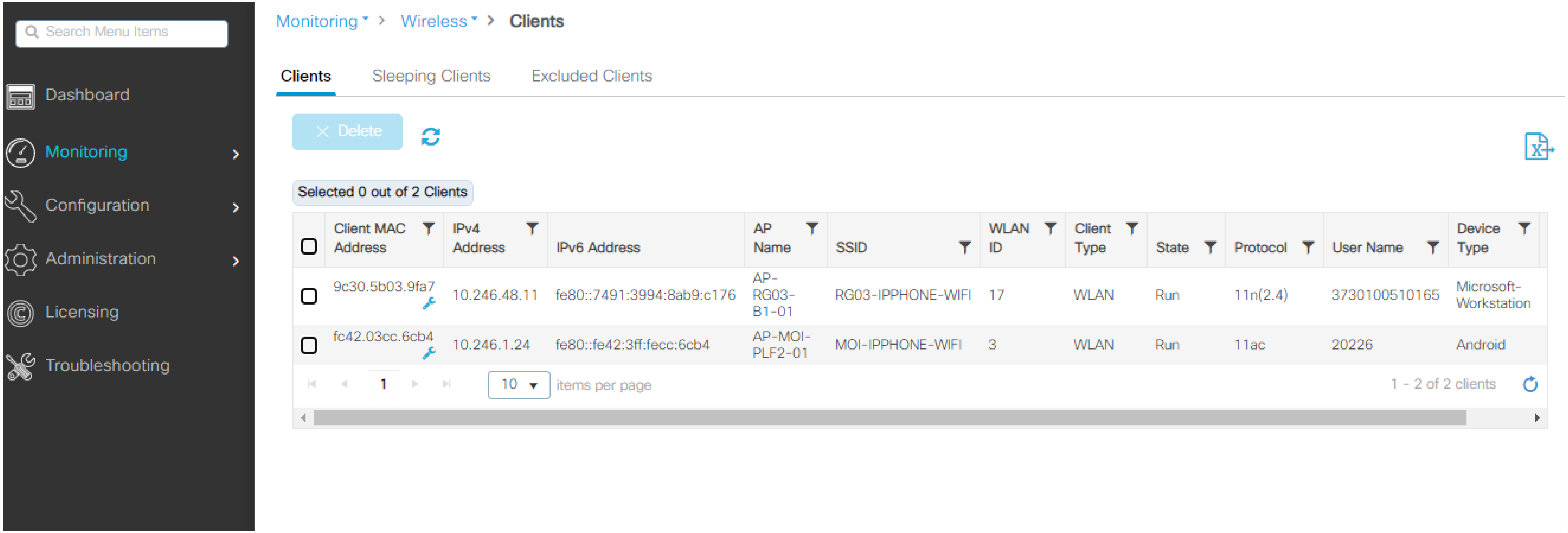


Monitoring › General › Ports

Port Name	Description	Status	VLAN/IP	RX	TX
TenGigabitEthernet0/0/0		⬆	trunk	211.00 Kbps	14.90 Mbps
TenGigabitEthernet0/0/1		⬆	trunk	2.31 Mbps	76.00 Kbps
TenGigabitEthernet0/0/2		⬇	1	0	0
TenGigabitEthernet0/0/3		⬇	1	0	0
GigabitEthernet0		⬆		0	0
Port-channel1	### To_COPI_AGA92_Po2 ###	⬆	trunk	2.52 Mbps	14.99 Mbps
Vlan1		⬇	trunk	0	0
Vlan132		⬆		2.46 Mbps	14.98 Mbps

1 | 10 items per page | 1 - 8 of 8 items

Monitoring Clients



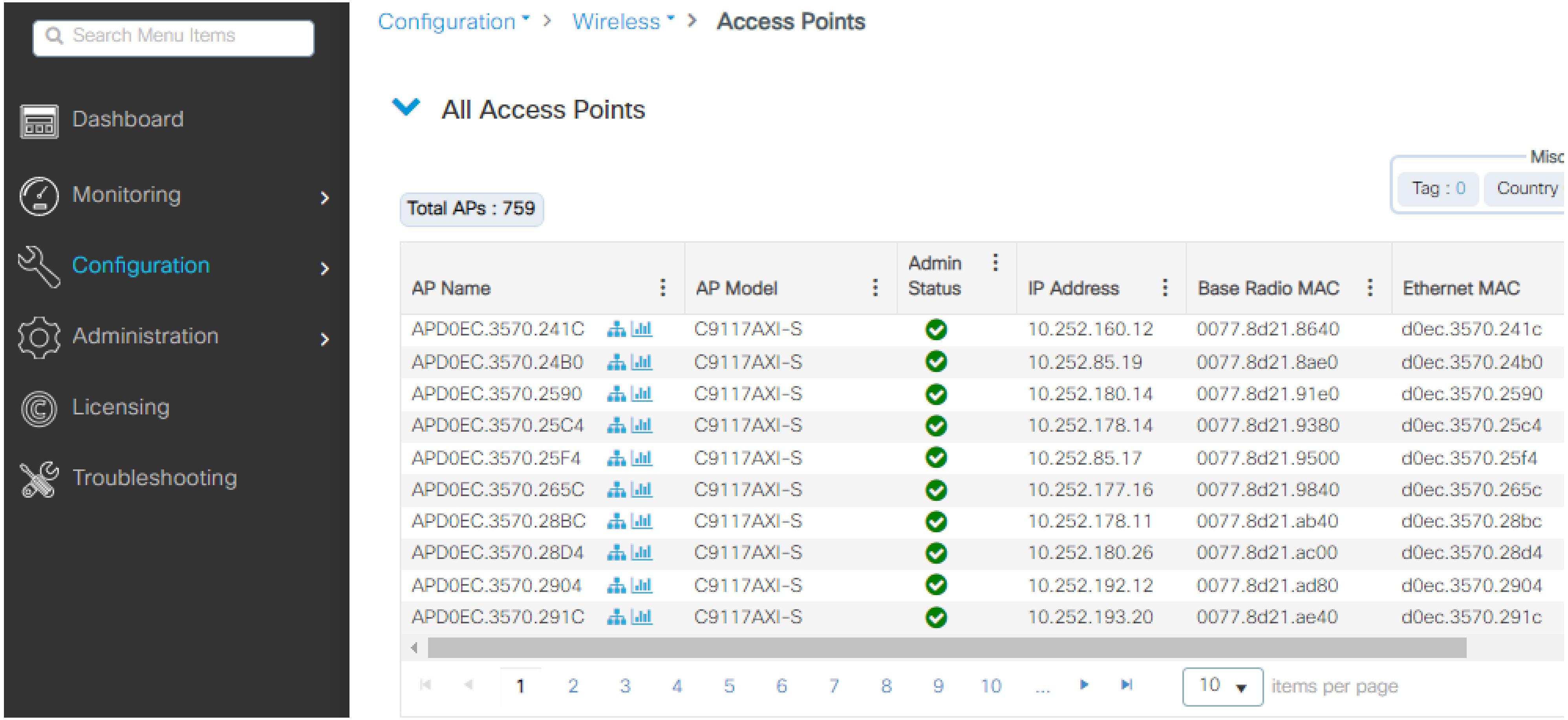
Selected 0 out of 2 Clients

□	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type
□	9c30.5b03.9fa7	10.246.48.11	fe80::7491:3994:8ab9:c176	AP-RG03-B1-01	RG03-IPPHONE-WIFI	17	WLAN	Run	11n(2.4)	3730100510165	Microsoft-Workstation
□	fc42.03cc.6cb4	10.246.1.24	fe80::fe42:3ff:fecc:6cb4	AP-MOI-PLF2-01	MOI-IPPHONE-WIFI	3	WLAN	Run	11ac	20226	Android

1 | 10 items per page | 1 - 2 of 2 clients

ALERT
ADAPT
ACHIEVE

Configuration Access Point



All Access Points

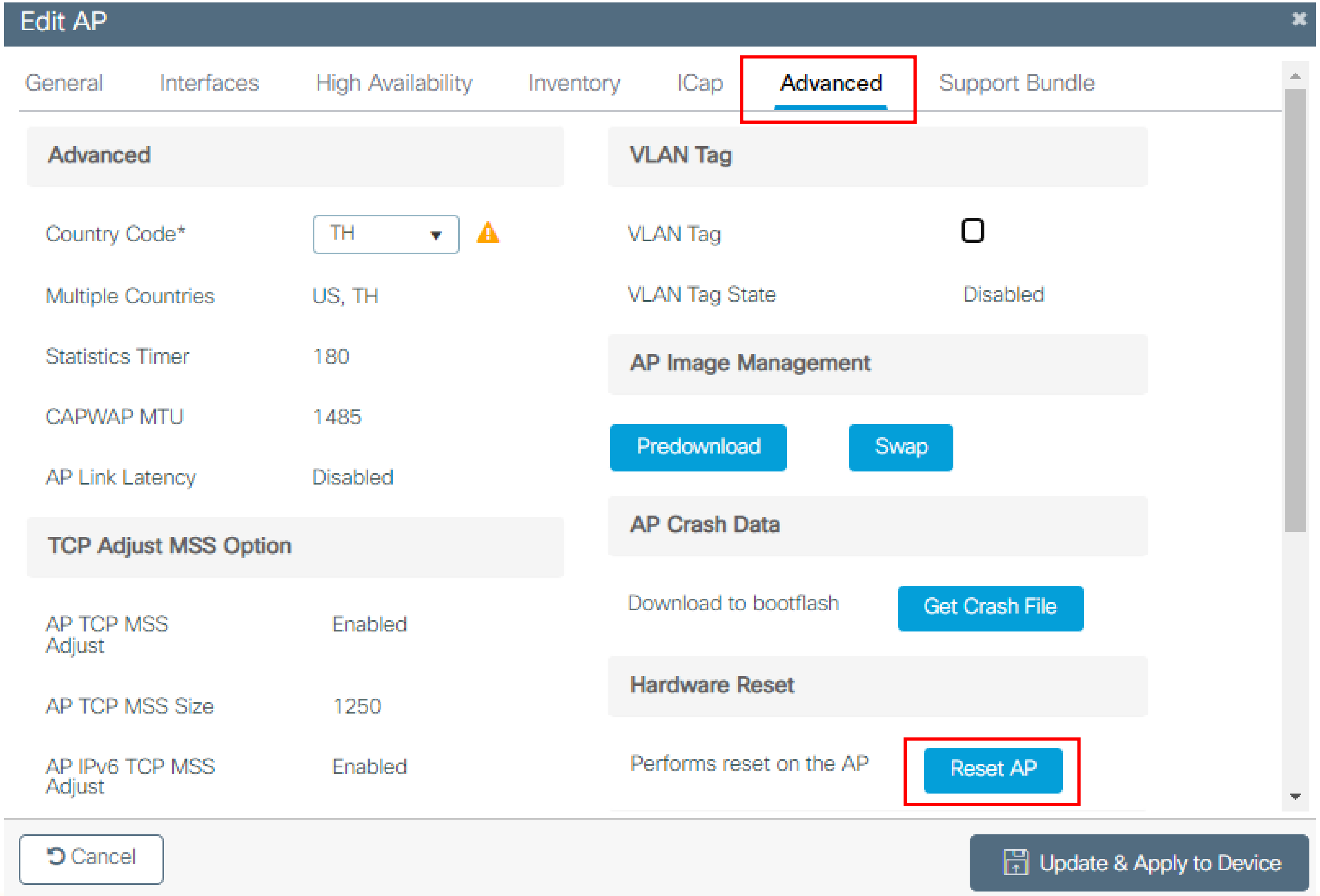
Total APs : 759

AP Name	AP Model	Admin Status	IP Address	Base Radio MAC	Ethernet MAC
APD0EC.3570.241C	C9117AXI-S	✓	10.252.160.12	0077.8d21.8640	d0ec.3570.241c
APD0EC.3570.24B0	C9117AXI-S	✓	10.252.85.19	0077.8d21.8ae0	d0ec.3570.24b0
APD0EC.3570.2590	C9117AXI-S	✓	10.252.180.14	0077.8d21.91e0	d0ec.3570.2590
APD0EC.3570.25C4	C9117AXI-S	✓	10.252.178.14	0077.8d21.9380	d0ec.3570.25c4
APD0EC.3570.25F4	C9117AXI-S	✓	10.252.85.17	0077.8d21.9500	d0ec.3570.25f4
APD0EC.3570.265C	C9117AXI-S	✓	10.252.177.16	0077.8d21.9840	d0ec.3570.265c
APD0EC.3570.28BC	C9117AXI-S	✓	10.252.178.11	0077.8d21.ab40	d0ec.3570.28bc
APD0EC.3570.28D4	C9117AXI-S	✓	10.252.180.26	0077.8d21.ac00	d0ec.3570.28d4
APD0EC.3570.2904	C9117AXI-S	✓	10.252.192.12	0077.8d21.ad80	d0ec.3570.2904
APD0EC.3570.291C	C9117AXI-S	✓	10.252.193.20	0077.8d21.ae40	d0ec.3570.291c

SAMART
TELCOMS

ALERT
ADAPT
ACHIEVE

Reset Access Point



Edit AP

Advanced

Country Code* TH

Multiple Countries US, TH

Statistics Timer 180

CAPWAP MTU 1485

AP Link Latency Disabled

TCP Adjust MSS Option

AP TCP MSS Adjust Enabled

AP TCP MSS Size 1250

AP IPv6 TCP MSS Adjust Enabled

VLAN Tag

VLAN Tag □

VLAN Tag State Disabled

AP Image Management

AP Crash Data

Download to bootflash

Hardware Reset

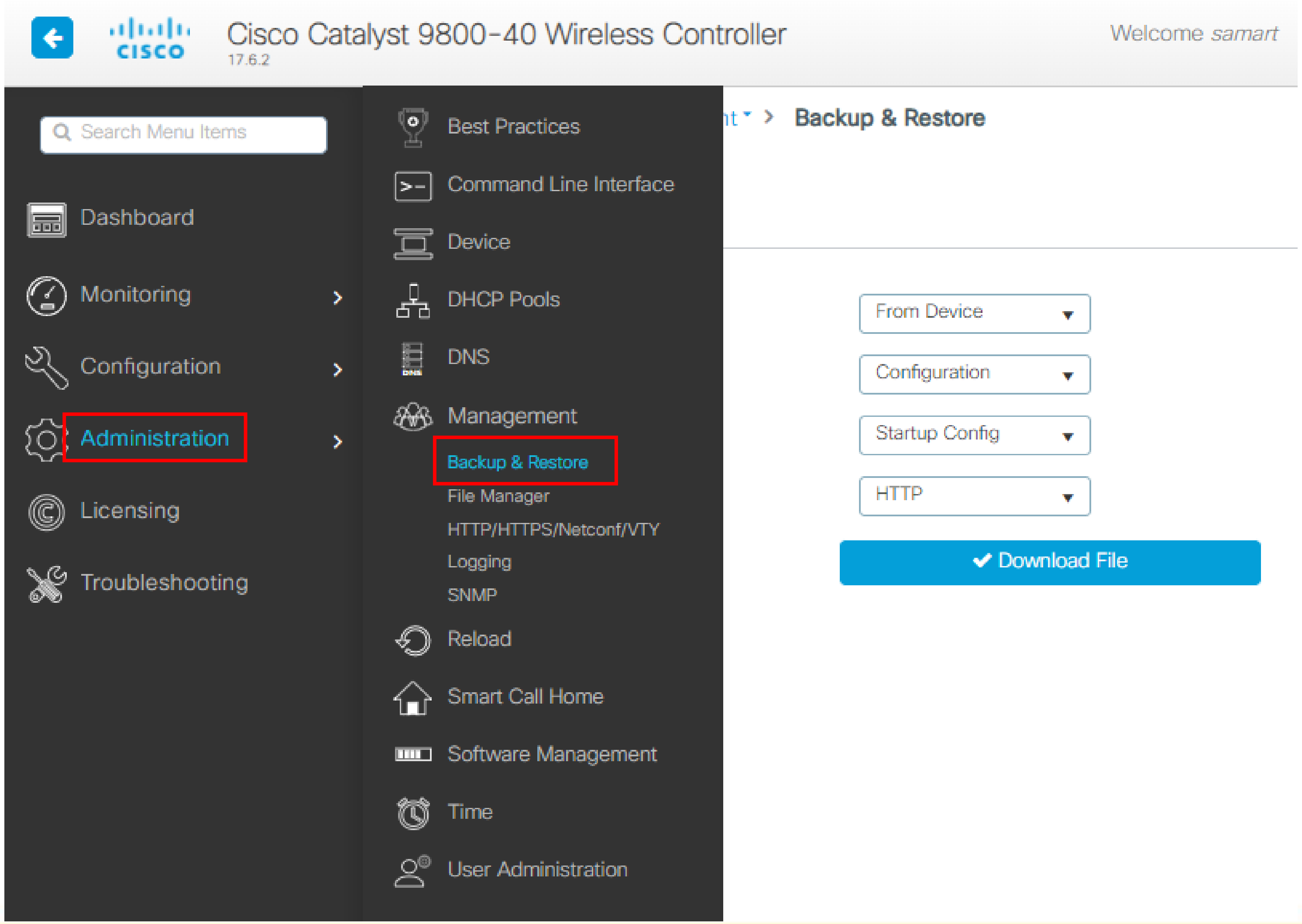
Performs reset on the AP

SAMART
TELCOMS

ALERT
ADAPT
ACHIEVE

Backup Wireless Lan Controller

Select Administration > Backup & Restore

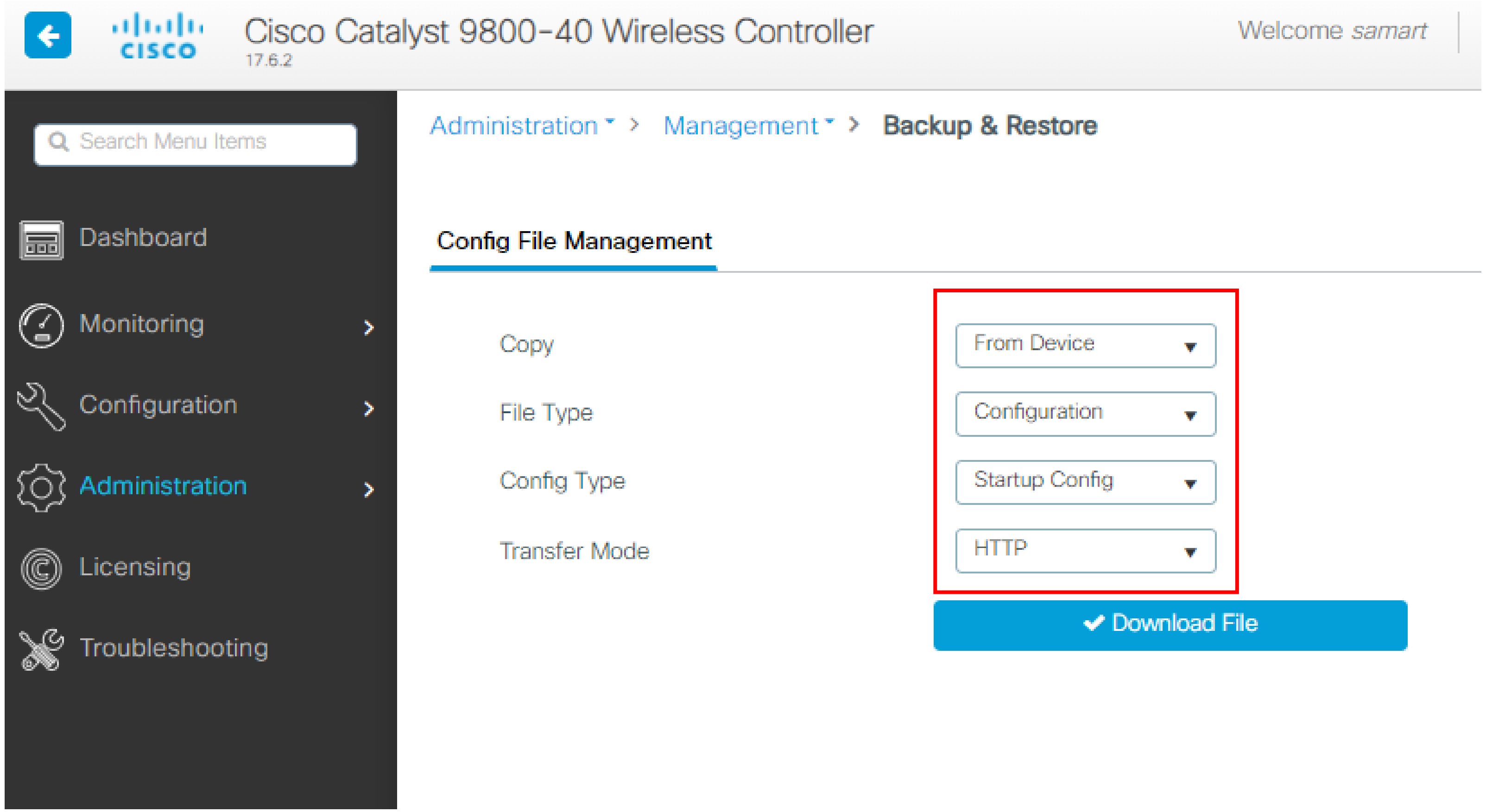


Cisco Catalyst 9800-40 Wireless Controller
17.6.2
Welcome *samart*

SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

Backup Wireless Lan Controller



Administration > Management > Backup & Restore

Config File Management

Copy: From Device

File Type: Configuration

Config Type: Startup Config

Transfer Mode: HTTP

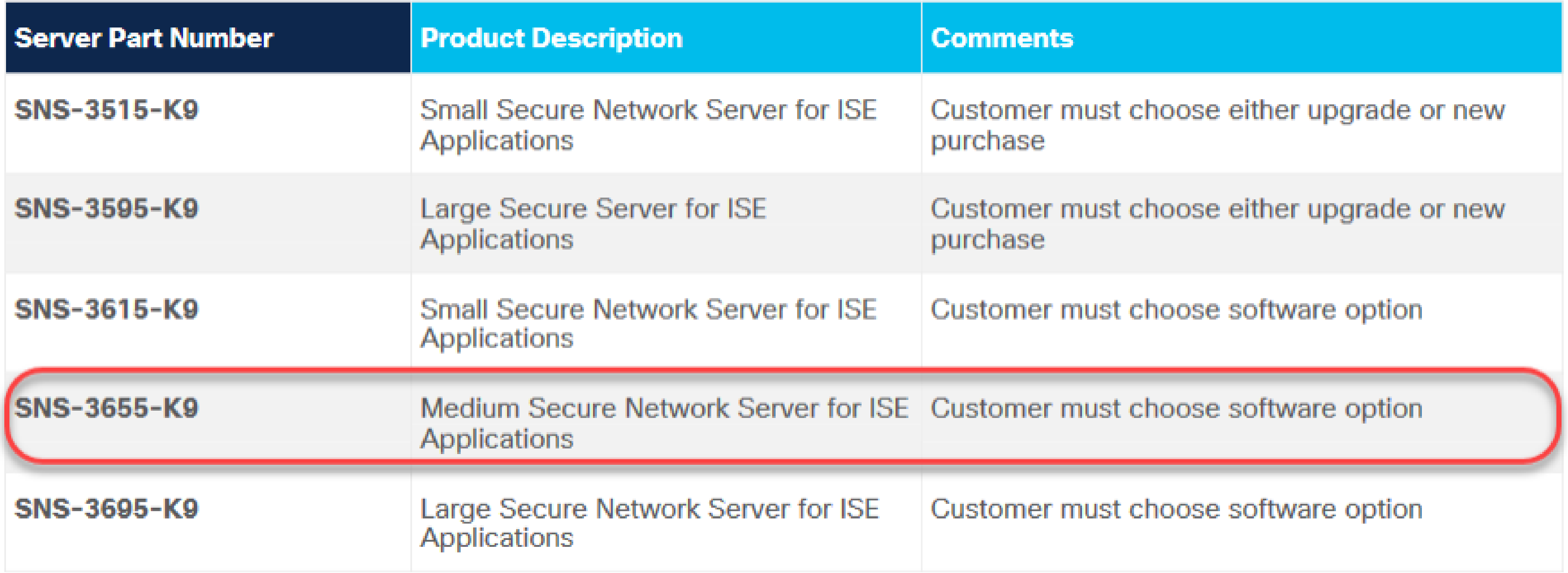
✔ Download File

SAMART TELCOMS

Identity Service Engine (ISE)

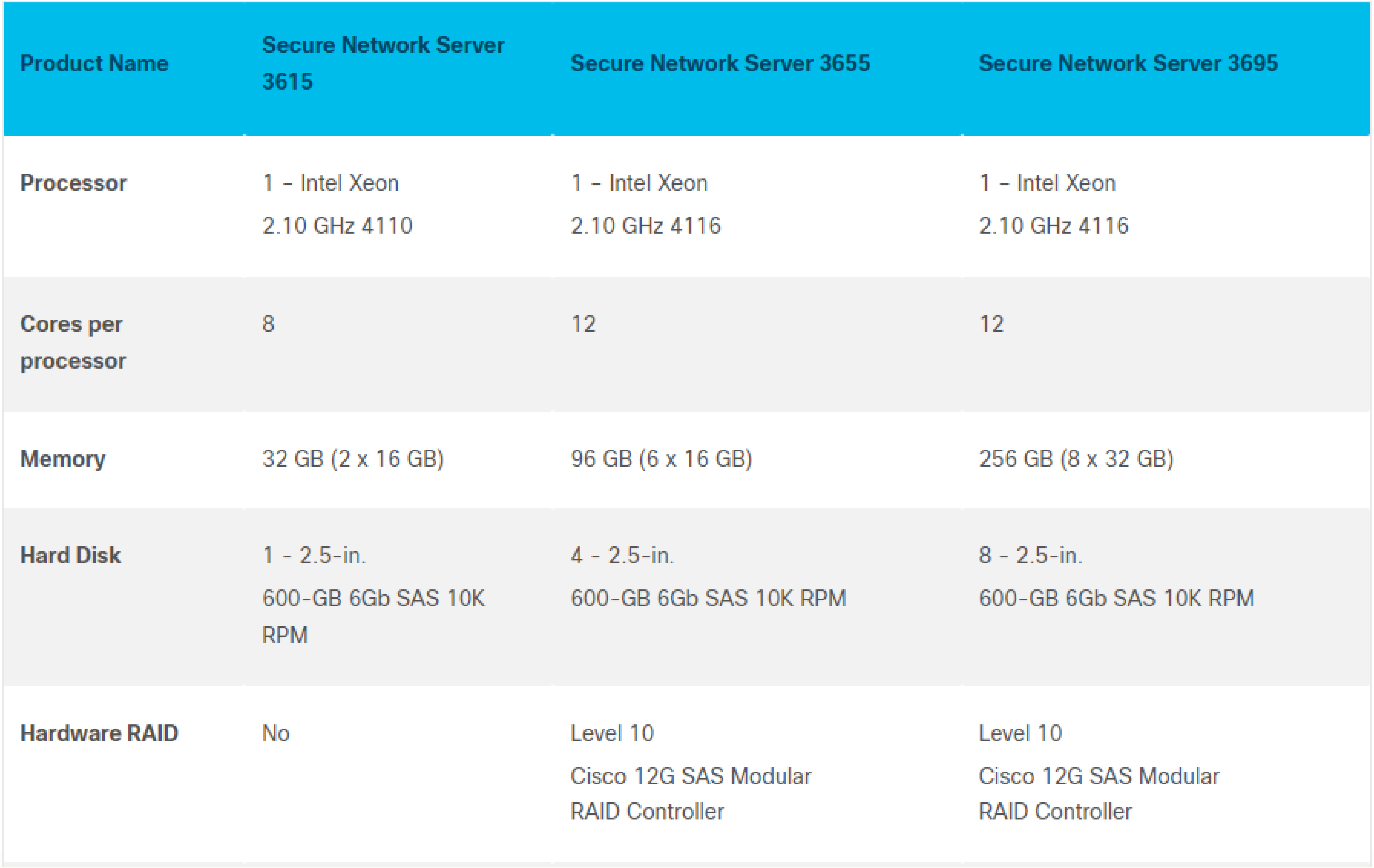
You make customer experience **possible**

Cisco ISE Hardware Appliance



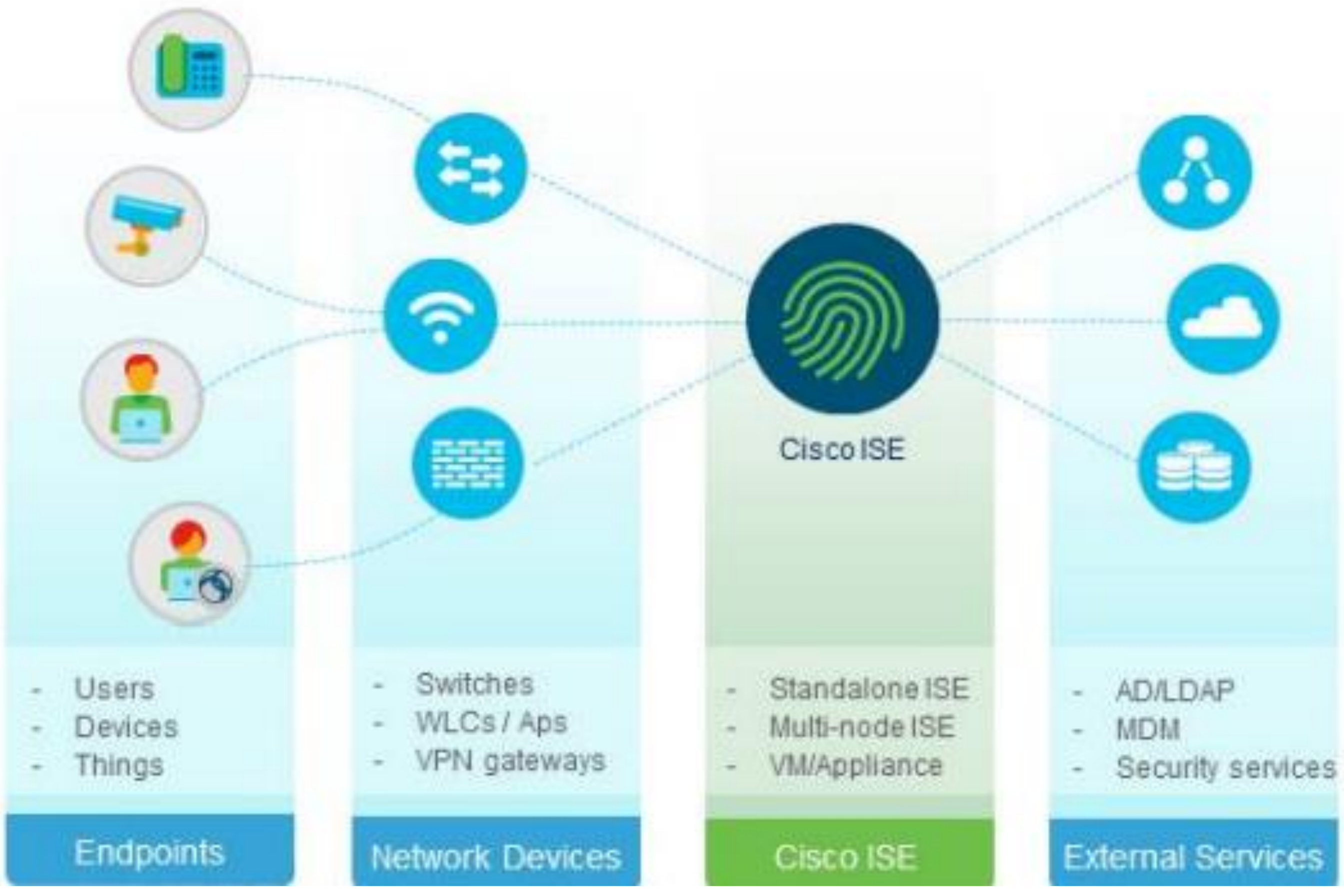
Server Part Number	Product Description	Comments
SNS-3515-K9	Small Secure Network Server for ISE Applications	Customer must choose either upgrade or new purchase
SNS-3595-K9	Large Secure Server for ISE Applications	Customer must choose either upgrade or new purchase
SNS-3615-K9	Small Secure Network Server for ISE Applications	Customer must choose software option
SNS-3655-K9	Medium Secure Network Server for ISE Applications	Customer must choose software option
SNS-3695-K9	Large Secure Network Server for ISE Applications	Customer must choose software option

Cisco ISE Hardware Appliance



Product Name	Secure Network Server 3615	Secure Network Server 3655	Secure Network Server 3695
Processor	1 – Intel Xeon 2.10 GHz 4110	1 – Intel Xeon 2.10 GHz 4116	1 – Intel Xeon 2.10 GHz 4116
Cores per processor	8	12	12
Memory	32 GB (2 x 16 GB)	96 GB (6 x 16 GB)	256 GB (8 x 32 GB)
Hard Disk	1 - 2.5-in. 600-GB 6Gb SAS 10K RPM	4 - 2.5-in. 600-GB 6Gb SAS 10K RPM	8 - 2.5-in. 600-GB 6Gb SAS 10K RPM
Hardware RAID	No	Level 10 Cisco 12G SAS Modular RAID Controller	Level 10 Cisco 12G SAS Modular RAID Controller

What makes up an ISE deployment?



Endpoints

- Users
- Devices
- Things

Network Devices

- Switches
- WLCs / Aps
- VPN gateways

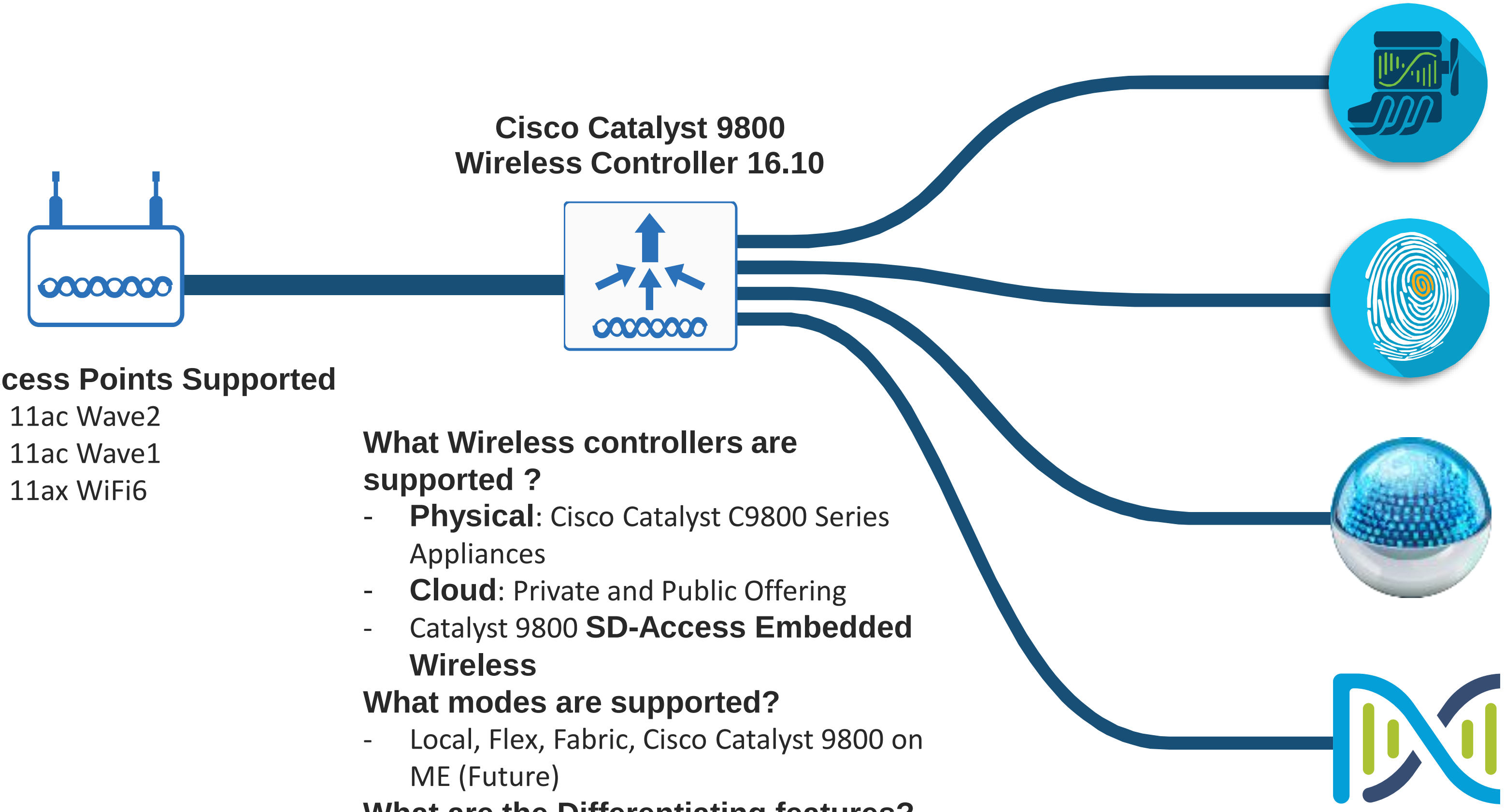
Cisco ISE

- Standalone ISE
- Multi-node ISE
- VM/Appliance

External Services

- AD/LDAP
- MDM
- Security services

Cisco Catalyst 9800 Wireless as a solution!



Cisco Catalyst 9800 Wireless Controller 16.10

Access Points Supported

- 11ac Wave2
- 11ac Wave1
- 11ax WiFi6

What Wireless controllers are supported ?

- **Physical**: Cisco Catalyst C9800 Series Appliances
- **Cloud**: Private and Public Offering
- Catalyst 9800 **SD-Access Embedded Wireless**

What modes are supported?

- Local, Flex, Fabric, Cisco Catalyst 9800 on ME (Future)

What are the Differentiating features?

- High Availability, Patching, ETA Programmability, Telemetry

Cisco DNA Center 1.2.10

- Automation
- Assurance
- Maps & topology

ISE 2.2/2.3/2.4

- BYOD
- Guest Access

Prime Infrastructure 3.5

- Configuration
- Monitoring

CMX 10.5.1 /Cisco DNA Space

- Connect / Detect / Engage
- Hyperlocation
- BLE

ALERT
ADAPT
ACHIEVE

Cisco Identity Services Engine

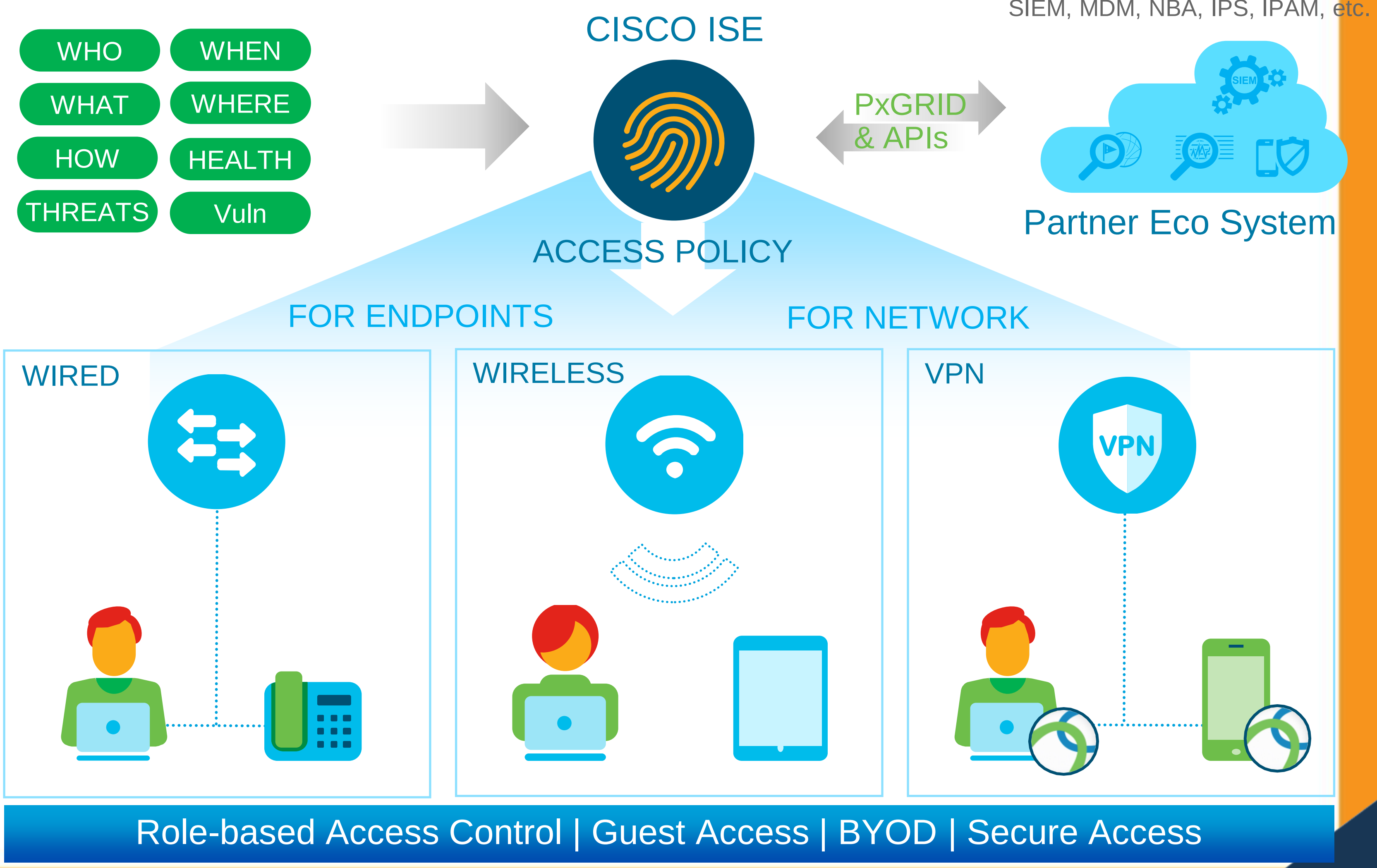
Cisco ISE

Cisco Identity Services Engine (ISE) is an industry leading, Network Access Control and Policy Enforcement platform

Visibility
Context about everything touching the network

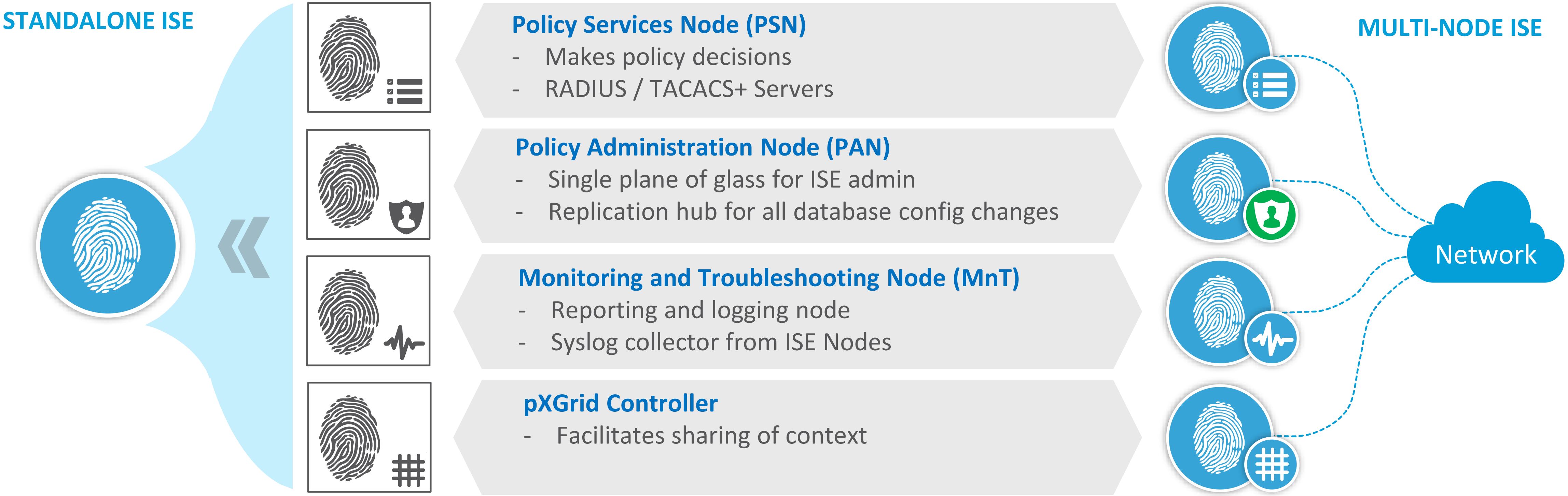
Control
Network access control and segmentation

Compliance
Enterprises comply to industry regulations



SAMART TELCOMS

ISE Architecture



Policy Services Node (PSN)
- Makes policy decisions
- RADIUS / TACACS+ Servers

Policy Administration Node (PAN)
- Single plane of glass for ISE admin
- Replication hub for all database config changes

Monitoring and Troubleshooting Node (MnT)
- Reporting and logging node
- Syslog collector from ISE Nodes

pXGrid Controller
- Facilitates sharing of context

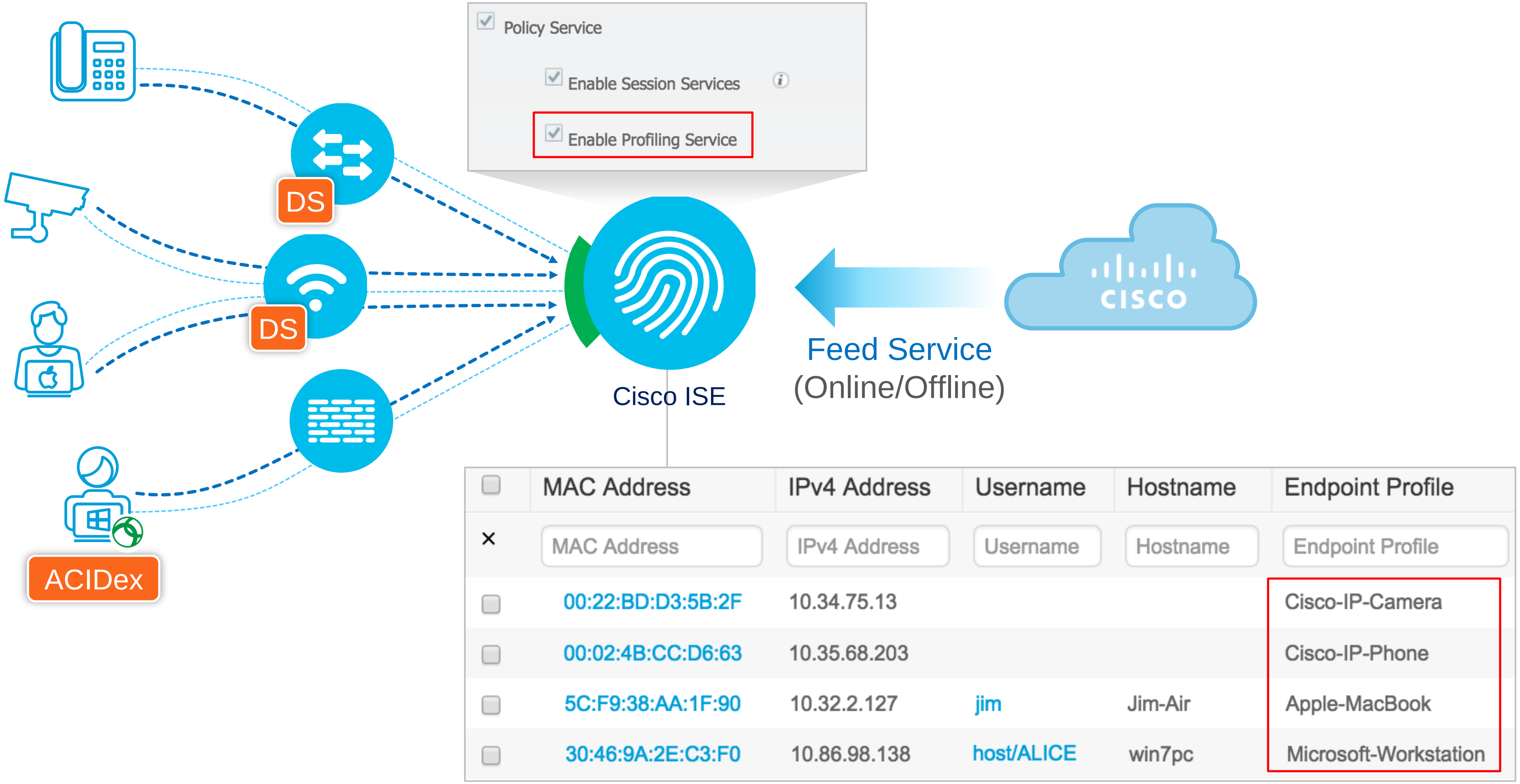
Single Node (Virtual / Appliance)	Multiple Nodes (Virtual / Appliance)
Up to 50,000 concurrent endpoints	Up to 500,000 (2M DOT1X/MAB) concurrent endpoints

ALERT
ADAPT
ACHIEVE

Visibility

The profiling service in Cisco ISE identifies the devices that connect to your network

Endpoints send interesting data, that reveal their device identity



☑ Policy Service

☑ Enable Session Services

☑ Enable Profiling Service

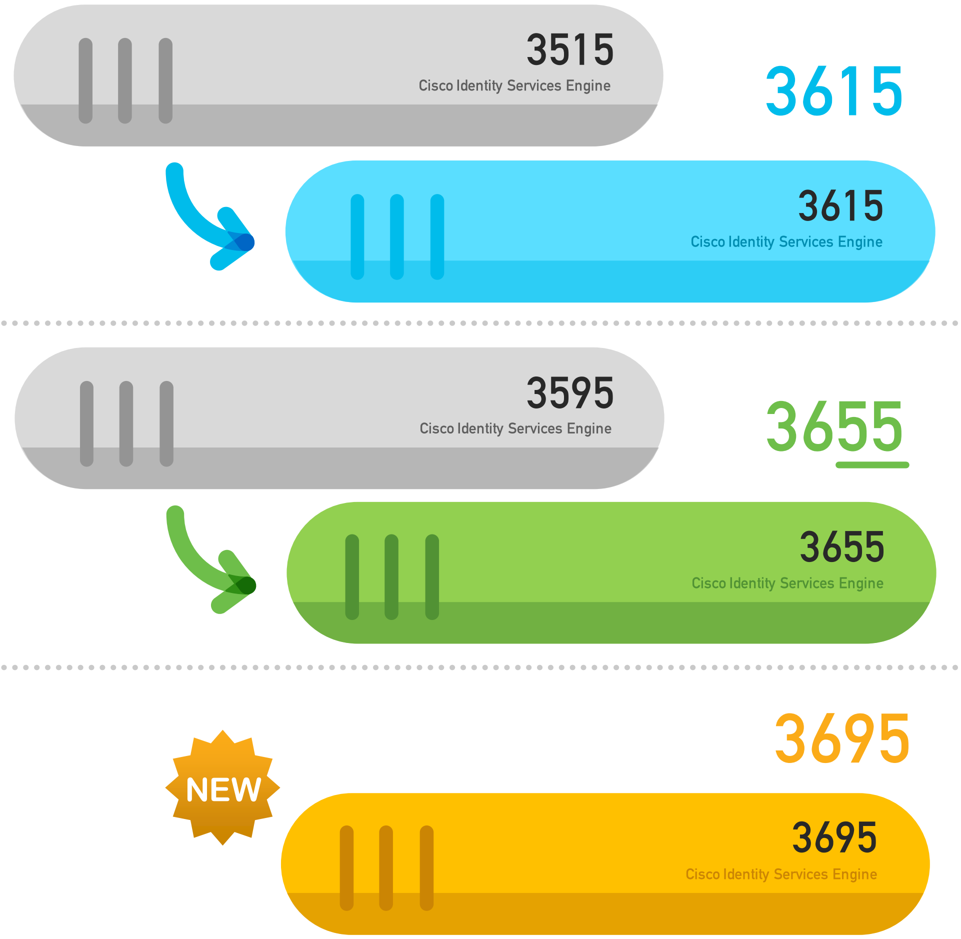
□	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
×	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
□	00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
□	00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
□	5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
□	30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

AnyConnect Identity Extensions (ACIDex) | Device Sensor (DS)

SAMART TELCOMS

Identity Service Engine

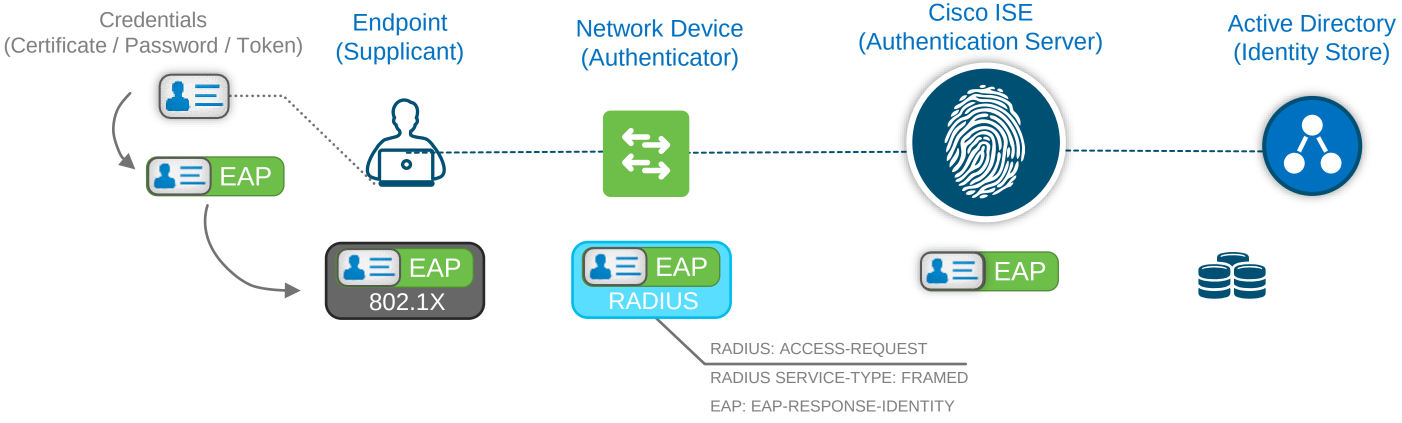
Hardware/Virtual appliances


3515
Cisco Identity Services Engine
3615
3615
Cisco Identity Services Engine
3595
Cisco Identity Services Engine
3655
3655
Cisco Identity Services Engine
3695
NEW
3695
Cisco Identity Services Engine

- **Small Secure Network Server for ISE Application**
- **Mediam Secure Network Server for ISE Application**
- **Large Secure Network Server for ISE Application**
- **Cisco ISE Virtual on Vmware ESX/ESXi 5.x/6.x and KVM Redhat Enterprise Linux (RHEL) 7**

ALERT
ADAPT
ACHIEVE

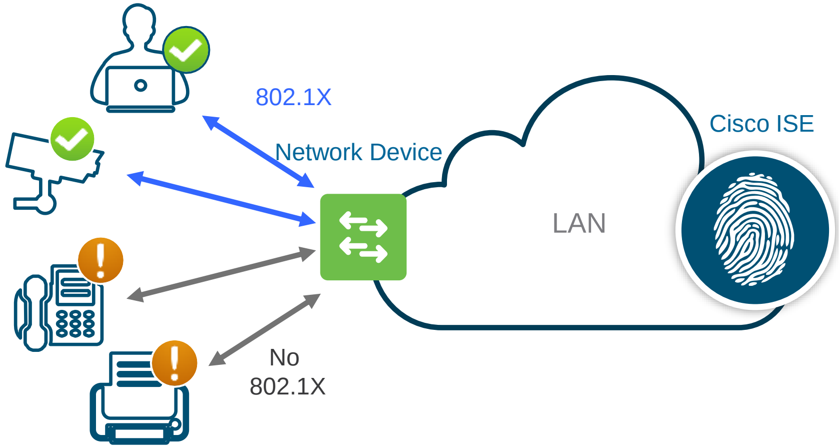
Fundamentals of 802.1x



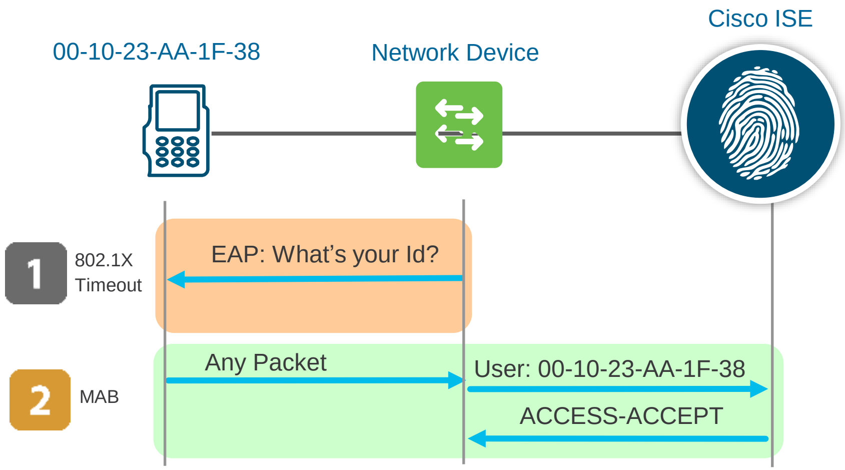
EAP: Extensible Authentication Protocol

MAC Authentication bypass (MAB)

Endpoints without supplicant will fail 802.1X authentication!



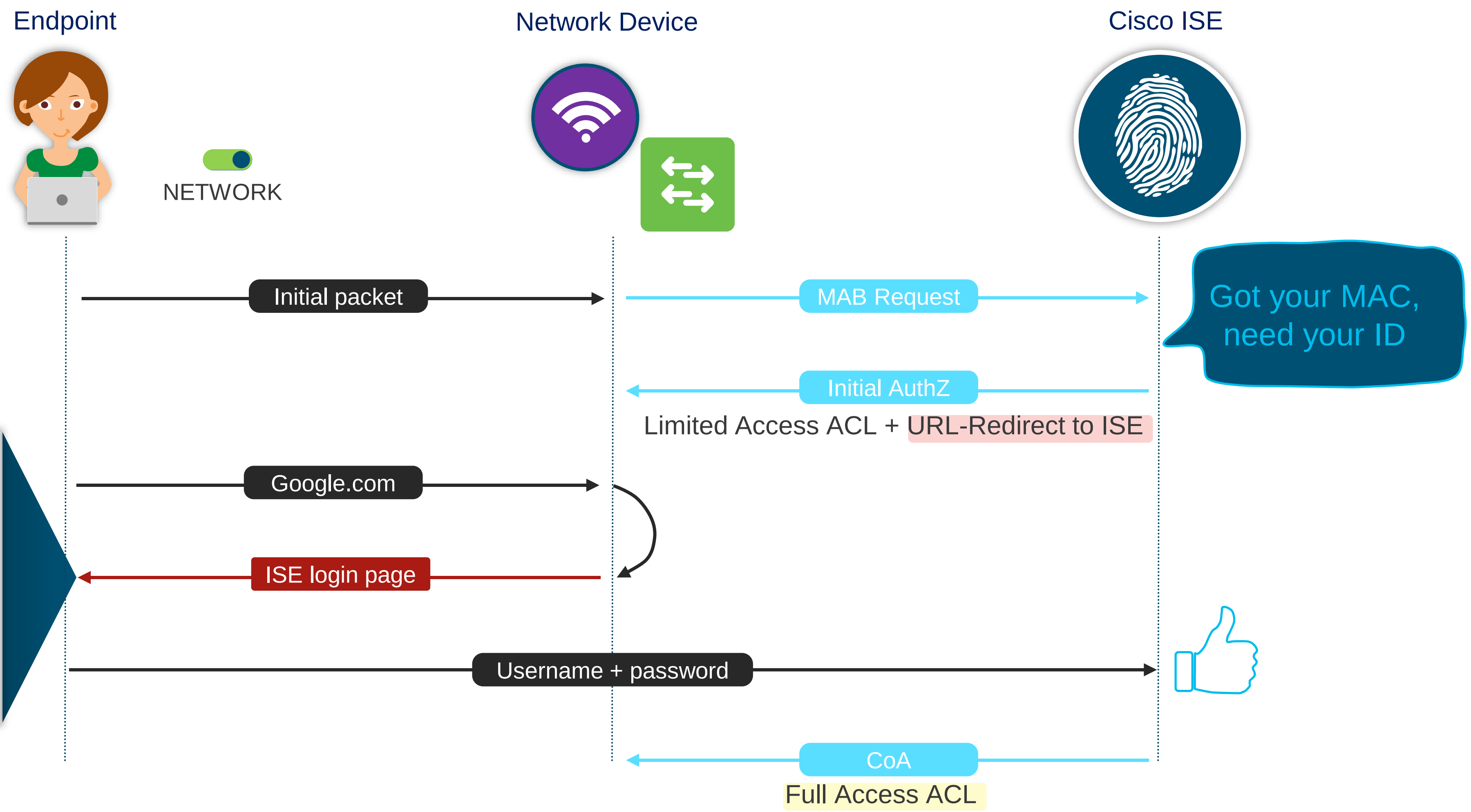
Bypassing "Known" MAC Addresses

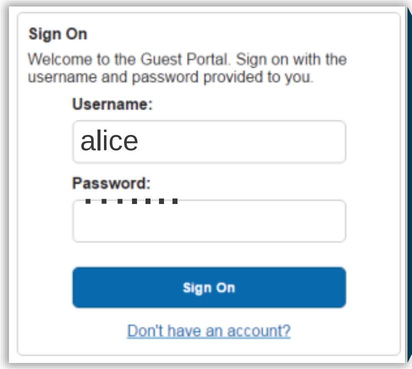


ALERT
ADAPT
ACHIEVE
SAMART TELCOMS

Authentication Methodology

Central Web Authentication (CWA)





Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username: alice

Password: ••••••••

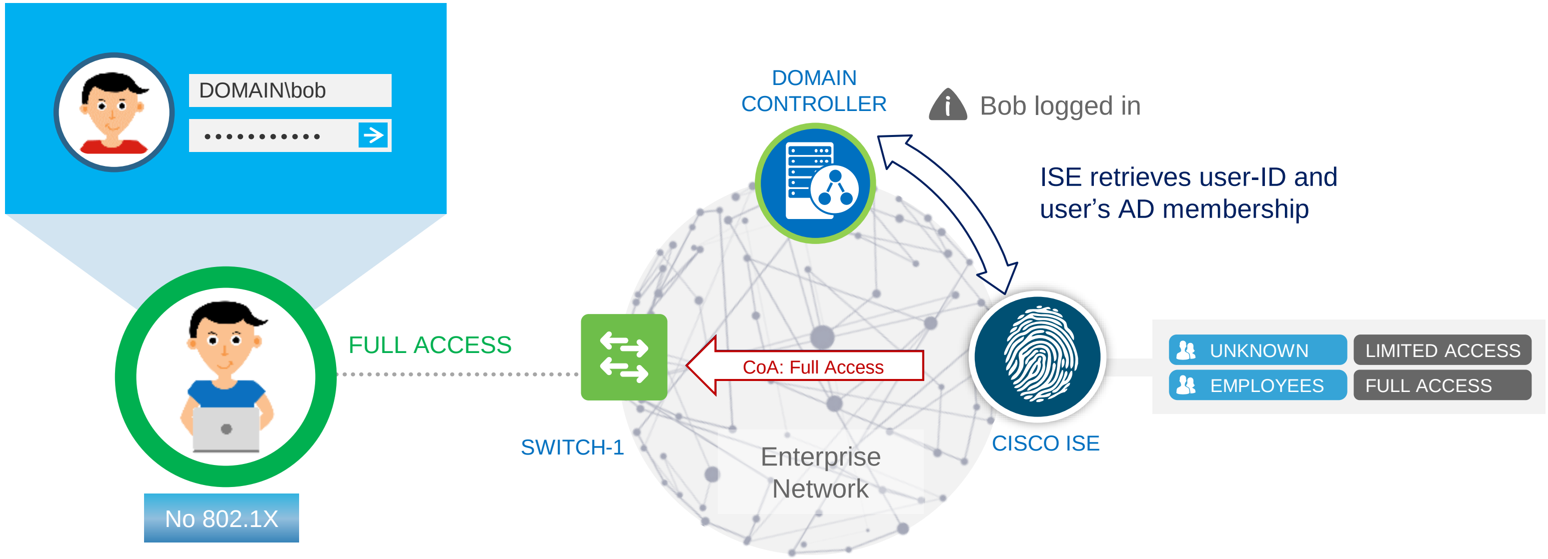
Sign On

Don't have an account?

ALERT
ADAPT
ACHIEVE

Authentication Methodology

Easy Connect- Identity based network access without 802.1x



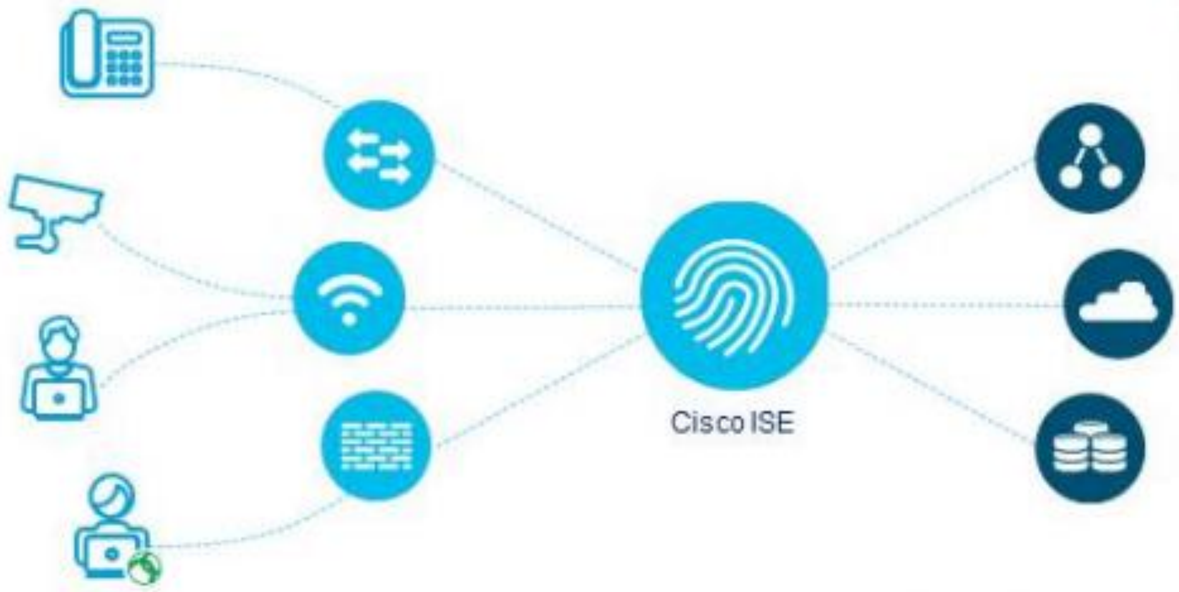
Immediate value
Leverage existing infrastructure

Increased visibility
into active network sessions

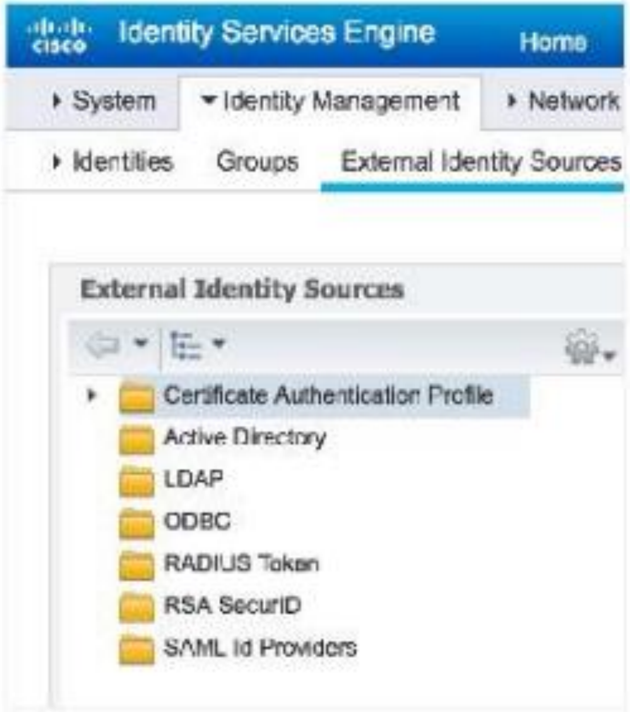
Flexible deployment
co-operates with other auth methods

SAMART TELCOMS

Identity Store integrations



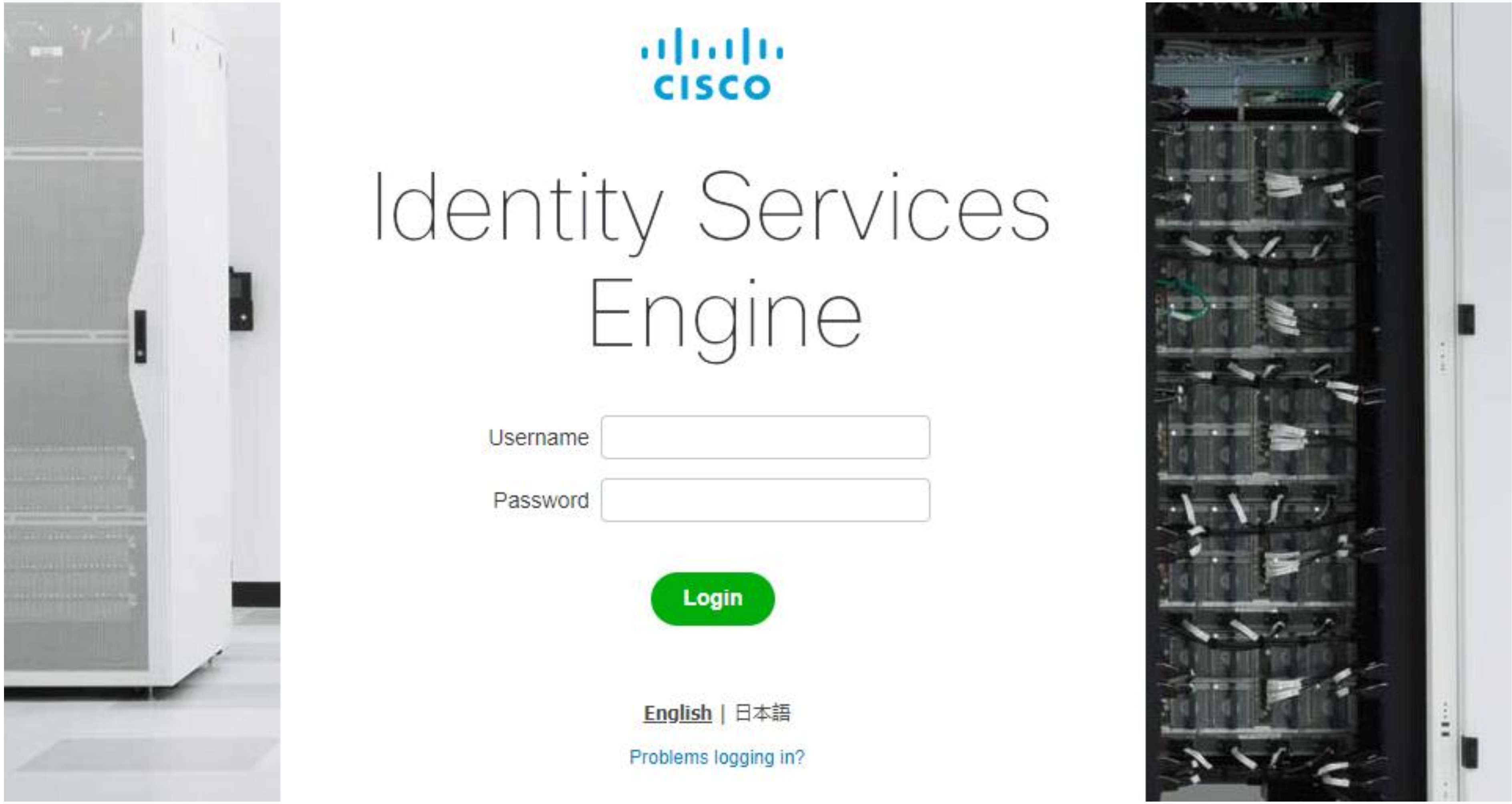
Validate Endpoints via External Identity Sources


Identity Services Engine
Home
▸ System ▾ Identity Management ▸ Network
▸ Identities Groups External Identity Sources

External Identity Sources

- ▸ Certificate Authentication Profile
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers

ISE Login



cisco

Identity Services Engine

Username

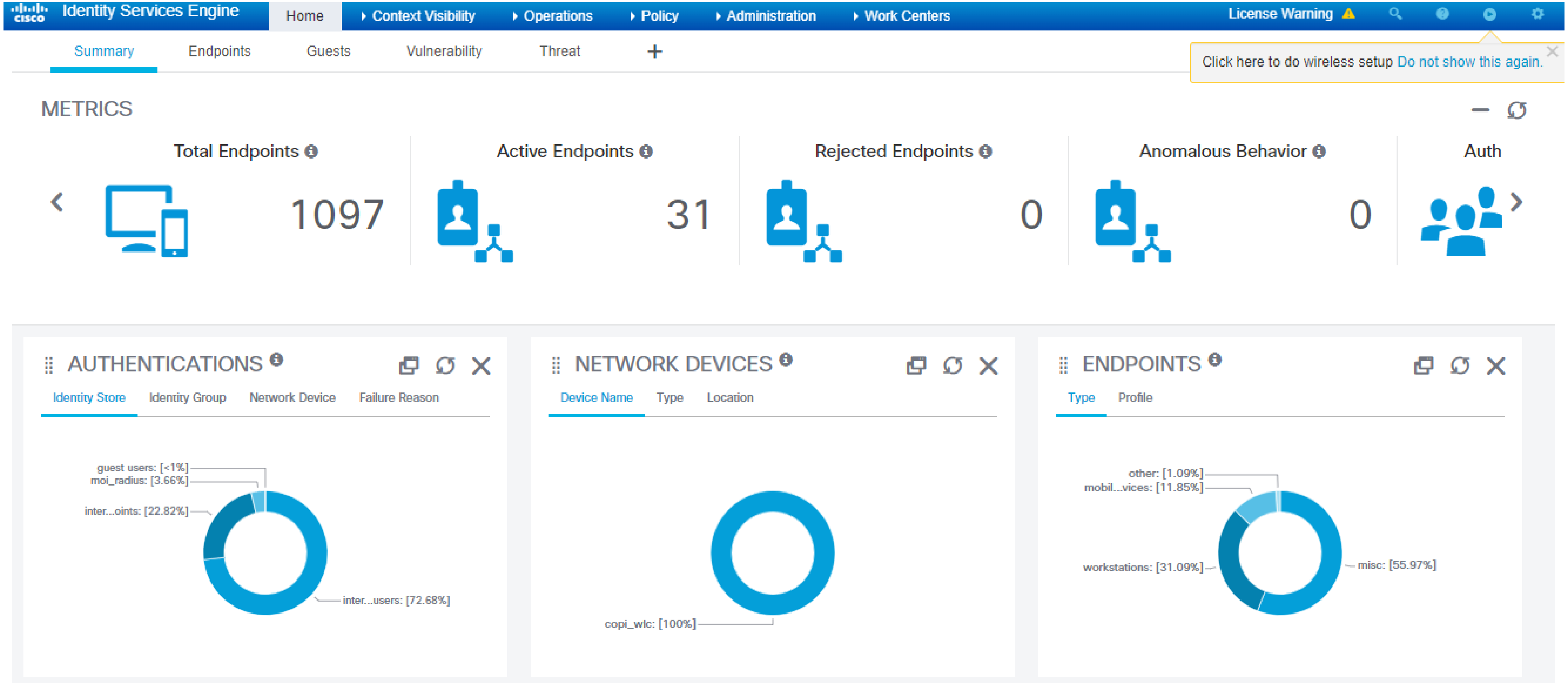
Password

Login

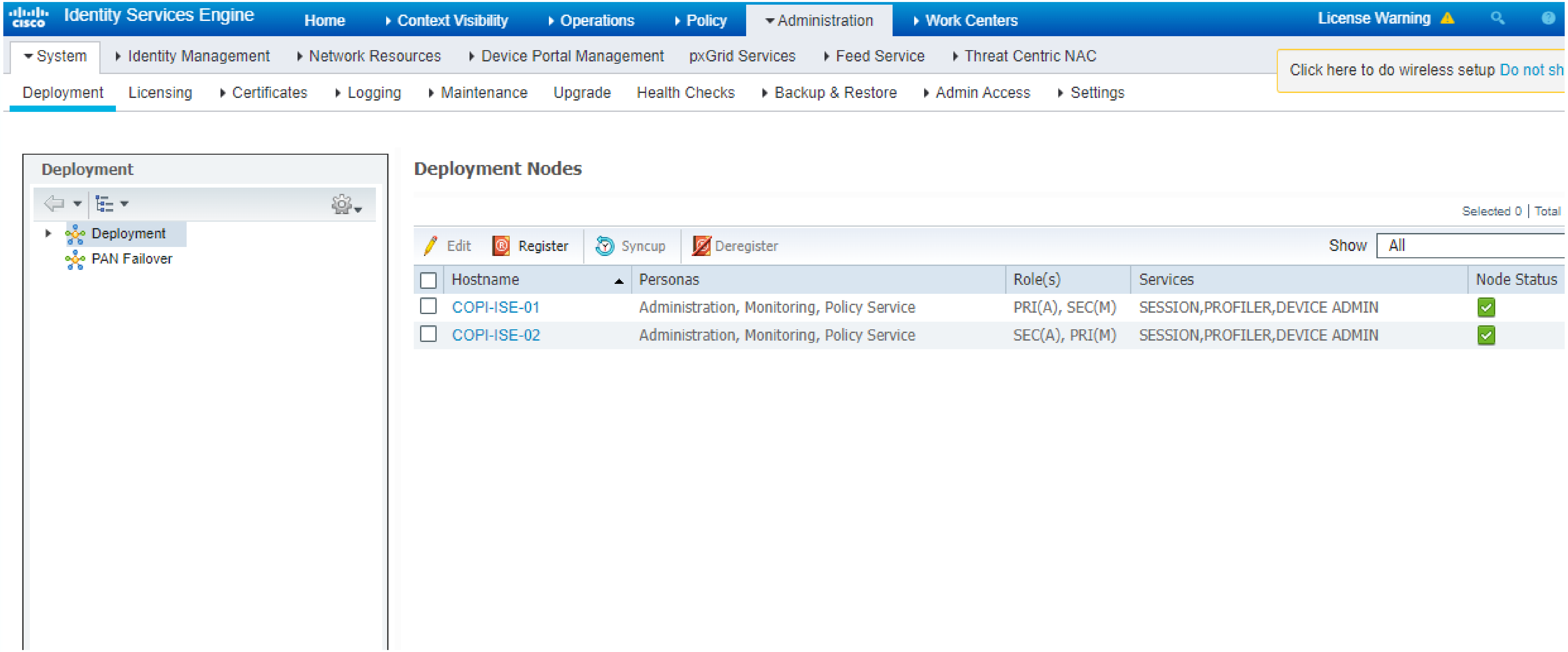
English | 日本語

Problems logging in?

ISE Dashboard



ISE Node Status

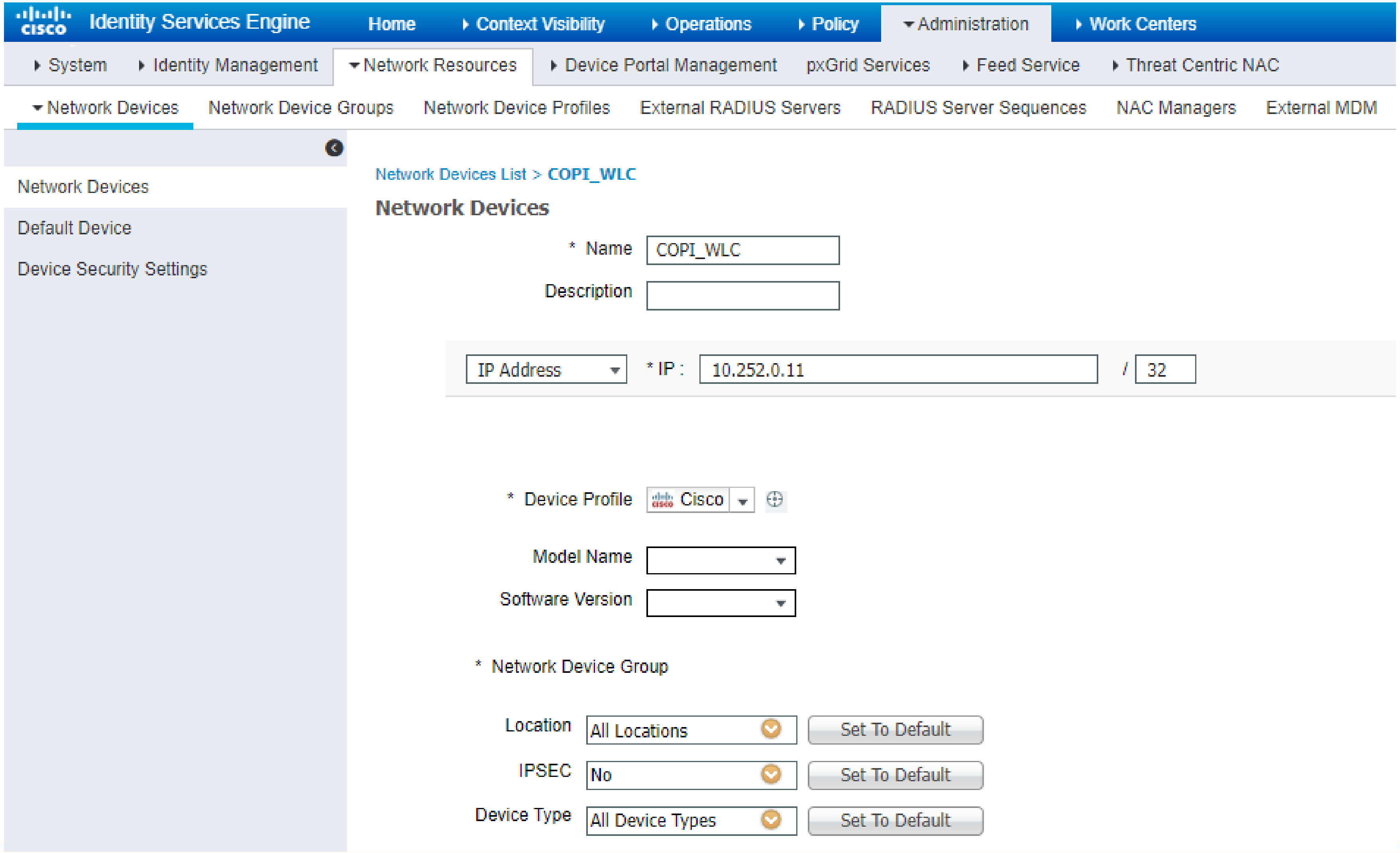


Deployment Nodes

□	Hostname	Personas	Role(s)	Services	Node Status
□	COPI-ISE-01	Administration, Monitoring, Policy Service	PRI(A), SEC(M)	SESSION,PROFILER,DEVICE ADMIN	✓
□	COPI-ISE-02	Administration, Monitoring, Policy Service	SEC(A), PRI(M)	SESSION,PROFILER,DEVICE ADMIN	✓

ALERT
ADAPT
ACHIEVE

ISE Network Device



Network Devices

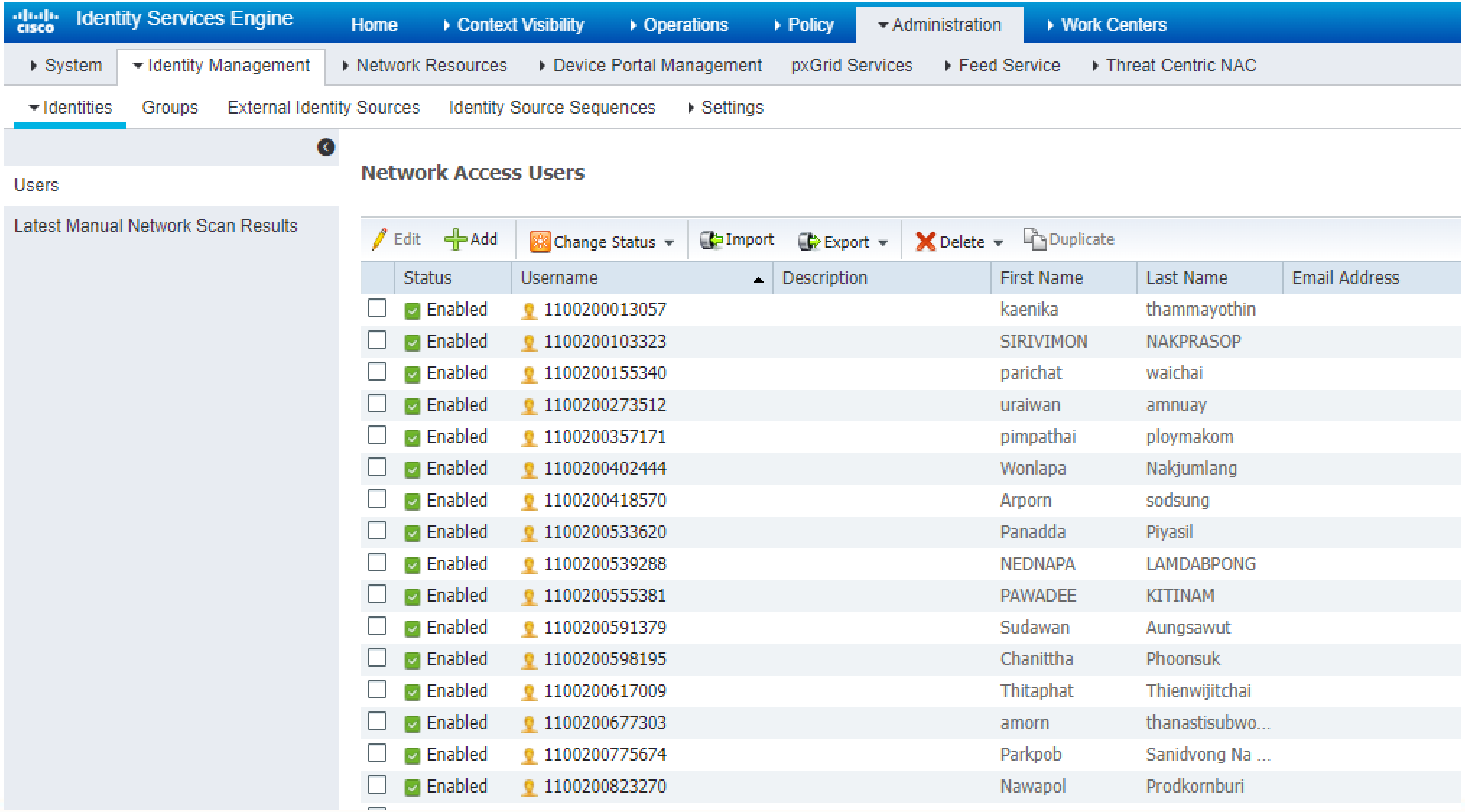
* Name	COPI_WLC
Description	
IP Address	* IP : 10.252.0.11 / 32
* Device Profile	Cisco
Model Name	
Software Version	

* Network Device Group

Location	All Locations
IPSEC	No
Device Type	All Device Types

SAMART TELCOMS

ISE Identity Management

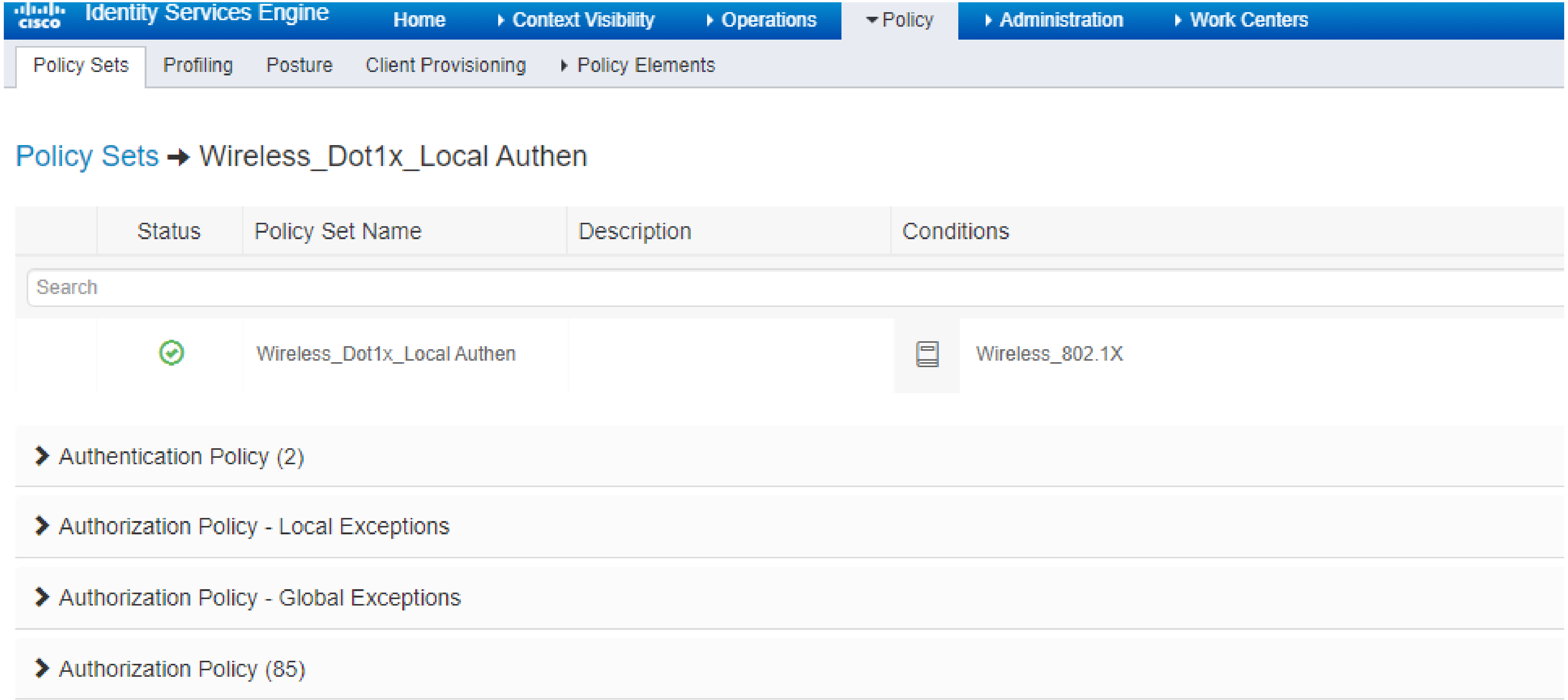


Network Access Users

	Status	Username	Description	First Name	Last Name	Email Address
□	✓ Enabled	1100200013057		kaenika	thammayothin	
□	✓ Enabled	1100200103323		SIRIVIMON	NAKPRASOP	
□	✓ Enabled	1100200155340		parichat	waichai	
□	✓ Enabled	1100200273512		uraiwan	amnuay	
□	✓ Enabled	1100200357171		pimpathai	ploymakom	
□	✓ Enabled	1100200402444		Wonlapa	Nakjumlang	
□	✓ Enabled	1100200418570		Arporn	sodsung	
□	✓ Enabled	1100200533620		Panadda	Piyasil	
□	✓ Enabled	1100200539288		NEDNAPA	LAMDABPONG	
□	✓ Enabled	1100200555381		PAWADEE	KITINAM	
□	✓ Enabled	1100200591379		Sudawan	Aungsawut	
□	✓ Enabled	1100200598195		Chanittha	Phoonsuk	
□	✓ Enabled	1100200617009		Thitaphat	Thienwijitchai	
□	✓ Enabled	1100200677303		amorn	thanastisubwo...	
□	✓ Enabled	1100200775674		Parkpob	Sanidvong Na ...	
□	✓ Enabled	1100200823270		Nawapol	Prodkornburi	

ALERT
ADAPT
ACHIEVE

ISE Policy



Policy Sets → Wireless_Dot1x_Local Authen

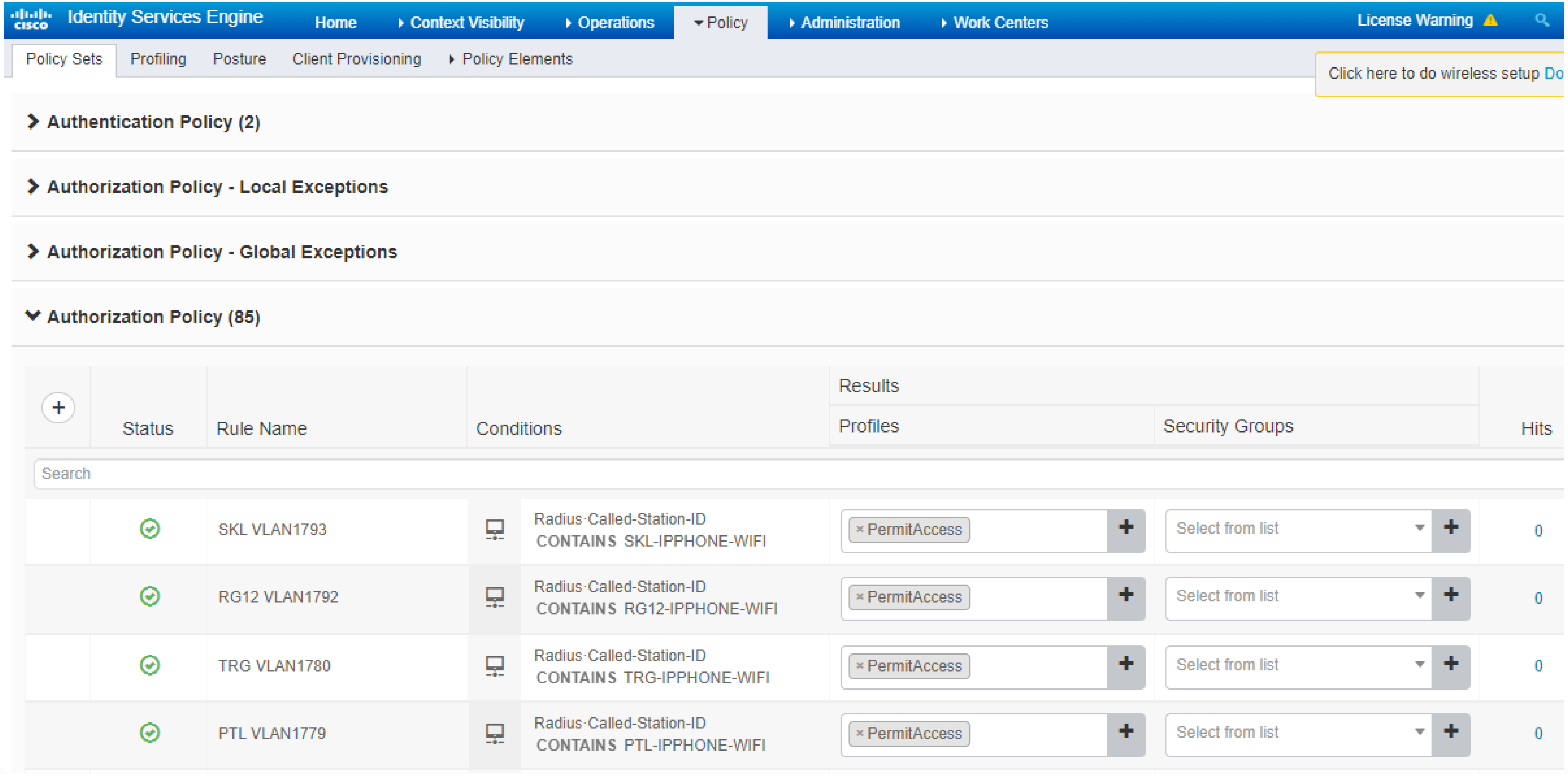
	Status	Policy Set Name	Description	Conditions
	✓	Wireless_Dot1x_Local Authen		Wireless_802.1X

- Authentication Policy (2)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (85)

SAMART TELCOMS

ALERT
ADAPT
ACHIEVE

ISE Policy



Authentication Policy (2)

Authorization Policy - Local Exceptions

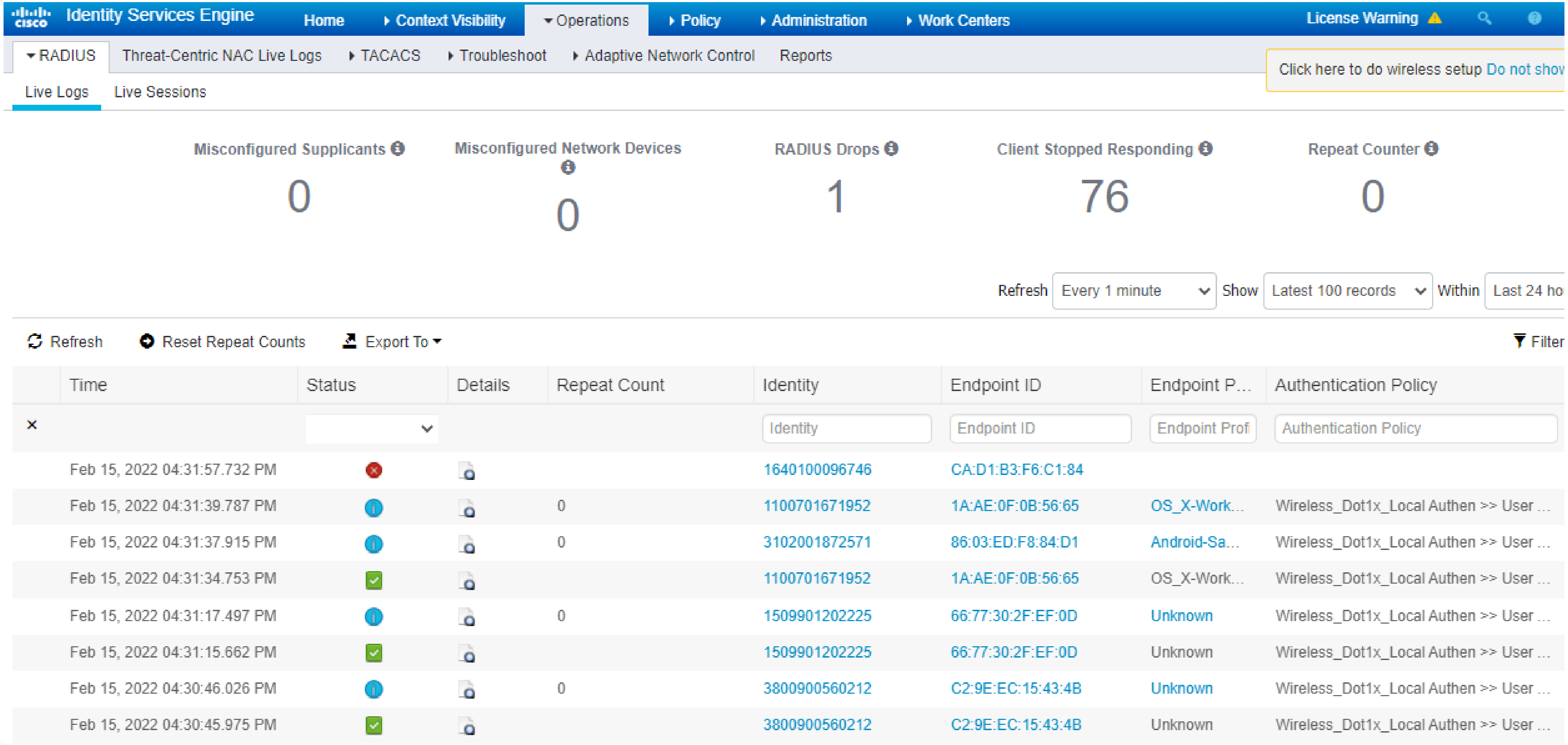
Authorization Policy - Global Exceptions

Authorization Policy (85)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits
✓	SKL VLAN1793	Radius·Called-Station-ID CONTAINS SKL-IPPHONE-WIFI	PermitAccess	Select from list	0
✓	RG12 VLAN1792	Radius·Called-Station-ID CONTAINS RG12-IPPHONE-WIFI	PermitAccess	Select from list	0
✓	TRG VLAN1780	Radius·Called-Station-ID CONTAINS TRG-IPPHONE-WIFI	PermitAccess	Select from list	0
✓	PTL VLAN1779	Radius·Called-Station-ID CONTAINS PTL-IPPHONE-WIFI	PermitAccess	Select from list	0

SAMART
TELCOMS

ISE Radius Live Logs



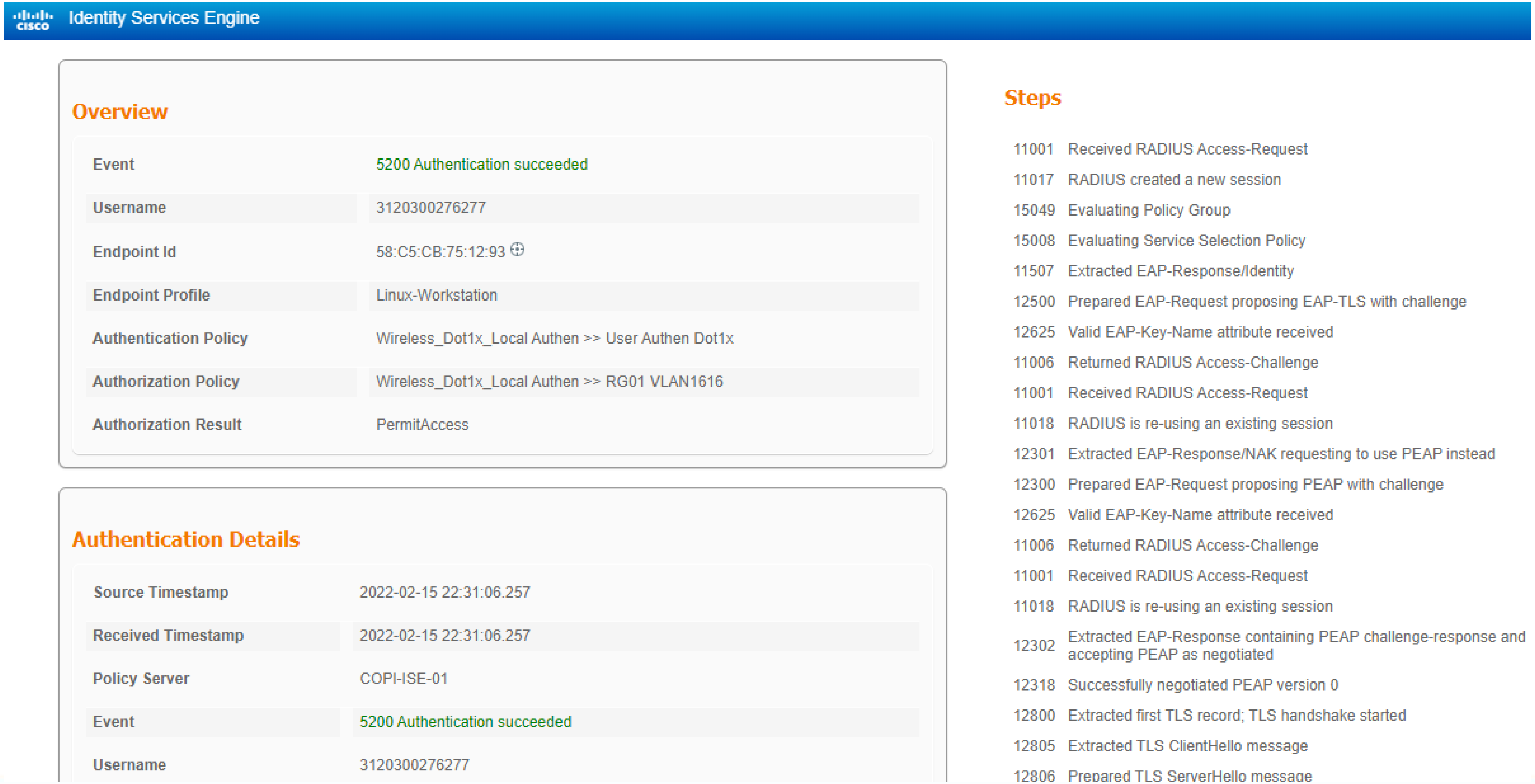
Click here to do wireless setup Do not show

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	1	76	0

Refresh: Every 1 minute Show: Latest 100 records Within: Last 24 ho

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint P...	Authentication Policy
Feb 15, 2022 04:31:57.732 PM	⊗	🔍		1640100096746	CA:D1:B3:F6:C1:84		
Feb 15, 2022 04:31:39.787 PM	ⓘ	🔍	0	1100701671952	1A:AE:0F:0B:56:65	OS_X-Work...	Wireless_Dot1x_Local Authen >> User ...
Feb 15, 2022 04:31:37.915 PM	ⓘ	🔍	0	3102001872571	86:03:ED:F8:84:D1	Android-Sa...	Wireless_Dot1x_Local Authen >> User ...
Feb 15, 2022 04:31:34.753 PM	✓	🔍		1100701671952	1A:AE:0F:0B:56:65	OS_X-Work...	Wireless_Dot1x_Local Authen >> User ...
Feb 15, 2022 04:31:17.497 PM	ⓘ	🔍	0	1509901202225	66:77:30:2F:EF:0D	Unknown	Wireless_Dot1x_Local Authen >> User ...
Feb 15, 2022 04:31:15.662 PM	✓	🔍		1509901202225	66:77:30:2F:EF:0D	Unknown	Wireless_Dot1x_Local Authen >> User ...
Feb 15, 2022 04:30:46.026 PM	ⓘ	🔍	0	3800900560212	C2:9E:EC:15:43:4B	Unknown	Wireless_Dot1x_Local Authen >> User ...
Feb 15, 2022 04:30:45.975 PM	✓	🔍		3800900560212	C2:9E:EC:15:43:4B	Unknown	Wireless_Dot1x_Local Authen >> User ...

ISE Radius Live Logs



Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	3120300276277
Endpoint Id	58:C5:CB:75:12:93 ⊕
Endpoint Profile	Linux-Workstation
Authentication Policy	Wireless_Dot1x_Local Authen >> User Authen Dot1x
Authorization Policy	Wireless_Dot1x_Local Authen >> RG01 VLAN1616
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2022-02-15 22:31:06.257
Received Timestamp	2022-02-15 22:31:06.257
Policy Server	COPI-ISE-01
Event	5200 Authentication succeeded
Username	3120300276277

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12301	Extracted EAP-Response/NAK requesting to use PEAP instead
12300	Prepared EAP-Request proposing PEAP with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated
12318	Successfully negotiated PEAP version 0
12800	Extracted first TLS record; TLS handshake started
12805	Extracted TLS ClientHello message
12806	Prepared TLS ServerHello message